This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Security Challenges to the Use and Deployment of Disruptive Technologies

Neil Robinson, Maarten Botterman, Lorenzo Valeri, David Ortiz, Andreas Litgvoet, Rebecca Shoob, Eddy Nason

Prepared for the European Commission

RAND EUROPE

The research described in this paper was prepared for the European Commission. The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org/
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

As technology changes the way we work and organise our lives, both individually and as a society, it is important to look ahead and explore what new technologies today may have a significant and possibly disruptive impact tomorrow. This report explores the security challenges to the use and deployment of five 'disruptive technologies' (VoIP, Trusted Computing, WiMAX, RFID, and IPv6) by presenting a short overview of the current state of the technology itself, as well as a case study on an actual implementation of each of these technologies. In undertaking these case studies, the authors have directed particular attention to the exploration and description of the way each technology has been implemented and its security challenges addressed. The report is supported by findings from a Delphi exercise, and a full draft version has been discussed in an expert workshop held in Brussels on 30 June 2006. The outcome of the discussion, which was based on this evidence provided by the project team and the experience of participants themselves, has been integrated in this report and includes a number of recommendations on policy options in the context of the i2010 element of the Lisbon Agenda, which consider security as one of the core enabling elements for the establishment of a Single European Information Space.

This Technical Report (TR) is prepared on behalf of Unit A3, Internet, Information and Network Security, DG Information Society and Media, European Commission.

For more information about this project and, in particular, this document, please contact

Neil Robinson,

RAND Europe
Westbrook Centre
Milton Road
Cambridge
CB4 1YG,
United Kingdom
Tel: +44 1223 353329
Email: neil_robinson@rand.org

Executive Summary

This report considers the security challenges to the use and deployment of disruptive technologies, which is a business and technology concept devised by Harvard professor Clayton M Christiansen. Disruptive technologies are those that sacrifice certain qualities in a product that are attractive to the majority of customers in favour of a different set of characteristics which may only be attractive to certain customers or which fulfil a certain specific niche need. Disruptive technologies or innovations are different from 'sustaining innovations'. Sustaining innovations maintain a constant rate of product improvement, leading to increasing functionality for the greatest number, or most profitable, customers. Disruptive technology can also create new markets by radically changing the market landscape, for instance, allowing new players to enter the market.

In trying to understand the security challenges associated with the use of these technologies, this report considers five specific disruptive technologies: Voice over Internet Protocol (VoIP); Radio Frequency Identification technology (RFID); Wireless Microwave Access (WiMAX); Trusted Computing and Internet Protocol version 6 (IPv6). Each technology was considered in the light of an implementation within an organisation, as a discrete case study.

To undertake the research, experts in Information Communications Technology (ICT) and information security were asked to participate in a Delphi exercise and workshop, where they rated their views on the security challenges to the deployment and use of the disruptive technologies. Overall, the research indicated that complex social and economic issues such as trust, risk and privacy were the most prevalent concerns. The experts also considered the business drivers for the implementation of these technologies, as security must always be seen in the light of hard-nosed business decisions. Following the classification of the different types of security challenges, the experts then helped in the design of a study framework that was used to guide the data collection for the case studies.

The case studies of the implementation of the five technologies were conducted in specific organisational settings. A combination of desk research, review of organisational documentation and first-hand interviews were used to collect the data, which was then reviewed and compared to other evidence.

The evidence showed that:

- The business case for the deployment of these disruptive technologies is not yet fully developed. As a result of this, the security considerations of the deployment

of these technologies may not be treated as seriously as they should, since these tend to be secondary to business concerns.

- Disruptive technologies present security challenges when organisations must transition from one version of the technology to another. These transitions must be properly managed if security is not to be undermined.
- The perception of the end user is an important issue, as it relates directly to usability and can also indicate how well the security message is understood.
- These technologies throw up reliability challenges; in particular as some of these technologies are key elements of the evolving European information infrastructure upon which governments, business and citizens increasingly rely.

On 30th June 2006, the European Commission and RAND Europe invited experts from industry, government and academia to Brussels to review the results of the case studies, express comment on the draft final report and debate the conclusions of the study at the Final Workshop. This event began with a presentation setting out the policy objectives and outlining the stages of the study, followed by an overview of the industrial and economic context (in particular, why it is important to study disruptive technologies and the market behaviours of disruptive technologies). An introduction to the study methodology was presented, and representatives from each of the case study organisations gave a short overview of their case study, reflecting: the general context of the deployment of the technology; business objectives and technical details of the implementation. Feedback provided during the workshop has been integrated in the conclusions and recommendations presented in this report.

In order to facilitate the successful treatment of these challenges, policy makers must adopt a supporting and encouraging role. The adoption of a disruptive technology is naturally self-regulated, spontaneous and 'bottom-up' due to the innovative and risky nature of these technologies. Policy makers in national governments and regional organisations such as the EU should not mandate that certain rules or standards are followed, or create overburdening laws that will hamper the dynamic growth of the single European Information Space. However, there is a role for targeted intervention in specific enabling areas, such as the implementation of IPv6 and legislation addressing issues such as privacy, data retention and monitoring.

This report makes the recommendations that governments should play a role where a societal benefit is expected, even if the market is not willing to pay for it. This role could be via: supporting pre-competitive research on the technology and its implementation and impact; regulating to reduce misuse and for certification; stimulation of standardisation and certification activities and awareness raising. Recognising that the successful and secure implementation of disruptive technologies requires the involvement of all stakeholders, policy makers should consider all likely market players, not just those with current market presence. Policy makers could define critical infrastructures and required minimum levels of operation, to better understand when specific regulatory or financial incentives are required to ensure their protection. In the context of the recently released strategy for a Secure Information Society: "Dialogue, Partnership and Empowerment" and the i2010 goals. We make recommendations to: ***inform*** all sectors at all levels about the security

challenges relating to these technologies and the policies in place to address them; ***stimulate*** good implementation by considering a coherent strategy for Europe-wide implementation of some of the technologies and by creating a positive regulatory environment to stimulate the development of new Ambient Intelligent infrastructures; ***integrate*** security in information systems to support prevention, for example by defining minimum levels of security or by using the buying power of the public sector; and finally ***implement*** risk assessment and protection mechanisms which could include improvements to law enforcement measures and laws. The report also presents specific policy recommendations for the European Commission, including: support of large scale demonstrators, exchange of good practice and standardisation, learning from industry good practice; ensuring avoidance of monocultures; providing continued support for pre-competitive Research and Development; improving education and training; and clarifying the legal implications of these new technologies.

Table of Contents

Preface iii
Executive Summary v
Table of Tables xi

CHAPTER 1 **Introduction 1**
1.1 Security as a key element for i2010 2
1.2 Definitions 2
1.3 Objectives and Approach of this Study 4

CHAPTER 2 **Voice over Internet Protocol (VoIP) 6**
2.1 Voice over Internet Protocol (VoIP): General issues 6
2.1.1 Why is VoIP disruptive? 8
2.1.2 Overview of Security Threats and Concerns 9
2.2 VoIP within the UK branch network of HSBC 10
2.2.1 Business drivers 11
2.2.2 Technical implementation 12
2.2.3 Security challenges 13
2.2.4 Conclusions 14
2.2.5 Review of the case study conclusions during the Final Workshop 15

CHAPTER 3 **Trusted Computing 16**
3.1 Trusted Computing: General issues 16
3.1.1 Why is Trusted Computing disruptive? 18
3.1.2 Overview of Security Threats and Concerns 22
3.2 ARM TrustZone 22
3.2.1 Business drivers 23
3.2.2 Technical Implementation 25
3.2.3 Security challenges 27
3.2.4 Conclusions 30
3.2.5 Review of the case study conclusions during the Final Workshop 30

CHAPTER 4 **Wireless Microwave Access (WiMAX) 32**
4.1 Wireless Microwave Access (WiMAX): General Issues 32
4.1.1 Why is WiMAX disruptive? 34

4.1.2 Overview of Security Threats and Concerns 35
4.2 WIMAX Trial from PIPEX & AIRSPAN 36
4.2.1 Business Drivers 37
4.2.2 Technical implementation 37
4.2.3 Security challenges 39
4.2.4 Conclusions 40
4.2.5 Review of the case study conclusions during the Final Workshop 41

CHAPTER 5 **Radio Frequency Identification (RFID) 42**
5.1 Radio Frequency Identification (RFID): General Issues 42
5.1.1 Why is RFID disruptive? 43
5.1.2 Overview of Security Threats and Concerns 44
5.2 AIRBUS RFID Solution for Tool and Instrument Tracing 47
5.2.1 Business Drivers 48
5.2.2 Technical implementation 49
5.2.3 Security Challenges 52
5.2.4 Conclusions 54
5.2.5 Review of the case study conclusions during the Final Workshop 55

CHAPTER 6 **Internet Protocol version 6 (IPv6) 56**
6.1 Internet Protocol version 6 (IPv6): General Issues 56
6.1.1 Why is IPv6 disruptive? 58
6.1.2 Overview of Security Threats and Concerns 63
6.2 DoD High Performance Computing Modernization Program implementation of IPv6 65
6.2.1 Business Drivers 65
6.2.2 Technical Implementation 66
6.2.3 Security Challenges 67
6.2.4 Conclusions 69
6.2.5 Review of the case study conclusions during the Final Workshop 70

CHAPTER 7 **Conclusions and recommendations 71**
7.1 Overview 71
7.2 Overall observations 72
7.3 Policy Recommendations 77
7.3.1 Overall policy recommendations 78
7.3.2 Role of the European Commission 80
7.3.3 Specific policy recommendations for each technology 81

REFERENCES 83
Voice Over Internet Protocol 84
Trusted Computing 85
WiMAX 86
RFID 86
IPv6 87

APPENDICES **88**

Appendix A: Case Study Framework **89**
Pre-workshop Delphi process 89
Results from the first stage 89
Results from the second stage 92
Workshop 93
Workshop approach 93
Themes from the business environment 93
Case study Research Frameworks 96
Overall security challenges 96
Expert participation 98
Appendix B: Case Study Interviewees **101**
Appendix C: Terms of Reference for Final Workshop **103**
Appendix D: Final Workshop participants **105**
Appendix E: Glossary **106**

Table of Tables

Table 1: The data available on the RFID chip 50
Table 2: Comparison of principal differences between IPv4 and IPv6 62
Table 3: Grouping of first stage Delphi results 91
Table 4: Expert ranking of groups of security challenges 92
Table 5: Expert participants in the Delphi exercise 98
Table 6: Attendees of the first workshop, Cambridge, 7th February 2006 100
Table 7: Case study interviewees 101
Table 8: Final workshop participants list 105

CHAPTER 1 Introduction

Developed by Harvard Business School professor Clayton M. Christensen, the term 'disruptive technology' refers to those new technologies that unexpectedly displace the position of established technology.[1] These are technologies that overturn existing ones even if they often initially perform worse than the leading ones. As argued by Prof. Christensen, "these technologies introduce a very different package of attributes from the one mainstream customers historically value, and they perform far worse along one or two dimensions that are particularly important to these customers". Organisations often tend to focus on established technologies because they know the market, and have mechanisms in place to develop services and applications. Conversely, organisations and institutions can have difficulties in examining the economic, technical, social and regulatory implications of disruptive technologies. In some cases, this may lead organisations to initially dismiss disruptive technologies and then be caught by surprise when these technologies mature and gain larger audience and marketshare.

In the area of ICTs, several disruptive technologies have gained significant popularity among organisations and individual users. They have brought, or are in the process of bringing, new functionalities upon which innovative services and goods are developed. Nevertheless, the rapid diffusion of these technologies is creating for organisations and individual users new information risks and security challenges. As they often change the operational online paradigms of organisations and individuals, technology alone cannot provide the solutions. Other appropriate management and policy responses are required.

This study presents the results of a study into the security challenges associated with the use and implementation of five selected disruptive technologies: WIMAX, RFID, IPv6, Trusted Computing and VoIP. Based on case studies and workshop discussion, the study presents a set of policy options to address these challenges.

[1] Christensen, Clayton M. (1997). The Innovator's Dilemma. Harvard Business School Press.. Also see Bower, J., & Christensen, C. (1995). Disruptive technologies: Catching the wave. Harvard Business Review, January-February, 43-53. An important element to the disruptive nature of such technologies is their market impact: see Schumpeter, J. (1975). Capitalism, Socialism and Democracy New York: Harper, [orig. pub. 1942], pp. 82-85 on the concept of 'creative destruction'. The original concept can be traced through Schumpeter to Karl Marx

1.1 Security as a key element for i2010

ICTs is seen as the engine for sustainable growth and employment in Europe. This is the core message that comes out from the *2005 i2010 Strategy* put forward by the European Commission in 2005. At the core of this strategy, there is the realisation that ICTs are an integral part of the lives of European citizens. This is primarily due to the rapid convergence between information society and media services, networks and devices. Building upon this convergence, there has been a call for a Single European Information Space based on faster broadband connections, interoperability, rich content and applications.

This single European Information Space is also linked to the concept of an Ambient Intelligent (AmI) environment, espoused in the European Commission's vision of an "Information Society which is much more user-friendly, more efficient, empowers users and supports human interactions. People will be surrounded by easy-to-use interfaces embedded into all kinds of objects and by an everyday environment that is capable of recognising and responding to individuals in a seamless, unobtrusive and invisible way."[2]

AmI will know itself, and will be able to change context accordingly; will be dynamic and reconfigurable under different scenarios; find and generate its own rules determining interaction with other systems and networks; be resilient and have speedy properties of recovery and finally be trustworthy, able to handle issues of safety, security and privacy.

The transformation of this aspiration into a reality, nevertheless, could be undermined by the lack of European citizens' trust and confidence towards new technologies. This aspect was emphasised in the European Commission's Communication detailing the i2010 strategy. It stated: "trustworthy, secure and reliable ICT are crucial for the wide take-up of converging technologies".[3] There was the need for appropriate awareness activities, self-protection mechanisms and appropriate and effective responses to cyber-attacks and general system failures based on user-friendly applications and services.

More importantly, it is essential to move away from a pure technological focus to encompass the "soft side" of the individual element of information security: confidentiality, integrity, availability, non-repudiation, authentication and privacy.

1.2 Definitions

In the context of this study, the expression '**confidentiality**' indicates that access to specific sections of an information system is limited to authorised users. The attainment of confidentiality involves several actions. First, data and information need to be classified at different levels of sensitivity and put into separate compartments. This classification

---

[2] Ambient Intelligence, European Commission DG Information Society and Media (11th March 2004) available at http://europa.eu.int/information_society/policy/ambienti/index_en.htm

[3] Communication from the European Commission COM 2005 (229) - i2010: A European Information Society for Growth and Employment; European Commission (1st June 2005) Brussels available at: http://europa.eu.int/information_society/eeurope/i2010/docs/communications/com_229_i2010_310505_fv_en.doc

hierarchy is structured according to the overall objectives and activities of an organisation and to specific national and international regulations. For example, intelligence organisations may protect the confidentiality of data for national security reasons. Commercial organisations may need to protect the confidentiality of their data to preserve their technical and economic advantage vis-à-vis the competition, or to fulfil regulatory and legal requirements. Health organisations are a good example of the latter since they handle data that is very sensitive, but which needs to be accessed by doctors.

Integrity is defined as the requirement to ensure that data and programs are only changed through authorised procedures. Although related, integrity is completely different from confidentiality since the former focuses on the preservation of the precision and accuracy of information systems, while the latter on regulating access to it. There are three different aspects to integrity. First, there is the issue of authorisation. Every modification of information systems or data has to be authorised. For example, only the bank account holder can authorise the transfer of funds between accounts. The second and third characteristics of integrity refer to the preservation of data consistency and separation of duty. The former aims at monitoring possible errors, omissions and unauthorised programme changes. Duty separation refers to the use of technical and management solutions to avoid integrity violations that may lead to frauds or mistakes.

The protection of **availability** specifies that an information system and its data should be available to authorised users. Therefore, it can be measured in terms of the timely responses of an ICT to the requests of authorised users, as well as its overall usability and utility.

Authentication aims to provide some form of identification regarding the authenticity of a human subject or, if required, information system. In particular, it aims to ensure that a particular user is who or what they say they are. **Non-repudiation** derives from authentication and aims at asserting that a particular action undertaken by an authenticated individual cannot later be refuted. Due to the impersonal environment of the Internet, the attainment of non-repudiation and authentication is directly connected to the preservation of the confidentiality, integrity and availability of those ICTs through which a particular exchange or set of relations is established and completed. If somebody gains illegal access to a password, he or she may be able to use an information system handling email or electronic signatures and claim to be somebody else.

The ability of the AmI to be realised is even more critical when we see how innovative business models are combining with new technologies to undermine traditionally held concepts of security. Where once organisations used solutions such as firewalls, Intrusion Detection systems and gateway anti-virus technology to protect their perimeter, the previously described AmI requires that 'de-perimeterisation' be considered as a major factor in risk management and security efforts.[4] This means that client side security will become more important and as more technology becomes embedded in everyday lives, end-users (whether they be citizens, consumers or employees) will have to become more responsible for their own security and safety.

[4] For more on de-permiterisation see the Jericho Forum http://www.opengroup.org/jericho/ (2006)

1.3 Objectives and Approach of this Study

The objective of this study is to provide a set of initial policy options to the information security challenges associated to the use and implementation of five selected disruptive technologies: WIMAX, RFID, IPv6, Trusted Computing and VoIP. IPv6, Trusted Computing and VoIP were chosen by the European Commission and the remaining two were suggested by RAND Europe. However, this is not an easy task since this exercise addresses a set of new technologies whose implementation has a very limited history and, therefore, solid evidence and experiences are difficult to uncover. In order to overcome this potential shortcoming, the project has developed a multi case-study research methodology.

Research methodology scholar Robert Yin encourages the use of case studies for projects examining situations, such as new uses of technologies that researchers cannot directly manipulate but only observe.[5] The topics of this project satisfy this requirement since it analyses the security challenges and solutions during the use and implementation of such novel disruptive information technologies as VoIP, WIMAX, Trusted Computing, RFID and IPV6. Moreover, as also argued by Yin, multiple case-study projects are more "robust" since they allow the collection of a larger set of data and, therefore, the provision of more compelling evidence. This last point is pivotal for the success of the current research endeavour since solid and robust evidence is required in order to provide a comprehensive set of policy options to the European Commission in its efforts to implement its i2010 strategy.

The effectiveness of a multiple case-study methodology depends on the capacity of creating a situation of logic replication. This terms refers to a situation when each case study "either (a) predicts similar results (a literal replication) or (b) produces contrary results but for predictable reasons (a theoretical replication)".[6] In order to satisfy this logic, each case study needs to refer back to the proposed research framework based on common threads as well as allow access to a similar set of primary and secondary data. The first condition was satisfied with the establishment of common approach to the case study research frameworks during the initial stages of the project.[7] This was achieved by undertaking a pre-Delphi exercise, followed by a workshop, where pan-European experts were asked to indicate what they considered to be the main security challenges associated with the use and implementation of these technologies and a set of common questions to unveil them in the case studies.

---

[5] See Robert Yin, Case Study Research: Design and Methods, Sage 1999 Second Edition

[6] ibid. page 25

[7] For the findings of this activity, please refer to Appendix A of this report.

The second condition proved to be more complicated since RAND Europe had to assess its capacity to access information and data within the timeframe of the project. The fact that this research endeavour addressed a set of innovative technologies made the case study selection pivotal for its success. Following an analysis of the literature and institutional professional contacts, and in agreement with the European Commission, RAND Europe has selected these five case studies based on two criteria:

a) *implementation status*: the case study had to refer to a case study that was either completed or in the process of being completed within the time frame of the project

b) *access to case study experts*: the case study had to allow access to experts within the time frame of the project

The selected five case studies satisfy these requirements. Upon the identification of the common questions through the pre-Delphi exercise and workshop, RAND Europe started the collection of information about the commercial players involved in the case study. In this context, particular attention was devoted to satisfy a specific requirement originating from the discussion among experts during the case study research framework workshop. It was emphasised that the value of these case studies would be augmented if RAND Europe were to assess the security challenges associated with the implementation of these technologies within the overall commercial and business objectives of the organisations involved in the case study. RAND Europe, therefore, developed a set of specific case study questions to guide its data collection through semi-structured interviews, which were conducted in March and April 2006.

The results of the case studies were presented to and discussed with a number of experts, invited by the European Commission and RAND Europe to come to a workshop in Brussels on the 30th June 2006 for this purpose. The Workshop began with presentations setting the out the policy objectives and outlining the stages of the study, followed by an overview of the project's industrial and economic context (in particular, why it is important to study disruptive technologies and the market behaviours of disruptive technologies). An introduction to the study methodology was presented and then participants heard from representatives from each of the case study organisations give a short overview of their case study, reflecting the general context of the deployment of the technology, business objectives and technical details of the implementation.

The Final Report is structured as follows. Chapters 2 – 6 present the detailed results of the case studies. This includes an overview of the technology, a description of some general issues surrounding the technology from a business and security standpoint, a short background to the organisation involved in the case study. Detail on the case study implementation includes: business drivers for implementation of the specific disruptive technology, security challenges found and conclusions from the case studies. Each chapter also presents the results of specific discussion, per case study, that was held during the Final Workshop. Chapter 7 presents a set of overall conclusions and recommendations for policy makers resulting from the case studies and final workshop discussion. The Appendices contain information on the development of the case study framework (representing deliverable D-1 of the study), participants and interviewees, and a Glossary of Terms.

CHAPTER 2 Voice over Internet Protocol (VoIP)

2.1 Voice over Internet Protocol (VoIP): General issues

VoIP is the transmission of voice (analogue) signals over Internet Protocol (IP - a set of rules used to control the transmission of data). It is particularly suited to broadband networks, but in its early development it was used over traditional analogue copper telephone wires. The main architectural difference with a VoIP network is the use of packet switched networks, rather than circuit switched networks such as the Public Switched Telephone Network (PSTN). Packet switched networks can be more efficient than circuit switched ones as the information can be routed in packets or 'pieces' over any number of possible paths. By contrast, with a switched network the entire circuit must be open for the stream of content for the duration of the transmission. Although various means have been developed to get around this problem, packet switched networking is becoming a standard for communications.

An important consideration with packet switched networks as they currently operate (particularly the Internet, with the current version of IP) is that transmissions are made on a best effort basis. Therefore, there is no certainty that the packets will arrive at the destination in the right order or even at all. Although the TCP (Transmission Control Protocol) part of IP alleviates some of this concern by carefully reorganising packets as they arrive at the destination so that they make sense to the receiving application (such as an email program) this is still not foolproof. Dealing with this problem while reducing to acceptable levels the chance of mistakes occurring is an important consideration for the widespread deployment of VoIP. The next version of IP, IPv6 has a set of rules called Quality of Service (QoS) which solves this problem to a certain extent by giving priority to packets that can be recognised as carrying voice or multimedia information.

As VoIP is not a network but an application that resides on top of an existing IP network (such as the Internet), those companies that already own IP networks (such as large multinational Internet Service Providers and Communication Service Providers) can recover the costs of running and maintaining such networks by charging for other IP services, including VoIP. This makes VoIP extremely attractive for non-traditional telephone companies to break into the voice market.

Several developments promise to boost the uptake of VoIP. These include the growing take-up of broadband services, which will result in less need to rely upon the traditional Public Switched Telephone Network (PSTN). The ability of new entrants to provide a

VoIP service without the need to obtain access to an incumbents network is also a key enabling factor for meeting increasing demand for VoIP. There are, nevertheless, several potential uses of VoIP, which have been categorised by the OECD according to the type of terminal and end-use device. These are:

Phone to Phone – by connecting a traditional telephone into a IP network via the use of routers, which change the telephony signals into IP and then vice versa at the receiving end.

PC to PC – Depending on the installation of compatible software on each party's PC, users do not need to use telephones to make VoIP calls. The users must be online for the duration of the call, which lends itself to broadband, (fast), always on connections. This form is often the most commonly used over the public Internet, using such applications as Skype[8], Teamspeak 2.0[9] and Roger Wilco.[10]

Phone to PC – the connection of a traditional phone at one end of the transmission and a PC at the other. This is possible via the use of specialised gateways which compress voice traffic coming from the PSTN (from the traditional telephone) and place it onto the IP network, reversing the process in the other direction. Clearly the PC user must be online with an active connection to an IP network for this to occur.

Mobile VoIP – By the use of 3G (IMT-2000) systems, it will be possible to make IP calls over mobile networks. One of the main 3G standards, CDMA2000 1x EV-DO supports all IP based voice, video and data communications. Push to talk (PTT; instantaneous walkie-talkie style communications) is another mobile VoIP service being developed. With PTT, only one person can speak at a time (a situation known as half-duplex).[11] The benefits of this are instantaneous communication (i.e. the caller does not have to dial a number and wait for access to the network).

Wireless VOIP - Is also possible by using Wireless Local Area Network (WLAN) access systems (e.g. WiFi or WiMAX) to transmit voice packet data. This is known in Europe as 'Wireless VoIP'. Although the market for WiFi technology has developed in recent years, it is still small, but growing rapidly. All the major US wireless carriers are rolling out versions of this service that is often called Push To Talk over Cellular (PoC). This class of VoIP system has the potential to radically destabilise the telephony market as it would allow non-traditional providers of voice telephony services to enter the lucrative mobile telephony market.

[8] Skype: www.skype.com

[9] Teamspeak: www.teamspeak.org

[10] Roger Wilco www.roger-wilco.com

[11] Techtarget Definitons: Half-Duplex (2006) available at http://whatis.techtarget.com/definition/0,289893,sid9_gci1186491,00.html

Examining the use of VoIP within the corporate world, it is possible to identify three additional types to those previously indicated:

Gateway – the addition of a gateway to a traditional Private Branch Exchange (PBX), which are telephony systems within an organisation that allow users to share a certain number of external telephone lines while having their own local ones.

IP-Private Branch Exchange (PBX) – the functions of a PBX are implemented in an IP device which allows for switching of all calls.

IP Centrex – an outsourced solution with a relatively high capital expenditure but potentially high costs savings. In this instance, installation, operation and management of an IP network is outsourced to a telecommunications company.

The effectiveness of the previously indicated services relies heavily upon a set of specific standards to be effective. These are:

ITU H.323 – the fully standardised VoIP specification, initially designed in the late 1980s. Originally this was a video-conferencing standard but it contains all the necessary requirements for call control and management; gateway administration and media traffic and user participation.

ITU.HJ.248 – important when equipment from more than one provider is in use, this implements Bearer Independent Call Control (BICC).

IETF-SIP Session Initiation Protocol – a real time signalling protocol for VoIP services developed in the mid 1990's by the Internet Engineering Task Force (IETF). It is used to establish and terminate call sessions over IP. SIP provides signalling to participate in a call and confirm that the client has received a final response. This is currently used in the majority of VoIP products such as Skype (but was originally developed for PC to PC applications). Some predict that SIP will be the successor to ITU H.323.

2.1.1 Why is VoIP disruptive?

VoIP can be viewed as a disruptive technology or service because it removes the source of profit of traditionally established players, by providing a telephone service over a non-PSTN network. This means that companies which have built or have access to IP networks can begin to market VoIP as a way of recovering their costs, eating into the traditional customer base of the incumbents. This further erodes their market position, as the explosive growth of mobile telephony means that incumbents have fewer opportunities to develop new customers for 'traditional' telephone services. Additionally, VoIP is an application that does not need access to a telephone network. Therefore companies that previously did not operate in the voice telephony market can enter the market with low priced offerings, destabilising current market balances.

In the consumer world, VoIP is highly disruptive to the telephony incumbents as it removes the equation of geography (a major source of revenue for established telephony players) from telephony. Using a popular application like Skype, home use consumers can call relatives and friends over long distances for the same rate as local calls, thus stimulating significant demand. The ex-patriate communities (geographically dispersed communities) are a good example of this dynamic, where they are often seen as early adopters for market led developments in telephony such as international discount phone cards (enabled by

deregulation of the telecommunications sector) and VoIP. In the commercial world the disruptive effect of this technology manifests itself in the way that it can free companies from expensive contracts with traditional telecommunication players, and allow them to move towards unified messaging and converge the management, administration and operation of voice and telephone networks.

The potential disruptive nature of VoIP can be seen by the growing size of the market. According the US telecoms research company TeleGeography, US VoIP susbscribers grew 248% from 1.3million in the fourth quarter of 2004 to 4.5 million subscribers by the end of 2005. Operator revenue growth increased by over 300%, from less than 200m in 2004 to over 1bn in 2005. The company projected that by 2010, almost 19m Voice over Broadband (VoBB) lines will be in service. These lines will largely be taking trade away from the incumbent telephone operators.[12] In early 2004 the OECD reported that it was estimated that by 2006, 50% of the world's telephone traffic would be based on VoIP.

As compared to international PSTN traffic, the share taken by VoIP has been slowly increasing since 1998. According to Telegeography / Primetrica research, in 1998 VoIP traffic constituted 0.2% of international telephone traffic (some 150m minutes of total telephone traffic of 93,150m minutes). In 2001 this had grown to 4.3% of international telephone traffic (5,954m minutes of VoIP traffic from a total of 137,891m minutes) and by 2003 VoIP market share made up 12.8% of the total telephone traffic (24,519m minutes of a total of 191,134m minutes).

2.1.2 Overview of Security Threats and Concerns

According to the VoIP Security Alliance, the following classes of potential categories of threats exist: [13]

- *Social Threats*; these include issues such as misrepresentation, theft of service and unwanted contact. The misrepresentation might occur to identity, authority, rights and content. Theft of service is defined as unlawful taking of an economic benefit of a service provider by means intended to deprive the provider of lawful revenue or property which can be accomplished via either unauthorized deletion or altering of billing records; unauthorized bypass of lawful billing systems; unauthorized billing or taking of service provider property. Unwanted contact can occur via either harassment, extortion, or unwanted lawful contact.
- *Eavesdropping*; can be cell pattern tracking, number harvesting, fax reconstruction, conversation reconstruction
- *Interception and Modification;* includes call black-holing, call rerouting, fax alteration, conversation alteration, conversation degradation; conversation hijacking

[12] US VoIP Revenue & Subscribers Post Triple Digit Gain in 2005 TeleGeography's US VoIP report TeleGeography 2006

[13] VoIP Threat Taxonomy: Voice over Internet Protocol Security Alliance available at http://www.voipsa.org/Activities/taxonomy-wiki.php

- *Intentional interruption of service includes Denial of Service and Physical Intrusion*. Denial of service can be VoIP Specific Denial of Service (DoS) itself including Request Flooding, Malformed Requests and Messages, QoS abuse, Spoofed Messages and Call Hijacking, Network Services DoS, Underlying Operating System / Firmware DoS and Distributed DoS
- *Unintentional interruption of service* which can include loss of power, resource allocation and performance latency.

2.2 VoIP within the UK branch network of HSBC

This case study describes the implementation of VoIP to support voice communication needs of the retail branches of HSBC in the UK.[14] The corporate use of VoIP presents a set some useful features that can be reviewed in a case study. HSBC is one of the world's major financial institutions. It is headquartered in the UK, where HSBC Group co-ordinates the activities of a number of business units from a headquarters at Canary Wharf in London. It has around 9,500 offices worldwide in 76 countries in Europe, Asia Pacific, the Americas the Middle East and Africa. It employs 284,000 staff looking after around 125 million individual and business customers by providing a wide range of services, including personal financial services, commercial banking, corporate, investment banking and markets, private banking and other activities. HSBC is listed on the London, Hong Kong, New York, Paris and Bermuda stock exchanges and there are over 200,000 shareholders in 100 countries and territories. [15]

HSBC's Information Technology (IT) function at the Group level is provided by HSBC Technology Services (HTS). Managed by the Group Chief Information Officer, this organisation has some 22,000 employees globally and total annual budget of over US$4bn. Decisions about IT solutions and projects, including VoIP implementation, need to be seen in the context of global resource management while maximising the status of a truly global and reliable financial institution. Therefore, any new IT technology needs to satisfy the key tenets of HSBC IT strategy: Standardisation; Self Sufficiency; Centralisation and Careful Timing of Technology Adoption.[16]

HTS itself is split into programming and non-programming divisions. Telecoms is placed within the latter functional category, which also includes data centres, desktops, servers as well as telecommunications. The Group Head of Telecommunications is responsible for all forms of telecommunications (call centres, voice, video-conferencing, data) and reports directly to the Group Head of IT Operations. The telecommunications function is represented at such a senior level due to the recognition of its importance to the overall

[14] This case study is based on telephone interviews conducted with representatives from HSBC Technology services team and a review of associated documentary material. For a full list of interviewees see Appendix A: List of Interviewees

[15] Presentation to Morgan Stanley European Banks Conference, London, 22 March 2006 available at http://www.hsbc.com/hsbc/investor_centre/

[16] HSBC Holdings: IT Strategy, (HSBC, 2003) available at: http://www.hsbc.com/hsbc/investor_centre/

business, and the need to manage the interlinking of a large number of domestic banks (e.g. in UK, USA, Hong Kong, Brazil, Mexico) and their high traffic requirements. HSBC, has one of the world's largest private networks and sends around 500 terabytes of data across its network internationally per year. HSBC has offshore business processing activities in five countries (including India, China and Malaysia), nine to ten centres with around 30,000 staff and opens a 2,000sq/ft contact centre roughly every three months. [17]

The 'in house' telecommunication provider is called *HSBC Group Telecoms*, which is organised into four regions: South America (headquartered in Curitiba, Brazil), USA (headquartered in Chicago) Europe (headquartered in Sheffield). Asia-Pacific (headquartered in Hong Kong). Organisationally, there is a form of matrix reporting structure, as each national telecom manager is part of the country line management structure and also reports to a regional functional telecom manager who himself reports to the Group head. The role of the Group Head of Telecommunications can therefore be defined as managing telecommunications across geographies. As such he has a keen awareness of the need to meet centralisation goals set out at a corporate strategic level. There is a total telecoms budget of over US$600m per annum with 800 telecom staff.

2.2.1 Business drivers

This section provides an overview of the business drivers that have pushed HSBC to undertake a 12-month project to deploy VoIP across its UK branch network. The key motivating factors for deciding to implement VoIP was cost reduction. These objectives were in line with the goals of centralisation and standardisation, which are key elements of HSBC's IT strategy. In 2004, HSBC was spending a significant amount of budget (in the region of millions of pounds) on a Centrex (private telephony services provided by the public network) solution provided by a major UK telecommunications provider. There was a keen sense that the technical means employed were secondary to the priority of achieving the required cost reduction. VoIP, therefore, was selected purely because of its ability to meet these objectives and nothing more. Indeed, negotiation with the existing provider of telephone services continued while VoIP was being considered, but the former option did not prove to be viable, so the decision was taken to undertake a VoIP implementation.

Even if potential cost savings were foreseen, HSBC remains unconvinced of the need to implement VoIP across its entire organisation. Senior telecommunications management indicated that they felt that there was no 'killer application' or use for VoIP in a banking institution. Although there were circumstances where the implementation of VoIP made sense from the perspective of future proofing infrastructure (for example, in the provision of telecommunications service in a new 'greenfield' site or newly acquired office), the widespread roll out of VoIP was not undertaken, due to the lack of persuasive enough reasons to do so. A more limited and controlled implementation was introduced, as in the case of the current case study.

[17] "Off shoring" is conceptually different from "outsourcing." In an offshore operation, the contact centre is still owned and run by the organisation, whereas an outsourced organisation may also run an offshore operation for a client. HSBC therefore has to meet certain requirements for each country where it maintains a contact centre and cannot delegate the management of these to another organisation

On the whole, VoIP within HSBC was described as being in a state of transition. The philosophy of "if it ain't broke don't fix it" was viewed as being highly appropriate and relevant for senior management decisions regarding the implementation of VoIP in the entire organisation.

Differences between consumer or retail use of VoIP (e.g. via applications such as Skype) and organisational or institutional rollouts were also cited as being key to HSBC's understanding the innate 'disruptiveness' of VoIP as a technology. For the consumer, VoIP is acutely more disruptive because of its removal of the geographic element in long distance communications (with subsequent ramifications for the public telephony providers) and is thus the main cost reduction factor. The cost of infrastructure (e.g. a computer running Skype or a VoIP handset to use with a PC running VoIP software) for a consumer is comparatively low. The same cannot be said for the large business like HSBC, which may have a huge installed base of PBXs and TDMs (Time Division Multiplex) to replace and large infrastructural costs associated with any implementation. These issues need to be taken into consideration when examining how HSBC approached its technical implementation of VoIP.

2.2.2 Technical implementation

VoIP was rolled out to 30,000 handsets across 1,500 HSBC UK branches. This was a large undertaking and involved the replacement of the entire phone network for these branches. However, it is important to emphasise that the organisation's main buildings, such as the Group Headquarter in London, remained on a TDM/ PBX system. At the end, there were around 100 PBX's remaining after the VoIP implementation, with CISCO Call Centre Manager (CCM) PBX software chosen as the solution. [18]

The VoIP implementation started with a pilot of 30 - 40 branches supported by the UK telecoms team involved in the implementation across the organisation, including 2-3 security experts. There was a gap of 6-8 months between the preferred solution being agreed and the pilots going ahead, and the roll out across the entire branch network. The full implementation was eventually led by the networks team and involved personnel from the following areas: server, telecommunications, networks, branch and physical access, equipment providers, local cabling companies and so on. The project was considered very much a 'business as usual' project, despite the innovative nature of the technology. VoIP was regarded as simply another one of the projects being undertaken at that time.

CISCO CCM was picked as the VoIP product. The CCM was running Microsoft's Windows Server Edition 2003, with which there were concerns as the server 'build' was not in line with HSBC standard for this particular version of operating system. CISCO eventually agreed to cut down the number of services on the CCM to meet HSBC's requirement. This process took two months following the initial period of testing. This concern existed as HSBC was worried that the device as provided might be vulnerable to DoS and virus attacks.

[18] For more information about CISCO Call Manager see
http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/index.shtml

To mitigate any risks from such threats, 'screening routers' which filtered traffic were placed in front of the VoIP server. This would mean that only authorised traffic could get to the device. Thus, in the event of a virus affecting HSBC's own internal network, the device would remain operational.

The CISCO CCM PBX software is thus connected to physically and virtually separate LANs (Local Area Network) within the data centres. Logically Separate Virtual LANs (VLANs) dedicated to voice were implemented to separate the voice IP traffic from the data traffic. Traffic from the voice VLAN is treated separately from traffic from the data network and is monitored more closely. This helped to prevent incorrectly configured or rogue end point devices from sending traffic into the voice IP queue thus undermining Quality of Service (QoS).

Two key characteristics therefore of the implementation were the creation of VLANS (Virtual Local Area Networks) and the use of a consistent, organisation-wide IP traffic allocation plan.

2.2.3 Security challenges

During the implementation HSBC carried out a formal risk assessment, which identified 23 separate risk areas. Detailed project engagement was then established between the IT security team and the overall project team. VoIP related risks were categorised in the following manner:

1. *Attacks on the telephony end point* – eavesdropping on unencrypted traffic on the network, DoS, Dynamic Host Control Protocol (DHCP) starvation[19] and attacks against the IP handsets themselves
2. *Attacks on Internet Protocol (IP) telephony servers* – viruses, worms, Trojans –the usual form of attacks against servers (in this case the CISCO Call Manager) connected to an IP network
3. *Attacks on the application itself* – unauthorised access to the telephone system, toll fraud and telephony fraud from interfaces to the Public Switched Telephone Network (the unencrypted VoIP has the same level of risk as the PSTN network or service).

Other key security issues identified included servers organisations, robustness, access control and vendor knowledge in the field of voice communications, with a specific focus on QSIG signalling.[20]

The nature of the implementation with its separate VLANs for voice and data meant that other security considerations, specifically relating to availability, had to be met. Chief amongst these was the need for a contingency centre capable of dealing with sites that are

[19] DHCP is the way in which IP addresses within a network are automatically assigned for a limited time, to devices on the network (e.g. PCs and laptops)

[20] QSIG is an internationally standardised signalling protocol for use in corporate or enterprise voice or integrated services networks, typically between Private Automatic Branch eXchanges (PABX). For more information see QSIG home page at http://www.ecma-international.org/activities/Communications/QSIG_page.htm (visited 26/04/06)

100km apart. Other availability issues come with the specific solution that has been devised – managing the requirement for staff to move around, within the constraints of the selected solution, for example.

HBSC, moreover, developed a traffic allocation plan to reduce congestion and mitigate availability risks. Particular attention was paid to the issue of Quality of Service (QoS) by indicating which traffic (multi-media, voice etc) has priority on a global scale across the entire network. This was considered necessary in order to maintain an acceptable level of service for VoIP calls and video conferencing.

As VoIP implementation was carried out, HSBC staff started to appreciate that higher level of security practices had to be undertaken with particular attention to servers since these were now carrying both voice and data traffic. Therefore, the IT security staff involved in the implementation of security devoted particular attention to security aspects relating to the VoIP servers.

Still, HSBC realised that it was not appropriate simply to place a VoIP PBX server such as CISCO CCM in a standard server farm and expect it to provide voice levels of quality. The introduction of PBXs into a standard server environment requires some specialist training and education for system administrators. This pointed the HSBC team to a wider concern about the user perspective of VoIP within the organisation. As VoIP PBXs run on standard server infrastructure there was a fear that IT departments would consider it as 'just another server to be managed'. However, this was not supposed to be the case since VoIP servers need to be monitored more closely. HSBC staff, in fact, was aware that users would not accept for voice communication the levels of quality associated with email communication, which suffers from occasional outages, reliability reduction and non-availability.

Finally, HSBC staff had to comply with a set of national and international regulations concerning the retention of communication data. From a technological perspective, the current PBX solution selected by HSBC can already record voice calls as necessary to comply with regulatory requirements so no new configuration or technology was required. The selected solution can also effectively meet regulatory requirements in the trading floor and contact centres.

2.2.4 Conclusions

This case study illustrates that VoIP is a highly disruptive technology from an end-user and market perspective, but at present is viewed less so from inside a corporation. In the example of the case study, the organisation adopted a 'wait and see' attitude and was not deploying the technology in a widespread fashion across the global organisation as at present it was felt that there was no clear justifiable business case. When deployed within an organisation, VoIP promises to act as a catalyst for important changes in internal operating structures (such as centralisation to achieve economies of scale) that in turn bring with them attendant security risks, in particular reliability. In detail, the case study highlighted the peculiar requirements of maintaining VoIP infrastructure and how the security of the infrastructure must be considered specifically in the context of the services it provides, not just as being more networks or equipment to maintain. It also illustrated how off the shelf VoIP equipment needed to be re-configured, in conjunction with the vendor,

to meet certain organisational security standards. The use of virtualisation and separation (and careful planning of traffic allocation schemes) were important methods used to mitigate the effects of some of the more complex risks arising from the deployment of this technology. Regulatory issues were not seen as important in any VoIP deployment as the means to meet these requirements were already deployed at a level above the VoIP infrastructure. The only issue that was raised was where regulatory environments require the separation of national and international traffic, but this was felt not to be that relevant in Europe. Finally, concerns over voice quality were accepted, but it was felt that this was a minor issue and not likely to have a great deal of impact from a security perspective.

VoIP brings an entire new business model for the delivery of voice communications services. This affects the way industry is organized, changing, redrawing roles, which have been historically defined for long periods of time. More so, the current legislative framework may not be built to deal with the new business concepts that VoIP introduces illustrated by Indian regulatory requirements to separate national and international traffic. This may not be a problem for those legislative measures that are truly technology neutral, but as this is not always the case in some instances legislative review may be useful and necessary.

2.2.5 Review of the case study conclusions during the Final Workshop

Comments on the VoIP case study at the Final Workshop proved to raise some interesting points not covered elsewhere. These included the realisation that the disruptive element of VoIP might not be permanent – if a company undertakes to deploy VoIP across its entire telecommunications infrastructure, sweeping away existing 'old' PSTN infrastructure which is provided by the incumbent company, then in the short term this might be extremely disruptive. However, in the longer term, if an electricity power failure alerts management to the dependency that has been created by total reliance upon VoIP, then the use of this technology can be considered to be sustaining (as the company has inadvertently become 'locked into' relying on a technology).

The case study highlighted another challenge (although this was not a property of the case study itself) that the recording of calls (to comply with regulatory requirements) can be complex with VoIP, especially if proprietary cryptographic and security algorithms are used. This was not an issue in the case study as recording was undertaken at a system level above that of the VoIP infrastructure. Indeed, some participants argued that VoIP might be *too* secure for some business processes undermining non-repudiation, as it would be possible not only to hide the content of the call, but also even that the call ever took place.

The different encryption standards in use within the VoIP market may have some impact upon interoperability, especially in regard to consumer use of software VoIP applications (such as Skype) between peers. It was important to make sure where possible that security was considered as part of the interoperability of separate products. Finally, the case study illustrated the use of VoIP within a single organisational setting that had control over its own internal network and could successfully establish a traffic prioritisation scheme and a coherent architecture to support its implementation. These concerns over interoperability (and consequently security) would become even more acute in the peer-to-peer application of VoIP over the public Internet, particularly with the current reliance upon IPv4.

CHAPTER 3 Trusted Computing

3.1 Trusted Computing: General issues

The term Trusted Computing or Trusted Computing Base (TCB), when used in the context of software protection (its most common iteration) is one of the key security technologies used to protect security features of software (defined as operating system, memory, files and objects).

The evolution of TCB has been a result of the drive towards virtualisation, as a means of achieving process isolationism. This process isolationism can be achieved only if it is possible to verify that the hardware and software in a machine has not been tampered with or altered since it was last started (or booted up). This concept was a characteristic of early PCs where the BIOS (Basic Input Output System – the core set of instructions indicating what disk drives are present, where memory is located what partitions are on the hard disk etc) was present in the ROM (Read only Memory) rather than the hard disk (where it could be affected by viruses). This idea of a 'trusted bootstrap', or starting procedure, for the newer sort of PC machines (where the boot-sector is located on volatile memory thus making it vulnerable to viruses) was first put forward by a paper in the 1997 Proceedings of the IEEE Symposium of Security and Privacy "A Secure and Reliable Bootstrap Architecture".[21] In 2001 this was registered as a patent by the US Patent office. The reference monitor (described below) was first developed in a paper written by James Anderson for the United States Air Force in 1972 and marks the beginning of the development of the thinking (in military circles at least) of secure systems development.[22]

One of the main industry led developments is that of the Trusted Computing Group (TCG). The TCG is a not-for profit industry standards organisation with the stated aim of enhancing the security of the computing environment in disparate computer systems. TCG was formed in spring 2003 and has adopted the specifications developed by the

[21]" A Secure and Reliable Bootstrap Architecture, William A. Arbaugh, David J. Farber, Jonathan M. Smith IEEE Security and Privacy Conference, 1997 available at http://ieeexplore.ieee.org/xpl/abs_free.jsp%3FarNumber%3D601317

[22] James P Anderson, Computer Security Technology Planning Study, Deputy for Command and Management Systems , HQ Electronic Systems Division (AFSC) United States Air Force, October 1972 available at http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf

Trusted Computing Platform Alliance (TCPA). The mission of the TCG, via a collaboration of platform, software and technology vendors, is to develop a specification that delivers an enhanced hardware and Operating System (O/S) based trusted computing platform that enhances customer's trusted domains. To do this it intends to:

- publish specifications defining architectures, functions and interfaces that provide a baseline for a wide variety of computing platform implementations;
- publish specifications describing platform implementations such as the personal computer (PC), Personal Digital Assistant (PDA), cellular telephone and other computing equipment;
- publish evaluation criteria and platform specific profiles that meet functional and reliability standards and thus allow increased assurance of trust that may be used as a common yardstick for the evaluation of devices incorporating TCG technology;
- Recommend practices and procedures for maintaining trust in deployed platforms to ensure operational integrity of maintenance processes after deployment.

Amid the controversy surrounding Trusted Computing, Professor Roger Needham put forward some clear explanations about why it is useful. He stated that there might indeed be some instances where it was necessary to constrain a user's actions – for example in the modification of an mile-ometer or odometer on a car with malicious intent (thereby preventing a crime).[23] Additionally, benefits for confidential document destruction have been identified, and the better implementation of access control policies.

As can be seen from the extensive list of applications below, trusted computing is an enabling technology for a myriad of applications.

The first Trusted Computing Group specification was published in 2000. Many Trusted Platform Module (TPM) chips have been made available in PCs, including many popular desktop and laptop models. For example, the IBM Thinkpad series of laptops have had this capability since May 2002.[24] Some argue that the Windows Registration features in Microsoft Windows XP are an element of a Trusted Computing system.[25] In addition to its work on the Next Generation Secure Computing Base (NGSCB, covered below) Microsoft has been trying to certify all device drivers since 2000 for compatibility reasons. This functionality is now built into Windows XP where if you try to load an unsigned driver, Windows will alert you to this. Enterprise Rights Management (to better support access control policies on corporate documents) features are installed in Windows Server

[23] Roger Needham, "Security and Open Source", Open Source Software : Economics, Law and Policy, Toulouse, France, June 20-21, 2002 available at http://www.idei.fr/activity.php?a=2491

[24]IBM / Lenovo Thinkpad Product line available at http://www-131.ibm.com/webapp/wcs/stores/servlet/CategoryDisplay?storeId=10000001&catalogId=-840&langId=-1&categoryId=2035724

[25] Ross Anderson's Trusted Computing FAQ available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

2003[26] and technical Trusted Computing development kits have been available since October 2003.

From the hardware perspective the two main vendors in the PC market, AMD and Intel, have both been working in this area. AMD has its Secure Execution Mode (SEM) about which very little is known but Intel's LaGrande Technology promises to ship in its next generation of Central Processing Units (CPU) (Merom, Conroe and Woodcrest) to be released in 2006.[27]

Microsoft has said that it intends to deliver Secure Startup, a hardware based security feature which uses a TPM (version 1.2) in the next generation of its O/S, Longhorn. This is intended to improve PC security by helping to ensure that the PC is running in a known good state and protecting data from unauthorised access via full volume encryption of the disk drive. Other developments after Secure Startup have been promised.[28]

3.1.1 Why is Trusted Computing disruptive?

The potential disruptive nature of Trusted Computing needs to be taken into account in consideration of the evolution of computing. With the drive to the Ambient Intelligent Environment, the existence of the PC as the principle form factor[29] of a computing device is expected to end. Mobile devices, whether they be smart phones, Personal Digital Assistants or other devices as yet unheard of, will have increasingly large amounts of information associated with them. This information will be of various kinds, but the most important will be personally sensitive information that end users will want to protect and the representation of money (either by bank account and credit card information such as numbers and PINs, electronic cash or other forms of payment). Additionally as devices become more capable, more and more types of content are becoming available, with quality ever increasing. This includes graphics, audio and video content. In order to preserve their revenue streams as content reaches mobile devices, content owners wish to protect this property and ensure that it is used in an authorised legal fashion. Thus the theoretical value of information contained on the device increases. In practice this may mean that customers must pay to have access to certain forms of content. If a transaction has taken place, then the providers will want to know that a protected file cannot be shared around illegitimately and end users will want to know that they can properly and easily access content that they have paid for.

Additionally, the role of Trusted Computing in the embedded space raises questions about corporate information assets and whether mechanisms can be put in place to allow the use of mobile devices to access documents and material that may be subject to strict

---

[26] Windows Rights Management on Windows Server 2003, Microsoft, available at http://www.microsoft.com/windowsserver2003/techinfo/overview/wrm.mspx

[27] Gabriel Torres Intel LaGrande Technology explained, December 20th 2005 available at http://www.hardwaresecrets.com/article/264/1

[28] Microsoft Next Generation Secure Computing Base available at http://www.microsoft.com/resources/ngscb/default.mspx

[29] Form factor refers to the appearance and physical design of an object – for instance a metal box with keyboard, monitor and mouse

organisational access control policies. Workers may want increasingly more flexible access to such information resources, not necessarily when they are sitting in front of a PC.

Finally, it is important to look at trusted computing in the embedded space in the greater context of crime reduction. Estimates suggest that out of the billons of dollars lost to telecommunications fraud, one of the biggest contributors is mobile phone handset cloning.[30] Indeed, around 50% of street crime is thought to originate from mobile phone thefts.[31]

Due to its security features, Trusted Computing can lead to a set of new or more innovative applications, as described in the following paragraphs based on the work currently undertaken by the TCG.

Trusted Computing is expected to have an impact on *Risk Management.* Protected Storage technologies as defined by the TCG can be applied to reduce the identified risk to information assets, resulting from a process of risk management where the goal is to minimise risk to corporate and personal assets due to malicious and accidental loss or exposure. Protected storage can be used to secure public, private and symmetric keys (as access to these important assets would allow other information assets to be compromised). The keys can be made less vulnerable to attack as protected storage is based on mechanisms that are implemented in an isolated sub-system. When information assets are protected in this way, the vulnerability factor present in risk equations used to compute annual loss expectancy will subsequently decrease.[32]

Another important application can be *asset management* through TPM. Asset databases can use owner or organisationally created identities (protected and not intended to be physically removed or replaced) to reliably associate platform asset information, thus reducing the ability of a thief to gain access to information assets should they be stolen (thus removing any possible profit and thus many forms of motivation).

Trusted computing may also lead to new forms of *E-commerce* as it gives platforms the ability to define an e-commerce context in which customer and vendor may establish a relationship based on information exchange. Customers are able to control preferences that may be important for both customer and vendor. With the appropriate consent and privacy safeguards, a vendor can identify repeat customers and trust customer managed preferences by verifying the relationship. It would also be possible to report platform configuration information which can define the relationship between customer and vendor.

Security Monitoring and Emergency Response is also an area of potential for Trusted Computing since it can reduce the amount of time IT managers spend patching PCs and responding to virus attacks. By using Platform Configuration Registers (PCRs), a TPM can report its configuration to system administrators at boot time, allowing them to easily

---

[30] United States Secret Service Financial Crimes Division available at http://www.secretservice.gov/financial_crimes.shtml

[31] Mobile Phone crime blitz launched, BBC, 17th December 2003 available at http://news.bbc.co.uk/1/hi/uk/3326171.stm

[32] ALE = Single Loss Expectancy x Annualised Rate of Occurrence (of a specific risk)

measure each of the components in the system (both hardware and software) to see if they have been changed and are thus vulnerable to virus attacks. System processes may also be installed that would allow IT managers to deny access to the network if the TPM were to report via the PCR that an unsafe configuration was present.

All of the previous examples, which are based on the work by TCG's Mobile Working Group, illustrate potential applications for TCG compliant equipment in mobile (cell phones, PDAs) devices.[33] Many of these applications may also be relevant for the desktop PC world, particularly in respect of device integrity, authentication, digital rights management and secure software download, as described in the following paragraphs.

Trusted computing can allow for *Platform Integrity* that helps to ensure that devices possess and run only authorized operating systems(s). An unauthorized version could, for example, be a modified version of the operating system which could broadcast false device identification data. Additionally, unauthorized hardware could be another component inserted to change or block signals with the mobile device. The maintenance of platform integrity means that platform hardware and principle components of the platform software (boot code and O/S) are in the state originally set by the device kernel. The user is thus able to rely upon the trustworthiness of the device and that it functions as per the manufacturer's intent and is able to defend itself against 'mal-ware' (e.g. viruses, worms, spoofs etc). Platform integrity is a key building block for other uses of the device (for example stronger platform integrity enables stronger data protection). With a greater degree of platform integrity, the mobile phone can be used for corporate applications and can be allowed onto the corporate network and to store corporate documents.

Another interesting area of trusted computing application is *Device Authentication* since it can assist in user authentication. The device, therefore, can store and protect identification information, such as keys that can be used to securely authenticate the identity of the device to a service provider or network provider. Device authentication may also prove the identity of the device itself without any reference to user authentication. Both types might be required in a Digital Rights Management (DRM) context. A Trusted Computing enabled mobile device can be able to store and protect all user and device identities possible in the context of multiple identities (for example, with more than one service or network provider) and use appropriate identities for each case. The user can benefit because if the service provider trusts the device then a greater number of services can be offered to the user. The user still has the option of being in control of which identity is used and can make a decision based on their own interpretation of the Service Providers privacy policy. Privacy can be further enhanced by robust device authentication measures designed to reveal no other information than is absolutely necessary about the users personal ID.

Robust DRM Implementation is one of the key attractive features for content providers. TCG specifications for mobile devices do not define a DRM system but simply provide the capability which can be used within a DRM system. The TCG specifications allow a robust (i.e. resistant to certain levels of attack determined as a result of a risk assessment)

---

[33] Trusted Computing Group Mobile Use Cases available at https://www.trustedcomputinggroup.org/groups/mobile/Final_use_cases_sept_22_2005.pdf

level of protection. Device manufacturers can gain additional guidance on steps necessary to establish and quantify the security of a robust DRM solution, in the framework of their own DRM trust model. Conformance to a standard set of specifications also provides for a degree of assurance to service and content providers that their interests are protected, helping them make a judgment as to whether client devices are robust or not. The user can benefit from DRM implementations that allow valuable content to be distributed to mobile devices with the permission of content providers. In turn, content providers can be assured that their content will be protected on such devices. Mobile users in particular may be more willing to use distribution channels that act with the content provider's permission. Additionally, DRM will encourage and facilitate the safer exchange of user generated content and in the corporate context can work with organisational access control policies to allow flexible access to sensitive company information.

SIMLock / Device Personalisation is the process whereby a mobile device remains locked to a particular network, network subset service provider or corporation, until the device is unlocked in an authorized manner. This allows network providers and device users to be assured that mechanisms to deter device theft are in place, such that stolen devices become less valuable for re-use and resale. Network or service providers need to be assured that if they subsidise the cost of expensive devices, end users cannot move their device to another network until the authorized end of the subscription contract. SIMLock enables a user to obtain a device at a reduced cost. Users can voluntarily lock a device to their own SIM, thus personalizing it and enabling the storage of personally sensitive information (as other users will not be able to use the device). Finally SIMLock can be used as part of a wider strategy against theft by deterring device theft.

Secure Software Download allows the secure download of application software or updates, firmware updates or patches. Such software could be installed into the device's O/S such as DRM agents or browsers, rather than applications requiring a specific execution environment. The application software upgrade or patch is conducted with appropriate security and then operates with the required authorization and privileges after installation. The benefits are the same as for signed software on PCs. The process of signing significantly reduces the chance of 'malware' being contained within the application or update as the originator of the software may be traced and the software is protected from change. This leads to reduced user inconvenience and risk and increased levels of assurance. The device can automatically trust certain software and reduce the number of security related decisions the user must make. Platform integrity can be increased and the risk that the secure download process is tricked or bypassed is dramatically reduced. It also supports secure management of IT within an organisation by enabling a more secure software download.

Secure Channel between Device and UTMS Integrated Circuit Card[34] *(UICC).* In this instance, the UICC (a UMTS equivalent of the SIM card) and security sensitive applications on the device can have a trusted connection. UICC are important because they allow the device to be compatible with legacy services and have useful qualities

[34] UMTS is a collection of technologies for 3rd Generation broadband mobile networks. For more information see the UMTS Forum at http://www.umts-forum.org

regarding physical security and portability for User credentials. A trusted mobile device would allow the trust status of the device to be established when the UICC is inserted and would help to support protection against malicious code appearing on the device. This would allow the user-friendly migration of sensitive information (a signature key, electronic money or electronic tickets) between devices. The UICC can establish whether the new device is trusted enough to store this information and if not retain it for use on the UICC. Additionally, it would be possible to improve the availability of some applications in the case where security applications are split between the UICC and the device (with a common, secure link between the two) because the protected core on the UICC will be easier to evaluate.

3.1.2 Overview of Security Threats and Concerns

There are a number of concerns that have been put forward about Trusted Computing. From a systems perspective many believe that it will reduce the security of systems, not increase it.[35] From a market perspective, there is an argument that it will ensure lock-in and remove choice, while reducing users' privacy. The literature has identified several potential security related issues associated with trusted computing.[36] The first major issue is related to the fact that trusted computing implementation leads primarily to the provision of services by removing the ownership of computer resources from the end-users. This situation requires, therefore, that the end-user is provided with the necessary assurance about the technical capabilities of the service providers in providing security functionalities. Moreover, due to its technology focus, Trusted Computing does not encompass the larger organisational, human and management side of information security. Reliance on Trusted Computing applications and services, therefore, may lead to a false sense of security within an organisation or towards a single instrument. Clearly it will be necessary not only to understand the socio-economic aspects of how DRM implementations of Trusted Computing may alter behaviours and the market, but also effort would need to be directed towards gaining clarity of understanding in the mind of the consumer and end-user about the difference between Trusted Computing and DRM and the advantages and disadvantages of both.

3.2 ARM TrustZone

This case study examines TrustZone, which is a set of hardware/software technologies currently being adopted by chip-designers and handset operators developed by ARM Holdings. As no organisational implementations of concepts of Trusted Computing have been implemented, this case study tries to illustrate the potentialities of the implementation of such a technology from an organisational perspective.

ARM Holdings is one of the world's leading semi-conductor Intellectual Property (IPR) suppliers. Listed in both the London Stock Exchange and NASDAQ in the United States, it has a number of regional subsidiaries in the United States, Korea, Taiwan, France, China

[35] Ross Anderson's Trusted Computing FAQ available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[36] ibid

and Belgium. The ARM business model involves licensing intellectual property rather than the direct manufacture of semi-conductor chips. ARM licenses its IPR to a network of partners which includes most of the world's leading semi-conductor and systems companies, known as ARM Partners. They use ARM's intellectual property, which they have licensed, to create and manufacture micro-processors, peripherals and System-on-Chip (SoC) designs (effectively all the components of a PC on a single miniature microchip). ARM also provides a range of tools, software and system intellectual property to help this process. Specifically, ARM's business model is that it licenses its intellectual property to a direct customer. Following this, ARM then receives a licence fee, possibly in the range of a few million dollars. The customer then designs a chip based on this intellectual property which takes 1 to 3 years to complete. When the chip manufacturer sells its product to its own direct customer (for example, a handset manufacturer) then a royalty is owed to ARM for every product ever sold containing this intellectual property. Royalties are usually 1-2% of the average selling price of the semiconductor or 2.5% of the average selling price of the completed SoC 'wafer'.[37]

ARM designed chips are present in wireless, networking and consumer entertainment solutions, to imaging, automotive security and storage devices. The company segments the market place into Home Solutions, Mobile Solutions, Enterprise Solutions, Embedded Solutions and Emerging Applications.

ARM is split into several divisions and business units, dealing with physical and processor intellectual property, development systems and services. The team that developed TrustZone is part of the software systems group and TrustZone was developed as a result of research investment towards fulfilling this particular need.

3.2.1 Business drivers

ARM's TrustZone hardware technologies were formally launched in 2003 and software technologies in early 2004. Since then they have been taken up in the ARM 1176 chip design and in early 2006 Philips released a statement that they would commence manufacture of a SoC with these extensions in place. [38]

This came about after some initial directed and speculative Research and Development (R & D) regarding security technology within ARM and the growing realisation that the focus on security provided by stand alone encryption mechanisms (most often the cryptography block) was no longer sufficient in a rapidly changing IT environment. This was an inherently disruptive development, as the concept of creating a parallel execution environment to meet security requirements (namely those of process isolationism) was not present in the strict CPU world. To a small degree this concept existed in the server and mainframe environment, but the disruptive aspect was about bringing this concept to embedded computing, which at the time was highly revolutionary. Introducing this concept of a parallel execution environment is closely linked with that of 'virtualisation', a

[37] Information taken from 2004 and 2005 ARM Annual Reports available at the Investor Relations website of ARM Plc, http://ir.arm.com

[38] For more information see TrustZone see http://www.arm.com/products/esd/trustzone_home.html

concept which has more in common with availability concerns and related to having more than one O/S running at the same time doing different tasks.

If the developments of process isolationism are considered on a timeline, then it can be seen that the first instantiation is that there are two separate worlds created (the parallel execution space model) and that the final goal could be multiple virtual worlds. This state is referred to as full virtualisation. However, TrustZone is seen as a pragmatic real world solution towards this possible end goal – it is not full virtualisation. ARM therefore wanted to implement some form of process isolationism for the embedded computing world. The key business requirements were that it had to be 'implementable' with minimal market disruption.

With the change in the focus from the desktop PC to the embedded (particularly mobile) device came the realisation that security needed to be addressed at the system level. This was also driven by a change in the threat, as a consequence of the greater take up of more high performance mobile and non-desktop computing devices. ARM was one of the companies to see that the cryptography centric approach to meeting security requirements for the desktop PC space was simply not sufficient. Therefore, they began work on TrustZone, which, among other more complex things, can be used to implement a TPM.

TrustZone can be summarised as an architectural way to enable one physical implementation of one CPU to 'pretend' to be two CPUs. The decision was first taken to complete some specific hardware extensions, but with this soon came the realisation that this could only solve one part of the problem. It was therefore decided to also work towards the development of software which would reside on the parallel (in actual fact the virtual) CPU to run the security tasks which can be fundamental security services and interfaces to other elements in the trusted chain, such as smart cards, O/S and general applications. This security specific software O/S (more commonly referred to as middleware) is not like a normal O/S. It is neither rich, flexible nor user-friendly like the more familiar O/S such as Windows or GNU/Linux. It simply provides the security functionality required and nothing more. Furthermore, and most importantly given the previously stated necessity for predictability as a key component of any secure system, it is provable (i.e. it is possible to computationally verify or certify its behaviour).[39]

The hardware components of TrustZone relate to the TCG TPM specifications, which focus upon a passive hardware element with has its own set of security concerns when interacting with the O/S software. TrustZone can be thus conceptually thought of as an environment where a virtual TPM can be instantiated in software within a secure execution environment.

Specifically within the embedded environment (particularly with mobile phones), the key business drivers for implementing a method of Trusted Computing into their chip designs are twofold. First, the need to implement some method of reducing costs from stolen devices or lost subsidies (usually achieved via SIMLock) and secondly, because of the increasing value driven by new services and business models deployed over networks to

[39] For a more complex overview see Tiago Alves and Don Feldon, TrustZone Integrated Hardware and Software Solution, White Paper, July 2004 available at http://www.arm.com/pdfs/TZ%20Whitepaper.pdf

deliver higher Average Revenue Per User (ARPU) via mobile content, m-commerce and protection of confidential information. [40]

This move from a closed system where security was predictable to a more open system where the user can download new content or applications, changed the operating parameters of a system and is an important development. The breadth of non-standard solutions (such as putting security on the SIM card, or adding another semi-conductor core) and the lack of provision for security in the embedded industry meant that barriers to entry for a security offering were very high.

With the growth in the corporate use of such devices (for example, Blackberry and Personal Digital Assistants (PDAs) based on operating systems that can easily integrate with the corporate IT environment), there is a new and emergent business driver to provision for the security of the device in a corporate context - for example with network logons and other organisationally sensitive information.

3.2.2 Technical Implementation

TrustZone is implemented within the micro-processor core, enabling the protection of on- and off-chip memory and peripherals (for example software drivers for cameras, connectivity etc) from software attack. As has been said, conceptually it is a second 'virtual' parallel execution space. TrustZone operates by enforcing a level of trust at each stage in the transaction, including system boot. The trusted code handles tasks such as the protected decryption of messages using the recipient's private key and verification of the authenticity of the signature based on the sender's public key.[41]

Data is passed between the TrustZone environment and the rest of the O/S via low-level drivers. As such all data from the secure world remains invisible to any software attacker.

A new secure state is introduced to the ARM architecture for both the user and privileged modes which can determine whether the system is operating in the secure or non-secure world. The Secure Monitor mode controls, via a Secure Message Interrupt (SMI) instruction set, switching between these two worlds. The Secure Monitor thus acts as a kind of gatekeeper and can reliably switch between these two worlds. Once the secure state is initialised the processor gains additional levels of privilege to run code from the secure execution environment.

Key hardware components of any TrustZone SoC are as follows:

- A TrustZone CPU used to run trusted applications isolated from normal applications and to access the memory space reserved for trusted applications
- Secure on chip boot ROM to configure the system
- On-chip non-volatile or one time programmable memory for storing device or master keys

[40] ibid.

[41] For an overview of TrustZone system design see http://www.arm.com/products/esd/trustzone_systemdesign.html

- Secure on chip RAM used to store and run trusted code such as DRM engines payment agents and hold cryptographic keys
- Other resources capable of being configured to allow access by trusted applications only.

Software consists of secure and non-secure elements. These will include the normal O/S (such as Symbian or Microsoft Windows Mobile Edition) and applications, and protected software components.

TrustZone optimised secure software components include the monitor software, managing the changing between the Secure and Non-Secure worlds, the Secure Kernel, Secure Drivers, Boot Loader and other basic secure software services that might be provided by ARM as part of the software solution. These elements are an evolution of the Security Module developed by Trusted Logic, a French company. The Secure Module operates as the secure kernel at the heart of the TrustZone secure execution environment.

The software may have exclusive access to dedicated protected memory, dedicated persistent storage, the Subscriber Identification Module (SIM) card and crypto-accelerators. It provides for integrity checking (for example to address previously stated IMEI & SIMLock requirements) access control, secure storage and cryptography. Future upgrades may include frameworks for DRM digital signatures and e-banking.

The benefits of the TrustZone solution are fourfold. *First*, it provides a safe environment for secure data on the chip, thus enabling a complete approach to security. *Second*, performance considerations, which were previously an issue with more complex secure execution techniques are expected to be no longer pertinent as TrustZone has mechanisms embedded in the heart of the CPU in place to more efficiently access and manage system resources when compared with custom hardware normally built outside the CPU boundaries. *Third*, the combination of hardware and software elements to TrustZone means that upgrades and customisation of the software is possible, after the SoC architecture has been finalised by the semi-conductor manufacturer. This is an extremely important aspect and is one of the key 'disruptive' qualities of TrustZone. That is to say that with TCG type specifications, the hardware element that provided for process isolation could not be altered once it had been finalised. With TrustZone, however, it is possible for the secure execution environment to be upgraded or extended (preferably by ARM licensed software, but this is not necessarily the case). *Finally*, as embedded devices are designed according to the SoC paradigm (i.e. where sound drivers, video codecs, and drivers and interfaces with peripherals such as cameras is all part of one physical piece of hardware) any security system is very likely to need to address each and all of these devices in a secure manner. TrustZone facilitates this through mechanisms such as integrity checks, dynamic sharing of peripherals between the secure and non-secure worlds, etc.

TrustZone can also be leveraged to implement software instantiations of TPMs according to the standard of the TCG. It is also viable to certify devices according to the Common Criteria level of security certification.

TrustZone is intended to be a 'foundation for other complementary security solutions' such as DRM modules, e-Wallet applications and protected O/S features.

To enable security within the device O/S, it provides integrity checking against possible attacks in three ways: verification that the O/S is unaltered before boot-up; verification of the integrity of critical paths, and the safe execution of an approved restricted set of functionality within the TrustZone.

The specific security features provided are:

- Platform identification and authentication
- Identity
- Key and certificate storage
- Low level cryptography
- I/O access control
- Safe data storage
- Smart card access
- Code & integrity checking

APIs (Application Programming Interfaces) provided with TrustZone include:

- TrustZone Software API – a simple message-passing interface to allow datastreams to pass between the two worlds
- TrustZone Native Services API – an API designed to allow access to commonly available security functionality residing behind the TrustZone security barrier. This API can be expanded with proprietary extensions.
- The TrustZone Software HAL (Hardware Abstraction Layer) API

Both the latter two allow developers access to the internal workings of the TrustZone Software.

Possible uses of the secure execution environment include the processing of secure data such as cryptographic keys, where any non-secure exposure would risk the key capture by a software attack or a logic analyser[42]; verification of the integrity (and blocking if necessary) of audio output from a DRM codec (to ensure that the output has not been tampered with) and execution of protected transactions such as OTA (Over The Air) upgrades.

3.2.3 Security challenges

The security issues which TrustZone addresses are as follows:

- Viruses propagating via the users' contact list;
- Vulnerability of end users private data (e.g. compromise of crypto keys or personally sensitive information);

[42] Given that in the embedded space around 1 in 12 devices have the same cryptographic key, this would result in a highly unacceptable level of risk for handset manufacturers and mobile network operators

- Compromise of the confidentiality of email messages and remote access to corporate networks
- Device integrity and proper operation compromised through software exploits performed with or without the physical control of the device.

Additionally, a TrustZone enabled device can support the protection of digital content owned by a content provider and ensure that this is not misused in any way. At a more general level a TrustZone enabled device or TPM meets the more exacting requirements for security in the pervasive wireless IT world where the concepts of use, ownership and management of a computing device are becoming extremely blurred.

Finally, at a physical level, TrustZone or a TPM enabled device can help in reducing the amount of fraud committed by criminals breaching and affecting the integrity of the IMEI and SIMLock[43] code as a way to illegally export mobile phones, thought to be a key motivating factor in street crime.[44]

ARM states that unless specific manufacturing steps are taken to guard against physical attack, no secure system can be guaranteed to be unbreakable against very sophisticated and sustained attacks. The goal of the deployment of this functionality is to raise security to the right level to meet the likely threat whilst remembering economic and practical imperatives. It is no use undertaking to develop an extremely sophisticated and highly secure system if the device has limited functionality for m-commerce or downloadable content, for example. As ever with security, deployment is a matter of risk assessment and careful weighing up of the estimated cost of protecting an asset versus the probable economic value of the consequences.

Security challenges to the deployment of TrustZone are complex and connected to the value chain and the way in which ARM's business model works.

One of the main series of challenges comes from poorly implemented instantiations (i.e. production examples) of chips designed with the TrustZone capability. If a customer uses a TrustZone chip design and subsequently, in their own manufacture, either fails to implement the security functionality, or improperly implements it, then the devices which will then be marketed as TrustZone capable, will not in fact have the required functionality and will therefore be less secure. A rare but not unheard of example is where memory in a device is taken to be secure and confidential information or keys are placed into this memory, but in fact the sensitive data has not been tagged appropriately thus rendering it useless from a security perspective.

Another key concern is the length and complexity of the value chain and the number of different partners in the ARM 'eco-system'. As there are overall many more semi-conductor and device manufacturers than in the desktop PC world alone, ARM's designs

---

[43] SIMLock is a technique whereby the phone is locked to that of a particular Mobile Network Operator (MNO)

[44] Stealing a phone and reprogramming it with a new IMEI number is illegal in the United Kingdom under the Mobile Phones Reprogramming Act 2002. Additionally, national databases can track IMEI numbers, but there is no global register of IMEI numbers so phones can be reprogrammed abroad with impunity

and its intellectual property are spread across many companies. An accepted possibility is that someone in a position of knowledge about the inner workings of a TrustZone SoC may try to undermine the integrity of the device at the time of design or production, thus rendering it less secure. If this were a mobile phone for example, then it might be a significant concern as the number of mobile phones manufactured (when compared to PCs) is extremely high.

To address this ARM has a number of approaches. Its standard licence agreements allow ARM to see how many copies of chips based on its intellectual property have been made. Additionally the Foundry program provides for even more assurance. With this program, a physical model of the chip is built and sold and the manufacturer then builds the SoC around this model and sends it off to a Foundry, which adds in ARM's intellectual property. ARM obtains statistics from the Foundries indicating how many SoCs using ARM intellectual property have been built.

This is also the case for key management in the embedded and mobile world, where around 1 in 12 cryptographic keys are identical. If even one key is broken, then this would render many devices vulnerable. In an ideal world every device would have at least three keys that change every year, so if one gets compromised it is possible to revoke it and switch to the next. However, this presents extremely complicated management challenges. Aside from the increasing quantities of device of each generation having three keys, which have to be changed every year there is also a series of management questions if the customer decides to change networks, namely: how does the key transfer take effect between the network operators? There are also questions over the security of the key database and the associated infrastructure required to adequately protect it as an asset. Key Management Infrastructure is thus a very difficult task.

These challenges, coupled with the easy availability of the required tools to debug and analyse ARM SoC designs at a low level (as part of the overall support and engineering package for customers), present some unique challenges for ARM as an implementer of the Trusted Computing concept. This has been recognised and although the release and sharing of debugging tools is widespread, TrustZone technology permits full system debugging in development but then allows this to be disabled once the device is shipped. Although there is still the possibility that this may be misused at the point of manufacture, risks arising from the misuse of debugging tools are further reduced by selling versions of the debugging tools in the language of the country where manufacture needs to take place.[45]

From the user perspective, there is a challenge in that the end user may decide to act more recklessly if he knows that he has a device with the TrustZone capability. However, an analogy can be drawn here with the use of seatbelts in cars. It is still impossible to tell whether the mandated use of seatbelts has led to an increase in reckless behaviour on the part of drivers. The same can be said for the user community for embedded and mobile devices. The user depends upon the manufacturers' implementation of TrustZone and whether this was successful. If a poor implementation was undertaken, then the user's sense of trust and subsequent reckless behaviour will expose him to a greater degree of risk.

[45] Hacking of the debugging tools is reportedly one of the more popular types of threat

3.2.4 Conclusions

Trusted Computing is still in its early stages of implementation. Despite controversy surrounding the potential functionalities of Trusted Computing, the capabilities are only now beginning to be designed into hardware and software. At an organisational level, Trusted Computing solutions have not yet been deployed to any extent (for example, in enterprise rights management or organisational system security). The growth in the number of devices such as PDAs and mobile phones with valuable content (not to mention personally and perhaps organisationally sensitive data) will mean that Trusted Computing will find more uses.

One of the main conclusions identified in this case study is the importance of virtualisation and separation as a key factor in the development of the concept of Trusted Computing. Virtualisation allows system designers to more appropriately secure parts of any computing system as it enables process isolation and thus means that any system or CPU activity can be authorised, monitored and verified. At present, with virtualisation as the main driving force, Trusted Computing activities are developing along two separate schisms; the drive to develop specifications to allow full virtualisation (i.e. the creation of *n* number of separate execution spaces) and a less ambitious activity (such as propounded by ARM and TrustZone) backing two virtual execution spaces. In this context, the drive to mass virtualisation could be considered the more sustaining innovation as it represents the natural extension of vendors trying to meet the needs of their most profitable customers.

The deployment of Trusted Computing also illustrates how the vendor understanding of where threats originate has changed significantly. Activities of the end-user are now regarded as being the main source of risk - for example reconfiguration (intentionally or unintentionally) of the device or the downloading of unauthorised content (which compromises the legitimate business models of content suppliers). DRM and the freezing of system configurations within the secure execution space have thus been developed as ways to mitigate these risks.

At a more systemic level, it is important to realise that any Trusted Computing platform can only be secure if it is properly designed according to architecture that companies like ARM set out. If the implementation of such technology is flawed or deliberately undermined (e.g. via compromise of the value chain) then any Trusted Computing capable device is not going to perform as expected and thus presents a lower degree of security. This raises important questions about outsourcing and security and managing long and complex value chains.

3.2.5 Review of the case study conclusions during the Final Workshop

Regarding the challenges identified with Trusted Computing, participants at the Final Workshop noted one of the key challenges revolved around the concept of liability and who now held responsibility for security. In the business model in evidence in the case study, those organisations developing equipment using TrustZone could (either maliciously or intentionally) leave flaws in their products which would then leave end-users vulnerable. In this case, the question of who owed liability to who was considered to be complex. Additionally, if liability was part of the contractual agreement between a company like ARM and its equipment partners, then the need for the end user to owe a

liability (by not downloading content which infringes any DRM, for example) to this business model becomes questionable.

Participants also considered the question of cryptographic key management as it related to Trusted Computing. Whilst key management is a complex and difficult task, it is not insurmountable. What is a highly complex task is generating trust in keys which have been generated on a Trusted Computing enabled device, where it is difficult to identify where, how and who generated the keys. To help build trust, it would be necessary to better elaborate the background to the generation of these keys.

Participants voiced the view that the ability of law enforcement to access data protected by Trusted Computing technology would not be made significantly harder with the advent of this technology. However, the question remains at a more general level, whether law enforcement (and indeed governments) can keep up with all the new technological advances in this field. Although many research institutes have good links to government, the applied commercial use of technology for security is evolving so fast that it is important to consider whether the law enforcement community's awareness of developments is adequate.

CHAPTER 4 Wireless Microwave Access (WiMAX)

4.1 Wireless Microwave Access (WiMAX): General Issues

WiMAX (Wireless Microwave Access) is not a single technology but rather a standard for equipment operating according to variants of the IEEE 802.16 standard. 802.16 and its variants are a specification for high speed, broadband wireless access at greater distances than 802.11 WiFi. WiMAX fits into the network access between LANs and Metropolitan Area Network (MAN) offerings.[46]

This standard was developed by the IEEE in December 2001 by Task Group No 1 and has been evolving since. In 2003 the IEEE approved 802.16a which was an amendment to the more general 802.16 standard. This specifies an air interface standard for broadband wireless access systems using point to multipoint infrastructure designs and operating at radio frequencies between 10 and 66Ghz. Average bandwidths were targeted at 70 Mbp/s with peak rates possible of up to 268Mbp/s. By way of comparison, most office Local Area Networks operate at speeds of up to 100Mbp/s and most consumer ADSL solutions will operate (download only) at up to 8Mbp/s, even if ADSL2 and VDSL are a lot faster.

At the time the original 802.16 standard applied only to line of sight deployments in the licensed spectrum, did not offer conformance guidelines and ignored the development of the European HiperMAN standard. This was addressed with the 802.16a amendment, which introduced a number of changes, most notably in the provision of lower wavelengths in the unlicensed spectrum band, allowed varying channel capacities to address different quantities of spectrum that carriers own in different markets and enhancements to the Media Access Control (MAC) layer.[47] This provides for enhancements between the subscriber terminal and the base station, meaning that user access to the network is intelligently scheduled, resulting in better latency and improving

[46] The difference between Local and Metropolitan is usually defined by distance, but there are technological differences. A Local Area Network usually covers distances of up to 100 metres and access methods can be via wired (Ethernet) or wireless (WiFi) means of up to 100Mbp/s although with the advent of 10Gb this can theoretically be exceeded. Metropolitan Area Networking, by comparison, covers distances of up to 10km and access methods are usually fibre or dedicated leased lines able to transmit up to 100Gbp/s.

[47] MAC addressing provides the connection between the hardware (such as a WiFi PCMCIA card) and the access interface (such as a WiFi network).

the capability to support Quality of Service (QoS) features such as the delivery of voice and video, retransmission and per connection QoS.

These standards developments have now been collectively titled 802.16-2004 (fixed). The 802.16e mobile standard has yet to be finalised.

Many regard WiMAX as the natural evolution of the increasingly popular WiFi or 802.11 standard (in all its forms such as b and the faster g standard). Evangelists of WiMAX, such as members of the WiMAX Forum, consider that this has the potential to go much further.

The WiMAX Forum was based on the model of the WiFi Forum, an industry level group intended to aggressively promote the evolution of the loose technical standard laid down by the IEEE. It is hoped that WiMAX will learn from the mistakes of WiFi, by being grounded in well defined standards and industry interoperability right from the start. One of the main lessons to be learnt is that, with the WiFi Alliance, equipment was marketed before the standard became available.

The WiMAX Forum consists of around 100 companies from a variety of different vendor areas, including infrastructure providers, semi-conductor manufacturers, software companies and vendors of network equipment and access products as well as telecommunication carriers. The WIMAX Forum hopes to eventually become a marketing collective, promoting WiMAX Forum certified products first to operators and then to end users. The WiMAX Forum is keen to get involvement from carriers. This is even more important than with WiFi because WiMAX's early success will depend upon the ease with which it can be deployed in carrier transport networks. WiMAX is seen as attractive for carriers to help them to backhaul the increasingly large volumes of traffic being generated by WiFi networks.

In 2005 a number of 'plugfests' were held, organised by the WiMAX Forum and conducted by independent labs, in an attempt to demonstrate interoperability between different vendor equipment prior to WiMAX certification. At each 'plugfest', five or six vendor products which are up for certification are interfaced in live demonstrations. Following this, process vendor certifications are released.

Certification testing began fully in July 2005 and by early 2006 there were a number of WiMAX certified equipment on the market.[48] Manufacturers such as Alvarion, Airspan, Redline, Towerstream and Radioland are selling pre-WiMAX or WiMAX ready equipment based on the 802.16-2004 standard. This equipment could be brought into compliance by a hardware or software upgrade. Some equipment manufacturers have formed their own groups to undertake initial interoperability testing to iron out problems prior to official WiMAX Forum testing.

It is likely that WiMAX equipment will arrive in stages and the first for fixed wireless systems using the current 802.16-2004 standard. This will be in offerings of a combination of tower equipment for operators and outdoor residential equipment to be mounted on the side of a house or apartment. In the second stage equipment will move indoors but remain

[48] E.g. Airspace EasyST CPE available at:
http://www.airspan.com/products_group.aspx?ProductGroupID=1&ProductID=6

fixed in one location. Mobility is likely to arrive in the third stage of rollout. Using the 802.16e standard, WiMAX enabled devices will encompass laptops, smart phones, PDAs car navigation systems and other non-traditional devices.

4.1.1 Why is WiMAX disruptive?

WIMAX can produce a set of disruptive effects since it may undermine some of the business and operational structure of the main players in the ICT market:

- Mobile network operators – WiMAX (in particular the 802.16e mobile standard) may enable new and innovative sorts of mobile telephony when coupled with VoIP, that would seriously undermine the business model of mobile network operators
- Traditional PSTN network operators – when coupled with VoIP over a wireless connection, customers have the opportunity to significantly extend their level of choice regarding provision of a telecommunications service.
- Telecommunications companies operating in the deregulated provision of xDSL products to the 'last mile' of customer premises.

Some analysts believe that the WiMAX market will be worth anywhere between $2bn to $5bn by 2009. Initial take up is likely to be amongst wireless ISPs.[49] In its WiMAX FAQ, Fujitsu USA notes that due to the nascent stage of the WiMAX market, it is difficult to identify the likely size, other than to say it would be significant, judging by the fervour and excitement seen from operators, system makers and other vendors. Any market would involve base stations and subscriber station. Many unknowns make it difficult to predict the market size. These include end-user adoption rate, collaboration between operators and service providers and equipment builders, available spectrum and licensing policies and other governmental broadband wireless access policies in each country. Mobile WiMAX will have an important role to play in the growth of this market and Fujitsu expects that this will be greater than the fixed WiMAX market. The mobile WiMAX equipment will include various mobile devices e.g. cellular handsets, notebooks and other multimedia devices.

One possible scenario for the future is that there is a pool of WiMAX connectivity in several different locations that will allow certain types of connectivity. The current emerging market is for indoor modems at the residential level that can be plug and play. The next natural step is for provision of WiMAX to laptops. At present it is possible to supply a WiMAX network to a set of WiFi access points that would then enable a laptop with a WiFi card to connect to a WiMAX network. Eventually it is the intention that the WiFi element would be removed and it would be possible to switch to pure WiMAX connectivity, via a USB device or card, direct to a base station.

The potential disruptive implication of WIMAX depends on whether it is fixed or nomadic. With fixed WiMAX, when a laptop connects to a base station in a café or street or shop, there is still a static connection between the device and the base station (much as

[49] Telephony's Complete Guide to WiMAX 2004 available at http://www.wimaxforum.org/news/press_releases/Telephony_WiMAX.pdf

there is with a WiFi 'hotspot' now). However, with a nomadic WiMAX infrastructure, it is possible to carry a single connection as the transceiver in the device moves from base station to base station (in much the same way as a cell phone does currently) where each cell hands over to the next as the transceiver moves. Mobile WiMAX infrastructure and capabilities are expected to appear around 2007–08 and for the devices to have this capability embedded a year later. In the short term, the main implementations will be for fixed nomadic (i.e. devices which can move around a fixed base station) WiMAX.

4.1.2 Overview of Security Threats and Concerns

The consumer risk aspects for WiMAX are similar to that of existing xDSL – open relays on customer equipment resulting in Distributed DoS. The wireless aspects are not to be discounted, but they are severely reduced by two main factors:

- The Customer Premises Equipment (CPE) and the 'base station mutually authenticate themselves to each other using cryptographic techniques'
- There is no 'ad-hoc' mode with WiMAX, thus reducing the risk from unauthorised access (e.g. via war dialling as there is with WiFi networks)

The OECD in its report on the 'Implications of WiMAX for Competition and Regulation', published in 2005 reported several issues for security and privacy.[50] This report said that the security risks facing potential WiMAX users should be comparable to users on other wireless networks. User sensitive data will require multiple layers of security and encryption to keep data private and the discovery of a flaw in the implementation of WiFi's Wired Equivalent Privacy (WEP) 128 bit encryption (which can now be broken in roughly three minutes using new techniques) has meant that WiMAX security has come under scrutiny.[51]

WiMAX cryptography currently uses the popular Data Encryption Standard (DES) or Triple DES (3DES) but it is expected that a stronger form of encryption called Advanced Encryption Standard (AES) will be used by the time of full commercialisation of the products.[52]

The OECD concluded that the reach of the signal was another important area where more security risks may be posed. By comparison to the short range of WiFi, where eavesdroppers had to be within several meters of the structure (whether that be CPE or transmitters) eavesdroppers do not need to be anywhere near as close when trying to listen in on traffic passing over a WiMAX network. Due to the outdoor nature and long range transmission of WiMAX signals, the expected security risks are likely to be much larger and new methods to mitigate them (such as special wall coverings for WiFi networks) will need to be developed.

---

[50] OECD: The Implications of WiMAX for Competition and Regulation; Paris; 2006

[51] Humphrey Cheung, The Feds can own your WLAN Too; Tom's Networking 31 March 2005 available at http://www.tomsnetworking.com/Sections-article111.php.

[52] Tim Hills, WiMAX Guide Unstrung 1st May 2005 available at http://www.unstrung.com/document.asp?doc_id=65348&print=true.

The report also concluded that oversight from government agencies to better ensure privacy would be required. The popularity of remote monitoring solutions enabled by WiFi may well be replicated with WiMAX and the increased transmission distances could mean that this sort of solution is possible over much greater distances, perhaps city wide. The reception of a constant video stream over QoS enabled WiMAX networks, provided as part of a monitoring service for a corporate customer, for example, would undoubtedly raise privacy issues that would need to be addressed. Such technology might also be put to good use, for example in the provision of a road monitoring system that helps to route traffic around a citywide road network.

Another security concern raised is in the area of law enforcement, specifically in the protection of the capability to collect data in the legitimate investigation of criminal activity. The increasing use of end to end encryption (such as provided by VoIP standards) and the increasing strength of encryption solutions in WiMAX networks (coupled with the IPSec possibilities allowed by IPv6) may result in it being much more difficult to recover traffic or content data. The complexity of such issues is compounded by the international nature of trans-border data flows and the need to be cognisant of international laws, which may be significantly at variance.[53]

Finally, there are certain health and safety concerns about the deployment of WiMAX. These relate specifically to emitted radiation and the application of WiMAX in safety critical scenarios. Mobile WiMAX base stations would require the deployment of antennae with similar power requirements to mobile phone masts, which have been the subject of some recent controversy for their electro-magnetic impact upon biological systems in close proximity to such masts. Such concerns would be important to people physically located close to transmitter equipment.

4.2 WiMAX Trial from PIPEX & AIRSPAN

This case study examines a trial WIMAX implementation in the Stratford upon Avon area in the United Kingdom. This implementation involved over 30 individual users for a six-month period. Different from other pre-WIMAX trials, this one involves the use of WIMAX certified tools.[54] PIPEX is a UK provider of integrated telecommunications and Internet services. Its customers include small home/offices and publicly quoted companies. It provides a comprehensive range of consumer, business and corporate voice, broadband, security, domain name registration and shared and dedicated hosting solutions. Pipex owns one of the UK's most extensive communications networks, including more than 100 Points of Presence (PoPs) across the United Kingdom and 20 point to multi-point radio PoPs offering wireless DSL. Pipex runs five data-centres that have 'round the clock monitoring' to ensure maximum availability and uptime. In order to exploit the potential offered by WIMAX, PIPEX has recently created a subsidiary called PIPEX Wireless with

[53] For an overview in the European domain please see http://www.csirt-handbook.org.uk

[54] This case study is based on telephone interviews conducted with representatives from PIPEX and the UK arm of Airpsan Networks and a review of associated documentary material. For a full list of interviewees see Appendix A: List of Interviewees

the financial support of Intel Capital. Following a series of trials, one of which is described in this report, Pipex Wireless anticipates a roll-out of its network to begin in London and Manchester in 2007 and target the top eight UK population centres by 2008. [55]

Airspan Networks provides fixed and wireless voice and data systems and solutions, including VoIP in licensed and unlicensed frequency bands between 700Mhz and 6Ghz. It has a product roadmap that includes products compliant with the new WiMAX 802.16-2004 standard. This was launched in 2005 with sales immediately. During 2005, moreover, Airspan has established Original Equipment Manufacturer (OEM) agreements with Nortel, Ericsson and Marconi. The company's products have been deployed with more than 350 operators in more than 100 countries, and Airspan places a great deal of focus on its products providing 'excellent area coverage, high security and resistance to fading'. Additionally, Airspan offers radio planning, network installation, integration, training and support services. It is based in Boca Raton, Florida in the United States and has its main operations centre in Uxbridge in the UK.[56] Airspan has been one of the founders of the WiMAX Forum.

4.2.1 Business Drivers

The driver pushing PIPEX and AIRSPAN to undertake this case study is to understand what kind of businesses WiMAX networks might be able to support, in particular for individual consumers. Moreover, the two companies wanted to verify that the equipment functions as intended. In detail, Airpsan wanted to see what sort of equipment worked best with the connectivity provided by PIPEX's network and from the perspective of PIPEX, to see which services (for example, voice calling over IP, gaming, email, web-browsing and file transfer and downloading) worked best with the technology. Additionally, the trial was used to gauge consumer reaction to the technology and its 'self-install' deployment, where customers would be expected to set up the equipment themselves and additionally chose to route voice calls over the infrastructure.

4.2.2 Technical implementation

The case study used AS.MAX and Airspan's EasyST Customer Premises Equipment (CPE), in conjunction with Pipex's home and business broadband services. EasyST are designed to work with any WiMAX Forum certified base station product from Airspan's AS.MAX family. The pilot was able to proceed due to the acquisition of a national 3.6-4.2GHz spectrum licence by Pipex.

Its objectives were the following:

1. *Technical*: Speed, transparency, etc, and issue of installation methods, including radio performance measurements designed to assess the long term stability and availability of WiMAX. Additionally, there is interest on how the CPE is installed by the user himself
2. *User experience*: to observe how the service operates over a number of months and what the user experience is.

[55] Information taken from PIPEX 2005 Annual Report and company news available at http://www.pipex.com

[56] For more information see Airspan corporate website at: http://www.airspan.com

It is thought future trial phases will include assessments of the performance of other WiMAX CPE types including laptop cards and handheld devices for both fixed and nomadic applications.

At the end of November 2005 the trial network achieved stable service delivery and drive tests using Airspan's CPE, which was successful in providing non-line of sight connectivity in excess of 1km from the base station. Software and capacity upgrades continue to be added to the trial installation to increase its range and throughput capacity for the remainder of the trial period. Speeds of up to 8Mbps were possible in March 2006, which increased the delivery of innovative and competitive broadband services (such as consumer VoIP). Additionally at the end of November 2005, Airspan officially announced the release of their AS.MAX fully nomadic WiMAX product range, compatible with the 802.16-2004 WIMAX standard and designed for indoor self install CPE. The main applications are web-surfing and browsing, VoIP and gaming.

At present, the trial has a single base station which is a sector base station covering multiple sectors (not omni-directional), multi-directional coverage (i.e. towards several sectors, not 360 degrees). It provides outdoor coverage which, specifically because of the geography, can be anything up to 10 km, and indoor coverage is 2-3 km depending on where the transceiver is located. The trial has provision for a base station that would be a symmetric point-to-point device capable of providing service to 20-30 users. This would be broadly similar to a 2Mb/ssec DSL connection.

A combination of outdoor and indoor CPE has been used within the trial. The outdoor CPE is a box on the side of the house, rather like a satellite dish, but much smaller. For the indoor CPE, Airspan's EasyST is used. This requires no special software and uses an Ethernet connection on the PC.

EasyST is intended to be self-installed by the end user indoors. It uses a sophisticated interface to indicate to the user when an optimal position has been reached. This is designed to help improve service speed and reduce network load caused by non-efficient installation. It is intended that three different deployment models can be used. First, an integral antenna can be used. Second an optional WiFi expansion can be used which means that the EasyST must be located by the window and finally a stick on-the-window external antenna can be used. The user is informed about the optimum place for the location via a visual indication system on the user interface. The EasyST has the form factor of two CD 'jewel' size cases. Its software supports Airspan's 'Autoconnect' feature, which automatically selects the Best Serving Base Station based on Transmission and Reception signal levels. Finally an 'Auto-config' mode is present which includes automatic download of service configurations over the air following successful registration of the CPE on the network. This can be used independently or in conjunction with an integrated SIM reader.

The software can be upgraded to take into account later system releases and ensures that the hardware is future proofed, as WiMAX networks are expanded and enhanced over the next 2-5 years. This means that investment by network operators and end users is protected as WiMAX rollout continues to evolve. Additionally, a built in web-server allows remote management of the device by technicians and advanced configuration by the end user.

4.2.3 Security challenges

Prior to the trial, no formal risk assessment by the two companies was carried out. This was mainly a business decision as the pilot was an early trial stage and it was not considered appropriate to undertake a formal risk assessment.

In the main, the user trial has indicated that significant security considerations are around confidentiality of communications. Users are of the impression that WiMAX is similar to WiFi, given a number of scare stories about the security provisions concerning WiFi networks.[57] However, the security aspects of WiMAX are markedly different from those of WiFi. Devices cannot communicate with each other directly over WiMAX – the CPE only communicates with the base station. Due to the establishment of an encrypted Virtual Local Area Network (VLAN) between the CPE and the base station, it is impossible for the connection to be eavesdropped or hijacked in a similar way that War Driving allows 802.11b or 802.11g networks to be compromised. There is no ad-hoc mode in WiMAX and the security is as robust as with a commercial mobile network like 3G or GSM.

Before a device can communicate with the base station it has to authenticate. A special certificate inside the CPE is used by the base station to authenticate that it the appropriate CPE. This authentication takes place via Public Key Infrastructure (PKI). Once the device is authenticated, all the user data is then encrypted, using the DES or AES encryption key.

The security risks facing WiMAX users are similar to those on other wireless data networks. In particular, there are concerns about confidentiality and surveillance of the signal that can be intercepted from a distance. Moreover, there are concerns about the preservation of the integrity of WiMAX signals, as this can hamper the functionalities of a wireless application and service. Another expected safety and security concern involves the availability of transmission due to lack of WIMAX signals.

Mutual authentication also exists which means that the CPE can also authenticate the base station, because the base station could be spoofed as well. All user traffic is matched into a VLAN, before being sent over the radio interface. VLAN traffic is then terminated into a user service flow and, then, into the core (PIPEX) network. Therefore, there should not be the possibility for users to see each other's data. Each of these services flows is guaranteed using QoS. This guarantees priority for VoIP rather than best effort Internet based routing.

From a security perspective, the main points for the users are that:

1. The devices communicate only to the base station
2. The data are encrypted
3. There is no possibility of the devices talking to one another: no eavesdropping can take place

Other considerations refer to availability and the user experience. This is mainly concerned with the correct placement of the CPE, and following instructions for placement to

[57] Matt Hines Worried About WiFi Security? News.com January 19th 2005 available at http://news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html

optimise performance. Exploration of availability issues arising from a radio interface installed by a non-technical person was a key conclusion from the trial.

At a higher level, PIPEX and AIRSPAN believe that they have learnt the lessons of 3G and WiFi, with the latter being hit by negative security considerations. The trial is indicating and proving that WiMAX will be the most robust security system ever created for a consumer radio interface. Mutual authentication based on a certification chain going all the way up to a root authority and robust DHCP mechanisms are the key security functionalities and illustrate how robust the system is. This is backed up by co-ordination via the base station, further reducing risk. WiMAX is IP focused and can be used as a bearer for core Internet protocols, in backbone networks. In this way, it reinforces the concept of end-to-end security, one of the key tenents of the design of the Internet.

4.2.4 Conclusions

WiMAX, as has been shown, is still in early stages of development. Although a version of the standard has been around for nearly two years, deployments of properly certified WiMAX equipment have only really begun in pilot form at the beginning of 2006. With the release of the version of the newer mobile standard, WiMAX deployment may increase considerably in the next one to two years.

This case study has illustrated several important issues regarding how WiMAX technology is perceived by the end-user. These centre on availability and reliability concerns such as placement of the end user transceiver equipment and appropriate geographical layout of the network infrastructure. Selling 'good' security as being an important feature of WiMAX compatible technology, and significantly more sophisticated than the security specifications of WiFi (802.11) networks, is also an important lesson of this case study. The end-to-end security over a wireless access interface that WiMAX delivers is a key part of the evolving nature of the Internet (particularly in conjunction with IPv6), and may contribute to its increased reliability. Finally the standards based nature of WiMAX means that interoperability is a big concern. This has a particular relevance for security as if technology from different vendors must work together, it must not compromise previously designed security measures.

It is only at the start of 2006, some 2 years after the finalisation of the newer version of the WiMAX standard, that any officially certified WiMAX equipment (as compared to widely marketed 'pre-WiMAX' technology, for example) has been deployed in a pilot. This illustrates the role that the WiMAX Forum, as the official 'guardian' of the standard is taking in making sure the certification is approached in a sensible fashion.

The WiMAX Forum is trying not to repeat the mistakes of the WiFi Alliance, which some say was an indirect contributor to the poor security features deployed in the technology. In a standards-driven innovation such as this, the role of specification bodies in including security measures in the specifications should not be underestimated.

Organisations seeking to deploy WiMAX should pay attention to the development of the different standards and particularly the security measures being built in. Additionally, user education plays a big part, particularly in the way in which they must be taught about concerns over availability with the installation of CPE.

For their part, public administrations must encourage the continued development of security as an integral part of the evolving standards and make efforts to promote the responsible use and take up of the security features of WiMAX where appropriate in any deployment. As WiMAX development is industry led, governments across the EU must be careful not to interfere too heavily in these developments, rather remaining at a distance to support the continuation of vigorous and dynamic and deployments and its ongoing evolution. In the rush to market that widespread WiMAX roll out will prompt (a consequence of the 'triple-play' binding of voice, broadband and video services that many companies see on offer), security may get sidelined as an unnecessary activity. While there is not much direct activity that governments can undertake to prevent this occurring, consultation with industry players through multi-stakeholder dialogue may reduce these risks.

4.2.5 Review of the case study conclusions during the Final Workshop

The WiMAX case study highlighted challenges from the user's perspective. As the majority of WiMAX (indeed any home networking equipment) was intended for home installation, the challenges included the ability of providers to provide a certain level of service for the user, as well as more traditional user issues such as education about the security of home networks and where to site equipment to obtain the best signal (an availability issue).

Comments were voiced that the provider establishing guarantees of availability was an important step in meeting the challenges associated with this problem – they would certainly encourage take up and stimulate demand.

The workshop also agreed with a view regarding the importance of perception of end users, specifically that due to adverse publicity with WiFi networks (and regardless of the technology used) users now assumed by default that any wireless network was insecure. Clearly addressing this is not just a matter of a well thought out and reasoned user awareness campaign, but also the need to educate users appropriately about the level of threat and risks to the particular application of technologies.

CHAPTER 5 Radio Frequency Identification (RFID)

5.1 Radio Frequency Identification (RFID): General Issues

Radio Frequency Identification (RFID) is not a new technology, but is one that has potentially disruptive properties if implemented in a certain manner. Early incarnations of RFIDs were the 1 bit Electronic Article Surveillance that have been in use for 40 years. These simply indicate to a reader whether a transponder is or is not in range. There is a clear evolutionary path visible from the early days of Optical Character Recognition (OCR) to bar codes and, now, RFID technology.

RFID technology is under continuous development due to increasing miniaturisation and ongoing technological developments. Currently there is a significant gap between the reality of RFID use in the public and private sector, and the perceptions of RFID use to track and trace people and reduce personal liberties.

RFID has two main classes of application.

1) Monitoring of goods (leading to supply chain benefits)

2) Monitoring of people (leading to new markets, products and channels)

All RFID systems consist of a transponder, a reader, a database and a software program for processing the data collected. RFID systems can be closed or open. A closed system is one that is defined for a strongly delimited environment. Closed RFID systems do not need to be compliant with other data formats or frequency allocation schemes. Open systems, by contrast, have interfaces to other systems outside their own area of definition and may be functionally or organisationally external. The greater number of partners increases the complexity in any RFID system and means that interoperability becomes a highly important factor.[58]

RFID transponders are made up of silicon memory chips and copper or aluminium antenna, and are often sealed in paper or foil covers. Passive transponders have no processing capability and no internal power source. By using innate properties of electro-magnetic fields, the chips are turned on when a electro-magnetic reader is present, allowing them to simply transmit a serial number. Passive RFID chips usually only work within

[58] C Floerkemeier, M Lampe. RFID middleware design – addressing both application needs and RFID constraints (Cremers, A.B. et al) Informatik 2005 Informatik Live Bonn (2005) pp 277-281

around a range of 5 metres, and are extremely reliable (more so than active transponders) with a near unlimited lifetime.

However, the real interest is in active transponders. These can transmit signals of their own accord as they have their own power supply and have more powerful processing and memory storage facilities and can act like small microcomputers. Generally, they can transmit data up to a maximum distance of 30 metres.

The transponder can emit a 96 digit serial number with the first digit of the series classifying the type of transponder and the rest referring to information about the product or good that the chip is attached to. The ID number can be linked to a database via a suitable middleware platform such as SAP.

5.1.1 Why is RFID disruptive?

RFID is clearly a disruptive technology from the perspective of business use. RFID has the potential, if deployed appropriately, to revolutionise the way that businesses monitor and manage their supply chains. This is because it allows the realisation of real-time, automated tracking of goods. The ever-decreasing form factor of the devices themselves means that very soon cost effective deployments will be possible, allowing chips to be implanted on at the individual item level. Several sources indicate that the market for RFID has expanded from some $1.3bn in 2003 to $2.4bn in 2005, with some 600 million tags sold. VDC, a US market research company, predicts that 2.5m RFID tags will be in use in the EU retail trade by 2008 and a quarter of these will be deployed in Germany alone. In the EU15 in 2004, 90% of the investment in RFID was from Germany, France and the United Kingdom according to Soren Research. This is expected to fall to 60% by 2006.

Three quarters of these sales are in passive tags (such as for access cards) and the remainder in active tags (such as for automotive applications). The growth of Supply Chain Management (SCM) applications is due to the decreasing cost of tags – previous estimates that the costs might level off at 10 cents per tag are being replaced by estimates of fractions of a cent per tag, a cost that makes unit level tagging a real possibility. This drive is also being helped by new demand for unit level tagging in pharmaceuticals, baggage, animals, books tickets and other non-retail markets. The successful development and implementation of individual item level tagging, particularly in the retail industry would significantly open up the RFID market. These predictions grow even more aggressive towards 2010 – Deutsche Bank Research predicts that growth of 57% will occur between 2004 and 2010. Worldwide, the RFID market may be worth €22bn by 2010. In the EU15 this may be likely to be €4bn. The most dynamic sectors are predicted to be in the RFID software and RFID services markets.[59]

Due to the large set of potential applications, this study has decided to focus on supply chain solutions because they are expected to become the dominant type of application in the next 18 months to two years. As previously indicated, RFID can improve business performance by enabling radical efficiency savings through automation and near real time reporting in the logistics chain. Additionally, the time and safety critical nature of some

[59] S. Heng,. RFID chips: Future Technology on Everyone's Lips: Deutsche Bank Research; Frankfurt Am-Main, February 20th 2006

SCM applications provides robust and useful evidence regarding how availability concerns are tackled at a system level (for example, transferring the data across the internet introduces its own set of risks) and at the chip level (if the chip is not resilient enough then there is a possibility that data will be lost). Evidence of the efficiencies of the use of RFID in the logistics and supply chain, coupled with the ever decreasing cost (research shows that the comparative price of RFID chips has decreased from €75,000 in 1976 to €0.03c in 2005) is likely to be the convincing factor in the mass deployment of RFID in the retail sector, and thus its greater acceptance and use in the mass market. Having said that, privacy and security issues will need to be resolved before RFID becomes an indispensable part of the value chain across the entire economy.

In the context of this case study, RFID could prove to be a disruptive technology as it allows such a radical overhauling of the labour intensive logistics processes that the companies Maintenance Repair Organisation (MRO) could be forced to be radically restructured.

RFID is also a key part of the growing AmI infrastructure. With RFID enabled objects, the vision of intelligent environments will become a reality in developed countries. RFIDs provide the underlying infrastructure for many of these developments.

5.1.2 Overview of Security Threats and Concerns

Various threats have been identified for RFID technology. These are characterised as spying or Eavesdropping, Deception, DoS and finally Protection. The recent EU consultation on RFID identified the following series of challenges.

Consumer and end user concerns:

- Invasion of privacy and the automatic collection of data – questions of ownership, and visibility of the data as well as control over it (is it accurate, is it being passed on to others etc?)
- Trust and Confidence (can we trust the technology to work correctly all the time?)
- Privacy and data protection (who gets access to personal data?)
- Health and safety (is the technology safe to use, does it create waste, radiation concerns and whether it will contribute to the 'electro-smog'?)

Security issues concern the RFID tag, the RFID reader and the system as a whole. These encompass confidentiality availability and integrity considerations, in varying amounts. For example, if the RFID tag contains personal information, then adequate confidentiality mechanisms must be put in place to protect this. If the data is passed to middleware over the open internet, then not only must there be confidentiality of the data, but proper procedures to ensure its availability (as the Internet is only a best effort network) must be in place. This is a more serious concern if RFID are used in safety critical or real-time operations.

Concerns about invasions into privacy have serious implications. The pervasive nature of RFID technology means that it is possible to seamlessly collect endless quantities of information as a background process. The storage of personal data on RFID chips also presents concerns and risks, particularly in open systems where data must be made

interoperable and conformant to other data exchange standards. Finally concerns have been expressed that the technology would allow individual tracking without the direct consent of users. This is already the case in organisations where RFIDs on access cards can legitimately enable the tracking of the physical location of employees for security reasons. There is a concern in the general public sphere that RFID will allow people's movements to be followed. The EU Article 29 Working Party on Data Protection is currently investigating this in its 'Working Document on Data Protection Issues Related to RFID Technology'.[60]

Privacy enhancing technologies (PETs) and Privacy Enhancing Measures (PEMs) are proposed solutions to these challenges, which have yet to be fully realised, but with the greater uptake of RFID technology for citizen or consumer focused applications, this is bound to continue. PETs are different from PEMs as they concern only the technology, not the entire suite of measures (which may include legal and regulatory instruments). PETs have four characterstics which may help to address the privacy concerns raised by the introduction of RFIDs into wider consumer applications: anonymity; pseudonymity (with its additional characteristics of authenticity and non-repudiation); un-linkability and un-observability. PETs are an important area and the successful establishment of these technologies may go a long way towards addressing consumer concerns over monitoring and privacy raised by the use of RFID technology.[61]

An example of a PET like technology is Credentica which is an enterprise access solution for identity and access management, enabling the sharing of identity related information across organisational domains in a manner that offers unique security, privacy, scalability and autonomy benefits.[62] RFIDSec is another product which aims to meet the resulting security challenges posed by RFID deployment, by providing tags that allow the safe sharing of data and active access throughout the life cycle of the product they are attached to.[63]

The previously stated role of RFIDs as an infrastructural component of the developing AmI also highlights the fact that current understanding of risks and types of attack may change as the AmI becomes more evident. An example of this might be with RFID where the presence of an RFID device triggers some form of incident. This could be physically harmful or it could be personal advertising or legitimate or unauthorised surveillance. Whilst in some circles (e.g. context sensitive advertising) this may be seen by some as more of a useful capability, this highlights how the applications of new technology in the rapidly changing AmI can be seen as either a benefit or a risk.

---

[60]Article 29 Working Party: Working Document on Data Protection issues related to RFID technology, Brussels, January 19th 2005 available at: http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

[61] Technology solutions to protect privacy in eGovernment, Horlings, E; 2003 (RE: view Vol 2 No 3) RAND Europe, Leiden

[62] Enterprise solutions for identity and access management: Credentica; 2006 available at http://www.credentica.com/

[63] Smart and Secure RFID Tags, RFIDSec, 2006 available at http://www.rfidsec.com/

Finally, concerns have been raised about the impact of RFID on health and safety. These are in the context of ongoing public concern about the electronic smog of radiation that is increasingly prevalent in society. Recent debates about mobile phone radiation are along similar lines and despite official reports and statements regarding the limited effects of Electro-Magnetic Fields (EMF) on biological systems, this remains an issue to be resolved if RFIDs are to be deployed seamlessly in the Ambient Intelligent Environment of the future.

Irrespective of their use, it is possible to indicate the following main categories of risks associated to the use of RFIDs:[64]

Eavesdropping the communication between the tag and the reader – via the air interface, dependent on the maximum read distance. For passive transponders this risk is less.

Unauthorised read access to the data – possible with normal read distance, but limited by the short range of some transponders.

Unauthorised write access to the data – similar risk profile to unauthorised reading of data – limited by short range but technically feasible and easy to execute. With passive RFID technology that is not rewritable, this is not a concern.

Cloning and emulation – the data content is read out by some means in order to write a new tag with the data. This tag is then used to simulate the identity of the original tag.

Detaching the tag from the tagged item – removal or switching tags with fraudulent intent in order to perpetrate theft or create confusion.

Mechanical or chemical destruction – in particular the antenna are specially vulnerable.

Destruction by exposure to an electro-magnetic field – this is common practice where EAS (1 bit 1st generation tags) are deactivated at the point of sale. A strong electro-magnetic field is required hence this attack must be conducted at close range. Electro-magnetic events occurring in close proximity may also cause the destruction of tags.

Destruction by misuse of a kill command – misuse of a function developed for privacy reasons to partially or wholly erase the data content.

Discharging the battery – causing the tag to transmit frequently as a result of repeated queries can render the tag to discharge its battery. This is only possible for active tags.

Blocking – use of passive blocker tags (that are actually not forbidden by law). Any attacker must carry with him a series of tags that can interoperate with the various protocols in use in the market, or a device capable of adjusting to the protocol in use by the target tag.

Jamming transmitters – interference with the transmission and operation of the tag over the air – a technically complex task due to the need for access to specialised technology.

Frequency detuning – placing certain materials (water, metal, ferrite) into close proximity with the electro-magnetic field or antennae.

---

[64] Institute for Futures Studies and Technology Assessment and the Swiss Federal Laboratory for Materials Testing and Research, Security Aspects and Prospective Applications of RFID Systems BSI, Bonn (2005)

Shielding – wrapping the tag in metal foil or placing in aluminium freezer bags to prevent transmission or the tag being read.

5.2 AIRBUS RFID Solution for Tool and Instrument Tracing

Airbus has been collaborating with suppliers LogicaCMG and Kortenburg on a fully integrated Radio Frequency Identification (RFID) solution for the tracking and tracing of tools and instruments as well as spare parts. This is enabling Airbus to generate significant cost savings while improving overall security. Airbus piloted the use of RFID technology in aircraft tool management in 1999. As a result, all Airbus tools with manufacturer serial numbers are now equipped with a microchip for radio frequency identification, offering electronic support for loan and repair management of tools. The microchips are installed on the tools as well as the toolboxes and contain data about the history of the tool as well as shipping, routing and customs information. Thus, Airbus can efficiently comply with airline regulations and effectively deal with tooling logistics.[65] Airbus is a leading aircraft manufacturer. With a production of 378 airliners and a turnover of 22.3 billion euros in 2005, Airbus is currently ahead of its main competitor Boeing in capturing slightly more than half of all commercial airliner orders. Headquartered in Toulouse, France, Airbus is jointly owned by EADS (80%) and BAE Systems (20%). It is a global enterprise of some 50,000 employees, with fully-owned subsidiaries in the United States, China and Japan, spare parts centres in Hamburg, Frankfurt, Washington, Beijing, and Singapore, training centres in Toulouse, Miami, and Beijing and 120 field service offices around the world. Airbus also relies on industrial co-operation and partnerships with major companies all over the word, and a network of some 1,500 suppliers in 30 countries.[66]

LogicaCMG is a large international IT solutions provider. It provides management and IT consultancy, systems integration and outsourcing services to clients across diverse markets including telecoms, financial services, energy and utilities, industry, distribution and transport and the public sector. The company employs around 21,000 staff in offices across 35 countries and has more than 40 years of experience in IT services. LogicaCMG's RFID Competence Center offers working experience and lessons learned, in the area of business cases, business modelling, integration with existing systems, technological development and choices.[67] Looking beyond supply chain management, the Center recognises the wider applications for the technology in areas such as logistics, aviation, healthcare and the pharmaceutical industry.[68]

---

[65] This case study is based on telephone interviews conducted with representatives from Airbus, LogicaCMG and Kortenburg Inc and a review of associated documentary material. For a full list of interviewees see Appendix A: List of Interviewees

[66] For more information see Airbus Corporate website at http://www.airbus.com

[67] LogicaCMG 2005 Annual Report

[68] For more information see LogicaCMG corporate website at: http://www.logicacmg.com/United_Kingdom/350232883

Kortenburg Inc. specializes in RFID systems for managing products, tools and equipment in the total logistics process.[69] It offers solutions to manage products by the customer's personally defined databank. It has a great deal of knowledge in the application of identification systems for both central, local and mobile data collection and data management, by client server systems. In the case study provided here, Kortenburg provided the RFID chips for the tools loan service.

5.2.1 Business Drivers

Like many other organizations, the aviation industry is constantly looking for efficiency enhancements and cost savings. The supply chain for tools, spares, and similar goods has long been recognized as an area offering potential. Administration and information flow within supply chains are areas where efficiency can be significantly improved through the use of RFID functionality. At the end of the 1990's Airbus started a pilot project to deploy RFID in its tools business. The motivation for this was to provide a better, quicker service to customers by improving the efficiency of administration in the tool loan business. At the same time, though, this service was chosen because it was a separate organizational division, and thus a relatively "safe" environment for experimenting with this new technology.[70]

During their lifetime, commercial aircrafts are regularly subjected to inspections and interchangeable parts are replaced regularly. Air safety regulations require full traceability of the servicing activities with the associated tools used and engineering staff involved.[71] This represents a huge administrative task. Through RFID technology, Airbus can benefit from faster inventory management, improved tools identification and the ability to record specific data to tools. This specific case entails tagging of 6,000 specialty tools and also an equal number of casings (in this case 'specialty tools' means that the tools are expensive and not used very often). These tools are kept at Airbus' Hamburg location and upon request are sent all over the world to the airlines that need to use them.

Among the advantages of RFID technology over the more widely used bar coding system is its ability to read the data contained in the chip, without line of sight and for the data to be instantly transferred by radio waves. Furthermore, the latest information on the tool can be stored on the chip, so that an engineer does not need to go through a lot of paperwork to find out what the status of the tool is. Theoretically, suppliers could use RFID to ensure tools are genuine, reducing the risk of unapproved tools entering the supply chain. In this application the RFID information is only read and used by the Airbus employees themselves in order to manage the calibration process of the tool. In doing so, they save time and effort on paperwork reducing the Turnaround Time (TAT) by over 25%. The test case was considered a success and consequently implemented into normal practice.

---

[69] Kortenburg Inc My RFID Solutions, 2006 available at http://www.myrfidsolutions.com/

[70] Information from "Airbus applies RFID technology to supply of aircraft spare parts", AIRBUS pressrelease, 18 September 2003; Logica CMG, "Casestudy: Airbus takes RFID into the spare parts supply chain" available at http://www.logica.com

[71] For an interesting overview of the complexities associated with such a task see certification and maintaince requirements detailed by the European Aviation Safety Agency in http://www.easa.eu.int

Airbus recognized the potential of RFID early on and since then has actively led RFID activities in the aviation industry – also backing an industry-wide standard for RFID-based information (ATA Spec 2000). At present, Airbus is investigating the possibilities of deploying RFID on future aircraft programs.

Airbus is actively promoting RFID through various projects where RFID is applied, for example in cargo and luggage handling. The company also facilitates knowledge transfer on these applications to customers through regular conferences. Other examples of RFID pilots at Airbus are:

- Elimination of paper documents for supplier parts. By application of RFID, the so-called 'yellow tags' identifying the quality control status of a part will no longer be required.
- A pilot project for an all RFID warehouse. Once a go-ahead decision has been taken, RFID can be introduced in three steps:
    1. Tools and ground support equipment will be equipped with RFID
    2. Repair management and quality inspection will be managed via RFID
    3. RFID will be extended to all spares stored in this warehouse
- Providing means for the identification of unapproved parts in aircraft engines through RFID.
- Investigating and deploying the use of RFID in the logistics of manufacturing.
- Equipping specific cabin interior parts with RFID to support catering requirements.

5.2.2 Technical implementation

The whole system examined in this case study revolves around optimizing the supply chain of tools for repairing aircraft. A tool is kept at the Airbus tool shop in Hamburg. Upon the request of the customer (an airline), it is shipped to the customer's location. After its use, the tool is reshipped to the Airbus tool shop, where it is sent into the calibration/repair cycle. Finally, the tool is returned to the tool shop and the loan cycle can begin again.

The Airbus supply chain management activities for tools are linked to an Enterprise Resource Planning (ERP) Supply Chain Event Manager (SCEM), which is the central system, functioning between the Airbus back office ERP system and the RFID infrastructure consisting of tag, RFID reader and middleware. The middleware is software specifically developed for Airbus to ensure communication between the RFID reader and the SCEM. The SCEM is linked to the ERP system via an ERP application interface. Using an ERP exchange infrastructure, the management console communicates with the RFID middleware via an eXtensible Markup Language (XML) interface. The data is then written to or read from the tag via the RFID server. The interface is open to allow incorporation of bar code scanning or other SCEM or ERP standard interfaces at a later date. The SCEM triggers the process and workflows, both internally and externally.

The supply chain cycle is as follows:

1. The cycle starts in the ERP system with a customer order, which triggers an event in the SCEM, starting the process. The ordered tool is then prepared for delivery to the customer.
2. The forwarder collects the tool shipment and updates the transportation data in the ERP system, resulting in a message that creates an event in the SCEM. The message is then passed via the middleware to the RFID reader and written on the shipments tag and tool-box.
3. The data is now available electronically and online, both on the RFID tags and via the SCEM capability on the Internet and can be accessed by the authorized supply chain parties.
4. When the tool is delivered to the customer by the forwarder, the delivery is acknowledged through a mobile device via the Internet signaling the SCEM that the delivery is complete. The tool data and status is available in the SCEM and online at every stage in the process enabling efficient shipment tracking and routing between customers, repair shops and Airbus warehouses.
5. Once the customer returns the tool, the tag on the tool is read and the SCEM automatically notifies quality inspection by email, avoiding any delay in the internal process. After this a quality inspection and packing is carried out. Once this is notified, the tool is registered as quality inspected and ready for delivery again.

Table 1: The data available on the RFID chip

Last certificate	Periodic check code	Test laboratory
Original receipt number	Serial number	Manufacturer
Last check	Designation	Original receipt date vendor
Original certificate	Net / gross tare	Last receipt date
Part number	Dimensions - length, weight, height	Customs code
Tool set	Owner	Shipping information
No. of units	Next check	Shipping advice

Source: LogicaCMG / Airbus (2006)

The process improvements include the return of tools to the tool shop by customers, transfer of tools from warehouse to repair shop, and return of tools from repair shop to the warehouse. The instant availability of administrative data (see Table 1 for a list of data contained on the RFID chip) provides better transparency of the supply chain, thereby minimizing idle time and improving tool availability. The next step will be to integrate customers and freight carriers into the RFID processes. They will then be able to update the data on the chip and track the location of a particular tool using the SCEM via the Internet.

The strength of the RFID solution lies in the cutting-edge chip, supplied by Kortenburg Incorporated, and the solution's integration with SAP business application software. The Kortenburg Master-ID chip was the first in the world to have achieved airworthiness certification from the Luftfahrtbundesamt, Germany's aerospace regulator. The chip can cope with extreme differences in temperature, enabling it to withstand the wide range of rapidly changing temperatures that aircraft experience on a daily basis. Being attached directly to parts, it is both robust and secure against any potential tampering. Furthermore, the chip is protected within a metal 'casing' to provide extra sturdiness.

The RFID chip features two-way interaction with a 'read-write' capability. Where historically inventory and logistics have been managed by read-only systems such as bar codes, this solution enables the writing of data to the chip. The 'read-write' capability could make the whole industry more secure by preventing counterfeiting through parts that are traceable right from their point of manufacture.

LogicaCMG worked to extend the capability of the Kortenburg chip using the SAP Netweaver exchange infrastructure and the web-based SAP supply chain event manager (SCEM). Changes to the tag throughout its lifecycle can be tracked with this solution, resulting in faster workflow processes, reduced paperwork, and the elimination of error-prone data entry with automatic tools and parts tracking.[72]

The solution provided requires high data density, as a complete, unambiguous part history is needed. Each component that is traced has a unique identification and history. It is not sufficient to know the number of units received, but more specifically: where did the part come from, where was it installed, how many hours was it operated, who repaired it, who installed what type of software last, and so on. Therefore, it requires short distance reading to ensure accurate readings, with communication taking place exclusively with a single tag at a reading distance within centimeters. The chips used in Airbus applications are set today at a capacity of 4 kilobytes with dimensions of 8 millimeters in diameter and can be flush metal mounted.

Although Airbus in itself is a very large player in the aerospace industry, cooperation across the whole industry was necessary for the success of the initiative. This is due to the fact that servicing technicians do not want to handle different RFID systems for each specific aircraft type they maintain, hence the need for international standardisation.[73]

---

[72] For a detailed description see LogicaCMG, "RFID in the Aerospace Industry" available at http://www.logicacmg.com/pSecured/admin/countries/_app/assets/rfid_in_aerospace_flyer-3292006.pdf

[73] Airbus leads international standardization activities through active participation at steering boards and regular industry conferences. Activities in this field are myriad e.g. participation in the ATA Spec 2000 Chapter 9 Task Force, Permanent Bar Code Parts Identification, and active dialogue with customers, suppliers and other aircraft manufacturers. The main focus of the efforts is to define harmonized identification information, to develop tag data standards, to define passive and active RFID usage in close cooperation with regulatory authorities, and to develop an agreed standard for data exchange between different parties while considering existing ISO standards for RFID systems that cover identification cards and smart labels and finally work on the ATA Spec 2000 definition of data structure.

5.2.3 Security Challenges

The use of the reading and writing equipment is quite user-friendly – no specific training session apart from some instructions were needed to use the equipment. Data can be accessed through a web-based user interface.

An important aspect of this trial is authorized password protection for data access and modification and also to back-up data on the ERP system. The RFID chips and readers are equipped with cryptographic software that does not allow for direct reading and writing of data without the appropriate equipment. The software checks user rights and prevents access to functions that are closed based on authorization against these user rights. Individual users are identified with a unique card number.

Although the use of RFID chips has significantly improved the throughput of tools through efficiency gains in the paperwork, Airbus could theoretically still revert to manual data handling. For manual handling, the most pertinent information, which is the product serial number, is printed on the protective casing of the chip.

Notwithstanding the improvement to linkages to the back office system, there seem to be some incompatibilities in the current system that will need to be removed in a subsequent version. The errors are minimal, and removing them was not deemed a priority.

In order to maintain data integrity, the complete destruction and revocation of a tag needs to be ensured if it is removed from a part or tool. This way, counterfeit parts cannot be equipped with tags from scrapped components. Manufacturers can use the chip to prevent unapproved parts entering the supply chain; therefore each tag must have a valid serial number.

Airbus performed safety tests with RFID tags to identify any risk of defect or interference in the hostile environments common in commercial aircraft operation. Tags were exposed to severe conditions followed by read and write experiments. Safety tests included temperature changes, chemical liquid exposure, humidity, lightning induced transient susceptibility, electrostatic discharge, shock and vibration as well as fire impact. None of the physical impacts had negative effects on the read write functionality or data integrity. Nor did the hostile test environment cause defects in the tags. The tag proved resistant against a temperature range from minus 50° Celsius to plus 70° Celsius, safe against aggressive liquids and safe from electromagnetic interference (EMI). The tags are glued to the tools and the cases with epoxy and are 'shielded' by a casing, so that they cannot be chipped off (which is a physical impact that could easily occur when shipping and handling the tool cases).

One of the main requirements for RFID use on aircraft is that RFID devices need to be of high integrity and radio frequencies used must be stable. National airworthiness authorities are working on airworthiness approval and regulatory policy for passive RFID to be used on board civil aircraft. In cooperation with a European airline, Airbus performed in-flight tests of RFID tags carried on Airbus A320 aircraft. During 6,000 flight hours in 12 aircraft, tests were conducted with zero defects. The tag received approval from the German Airworthiness Authorities (LBA) after this successful test, paving the way for future approval and certification of the technology.

On 13th April 2005 the US Federal Aviation Agency (FAA) issued policy guidance memo for passive RFID (13.56 MHz). Airbus expects the FAA memo to be followed by similar action from the European Aviation Safety Agency (EASA) in early 2006. The main objectives of such a safety policy are that data regarding parts must be accessible any time, anywhere, by anyone and need to be in line with data protection rights. Components need to be easily traceable with full transparency of the product life cycle and the capability for round the clock verification information from one central secure database. [74]

Until clarity has been given about the standardized use of RFID and the whole range of stakeholders involved in the process, Airbus deems it unwise to provide general information on its RFID use in all operations.

Airbus was quite proud in looking at options to embed RFID in their supply chain and service management processes. The specialty tools tracking case was, however, specifically selected because it did not interfere with Airbus' primary process and as such was a safe 'testbed' to try new technology. As indicated above, the Airbus personnel could – if needed – revert to manual data entry and paper handling, should the system fail. As such, it could be seen rather as an efficiency evolution (through efficient carrier of data) than a truly disruptive revolution. Nevertheless, the implementation was very successful and led to a significant reduction in the turnaround time. Before releasing RFID to end-users or consumers, it may be more acceptable to deploy the technology on in-house asset management systems like the case described here.

As this RFID project was started as a pilot, the availability of the technology and service providers were not deemed an important aspect. However, future applications should certainly adhere to standards set by the industry.

The introduction of RFID has helped Airbus reduce the Turnaround Time (TAT) by over 25%; Processes throughout the supply chain were accelerated, among them the requirements for data entry control and quality inspection, as the required data was more easily available. This means that tools managed with RFID had a higher effective availability; Reduced paperwork led to significantly reduced administration and fewer error rates.

The use of RFID has accelerated the processes of goods receipt and quality inspection due to faster and more accurate data availability with the help of automatic data capture, thus avoiding 'carry forward' and multiplication of data entry mistakes. The easier, faster and improved flow of information between all participants in the supply chain led to process acceleration and thus to faster loan tool re-availability.

For the purposes of its use, the technology was deemed reliable, but an additional level of reliability was provided because the data on the RFID tag is duplicated elsewhere (on a physical serial number on the back of the toolbox) and is not the sole repository.

---

[74] Federal Aviation Authority, "Passive-Only Radio Frequency Identification (RFID) Devices" Policy document available at http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgPolicy.nsf/0/4953670dd1bd773e18625715400718e2e?OpenDocument

Future possibilities for Airbus use of RFID are, among others:

- A possibility to completely trace a part's history from 'cradle to grave'
- Standardized documentation in compliance with aerospace industry standard ATA Spec 2000.

5.2.4 Conclusions

RFID is clearly perceived as a controversial technology from the perspective of the general public. This case study has concentrated upon RFID in a supply chain environment, which is not the most controversial application but certainly one where the technology is currently being deployed in a widespread fashion. Furthermore, initial take up and growth of RFID use (as a precursor to the Ambient Intelligent environment) is likely to be spawned by use in the logistics and supply chain environment.

Given that, it is interesting to note that in the case study the use of RFID was implemented only in conjunction with back-up paper processes. Indeed, RFID was only used in a 'safe' organisational area regarded as a 'test-bed'. This illustrates that the case study organisation has obviously considered the ramifications of any failure of the RFID system, but second and third order dependencies may not have been adequately planned – for example, assuming the organisation needs to resort to paper processes in the event of a failure of the technology, there are adequate staff to complete the work (as paper based bureaucracy is notoriously labour intensive) etc. Another important consideration surrounds confidentiality and the transmission of RFID data over open networks, specifically the Internet. In a logistics environment this may not be a crucial issue, but of course where anything being transmitted falls under data protection law (e.g. with personally identifiable information), then this becomes a very important matter.

Finally, the organisation in the case study was attempting to lead take up of logistic RFID solutions in the aviation industry: thus the need to include aspects of security in any industry led 'self regulation' is critically important.

Organisations seeking to securely implement RFID solutions need to be aware of a myriad of issues. In the supply chain field these relate mainly to availability and reliability concerns but in the medium to long term, as RFID begins to be deployed for a greater number of applications due regard to privacy considerations along with appropriate management of consumer perceptions will need to be established.

Public administrations can support the appropriate use of RFID by encouraging Research and Development funding to further explore the security features of RFID infrastructure and investigate how appropriate means to meet consumer perceptions regarding security can be implemented (e.g. 'kill switches' for the tags as a consumer leaves a store). However, further research still needs to be done on the privacy implications of RFID use and the ongoing EU consultation on RFID[75] should be encouraged and its results disseminated as openly as possible. Means should be sought to precisely describe how privacy could be protected in the AmI, enabled by mass RFID use. To this end the EU Article 29 Working

[75] RFID Consultation website: Towards an RFID Policy for Europe available at http://www.rfidconsultation.eu/

Party may wish to consider a further technology neutral consultation on privacy aspects of the AmI as a whole, rather than just RFID technology. Governments and the EU should also begin to consider, in the context of the emerging AmI, whether current ombudsman structures (such as data protection or information commissioner authorities) are appropriate for the sort of technological environment that is so rapidly evolving.

5.2.5 Review of the case study conclusions during the Final Workshop

Although the RFID case study did not explicitly cover concerns closer to the heart of consumers regarding this technology (such as a perception over unwanted monitoring and invasions of privacy) the specific application of RFID in the logistic environment was agreed by participants to be highly pertinent.

The challenge of synchronicity and concurrency of datasets (hence availability and integrity) was identified as a major issue for RFID technology, whether in the application of this technology to logistics or consumer driven applications. Given existing uncertainty (in evidence in the debate) over how much data is can be stored on a chip (and whether this is simply a serial number referencing other, comprehensive data held on a central database) a possible challenge might be in trying to ensure that remote data warehouses holding the complete 'record' for the RFID chip might become outdated or out of sync with information on the chip, leading to a general loss of integrity in the system.

RFIDs are a key element to the take up of an AmI environment and it was pointed out that consideration of RFID technology as part of an open network (not a closed network as in the case study), was critical to identifying further challenges that might threaten the growth of the Information Society. The accessibility of data in an RFID system was identified as a key driver for obtaining the benefits of the technology. However, coupled with this must be the realisation that such a system must be made as a secure as possible to minimise data leakage (which may be important in either the consumer or logistics application of these technologies).

CHAPTER 6 Internet Protocol version 6 (IPv6)

6.1 Internet Protocol version 6 (IPv6): General Issues

The need for a new generation of the Internet Protocol (IP), the suite of communication protocols that govern how data packets are routed around the Internet, is clear. The growing Internet user population coupled with the increasingly pervasive nature of ICT means that the current standard for governing Internet traffic, IPv4, will be unable to cope with increased demand for IP addresses. If the current proposals for ubiquitous and pervasive computing are to be realised then the Internet infrastructure must be capable of supporting such developments. Although the reality of universal access to the Internet for everyone on the planet is still a distant vision and such as concept may seem fanciful when there are greater challenges for much of the worlds population, failing to address this problem will ultimately deny developing nations an opportunity to participate in the 21st century economy.

The drivers for the implementation of IPv6 are collectively known in the industry as 'IPv4 pressure'. It includes the requirements that all devices connected to the Internet must have a unique IP address. The classes of these devices are expanding from computers to PDAs, mobile phones, home appliances, and automobiles. IPv4, with 4.3bn unique addresses, does not have a large enough address space to support this expansion. The theoretical maximum number of unique addresses in IPv6 is 3.4×10^{38}. This is a very big number that defies description: we could allocate an IPv6 address to every grain of sand on all of the beaches on the Earth and not come close to exhausting the range of possible addresses.[76] 'IPv4 pressure' also refers to the absence in IPv4 support for mobile devices, requirements for end-to-end security, and flow control.

For example, as the address space of IPv4 became scarce, network operators began to employ tools to more fully use it. Network Address Translation (NAT) is a means through which hosts on private networks can communicate with external Internet hosts. In NAT, a network device with at least one (but more often several) public IPv4 addresses multiplexes traffic from hosts on a private network to hosts on an external network. In

[76] Glen Mackie.. To see the Universe in a Grain of Taranaki Sand. Swinburne University of Technology, Melbourne Australia, February 1, 2002 Available from http://astronomy.swin.edu.au/~gmackie/billions.html.

engineering terminology, NAT is a kludge – a cobbled-together solution that is suboptimal – but it has become commonplace. In addition to saving address space, NAT provides a certain amount of security from external servers contacting internal hosts directly. NAT does have drawbacks: it obviates any attempt at end-to-end security and limits the topology and resilience of the Internet. Firewalls are similar to NAT in the sense that they control the flow of traffic to sub-networks. Paradoxically, NAT has become so common that it is regarded as an impediment to complete deployment of IPv6. Some observers feel that the vast address space of IPv6 will facilitate a return to the end–to-end nature of the Internet as it was originally designed, with each device being logically locatable via a unique Internet Protocol address.

There are also important policy issues to resolve, most notably around ownership of IP address space and management of the resource that will be the underlying enabler of the 21st Century Information Society. Security plays an important role too, because IPv4 was designed without any explicit security measures. Some experts feel that the restoration of the end-to-end paradigm may deliver increased security of the infrastructure as a whole. The current security paradigm is perimeter-based, which seeks to protect sub-networks individually and is implemented locally by network managers. IPv6 offers the possibility of improved end-to-end security, facilitating connections and transactions among nodes and users.

Thus, the global implementation of IPv6 thus has the promise to radically improve the resilience of the Internet to the benefit of the Information Society as a whole.

The design and implementation of IPv6 networks is a decision making process that is now subject to the views and whims of many more stakeholders than was with the original Internet. As some of the 'fathers' of the modern Internet, state, there will be "…a struggle to find the next social structure that will guide the Internet in the future. The form of that structure will be harder to find, given the large number of concerned stakeholders."[77]

Much of the struggle is due to the relatively few unique addresses that IPv4 offers. In the early days of the growth of the Internet, the United States was allocated a high number of addresses. Other geographical regions, most notably Europe and the Far East, were allocated relatively smaller blocks of IP addresses. Since these regions account for much of the current growth of the Internet today, 'IPv4 pressure' is strongest there, since IPv6 offers the address space that these regions need for economic development.

The IPv6 Forum was founded by the IETF Deployment Working Group in 1999 to drive IPv6 deployment worldwide. To do this it has created over 30 IPv6 Country Fora and Task Forces.

Adoption of IPv6 is expanding. The US Federal Government has mandated that all of its federal agencies must adopt IPv6 by 2008.[78] In 2003 Japan, South Korea and China made

[77] B. Leiner B., V Cerf, D Clark, et al A Brief History of the Internet 20th February 1998 available at: http://www.isoc.org/internet/history/brief.shtml

[78] Chloe Albanesius OMB: Agencies Must use Advanced Internet by 2008 GovExec.com June 29th 2005 available at: http://www.govexec.com/dailyfed/0605/062905tdpm2.htm

an important public announcement that they would seek to jointly develop IPv6 and completely adopt it by 2005.[79]

To facilitate the transition to IPv6, in July 2004 the Internet Corporation for Assigned Names and Numbers (ICANN) announced that the root Domain Name Servers (DNS) for the Internet were modified to use IPv4 and IPv6.

Drivers for IPv6 deployment include:

- Growing volume of peer to peer traffic
- Projected exponential increase in the volume of Internet traffic
- Rapid development of broadband (including wireless) Internet-access infrastructure
- Necessity to cope with machine-to-machine communications
- Need to route 3G UMTS mobile communications via the Internet.

Three Regional Internet Registries (RIRs) are responsible for the assignment of IP addresses to Internet Service Providers (ISPs) or more specifically Autonomous Systems (AS) which may be ISPs but may also be large organisations owning significant network infrastructure. The RIRs are Réseaux IP Européens (RIPE), American Registry for Internet Numbers (ARIN) and Asia Pacific Network Information Center (APNIC).

In Europe there are two main pan-European trials: 6Net and Euro6IX. These large-scale trials complement and work at national level with National Research and Education Networks (NRENs). Additionally other European test-beds exist such as GEANT.

6.1.1 Why is IPv6 disruptive?

IPv6 is a disruptive technology because it possesses capabilities not included in IPv4 that are expected to lead to the development of the Ambient Intelligent Environment (AmI). IPv6 has the ability to improve Quality of Service (QoS) for certain kinds of IP traffic, and has built-in support for mobile applications, which will facilitate the faster growth of mobile communications technology. The European Commission stated in its Communication on 3G that IPv4 was hindering the full deployment of 3G services in the long run.[80] Increased deployment of wireless Internet access technologies, such as WiMAX and 3G can be made more efficient and effective through the use of IPv6. Due to the absence of fixed infrastructure and ease of deployment of wireless Internet solutions, developing countries can leapfrog older economies by more easily deploying Internet infrastructure to exploit the opportunities of the 21st Century economy. IPv6 is thus an enabling force for this activity as it makes the deployment of mobile and wireless Internet more effective.

---

[79] Report: Japan, China, S. Korea developing next Net; CNet, 30 December 2003, available at http://news.com.com/2100-1032_3-5134110.html

[80] The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward COM(2001) 141 available at http://www.europa.eu.int/ISPO/infosoc/telecompolicy/en/com2001-141en.pdf

Applications of IPv6 are derived from the features that IPv6 offers over IPv4 (see below). Some observers point to the differences between IPv4 and IPv6 and note that the new protocol will enable a new set of Internet applications and business models. For example, the large address space could enable every electronic device to have a publicly available IPv6 address, including cellular telephones, radio-frequency identification tags, home appliances, inspection kiosks, and so on. The QoS and flow control features of IPv6 might enable true broadcast of multimedia content via the Internet. Support for mobile devices will allow every cellular telephone to connect to the Internet as a host, possibly enabling additional applications. To deploy an application via IPv6 requires that the source and destination nodes communicate through IPv6, and widespread development of new applications will require widespread, but not necessarily universal, support for IPv6. The security implications of this much broader and more pervasive Internet topology are of concern to policy makers.

IP is the protocol operating the network layer of the Open Systems Interconnection (OSI)[81] standard for data networks.[82] The Internet is the interconnected set of computer networks that transmit data to one another using IP. Each host is unique accessible through an IP address.[83] The networks are connected to each other through gateways, which look like nodes to other computers on the Internet. The purpose of IP is to route datagrams[84] from network to network. All traffic on the Internet is handled identically, according to the rules of IP. IPv4, and IPv6, execute a seemingly simple set of tasks: (1) to route datagrams through the Internet; (2) to provide addressing information for all networks connected to the Internet that act as sources and destinations for datagrams; (3) to fragment datagrams into smaller components when required by the data link and physical layers.[85]

---

[81] Each layer of the OSI network architecture provides a communications link with properties that it passes to the next higher layer. The lowest layer is the physical interconnection among sites, ranging from a twisted pair of wires to a satellite relay. Above the physical layer is the data link layer, which provides a standard interconnection for transmitting bits through the physical layer. Next is the network layer, which provides a means for reliable transmission of data, handling addressing and routing. The transport layer breaks data into packets and provides services for error detection and recovery. The session layer provides a link for the transmission of messages among parties. The presentation and application layers provide complete network services from terminal to terminal.

[82] Dimitri Bersekas and Robert Gallager. 1992. Data Networks. Second ed. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

[83] It is important to distinguish between the WWW and the Internet. The WWW is a set of interconnected data files that are linked to one another through hyperlinks. Users access content on the WWW through uniform resource locators (URLs), which specify the location of the data file, and how to access it. Common access modes include the Hypertext Transport Protocol (HTTP), and the File Transfer Protocol (FTP).

[84] Data to be sent over the Internet is broken into packets, a task typically done by the transport layer. A datagram is a packet that includes source, destination, and other information such that it can be routed through the network independently of other packets.

[85] Dimitri Bersekas and Robert Gallager. 1992. Data Networks. Second ed. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

The six principal ways in which IPv6 differs from IPv4 are listed in Table 2 below.[86] Due to the fixed-length header, the specification of special services, such as ordering of streams of packets, becomes part of the payload of the datagram, rather than part of the header. In IPv6, the security protocol IP Security, or IPSec, is now a required component of IP, rather than an optional component; IPSec's features are enabled via a specific extension header. A flow is a sequence of packets from one source to one destination.

In IPv6, flow control may be handled by the network layer, rather than by the transport layer, as it is implemented in IPv4. To exploit the capabilities of IPv6 requires that the source and destination nodes both use IPv6 to route packets through the Internet. It is expected that IPv4 will linger, impeding the full implementation of the new protocol.

The principle technical differences are:

128-bit address: The IPv6 host address is 128 bits whereas the IPv4 address is 32 bits. One purpose of the 128-bit address is to ensure that address space will be available for the foreseeable future; the other is that the vast range of addresses allows the allocation of addresses in methods other than the common sequential manner now used. The use of 128-bit addresses will allow network administrators to allocate addresses non-sequentially, spreading IP addresses in a pseudo-random manner to thwart scanning attacks. There are several types of addresses in IPv6: unicast, multicast, and anycast. Unicast addresses are unique destination addresses and IPv6 delivers the packet to the identified address. Multicast addresses identify groups of hosts and a multicast message is delivered to all hosts represented by that address. Anycast addresses identify a group of addresses, but in contrast to multicast addresses, the packet is delivered to a single host within the group.

Auto-configuration of hosts: IPv6 hosts, when connected to an IPv6 network, configure themselves. Given the large address space, autoconfiguration is a necessity in IPv6. This property of the protocol has the potential to ease the proliferation of IP-enabled devices and appliances, since manual configuration by the user/consumer will not be required.

Fixed length header and extensions: The header in IPv6, unlike that of IPv4, is fixed at 40 bytes; to support optional services extension headers are used. The fixed-length header eliminates the need for a checksum and allows for a simpler hardware implementation of the protocol. In principle, the simplicity of the header speeds processing by routers, but in practice, the presence of extension headers may eliminate any benefit. Elements of the header include: version (IPv6, 4 bits), traffic class (1 byte), flow label (20 bits), payload length (2 bytes), next header (1 byte), hop limit (1 byte), source address (16 bytes), destination address (16 bytes). The traffic class field allows the router to apply special handling to packets and is expected to be used to support enhanced QoS. The flow label allows hosts to specify groups of packets as a flow, facilitating processing and transmission by routers.

Extensions and special services: As mentioned, extension headers specify special handling and properties of the datagram. There are six extension headers: Hop-by-Hop Options; Routing; Fragment; Destination Options; Authentication; and Encrypted Security Payload

---

[86] Internet Protocol, Version 6 (IPv6) Specification (Internet Engineering Task Force) available at: http://tools.ietf.org/html/2460

(Hagen 2002). The destination node processes the extension headers. It is through extension headers that IPv6 enables specialized routing and security features.

Required Implementation of IPSec: When fully deployed, IPv6 will allow all hosts to use IPSec as an end-to-end protocol for ensuring security of communications over the Internet. At present IPSec is not deployed widely in IPv6 implementations. It is an important part of the basic elements of IPv6 but at present is only deployed to meet security requirements at the network backbone level, between service providers who use the BGP (Border Gateway Protocol) to communicate with each other.[87]

Flow labelling and control: Through the Flow Label field in the header, IPv6 allows hosts to label groups of datagrams as a flow. Doing so allows routers to simplify and speed processing of datagrams, improving support for certain types of communications.

Mobile support: IPv6 has explicit support for mobile applications, which will allow a large number of devices to connect directly to the Internet.

[87] Border Gateway Protocol Filtering Guidelines Policy and Best Practice Id. 00392, 01 April 2004, National Infrastructure Security Co-ordination Centre (NISCC) London 2004

Table 2: Comparison of principal differences between IPv4 and IPv6

	IPv4	IPv6	Notes
Number of unique addresses	$4.3 * 10^9$	$3.4 * 10^{38}$	"Unlimited" address space obviates need for NAT
Server configuration	Semi-automatic with DHCP	Autoconfiguration standard	Autoconfiguration is considered a requirement given the 128-bit address and still requires appropriate oversight by the administrator
Header format	Variable length	Fixed length of 40 bytes	Simplifies implementation and eliminates requirements for a checksum
Extensions and special services	Part of header	Part of body	
Security features	IPSec available but not mandatory	IPSec mandatory	Availability of IPSec in IPv6 may encourage more widespread use
Flow labelling and control	Part of transport layer	Labelling for priority; anycast, unicast, and multicast transmission	IPv6 is capable of broader range of services
Support for mobile applications	None explicit	Explicit support	May allow broader range of services

Source: S. Hagen, IPv6 Essentials (2002)

Because the current structure of the Internet, including the workarounds, provides the services required for most service providers and users, the transition to IPv6 is expected to be a long process. A U.S. National Institute of Science and Technology (NIST) study estimates that 30% of Internet Service Providers (ISPs) in the United States will implement IPv6 by 2010; the penetration rate will not reach 90% of ISPs until after 2015.[88] Users of the Internet are expected to lag behind ISPs by several years in their adoption of IPv6. The long transition period will require firms to operate systems capable of sending both IPv4 and IPv6 datagrams. There are several technical options to solve this problem, but a drawback is that a heterogeneous IP environment makes users vulnerable to threats to IPv4, IPv6, and technical workarounds to ensure communication between

[88] Michael P Gallaher and Brent Rowe. 2005. IPv6 Economic Impact Assessment: Final Report. Research Triangle Park, North Carolina: RTI International.

them.[89] Additionally, special security features of IPv6 are unavailable in a heterogeneous environment. Compared to the United States, member states of the European Union have fewer ISPs and more centralized oversight of their information networks. Hence, it may be possible for policy makers to more forcefully require transition to IPv6. The case study of DREN's implementation of IPv6 will provide insight into this decision.

The question for policymakers is how to understand the motivations of firms and ISPs for switching to IPv6 and the implications for security of those decisions. The shift to IPv6 will occur within organizations as the opportunity and market permits. However, IPv6 may be disruptive in the sense that the methods for which it accomplishes the same tasks as IPv4 are fundamentally different. The vast address space facilitates many different methods for allocating and managing addresses within organizations, and the requirement to include IPSec into the implementation of IPv6 might allow new methods for achieving security.

A recent study commissioned by NIST expects that the transition to IPv6 will occur through normal equipment replacement. Equipment makers are currently shipping equipment that is IPv6-enabled. For most small and intermediate sized organizations, the costs for converting to IPv6 will be incorporated into the costs of upgrading and replacing equipment. For larger organizations and those that provide network services, however, the transition to IPv6 is expected to be significantly more complicated and more expensive.[90]

6.1.2 Overview of Security Threats and Concerns

To date, security has been an add-on to the Internet. In part because of the original application of the Internet and the relatively small user community, IP initially contained no security mechanisms. Certain applications, such as "secure shell" and "telnet" for terminal communications, and the File Transfer Protocol (FTP) for sending files were password protected, but most routing protocols were unsecured. Included in IPv6 is a set of protocols for securing communications throughout the Internet, regarded as one of the principal features of the new protocol. The set of security features is known as IP Security, or IPSec, and is currently available in IPv4, but not widely used.[91]

Security in IP refers to preventing the malicious routing and manipulation of datagrams. Security on IP networks focuses on preventing or mitigating the damage from four canonical attacks: DoS, eavesdropping, modification, and fabrication.[92] A DoS attack prevents datagrams from a sender from reaching the receiver. Eavesdropping is the receipt or rerouting of a datagram to an unauthorized third party without the knowledge of the

[89] There are three generally recognized options for operating IPv4 and IPv6 networks together. A "dual-stack" network is one in which IPv4 and IPv6 coexist. Since much of the existing infrastructure is IPv4-compatible, tunneling allows IPv6 datagrams to be transmitted through the IPv4 infrastructure. It is also possible to "translate" IPv6 addresses into IPv4 addresses, and vice versa, so that nodes running different protocols may communicate. It is expected that all of these techniques will be used during the transition to IPv6 (Hagen 2002).

[90] Michael P. Gallaher and Brent Rowe. 2005. IPv6 Economic Impact Assessment: Final Report. Research Triangle Park, North Carolina: RTI International.

[91] Interview with Rodger Johnson, Arlington, Virginia 18th April 2006

[92] Silvia Hagen, IPv6 Essentials. Sebastopol, California: O'Reilly Media, Inc. 2002

sender or receiver. Modification is the routing of a datagram to a third party who changes the payload of the datagram before sending it to the intended recipient. Fabrication is the creation and sending of a packet from an unauthorized sender to a receiver; a common attack today that involves fabrication is "spoofing" in which an attacker poses as a legitimate website to gather information from a victim.

IPSec is a framework for providing protection against the attacks listed above by ensuring four aspects of the transmitted or received data: confidentiality; integrity; authenticity; and obligation.[93] It is a mandatory component of the IPv6 protocol suite, though it is not required that IPSec be enabled in any given implementation of the protocol. There are six elements to IPSec: (1) security requirements; (2) encryption; (3) authentication; (4) cryptographic algorithms; (5) security associations; and (6) key management.[94] Security associations are agreements between two communication parties regarding the authentication or encryption algorithms to be used during secure communications and the keys to be used to encode those communications. Security associations occur between nodes and require that both the sender, receiver, and intermediate nodes route datagrams using the same protocol.

IPSec in IPv6 envisions end-to-end security. A common security framework today is perimeter security. In this framework, the network administrator controls access to his or her network through a single point of access, which is typically a packet filter or a firewall. Variations include intrusion detection systems and layered networks in which users and communications require an increased level of authentication to gain access. The assumption is that all internal communications are secure and that malicious communications can be kept out of the network. End-to-end security refers to secure communications between any two hosts. In IPv6, extension headers (recall that an IPv6 datagram has a fixed header length of 40 bytes) are used to manage authentication and encryption function.[95] IPSec and perimeter-based security are not mutually exclusive: IPSec, when implemented properly, only secures the communication among network hosts. However, the OSI architecture offers many other potential vulnerabilities through the application layer and through personnel.[96] The U.S. Department of Defense (DoD) information security model incorporates multi-level access control lists and intrusion detection systems; it is not necessarily compatible with IPSec.[97]

During the transition to IPv6, use of these features will be particularly difficult. Consider the example of tunneling, which encapsulates IPv6 datagrams within IPv4 packets. In this case, rather than the security association occurring between two hosts, the security association occurs between a host and a security gateway such as a firewall, which is not the

---

[93] ibid

[94] Documentation for the six components of IPSec may be found at the Internet Engineering Task Force WWW page: http://www.ietf.org/.

[95] Hagen, IPv6 Essentials

[96] Johnson 2006

[97] Ron Broersma,. IPv6 on DREN & Status of DoD Pilot. Paper read at U.S. IPv6 Summit 2003, December 17, at Arlington, Virginia.

ideal model for this type of security. Past the gateway, the communication would not necessarily be secure. There is a concern that perimeter security would be unable to monitor communications at all layers of tunnels. Solutions are sure to be complex: it is possible to implement IPSec at the IPv4 layer in addition to the IPv6 layer. The recent NIST reports cite the complexities of operating IPv4 and IPv6 together as a significant security concern: there is not an established method to change from perimeter to end-to-end security, and many networks will have to operate using both protocols for an indeterminate time.[98]

6.2 DoD High Performance Computing Modernization Program implementation of IPv6

This case study examines in detail the experience of the DoD High Performance Computing Modernization Program (HPCMP) in its implementation of IPv6 on two networks. Since HPCMP is an early adopter of the protocol, the factors that influence its decisions probably will be different from those that influence decisions as the use of IPv6 becomes more prevalent.[99] The Defense Research Education Network (DREN) is the information network of the DoD that is specially designated for research and engineering.[100] It is part of the HPCMP. DREN connects 4,500 users across the United States via commercially provided wide area network.[101] DREN network has 10 "core nodes" and approximately 100 smaller "service delivery points".[102] Sites are connected via high-capacity optical links provided by Verizon. DREN acts as a virtual private network over the commercial infrastructure. A goal of HPCMP is to test and transfer leading-edge communications technologies to other agencies throughout the DoD and U.S. government.

6.2.1 Business Drivers

The need to understand the strengths and weaknesses of IPv6 was the principal driver to the decision to build IPv6-capable networks. Since 2001, DREN IPv6 pilot has supported testing and experimentation in interoperability, network performance, and architecture.[103] Understanding and solving these issues is critical for the DoD given the timetable for

---

[98] Michael P. Gallaher and William A. Jeffrey. 2006. Technical and Economic Assessment of Internet Protocol Version 6 (IPv6). Alexandria, Virginia: National Institute of Standards and Technology, U.S. Department of Commerce.

[99] This case study is based on telephone interviews conducted with representatives from the Department of Defense, Defense Research and Education Network and the High Performance Computing Modernisation Program and a review of associated documentary material. For a full list of interviewees see Appendix A: List of Interviewees

[100] Defense Research and Engineering Network Definition Department of Defense, July 8th 2004 available at http://www.hpcmo.hpc.mil/Htdocs/DREN/dren-def.html

[101] John Baird, DREN IPv6 Pilot Network. Paper read at Supercomputing 2004, November 8-11, at Pittsburgh, Pennsylvania.

[102] Broersma; IPv6 on DREN and Status of DoD Pilot

[103] Baird; DREN IPv6 Pilot Network

implementing a dual-stacked IP network for all of DoD and the security risks inherent in such a transition. Unlike other early adopters of new technology, there is no risk/reward threshold that the HPCMP must surpass[104]; HPCMP was not required to build a traditional business case before implementing either DREN IPv6 pilot or IPv6 on DREN.[105] Decision makers at other organizations looking to the experience of the HPCMP with respect to DREN IPv6 pilot and the full-scale DREN network should regard the experience as a best practice with respect to implementing a potentially disruptive technology. In particular, DREN IPv6 pilot and DREN together allow the DoD to approach a transition to IPv6 with the least disruption.

6.2.2 Technical Implementation

HPCMP operates two distinct IPv6 networks. The IPv6 test network, initially called DRENv6, is known as the DREN IPv6 pilot. DREN IPv6 pilot was built as an IPv6 test environment in 2001. This network operates only IPv6 and exists as a distinct entity from DREN. DREN IPv6 pilot is used to connect other IPv6 test networks, such as Moonv6 (http://www.moonv6.org), and the 6bone (http://www.6bone.net), and as a platform for experimentation with the protocol[106]. DREN IPv6 pilot has been used to support performance studies, interoperability tests, and architecture experiments within DREN and with partner institutions and networks. In July 2003, the Chief Information Officer of the US Department of Defence (DOD) asked HPCMP to used DREN as the prototype network supporting a DoD transition to IPv6; the DoD plans to have complete dual-stack capability by fiscal year 2008.

As a result, for approximately two and a half years, DREN has offered dual-stack capability to HPCMP sites and contractors. Infrastructure support for DREN is provided via a contract with Verizon. DREN supports the needs of HPCMP's research community. In the long term, the DoD hopes to use many of the features of IPv6 to support future field operations.

HPCMP supports DoD researchers who require state of the art network services, therefore, all components of DREN are modern; HPCMP staff emphasized that having the proper equipment was critical to the successful deployment of IPv6 on DREN.[107] The DoD is a large organization with a significant user base of network services, so it naturally falls into the latter category. DRENv6 and DREN2 provide experience in implementation and management of IPv6 to ensure as smooth a transition as possible to IPv6 throughout DoD.

Though IPv6 has the potential to offer improved performance in the routing of datagrams, current experiments have shown that the performance is comparable to that of IPv4. As is common with many early adopters, HPCMP found that the features of IPv6 described above are not available. For example, auto-configuration is a feature that has the potential to ease the task of network administrators. However, DHCP servers perform this task

---

[104] Interview with Brent Rowe, Arlington, Virginia, February 10 2006

[105] Johnson 2006

[106] HPCMP IPv6 Technical Staff 2006

[107] Johnson 2006

today for many networks. It is possible to convert a private network to IPv6, but since most IP nodes continue to use IPv4, it is essential that the system administrator understand the intricacies of both protocols. Because of the requirements for either dual stacking or tunnelling to ensure communication between servers running IPv6 and IPv4, the end-to-end security paradigm will not be available during the transition period. Like security, other features of IPv6 probably will not have an effect on network performance until a critical fraction of the Internet uses IPv6 exclusively: the fixed header length simplified implementation of the protocol in routers; the flow labelling capability requires IPv6-only traffic to be functional. Finally, many of the network management tools that are commonly used to support network administrators are not yet available in IPv6.

6.2.3 Security Challenges

HPCMP considers the implementation of IPv6 on DREN and the construction and ongoing operation of DREN IPv6 pilot a success. When building the DREN IPv6 pilot, HPCMP engineers simply enabled IPv6 on a new network and began to experiment. Such experimentation was possible because HPCMP maintains up-to-date networking hardware and software. Because DREN is a production network that supports a research community, the planning process for the deployment of IPv6 on DREN was much more involved.

The planning for the deployment of IPv6 on DREN was detailed and thorough. HPCMP formed an IPv6 pilot team to coordinate the deployment across 15 sites. The goals of the transition were to minimize the need for workarounds and dual protocol operations on the final dual-stack network: the fewer tunnels and translators among components, the more robust and secure a network. No architectural changes were made. Over the course of several months, project managers adapted the Carnegie-Mellon University Software Engineering Institute process for technology transition planning to the case of IPv6.[108] The result was a set of transition plans in seven functional areas: IP transport and infrastructure; infrastructure services; network management; security; applications; "planning for the future"; and the high-performance computing community.

Project managers briefed IPv6 pilot team members at the sites regarding requirements for the transition in half-day training sessions. These processes coordinated the deployment and successfully managed risk. The site teams smoothly deployed IPv6 according to the requirements of the process. Security of the dual-stacked DREN is equivalent to that of the IPv4-only version; HPCMP achieved this goal by deploying IPv6 versions of its existing IPv4 security strategy.

The remainder of this section describes some specific aspects of the IPv6 transition from the perspective of managing security within the different communities at HPCMP. Typically, the decision maker weighs costs, benefits, and risks and decides to adopt an emerging (and potentially disruptive) technology. This is not the case for HPCMP: the chief information officer of the DoD mandated that HPCMP prepare the DoD for the deployment of IPv6 on DoD networks. Key decisions regarding the deployment of IPv6

[108] More information regarding this process, known as TransPlant, is available at http://www.sei.cmu.edu/news-at-sei/features/2001/4q01/feature-4-4q01.htm.

on DREN were made by IPv6 implementation team project managers who planned the transition; these are the decision makers in our case study. Network managers at HPCMP sites were the persons responsible for carrying out the IPv6 plan for deployment.[109] Ideally, the network protocol will be transparent to most users of network terminals, so the term "user" in this case study refers to programmers who write applications to manage network resources or exploit features of the protocols.

HPCMP decision makers derive several general lessons from the deployment of IPv6 on DREN. First, thorough planning is critical. DREN is a high-performance computing network that supports research and development; there was no margin for error regarding deployment of IPv6. The Carnegie-Mellon methodology for technology transition offers a good model. Second, involving a broad range of people facilitated the transition; HPCMP employed persons on a part-time basis, including in the field of security, throughout its organization to perform the transition and feels that it was a successful strategy. Third, demanding the support of commercial vendors is critical. The DoD decision to deploy IPv6 also included a requirement that all equipment be IPv6 capable. HPCMP demanded that IPv6 be supported fully, which it regards as a significant motivator to the equipment vendors to upgrade their equipment and provide appropriate network management tools. The long-term value of using IPv6 will be the support of the overall DoD mission.

One of the challenges for the transition was the less than complete vendor support. DREN project managers knew that it was impossible to run IPv6 alone. There are a number of network management tools and applications that simply do not yet support IPv6. The vendor community has been addressing the issue, but capabilities often arrive with new generations of equipment. For example, simple networking debugging tools such as "ping" and "traceroute" have become almost universally available. Until recently, domain name service had been an issue too. Vendors offer no "schedule" for delivering all of the required functionality to users. Firewalls, routers, and switches are now IPv6-capable. This is particularly relevant in the case of IPSec.

As mentioned, the principal security feature of IPv6 is mandatory support for IPSec. HPCMP observed early in its implementation that there is a difference between stated support and actual support from vendors: over 90% of products that supported IPv6 at the time did not support IPSec, and those that did were not as good as the support for IPSec in IPv4. Moreover, many of the security issues encountered were common to both IPv4 and IPv6. Key management was seen as a critical issue and many organizations do not have appropriate infrastructure to support such functionality. IPSec communications may not be subject to the same requirements as normal communication and if used improperly may bypass traditional defences, leading to the insertion of a worm or virus through a "secure" communication link. Appropriate tools to manage IPSec did not exist, making implementation difficult. Finally, during the transition is was evident that most current experience with IPSec has been in the enabling of virtual private network functionality, which is often specific to certain vendors; it is unclear how transferable this experience can

[109] Since IPv6 is a networking protocol rather than a specific user application, the term "user" in this context refers to persons who develop and operate applications that rely on the protocol for routing information through the Internet. Hence, the "users" in the case study are a subset of what most observers would label "network administrators".

be in general. Though HPCMP has not observed any decrease in security post deployment of IPv6 and has seen no increase in attack, it was also evident that that maintaining security of DREN in a dual-stack environment requires additional resources.

6.2.4 Conclusions

The use of IPv6 is an important factor in increasing the overall reliability and stability of the public IP network and its deployment within DREN is clearly crucial from the perspective of a precursor to the widespread use of IPv6 amongst all US federal government departments. Useful lessons for the future deployment of IPv6 have been drawn from this case study, most notably regarding the need to run a dual stack environment and the need to obtain a positive level of support from vendors and engage them in any IPv6 deployment, specifically in their levels of stated support for IPSec. Additionally, the role of regulatory authorities in encouraging the use of IPv6 was also identified. This is particularly important in the context of security, as a heterogeneous environment, with both IPv4 and IPv6 in operation and organisations transitioning from one to the other may introduce other risks (e.g. tunnelling between IPv4 and IPv6 which undermines security aspects present in IPSec) that generally serve to undo the implementation of the end-to-end security paradigm. The need to maintain the same levels of security in this period of transition may also have second order effects, such as the additional resources required in the organisation.

The case study also showed how little margin for error there was in deployment of IPv6 within an organisation (even at a pilot stage) and how the transition scenarios (e.g. in respect of vendor expertise in IPSec in IPv4 compared to IPv6) needed to be effectively managed. The organisation in the case study was able to trial the pilot of IPv6 without having to perform a full business case. This is an important fact as it shows that no management / finance hurdles had to be overcome to justify the deployment of this technology. This in turn leads to the thought that if a full blown business case was required, would the pilot still have been allowed to proceed? The involvement of security personnel from an early stage in the deployment of IPv6 helped the transition, illustrating the need to involve security at the heart of any implementation or use of a disruptive technology.

Organisations wishing to deploy IPv6 should be aware of these issues and should make sure that any transition is completed quickly and effectively to minimise risks associated with running a 'dual-stack' environment. Management of this transition should be carefully planned to minimise associated risks. As with many projects, organisations should plan for a worst-case scenario and be prepared to consider second order dependencies and effects should the plan run into trouble. Finally, organisations must be aware of vendor support for IPSec and be prepared to aggressively negotiate with equipment suppliers in ensuring that appropriate security functionalities are in place.

Public administrations can try to promote the widespread use of IPv6 amongst as many organisations as possible, to maximise the effects of network externalities and raise the game of security overall within Europe. IPv6, with its QoS functions and added security, will be a key part of the evolving Single European Information Space and if Europe is to compete on the same footing as many of the Asian states (who have already implemented national plans to deploy IPv6) then a coherent strategy is needed for encouraging its use in

public administrations and the private sector, otherwise security and competitiveness may suffer.

Furthermore, public private partnerships with industry should be used as a vehicle to explore the implementation of the security features of IPv6 and encourage the design of equipment with realistic levels of support for IPSec, as was pointed out in the case study.

6.2.5 Review of the case study conclusions during the Final Workshop

There was a general level of agreement at the Final Workshop that in the case of IPv6 deployment, security had to be explicitly considered as part of the business case and subsequent development of new infrastructure using such technology.

The ongoing upkeep and maintenance of a 'dual stack' environment (with IPv4 and IPv6 environments running concurrently), which may introduce new forms of risks was also agreed to be an important issue. Given that the security benefits of IPv6 are increasingly realised the more organisations that use it (a system level issue), the need for policy makers at European level to encourage, or strongly support the use of the new protocol is obvious.

Following recent debate on the neutrality of the Internet ('net neutrality', as demonstrated by the recent United States House of Representatives and Senate Commerce Committee activity) the question over whether IPv6 could compromise such regulations was raised. If IPv6, with its new QoS functionalities, allows the more effective transmission of multimedia and IP packets over mobile networks (thus stimulating richer content delivery and the take up of mobile Internet) then this could compromise any 'net neutrality' regulation that might be enacted (like that proposed by the Democrat Party in their recent amendments to the proposed US Communications, Consumer's Choice, and Broadband Deployment Act). 'Net neutrality' regulations try to equalise the playing field for all types of application (such as voice, data, video or others) and prevent abuse of market power, in particular by infrastructure providers and ISPs. The take up of IPv6 with its provision for treating data for different types of application differently might compromise other efforts to establish net neutrality. Policy makers will have to be aware how general calls for organisations to encourage public and private sector organisations to use IPv6 should be balanced against its enabling ability to compromise 'net neutrality'.

The issue of mobile security (specifically availability) was also highlighted. Although the case study did not include any implementations of IPv6 in a mobile environment, the need to explore challenges arising from the mobile use of IPv6 was clear. For example, when using IPv6 in a fast moving mobile environment (for example with a 3G phone over a wireless interface) there was a great deal of concern over availability when undertaking specific application tasks (as a connection had to be re-established every so often as the device moved from one base station to another). This also served to undermine the end-to-end nature of security that IPv6 is intended to promote.

CHAPTER 7 Conclusions and recommendations

7.1 Overview

At the end of a project with a strong focus on five identified technological developments, the following general conclusions can be drawn regarding initial work and outcomes of the study, with regards to the set-up and outcome of the study.

Firstly, the selected so-called "Disruptive Technologies" are not so much "disruptive" in themselves - the disruption comes with the way they are used or their application.[110] This means that several of the lessons learned apply to a wider set of new technologies that reach the market and may be deployed more widely. When considering the security challenges that come with new technologies it is these issues around wider deployment that need to be taken into account. A focus on "disruptive innovations" as a concept is therefore recommended. Furthermore, more attention needs to be put on what defines a 'good' implementation. Effort also needs to be directed towards trying to pre-empt disruptions, for example via the use of foresight exercises, scenarios planning, awareness raising and multi-stakeholder debates.[111]

Secondly, exploring the issues and impact of "disruptive innovations" based on one case study per innovation means that the results cannot represent the entire suite of issues connected to deployment of that specific technology: the case study focuses on one specific application of it.

Finding the right case studies on the application of these new technologies is not easy. Few "mature" applications exist when considering Trusted Computing and WiMAX, and for RFID and IPv6 case studies do not representing the wider use of the technology in other applications (although the RFID case study does represent the most common use of the technology). Positive experiences with new technologies lead to competitive advantages that are not always eagerly shared. Negative experiences for which solutions have not been found are unlikely to be brought up by the organisation concerned in the case study. From

[110] Christiansen, C. M. Overdorf, M; Meeting The Challenge of Disruptive Change Harvard Business Review: March April 2000

[111] See for instance the work on Cyber Trust and Crime Prevention by the UK Government www.foresight.gov.uk/ctcp

the limited number of case studies carried out, some useful insights can be drawn. Keeping track of new developments and expanding the number of available case studies can therefore play a major role in acceptance and good implementation.

In general, the results from the case studies were well received during the Final Workshop on 30 June in Brussels. Recognising the potential security challenges of disruptive technologies allows better comprehension of what needs to be done to be able to benefit as much as possible from the new opportunities, and avoid taking unnecessary risks. By taking the security challenges into account as early as possible it is possible to steer away from working in an environment in which security is considered as an add-on to an environment where all the issues, including the role of security, are fundamentally addressed from the outset.

Actions to pre-empt and prevent problems arising from new technologies are underway. It is generally felt that we are beginning to understand what needs to be done. Focus should now be on the question of how to accomplish these pre-emptive measures and where the balance lies between the roles of the different stakeholders in designing appropriate and effective policy.

One of the most significant conclusions from the workshop was again emphasised – it is not so much the technology but rather its implementation or application.

This chapter summarises the issues identified in this study and proposes some recommendations on what needs to be done to best manage the security challenges that implementation of these technologies raises in the light of, for example, the recently released communication on Network and Information Security strategy[112] (in the context of the Lisbon Agenda) and the need to encourage trust and confidence in the information society. The results, as discussed during the workshop, are summarised below.

7.2 Overall observations

Based on the case studies we conclude that some security challenges that arise are technology specific, yet we can also conclude that some security challenges apply to multiple, or even all technologies. This section is structured into two parts. Firstly, based on the introductory material and views from the Delphi exercise, we identify security challenges arising from the general implementation of disruptive technology that are not specific to a single technology. Then we describe general security challenges arising from the technologies under review in this study. General and specific policy options at both levels are presented in the next section.

[112] Communication from the European Commission: "A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" COM 2006 251: Brussels 2006

A recent report indicated an important dynamic in the current technological climate of convergence.[113] This refers not only convergence between different technologies in each sector (for example, mobile phones and PCs) but also between different scientific areas. A good example is the way in which biological sensors of the future might employ nanoscale sensors and many technological developments from the world of ICTs. Similarly, nanosciences has the promise to bridge the gap between the biological and non-biological world either via the bottom up manipulation of atoms and molecules or the top down control of physical processes to coerce atoms or molecules en-masse to arrange themselves in a desired location or structure. Indeed, experts have commented that nanotechnologies, as an enabling technology for all sorts of developments in biotechnology, medical, pharmaceutical, engineering, manufacturing and environmental markets, is in itself a 'disruptive technology.[114], Yet the real disruption will come only when the new technology is applied at sufficient scale to make a difference. As this is dependent on the market, both in terms of take-up as in terms of actual application of the technology, it is not always predictable which technologies will become disruptive, and which will not. Security challenges might be:

- Unexpected risks arising from 'mission creep'. As new technologies are implemented, the utility of them grows. This is unavoidable and in a sense exactly what makes such technologies intrinsically 'disruptive'. As the expanding applicability of such technologies increases, new and unknown security issues may arise. For example, who, in the early days of the Internet, would have thought that the problem of 'phishing' would arise to such an extent (as the Internet was assuming to be of no commercial interest at that time)
- Convergence between nanotechnologies, biotechnology, material science and information technology may introduce unexpected multi-disciplinary security consequences (e.g. privacy might be infringed by a country implementing aspects of human genome research) or physical safety might be compromised by telemedicine enabled applications.
- Privacy may be even more at stake. Although privacy (a complex topic but understood at one level as the right to control personal information) may be at odds with security, there may be a need to introduce a common set of principles for privacy as well as information security (e.g. extending or amending the OECD principles). There would also be a clear need for some kind of effective ombudsman or external third party who could be trusted to act in cases where privacy has been breached.technology has breached common privacy guidelines.
- The integrity and reliability of the network will be at further risk as dependency becomes almost unavoidable. Many of the technologies (including those explicitly identified in this report) rely upon a global information infrastructure to one degree or

[113] Silberglitt, R. et al; The Global Technology Revolution 2020: In Depth Analyses - Bio/Nano/Materials/Information Trends, Drivers, Barriers and Social implications TR 303-NIC RAND, Santa Monica, Calif. 2006

[114] The Royal Society Report of Nanotechnology (Royal Society, London, 2004) available at: http://www.nanotec.org.uk

another. We accept that this does not resolve ongoing highly pertinent debates around the ongoing 'digital divide' between the digital 'haves', 'have-nots' and 'don't wants' however, this situation is fast becoming a reality for the more well developed nations in Western Europe (and even for those nations that demonstrate the ability to 'leapfrog' in technological advancement). The increasing integration of different sensor networks, coupled with nanotech enabled infrastructure will mean that the intelligence in the network will become ever more smarter, with the consequence of increasing frailty and fragility.[115]

- Security challenges will arise from social quarters, more so than more harder technological aspects. Consider the example of GM crops, where the technology has existed and the economic case appeared sound, but social and environmental concerns became the dominant focus in deciding the extent of its take up. Similar examples may be seen with stem-cell research (even religious concerns may, as some experts have interpreted, play an important role in the take up of some of these technologies).

The following observations on security challenges to the successful use and deployment of disruptive technologies, can be drawn across two or more of the case studies, beyond the individual findings per case study:

- It is important to include security in the business case when considering the introduction of new disruptive technologies
- The security implications of transitioning from old technology to the new 'disruptive' technology must be properly considered
- Technology forums, standards organisations and industry bodies have an important role to play in highlighting security in evolving disruptive technologies
- The perception of security is an important issue for many stakeholders
- The reliability of infrastructure may be a challenge when using disruptive technologies

It is important to include security in the business case when considering the introduction of new disruptive technologies.

In the case studies of VoIP, IPv6 and RFID the organisations applying these technologies had not done so fully because some felt that the business case was still not mature enough or was not necessary. Organisations had developed limited pilots in a small and controllable environment (such as with the RFID deployment). In the case of VoIP, despite a business strategy of centralisation and simplification, the organisation had not elected to deploy the technology in a widespread fashion due to the absence of a readily understood business case. In the case of IPv6, questions remain over whether the

[115] The workarounds of the development of Border Gateway Protocol, Network Address Translation and Classless Inter-domain routing are all testament to this. For more information see: Handley, M.; Why the Internet only just works; BT Technology Journal Vol 24 No 3 July 2006 Springer Dordrecht 2006

deployment would have successfully passed any acid test of a business case, given that none was required and its deployment was mandated by authorities senior to the case study organisation.

This shows that a considerable amount of doubt exists about proving the worth of deploying disruptive technologies, despite the considerable maturity (in Internet terms at least) of some of the technologies. This is not unusual for 'disruptive technologies' (as organisations will tend to favour the 'sustaining technology' until an inescapable 'tipping point' arrives) but the perception of these technologies from a business perspective may be paralleled in the view of how they contribute to the organisations overall security posture.

This may lead to the poor implementation of disruptive technologies (as illustrated in the concern raised in the Trusted Computing case study, about flawed implementations of TrustZone architectures), which in turn could lead to poorer security posture. Clearly this will have an adverse effect on the overall security of the Single European Information Space, leading to greater risk and a loss of trust and confidence.

The security implications of transitioning from old technology to the new 'disruptive' technology must be properly considered

In the Trusted Computing and IPv6 case studies, the security implications surrounding how organisations transitioning from one evolution of a technology to another were highlighted. For IPv6, the need to keep IPv4 and IPv6 running together until a point where use of IPv6 was widespread enough to take full advantage of its security features, introduces security challenges by undermining the end-to-end nature of the security mechanisms built into the protocol. With Trusted Computing, the case study identified a better solution to the question of transition from the paradigm of a single execution space (where secure and insecure processes exist side by side), to a new model of multiple virtual worlds (allowing process isolation and the creation of many secure execution environments). This was to design only one additional virtual secure world (implemented via TrustZone). This approach could minimise or avoid attendant complexities (and thus potentially greater risks) that mass virtualisation might present and presented a disruptive attempt to devise a solution to the transition from single execution space to multiple virtual execution spaces (as the new technology was a simpler solution to the problem).

Technology forums, standards organisations and industry bodies have an important role to play in highlighting security in evolving disruptive technologies

Some of the case studies illustrated the role that authorities or bodies set up for the common good (such as industry forums and standards bodies), may have in helping to meet these security challenges. These might be regulatory authorities or industry led organisations or independent bodies like the International Standards Organisation (ISO). In the case of WiMAX, the WiMAX Forum, which is the main organisation driving forward the adoption of the standard, was keen that it did not repeat the mistakes of the WiFi Alliance which may have had a significant contribution to the poor implementation of security (as vendors rushed to get poorly secured products to market). Similarly, the Trusted Computing Group who are playing a key role in the establishment of

specifications for Trusted Computing in a number of areas (such as desktop computers, mobile phones etc) have a role in trying to make sure, where possible, that security engineering is up to the task of properly implementing the specifications.

The perception of security is an important issue for many stakeholders

This was one of the main challenges identified in the WiMAX case study and the user perception of WiMAX networks being similar to WiFi was something that required special consideration from those undertaking the pilot (specifically the service provider and vendor trying to illustrate that WiMAX was not the same as WiFi and the relative security features of both). Users had to be informed and educated that WiMAX was more secure than WiFi.[116] Perceptions of security were also raised as an issue in the Trusted Computing case study, as companies that had implemented some form of Trusted Computing system, architecture or specification might improperly deploy it leading to misplaced trust in a device marketed as specifically secure. This is particularly acute in the market for embedded devices (such as mobile phones, PDAs and home entertainment systems), where such technology is much more widespread than the 'traditional' desktop computer. Similarly, with IPv6, the auto-configuration features allow a IPv6 network to be easily implemented without end user configuration. However this could easily be undermined if the system administrator behind the network is poorly trained or more likely, has been forced by legacy IPv4 installations to engineer some workaround between the two versions of the protocol, thus rendering useless the security features that IPv6 offers.

The reliability of infrastructure may be a challenge when using disruptive technologies

With VoIP, reliability is a major concern over distributed geographies when the technology allows a massive degree of centralisation to achieve economies of scale. Even over privately owned networks, the reliability concerns are high and although the economic possibilities offered by centralisation of telecommunications at a regional level are attractive, the risks cannot be underestimated, particularly from a denial of service attack or freak natural phenomena such as the 2005 Asian tsunami. Despite the hype, VoIP is still only regarded as suitable for home user communications, where best effort transmission is acceptable – until IPv6 becomes deployed on the public Internet allowing more certainty about the transmission of VoIP traffic it seems that VoIP will be mainly a consumer / end-user phenomenon.

The challenge is true of RFID where data (at present mainly logistical data such as the whereabouts of tools, in the example of the case study) is passed over the public Internet. How to assure that safety critical data arrives when it should over a best effort network is a question that should be of some importance to any organisation deciding to implement a

[116] This has an interesting psychological effect as with wearing seat-belts, the more secure people feel, the more they are inclined to act recklessly

complete RFID architecture using elements of public IP networks for data transmission.[117] Of course, with the increasing use of personal data in any RFID system, further questions will no doubt become obvious.

Systemic questions of reliability were also present in the WiMAX study but from the perspective of the end user, who had to be educated as to where to install the equipment to maximise the reliability of the connection. Such self install Customer Premises Equipment CPE) (typified by the ever increasing popularity of WiFi home networking solutions) is at the forefront of driving the boom in consumer take up of ICTs and is a significant factor in broadband deployment. However, if the confidence of consumers must be retained then means to educate them about reliability in all its forms (for example in the placement of equipment) must be high on the agenda of vendors and service providers.

7.3 Policy Recommendations

At a general level, policy options must address the increasing convergence of different sorts of technology (for example, biotechnology and nanotechnology) to deliver unique applications (such as highly targeted clinical interventions). As these technologies become more bound up with human evolution, reaching into every aspect of our lives, policy must adjust to provide appropriate levels of safety. Such adjustments must be technologically neutral – although this is easier said than done (as regulation and the law will inherently lag behind faster paced technological change) policymakers might consider the use of sunset clauses in regulations or laws, to ensure that they get regularly refreshed in order to keep pace with the changing social, political and economic, and environmental climate.

Research and development observatories such as the European Observatory on Health Research Policies and Systems provide a good model for providing a pan-European view on the effectiveness of different health research – this approach could be utilised in trying to better understand the multi-disciplinary social and economic implications of new disruptive technologies (not just information technology) across Europe.

Clearly the role of industry is important as many of these technological advances are industry led. Policy makers should seek to encourage dialogue between industry and governments, at national and also pan-European level, regarding the applications of new technology and security issues arising from not only specific information security issues, but also broader social and economic considerations.

The multidisciplinary nature of innovative technological development, coupled with growing convergence between the different areas, may require that policy makers incorporate a wider conceptual view of network and information security – moving from simply information security to information assurance, a much more holistic view which can accommodate social and human issues as well as the harder technical concerns.

[117] The same concern was raised about data being transmitted over the Internet in Supervisory Control and Data Acquisition (SCADA) systems where electronic networks are used to pass around control information for electric power stations, energy transmission systems, public utilities, telecommunications networks etc

7.3.1 Overall policy recommendations

The following policy options are put forward, in the context of the i2010 objectives and the recently released strategy for a Secure Information Society: "Dialogue Partnership and Empowerment".

Awareness of disruption: As can be seen from the growing convergence between different scientific advancements in various technologies (nano-technology biotech, materials science as well as information technologies), disruptive technologies may evolve in ways that cannot be easily predicted based on past experiences. Particularly where the disruptive application of such technologies presents a challenge: perhaps from a pure security perspective but also from a social or political perspective, it will be worth having some mechanism to explore these challenges, codify them and form an evidence base for developing policy intervention.

Policy recommendation: awareness of potential for technological applications to become disruptive can be increased via the use of Horizon Scanning and Foresight exercises. The essence of horizon scanning is identifying the major dimensions of the future that may influence our lives, and then establishing which policies, delivered in a timely fashion, may favourably alter the situation. at the right time may make a difference. Depending on the breadth and depth of the scan—which in turn depends on the topic of interest—the issue to be addressed may be one of the influence of a new technology or technologies, important societal developments, or changes in the natural environment. A key characteristic to this activity is a search for the potential drivers of change; because this future horizon is inherently uncertain and multidimensional, reliance on one or only a few points of focus on this horizon will not be sufficient. The drivers of change are rarely fully controllable and typically only partially controllable. The changes to be understood may be almost continuous, each so small as to be barely perceived, or they may be discrete events. They may be natural changes, those made with intent or the by products of other directed changes.

In this way horizon scanning can be seen as an early component of a Foresight exercise. Foresight is based on insights originating from a horizon scan, that examines what the potential exogenous change might be, the relationships between those social, technological, economic, environmental and political aspects identified on the horizon, and those which may be affected by policy. Horizon scanning also identifies those factors that themselves may be subject to change as a result of a policy shift. The next step of a Foresight exercise is to construct potential levers of policy action in order to try to steer the course of history away from undesirable aspects and towards desirable aspects of the future. Such activities would need to involve stakeholders from the research and applied sciences community as well as industry and of course policy makers in order to adequately scope any upcoming likelihood of a certain technology or group of technologies becoming disruptive. These activities must also include representatives from other fields of research in order to investigate multi-disciplinary aspects of evolving future technologies and innovations.

Risks of disruption: The first realisation was that as we have seen, disruptive technologies show enormous promise but with that also comes a great deal of investment and also risk, not only to the market (from definition this study started with) but also to those organisations implementing them. In order to reduce the overall risks, government can play a role where a societal benefit is expected, even if the market is not willing to pay for it.

Policy recommendation: Risks can be reduced by support of (pre-competitive) research, not only on technology development itself, but also on implementation issues and impact. Other measures can include regulation (avoid misuse, certification), stimulation of standardisation, certification, and awareness raising.

Implementation requires involvement of all stakeholders in the value chain: In any policy formulation, all participants, not just the incumbents, must be taken into account. This means that existing and future market players (not just those present when policy is designed or implemented) must be considered – as we have seen the disruptive application of new technology can include creation of new markets as well as new business models emerging in existing markets. Whereas this leads to innovation (at least in services and application of technologies) government may feel the need to ensure a less disruptive transition towards new markets and business models, in order to ensure adequate continuity of provision of certain services to avoid societal disruptions.

Policy recommendation: Define critical infrastructures and their required minimum level of operation, thus to know when specific (regulatory or financial incentives) measures need to be taken in order to ensure protection of the functioning of those critical infrastructures.

Pursuing sustainable growth and employment: In the context of i2010, ICTs are seen as the engine for sustainable growth and employment. Trustworthy and secure ICTs are seen as vital enablers to this outlook.

Policy recommendations: A number of potentially useful actions were identified that could help realise the Vision by 2010, with regards to the five technologies explored. These include:

- **Ensuring justified trust**: informing all sectors at all levels about the security challenges and the policies in place to address those in a coherent way, as well as about specific measures citizens and business can take in implementation of the explored technologies to ensure that security challenges are adequately met, and unjustified risks will not be taken;
- **Stimulation of good implementation**: it was suggested to consider a strategy for wide deployment of IPv6, facilitation of WiMAX deployment and development of a positive regulatory environment stimulating the development and implementation of new Ambient Intelligent infrastructures;
- **Prevention through the integration of security in information systems**: by building in security requirements already in the design phase of new products and services, these will be more secure, by definition. By defining minimum levels of

security for new products or services, possibly via certification of "good practice", nasty surprises can be avoided resulting from innovative use of any of the five explored technologies and services. Additionally, governments could use their purchasing power (particularly in the context of new e-government developments) to require better security in new ICTs.

- **Risk assessment and protection mechanisms:** may include, but should not be limited to, improvements in law enforcement measures (legislation, law enforcement capability) to deal with challenges that the disruptive application of new technologies presents (such as identity theft, monitoring and breaches of privacy).

7.3.2 Role of the European Commission

Furthermore, it was seen that the European Commission could play a useful role in stimulating good practice in the implementation of disruptive technologies. For all of these points the intervention logic is based on the trans-European character of the issues, and of the specific measures addressing those. The following policy support was highlighted as being useful and important:

- **Large scale demonstrators**: The support of pilots and demonstrators to exchange experiences in deploying disruptive technologies. European level investment is justified by the border-independent character of the explored technologies and services, and it was recognised that exploring possible disruptive effects to the market would possibly lead to early identification of issues;
- **Exchange of good practice and standardisation**: Support and encouragement of industry forums, task forces, standards bodies, to include security in their specifications of good practice and standards is a role that could be usefully played at European level. It was recognised that some of the "established" bodies may need to adapt their ways of working towards the changed structure of governance and markets, and new technologies, or make place for new bodies taking these new circumstances into account from the outset;
- **Learn from industry practice**: In particular international business has already had to address security issues over the years, across borders. For instance banks, but also in other industry sectors, valuable experience has been obtained that could inform a better understanding of how security is treated in the deployment (disruptive or not) of new technologies;
- **Ensure avoidance of the emergence of a monoculture:** where one product or solution dominates an ICT market. In a sense this is about promoting measures in the market to allow disruptive innovations to flourish, in the pursuit of a heterogonous and therefore more robust single European Information Space;
- **Continue to support pre-competitive Research and Development** in security technologies so that technological development can be brought from scientific investigation into the market to better secure the benefits of the disruptive application of new technologies;

- **Education and training** to deal with disruptive technologies is an important way to better help those consumers or end users implementing or using disruptive technologies to become aware of the security ramifications;
- **Clarify legal implications and responsibilities:** Not only with regards to continuing debates over access to cryptographic keys, but also regarding whether the law is currently adequate to deal with the challenges to privacy that RFID pose, or that market regulations are appropriate in dealing with the restructuring of the telecommunications landscape with widespread WiMAX or IPv6 deployment.

7.3.3 Specific policy recommendations for each technology

VoIP: In conclusion it can be said that widespread VoIP application is achievable, and their application has not led to few specific security concerns. The major disruption is much more towards the business model of voice telephony delivery: old business models based on the circuit switched PSTN, and by the minute charging (with premium charges for cross border connections) are no longer feasible.

However, those businesses providing communication services have mostly recognised the emergence of new ways of delivering services, and government intervention is not necessary to ensure that these services will continue to exist: the market addressing these needs is extremely dynamic. New security policy measures are not called for.

Trusted Computing: It is clear that trusted computing is not yet in great evidence in the organisational setting, although DRM applications continue to grow (for example in online media applications for the consumer). Its application so far seems to be focused on protection of Intellectual Property Rights (IPR). Sometimes this leads to applications that place barriers in the way of the user experience, but from a market perspective it is an enabler of business models exploiting IPR and thus stimulating innovation.

As the presence of these technologies and the impact they have on the application is not always clear, users are sometimes confused or unaware of this technology. A clear indication of the presence of Trusted Computing technologies, their purpose and any impact on the functioning of the application would allow end-users to make more informed decisions. Regulation to require such information could be considered.

WiMAX: At present there are not a many properly certified WiMAX applications present in the market, although there are a number of trials and demonstrators ongoing. As the standards evolve more equipment is likely to become certified and business models develop. WiMAX is one of the most disruptive innovations in terms of its impact upon the market due to the potential market destabilisation for communications service providers.

At present, with the standards and certification bodies still developing standards and equipment manufacturers in the early phase of bringing fully WiMAX certified equipment to the market, no immediate policy changes are required, save for creating a positive environment for the deployment of this technology and monitoring developments. However, it will most certainly be necessary to review policy when and if widespread WiMAX deployment occurs. Regulatory authorities and governments should be ready to act.

RFID: Whereas RFID has already existed for many years, wider application of RFID for identification of objects (as discussed in the case study) or persons is extremely likely to affect the availability of data on these objects or persons.

For the case study (an application to easily track and trace specific high value objects) no specific policy measures seem to be needed. However, when this technology concerns people (citizens or consumers), it is clear that measures will be needed to ensure the privacy of people directly or indirectly using such tags.

IPv6: Across the world, numerous IPv6 pilots and demonstrators exist, although some vendors have not been clear in their support of its new security features. It is obvious from the case study that IPv6 has the potential to improve the resilience and security of the infrastructure. National level strategies are an important context for such demonstrators and should stimulate supply.

The case study illustrated how a national mandate for IPv6 deployment can spur the development and implementation of this technology. Work on IPv6 roadmaps and strategies should be supported at national and regional levels. Specifically, the European Commission should consider the viability of strongly encouraging the creation of IPv6 deployment strategies at European and national level amongst the member states. There is also scope for policy to encourage vendors to include the security functions of IPv6 as standard in their implementations.

REFERENCES

References

General References

Clayton M. Christensen, *The Innovator's Dilemma*. Harvard Business School Press 1997

European Commission, Communication from the European Commission COM 2005 (229) – "i2010: A European Information Society for Growth and Employment"; European Commission (1st June 2005) Brussels 2005 available at: http://europa.eu.int/information_society/eeurope/i2010/docs/communications/com_229_i2010_310505_fv_en.doc

European Commission Ambient Intelligence, DG Information Society and Media; European Commission (11th March 2004) Brussels 2004 available at http://europa.eu.int/information_society/policy/ambienti/index_en.htm

European Commission Communication from the European Commission COM 2006 (251) – "A Strategy for a Secure Information Society: Dialogue Partnership and Empowerment"; European Commission (9th June 2006) Brussels 2006 available at: http://ec.europa.eu/information_society/doc/com2006251.pdf

Voice Over Internet Protocol

Alan Jebson, Group Chief Operating Officer, HSBC Holdings: IT Strategy, (HSBC, 2003) available at: http://www.hsbc.com/hsbc/investor_centre/ (visited 23/03/2006)

General Datacomm Customer Profile: The HSBC Group

CISCO Call Manager product brochures: CISCO, 2006 available at: http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/index.shtml (visited 26/04/06)

KPMG, "VoIP: Decipher and Decide: Understanding and Managing the Technology Risks of Adoption", KPMG, Sydney 2004 available at: www.kpmg.com.au/Portals/0/irm-voice_over_ip_report_2004.pdf (visited 24/04/2006)

QSIG home page at http://www.ecma-international.org/activities/Communications/QSIG_page.htm (visited 26/04/06)

Stephen Green, Group Chief Executive, HSBC Holdings plc, Presentation to Morgan Stanley European Banks Conference, London, 22 March 2006 available at http://www.hsbc.com/hsbc/investor_centre/ (visited 23/03/2006)

The Policy Implications of Voice over Internet Protocol", Working Group on Telecommunication and Information Services Policies, OECD, 13 February 2006, available at http://www.oecd.org (visited 23/03/2006)

Voice over IP Security Alliance, *Voice over IP Security and Privacy Threat Taxonomy version 1*, 24 October 2005, available at http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf (visited 23/03/2006)

Trusted Computing

AMD Secure Execution Mode: available at http://www.amd.com/us-en/Weblets/0,,7832_11104_11105,00.html (visited 29/03/2006)

ARM Annual Report and Accounts 2005: ARM, Cambridge 2005

Intel LaGrande Technology: http://www.intel.com/technology/security/ (visited 23/03/2006)

Press Release: New ARM API Reduces Development Time and Cost for Mobile and Consumer Security Applications: ARM, Cambridge, 07th September 2005

Press: Release: ARM and Trusted Logic Develop Trust-Zone-Optimised Software To Increase Security for Mobile Industry: ARM, Cambridge, 14th July 2004

Press Release: Texas Instruments and ARM accelerate Deployment of Secure Applications to Mobile Devices: ARM, Cambridge, 4th April 2006

Mobile Telephones (Reprogramming) Act 2002 available at: http://www.opsi.gov.uk/acts/acts2002/20020031.htm (visited 23/03/2006)

Microsoft's Next Generation Secure Computing Base: http://www.microsoft.com/technet/archive/security/news/ngscb.mspx?mfr=true (visited 23/03/2006)

Ross Anderson, Trusted Computing FAQ, available at: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (visited 23/03/2006)

Trusted Computing Group Frequently Asked Questions available at: http://www.trustedcomputing.org (visited 23/03/2006)

Tiego Alves and Don Felton, TrustZone: Integrated Hardware and Software Security: ARM White Paper; ARM, Cambridge, July 2004

TrustZone System Design overview: ARM, Cambridge, 2006 available at: http://www.arm.com/products/esd/trustzone_systemdesign.html (visited 23/03/2006)

TrustZone Overview: ARM, Cambridge 2006 available at: http://www.arm.com/products/esd/trustzone_home.html (visited 23/03/2006)

WiMAX

Airspan Networks Corporate Overview available at: http://www.airspan.co.uk/investors_home.html

Airspan – Products – EasyST Overview: Airspan, Uxbridge, 2006 available at: http://www.airspan.co.uk/products_group.aspx?ProductGroupID=1&ProductID=6

Airspan – Products – AS.MAX Overview: Airspan, Uxbridge, 2006 available at http://www.airspan.co.uk/product_downloads/ASMAXBROCHURE.pdf

PIPEX 2005 Annual Report available at: http://www.pipex.com

Matt Hines, Worried about WiFi Security? News.com 19/01/2005, available at: http://news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html (visited 24/04/2006)

David Meyer, Photos: WiMAX in Action ZDNet 22/06/2006 available at: http://news.zdnet.co.uk/communications/wireless/0,39020348,39276473-8,00.htm (visited 01/07/2006)

"The Implication of WIMAX for Competition and Regulation", Working Party on Telecommunication and Information Services Policies, OECD, 2 March 2006 available at http://www.oecd.org

WiMAX Forum: What is WiMAX? http://www.wimaxforum.org

Press Release: The WiMAX Forum™ Showcases Equipment and Breadth of Applications, Opens Test Lab available at http://www.wimaxforum.org/news/press_releases/WiMAX_VancouverRelease_FINAL_07_12_05.pdf (visited 20/04/2006)

RFID

Airbus website, Toulouse, 2006: available at: http://www.airbus.com/en/airbusfor/analysts/ (visited 29/03/2006)

Airbus press release, Airbus applies RFID technology to supply of aircraft spare parts, 18 September 2003

Airbus, RFID, Radio Frequency Identification, Supporting the aircraft supply chain

LogicaCMG, Case study: Airbus takes RFID into the spare parts supply chain: available at: http://www.logicacmg.com/pSecured/admin/countries/_app/assets/airbus_casestudy-3292006.pdf (visited 29/03/2006)

LogicaCMG, RFID in the aviation industry: RFID in the aviation industry by LogicaCMG and SAP, Hong Kong, 10 and 11 August 2004

PRNewswire, LogicaCMG and Airbus Reach New Heights in RFID, News Release, 10 August 2004

IPv6

Brent Rowe, 2006. Interview. Arlington, Virginia, February 10.

Defense Research and Engineering Network Definition 2006. High Performance Computing Modernization Program, July 8 2004: available from http://www.hpcmo.hpc.mil/Htdocs/DREN/dren-def.html (visited 29/03/2006)

Dimitri Bersekas and Robert Gallager. Data Networks. Second ed. Englewood Cliffs, New Jersey: Prentice-Hall, Inc. 1992.

Glen Mackie, To see the Universe in a Grain of Taranaki Sand. Swinburne University of Technology, Melbourne Australia, February 1, 2002 1999: available from http://astronomy.swin.edu.au/~gmackie/billions.html (visited 24/04/2006)

John Baird. DREN IPv6 Pilot Network. Paper read at Supercomputing 2004, November 8-11, at Pittsburgh, Pennsylvania.

John Osterholz. Building the Foundation for Transformation: Net-Centric Operations and IPv6. Paper read at U.S. IPv6 Summit 2003, December, at Arlington, Virginia.

Justin Blount, Technical Report: IPv6 testing using DREN test bed. Army Research Laboratory 2002: available from http://www.arl.hpc.mil/PET/intern/intern01/justin/justin.html (visited 29/03/2006)

Michael P Gallaher, and William A. Jeffrey.. Technical and Economic Assessment of Internet Protocol Version 6 (IPv6). Alexandria, Virginia: National Institute of Standards and Technology, U.S. Department of Commerce, 2006

Michael P Gallaher, and Brent Rowe, IPv6 Economic Impact Assessment: Final Report. Research Triangle Park, North Carolina: RTI International, 2005

Phillip Dykstra, DREN Overview. Paper read at JET Roadmap Workshop, April 13-15, at Jefferson Lab, Newport News, Virginia, 2004

Ron Broersma, IPv6 on DREN & Status of DoD Pilot. Paper read at U.S. IPv6 Summit 2003, December 17, at Arlington, Virginia.

R.V. Dixon, IPv6 in the Department of Defense. Paper read at North American IPv6 Task Force Summit, June 23-272003, at San Diego, California.

Silvia Hagen, IPv6 Essentials. Sebastopol, California: O'Reilly Media, Inc. 2002

APPENDICES

Appendix A: Case Study Framework

This appendix provides the results of the process leading to the creation of a common approach to research frameworks to be applied to five case studies depicting the security challenges of the implementation of the five information technologies: VoIP, Trusted Computing, WIMAX, RFID and IPv6. The need to devise this common approach to research frameworks was due to the fact that this project espouses a multiple case study methodology. In this context, similar sets of data among the five case studies need to be collected in order to avoid evidence discrepancies and consistency.

In devising this common research framework, RAND Europe has undertaken two interlinked activities: a Delphi exercise and expert workshop. This two-stage process was required since this project addressed the security challenges of these new technologies. This situation required that RAND Europe engage in the process leading European experts both from a distance and through a workshop in order to get the most comprehensive and methodologically correct research framework for the collection of case study data. RAND Europe's final objective was to gather solid and robust evidence upon which to formulate policy options on behalf of the European Commission in its efforts to implement its i2010 initiative.

Pre-workshop Delphi process

A Delphi exercise is a way of forecasting the challenges and likely futures associated with an issue through the knowledge of experts in the field.[118] In the context of this project, the exercise, which consisted of two different phases, aimed at the identification of main security challenges associated with implementation of the five technologies.

Results from the first stage

The first stage of the DELPHI exercise started in mid December 2005 when RAND Europe asked 27 internationally recognised experts the following question:

"What are the key shared security challenges to the use and deployment of the five technologies mentioned above?"

[118] The literature on Delphi is quite large. For an interesting starting perspective, see Donal Pyke, A Practical Approach to Delphi", *Futures*, n.2 June 1970. Regular articles about the applications of DELPHI methodology for assessing new technologies are published in *Long Range Planning* and *Futures*

They were asked, in particular, to produce a list of security challenges and, if possible, to provide general comments in a concise format by mid-January 2006. Of the 27 invited experts, 15 of them responded providing RAND Europe with a list and set of comments. Afterwards, these were examined in order to eliminate duplicate findings. It is interesting to notice that those who responded went merely beyond the technology and addressed a large variety of socio-economic, regulatory and economic challenges, including privacy, operational risk and consumer protection. Moreover, some of the security challenges were not obviously applicable to all five technologies but deemed useful in stimulating discussions. In order to simplify the overall process, RAND Europe reunited similar challenges into groups. These groupings are understandably vague and difficult to prioritise. This was because of the wide variety of responses returned to the study team and the need to return a manageable list for the next phase of the exercise. Whilst this grouping was undertaken by security experts within RAND Europe, a great deal of effort was made to explain, at every available opportunity, what these broad groupings represented and what sort of challenges came under them. These are reflected in Table 3.

Table 3: Grouping of first stage Delphi results

Challenge identified	Groups
Monitoring of sensitive items Tracking of individual items Physical tracking Loss of location privacy	**Monitoring of items and people**
Monitoring customer use Confidentiality Harvesting personal information Interception of voice calls Consumer protection	**Invasions of privacy**
Effective testing of software Effective testing of hardware Fixing breaches caused by malware is difficult because the system is too secure Compromise of CPU keying algorithm which implies high redeploy cost De-confliction of radio frequencies	**Hardware, software and system design**
Use of encryption Use of security protocols Software vulnerabilities	**Use of security mechanisms**
Infrastructure vulnerabilities Vulnerabilities of large and critical infrastructures Weak security easy to break into	**Vulnerabilities**
Tag counterfeiting / copying of data Interception of messages Spoofing Call redirection Hiding of sources of attack in 'black' or unused address space Identity theft Denial of service Man in the middle attacks (OTA)	**Misuse of information and data**
Usability of new technologies Poor usability implies poor security (but the reverse is not true either)	**Usability**
Homogenous digital eco-system Reliance upon Internet for voice and data Dependency on common Internet infrastructure	**Dependency upon technology**
International standards Sovereignty of network resources Co-ordination of security investment Off-shoring	**Legal and policy drivers**
Increased difficulty for those dealing with abuse of the network	**Responding to misuse**
Consumer rights on levels of trust Binary trust not complex enough to deal with heterogeneous environment	**Trust**
Data authenticity Data integrity Security for business use No global PKI	**Security requirements**
Reduction in consumer freedom and choice Citizens trust in digital signatures	**The role of the consumer**
Transition scenarios and their security Boundaries of expansion of RFID applicability Authorisation of access to RFID	**Governance of information technology**
Monopoly of software companies forcing out small companies Vertical monopolies (e.g. SkyTV)	**Market environment**
Difficulties in cross network collaboration due to DRM technology	**Social and philosophical**
New technologies making existing security mechanisms less secure New technologies making existing infrastructure more vulnerable	**Transition to new technologies**
Shift of security responsibility to end users	**End user security responsibility**
Users tracking & ownership of logging data across multiple domains	**Tracking data and ownership across multiple domains**
Reliability of government operations Availability of network Continued stability of the network	**Reliability of technologies**

Results from the second stage

The second phase involved experts rating the groups of security challenges identified in the previous stage with 1 being the maximum and 10 the minimum, Of the 15 experts that responded to the first phase, 10 proved the ranking as follows[119]

Table 4: Expert ranking of groups of security challenges

Participant	1	2	3	4	5	7	8	9	10
Monitoring of items and people	3	3	1=		4=				
Invasions of privacy		9	1=		7=	4	5	2	1
Hardware, software and system design		2	9=	9		7	8	6	
Use of security mechanisms	6	8		6			7		4
Vulnerabilities		4	4=	7	4=	5	4	3	4
Misuse of information and data	9	7	1=		1=				
Usability	4	1			1=				
Dependency upon technology		10			7=				
Legal and policy drivers	5	5	8=						
Responding to misuse		6				5		4	
Trust	1		4=	4		4	4		
Security requirements		7	8=	8			8		8
The role of the consumer	10	10			7	10	8		7
Governance of information technology				10				7	
Market environment	7			5					
Social and philosophical									7
Transition to new technologies	8		9=	2	7=				
End user security responsibility					4=			6	
Tracking data and ownership across multiple domains	2		4=		1=			4	
Reliability of technologies		10			10		10	10	

It is evident from the results of this exercise that no single security challenge was consistently rated highest. There was a wide variation amongst participants about the relative importance of each of the challenges. However, one or two limited conclusions could be drawn. Intangible issues like trust and usability were rated highly by the majority of participants. Monitoring of items and people were also rated highly. Rated least important was transitioning to new technologies (from old incumbent technologies) and defining specific security requirements.

[119] Where some participants had scored challenges equally, they were classed as 'joint' and the subsequent level excluded. So for example, if one participant had ranked two challenges as third most important, then the next challenge would have been ranked as being 5th most important.

Workshop

The intended aim of the workshop was to bring together the experts that participated in the Delphi exercise to comment the results of these activities and develop a common approach to case study research frameworks.

Workshop approach

Held in the Cambridge offices of RAND Europe in 7 February 2006, this one-day workshop was split in the following sessions:

Session 1. Developing the business environment for disruptive technologies

Session 2. Overview of the results of the DELPHI workshop

Session 3. Brief description of the case studies

Session 4. Breakout sessions for discussions on each technology

Session 5. Conclusions

The main method used to facilitate discussion was via the use of 'hexies' a device that allows participants to link and cross reference ideas between two concepts. Large 'hexies' were used to represent the technologies and then the participants were led through a moderated discussion where they identified related concepts in the context of the business environment. These were then surrounded and the moderators tried to relate the concepts to each other. Once of the interesting research side effects of this process is that if the concepts have something in common (in this case they are all disruptive) then as the discussion goes on, the breadth of discussion decreases, until the participants are going over points already made. This provides a useful cross referencing mechanism to ensure that a robust set of data is being gathered.

Themes from the business environment

During the first three sessions, it was evident participants wanted RAND Europe to consider the security challenges of these technologies within their business and commercial context, with a particular focus on the business model for their use.

With *Trusted Computing*, participants identified that its success would be entirely dependent upon the complex ways in which users interact and how the dynamic of users is evolving with the changing ICT environment (for example, more embedded systems, more and more powerful personal computing capabilities). The power relationship, it was thought, would change significantly between technology provider, service provider and end user. This was relevant for the world of mobile phones. The concept of a trusted node was found to be somewhat vague as it had a lot in common with the idea of identity. Trusted Computing was also a worrying development from the perspective that it may create a false sense of security in the users, and depending on its implementation, they may be more willing to act recklessly if they are using computing technology that is Trusted Computing capable.

Participants viewed that there was a significant difference from the perspective of defining what a trusted system was: some people may have thought that they were getting a high

trust system but in actual fact a TC capable system is highly secure and therefore, it could be argued, not as effective. There was a view that the business model for Trusted Computing was likely to fail in the marketplace, due to the user complexities involved. Finally, differences in culture needed to be taken into consideration – for example, in many countries it is the norm to share content and breach copyright. Irrespective of these issues, participants clearly indicated the need to consider any of the issues associated with TC in light of their business and technical settings.

The discussion then moved to *IPv6*. Participants started by stating that this was not a technology. Many of the functionalities of IPv6 existed in IPv4 but these were optional. The increasing popularity of IPv6 would lead to a new form of address based governance whereby each device having an IP address would mean that new governance models would need to be defined. The qualities of IPv6 that allows auto-configuration and '0' configuration were identified, as was its 'plug-and-play' characteristics and the ability to more easily create linkages between organisations. These easy installation aspects were seen as a major learning factor, particularly for some of the larger software companies.

Participants, moreover, observed that the existing IPv4 infrastructure allocating IP addresses via Network Address Translation (NAT) has security qualities that may be compromised by the wholesale introduction of IPv6, where each device may have an IP address. Moreover, the widespread capabilities of IPv6 for holding information about the sender and or recipient should not lead to identity being needed for every transaction. Indeed, in many cases all that is required is simply authorisation.

VoIP was a form of technology that had unique qualities in regard to usability. Participants felt that a great deal of user awareness is needed concerning availability e.g. where a power supply goes down, then in the case of a VoIP telephone system, there would be no telecoms connectivity. Therefore, voice calls passing over data networks has to be treated from an implementation perspective very much like data communication, although more careful security practices needed to be set up to try and maximise the same level of availability as the 'old' PSTN.

Quality aspects regarding VoIP were also discussed – specifically, how voice quality was the main consideration, particularly in tense situations such as negotiations and sensitive business dealings. It was pointed out, however, that the tolerance for poor quality has gone up with the increased use of mobile phones and other developments. Technical considerations such as bandwidth were also an issue since, for example, on a wireless network with limited access, it may be possible only to provide services to a few users at a time, and usability will then suffer. Finally, applying the regulations and rules of the 'old' PSTN to VoIP was also cited as a concern. For example, how will free access to emergency numbers be managed? Will this still be possible?

With *WiMAX*, the main concerns identified were regulatory in nature. These included the potential for lock-in of the end user from the perspective of the hardware provider, software provider and service provider. Similarly, the end user may get locked in as a result of choice: the wealth of choices available may confuse the end user and similarly lead to 'lock-in'. The need to have some form of business agreement with an infrastructure provider was also highlighted – providing WiMAX infrastructure was not cheap and therefore the business model relies upon having an infrastructure provider as a partner in

any deployment. Finally, the user requirement for easy set up and installation and 'no-fuss' connectivity was also identified as a major business driver.

WiMAX was also a good example of how a disruptive technology must be harnessed to the advantage of any company wishing to deploy it – not merely as an experimental test but as something to bring real business advantage. This is particularly well illustrated with Google, which is piloting a fibre connected mesh network in the United States using WiMAX technology, to provide every home in a city with wireless access.[120]

RFID was a much more contentious issue. The security benefits of using RFID, for example to connect baggage to a passenger ticket in an airport are clear. The benefits of RFID in the consumer foodstuffs industry were also highlighted, where RFID might alleviate a great deal of food being disposed of (by creating greater efficiencies). However, the privacy issues with this technology still must be understood. It was observed that the potential fear of RFID came from the possibilities of it being used to facilitate intrusive direct marketing and invasion of privacy. Nevertheless, the experts also suggested that RFID has to be examined within supply-side situations where issues of data availability and integrity were extremely important.

Three important keywords identified with the RFID debate were persistence (identifying the longevity of the data on the RFID system); linkage (how data can be linked between RFID and other systems); and finally visibility (who knows that the RFID chip is present and who has access to what information on the chip). This last issue related to consumer awareness again – specifically it was observed that in some cases people did not know what to do with the technology and wanted to abdicate responsibility for decision-making to someone else. Finally, performance was still seen as an issue with RFID, particularly with regard to real-time processing operations.

Having discussed the business perspective of each technology, the experts concluded that the case-studies were not only to focus on the security challenges. Instead, it was important to understand the overall business and commercial context leading to the implementation of these technologies and, afterwards, assess the security challenges.

They also emphasised that disruptive technologies were at the forefront of a changing dynamic between the user, provider and technology vendor, a situation leading to a set of new security challenges. The fact that switching costs (the cost of a user moving to a another provider or telecommunications network, for example) were being made deliberately high was evidence of the ownership model changing to value being obtained via "ownership" of the user (whereas before it might have been the hardware or software). This has an important ramification for security, as it means that the notion of responsibility must change as the model of ownership changes.

Some specific security problems with the disruptive technologies were then identified – for example, TC is perceived to be controversial as some consider it to increase switching costs for the end user by making it more difficult to change operating systems. Additionally, the

[120] Alan J Weissberger Google and Earthlink bid to provide city-wide WiFi to San Francisco WiMaxxed 28th March 2006 available at http://www.wimaxxed.com/wimaxxed_news/20060328/google_and_eart.html

quality issues in respect of VoIP have ramifications for certain applications – for example in the highly regulated insurance industry or in a trading floor environment in a bank.

Case Study Research Frameworks

The last session of the workshop involved two breakout sessions where experts were asked to provide detailed suggestions about the research framework for each case study. In particular, they suggested a set of questions to ask that would have been interesting and useful to explore during the case studies. These are repeated in the next paragraphs.

Overall security challenges

IPv6

- What drove the adoption of Ipv6?
- What were the business goals?
- What, if any, unintended limitations have appeared?
- What sort of security issues were you looking for IPv6 to help protect you against?
- What do you consider to be the security benefits of the deployment of IPv6?
- How have you implemented governance of the network address space with IPv6 within your organisation?
- How widely are you enabling use of IPSec?
- Are you pushing specific features of the autoconfig capability of IPv6?
- How does interoperability with other security tools work with IPv6?
- What is the perception of the user to this technology?

VoIP

- Why did you implement this technology?
- Please explain the business motivation for doing so?
- What user group was this implemented for? Executives? What sort of staff level? What were the reasons behind this decision?
- What cost savings do you expect to realise?
- Have you done a Risk Assessment for its implementation?
- Do you have any concerns over telephone tapping / eavesdropping with your new architecture? How are these being met?
- What are your data retention policies and how have these changed since you have implemented your VoIP solution?
- What is the nature of your architecture of your implementation?
- What technologies do you use for backup? Do you resort to the PSTN?
- What measures have you taken to undertake anti-DoS capability?

- What level of trust do you place in your VoIP service – both in a functional way but also in a usability way (e.g. for traders using it for delicate negotiations)
- How has your relationship with your telephone provider changed since you have begun to implement VoIP? How do you see them now? As unnecessary?

Trusted Computing Base / Trustworthy Computing

- What drove the deployment of TCB?
- Have you taken any steps to quantify or measure the benefits?
- What assessments have been made as to the specific risks and benefits to ultimate consumers?
- How would you quantify the risk from a technological perspective? How much can this be done?
- What measures have you put in place for authentication / to support authentication? Specifically attestation of the device.
- Have you considered how the initiation of civil or criminal investigations might be altered with data stored on a TCB?
- How have you made provision for dealing with the consequences of a failure of a TCB enabled chip?
- Is TCB deployment driven from business aspects not the end-user or consumer?
- Have you considered the likely changes in user behaviour if they think that their machines are now secure and how this may alter the dynamic of security of the machine?

WiMAX

- What were the business and operational objective associated with the case study?
- What is its availability and scalability?
- What type of applications are allowed through the channel?
- Are you looking for wireless location based services?
- Do they address confidentiality, integrity and availability?
- Is there authentication and encryption? Are they aware of security issues? Do they educate users?
- What happens if the provider or the user uses different hardware (interoperability – user lock-in)?
- What is the coverage? How much planning was put into the infrastructure?
- What anticipated and unanticipated needs are recognised?

RFID

- How reliable are the devices used?

- How does this fit within the commercial and operational objective of the organisation?
- What about integrity and authenticity? Is there a false sense of security/accuracy?
- What is being done with the data? How is it analysed? What other attributes are connected to the data collected?
- What is being done about data integrity?
- What kind of risks have you encountered in the implementation?

Expert participation

The following list details the experts that were invited to participate to the DELPHI exercise.

Table 5: Expert participants in the Delphi exercise

Name	Affiliation	Phase 1	Phase 2
Danilo Bruschi	Professor, Computer Science, State University of Milan	√	√
Uwe Bendistch	SIT Fraunhofer Institute		
Ian Brown	Co-ordinator, Security Working Group, Communication Research Network, Cambridge MIT Institute	√	√
Anne Carblanc	Principle Administrator, Working Group on Information Security and Privacy, Organisation for Economic Co-operation and Development		
Jon Crowcroft	Marconi Professor of Computer Science, University of Cambridge	√	√
Hans Graux	Consel, Lawfort	√	
Gwendel Legrand	ENST Paris	√	√

Yves Le Roux	Security Strategist, Computer Associates	√	√
Melanie Libraro	Director Business Development, Skype		
Rian Liebenberg	Director Information Systems, Google Europe		
Eric Luijif	Principle Consultant, TNO Security and Safety		
John Madelin	Business Development Director, RSA Security EMEA	√	
Tyler Moore	Doctoral Fellow, Department of Computer Science, University of Cambridge	√	√
Phillip Nobles	Senior Lecturer, Cranfield University	√	√
Stuart Okin	Associate Partner, Infrastructure and Enterprise Architecture Technology Consulting Accenture Technology and Delivery Group	√	
George Polk	Chief Executive Officer, Cloudnet Wireless Service		
Kai Rannenberg	Professor, Mobile Commerce and Multilateral Security, Goethe University, Frankfurt		
Martin Sadler	Director, Security Research, HP Bristol	√	
Angela Sasse	Professor of Human Computer Interface and Security, University College London	√	√
Richard Skaife	Vice President, Government Programmes, Nortel Networks	√	√
Diomidis Spinellis	Associate Professor, Department of Management Science and Technology, Athens University of Economics and Business	√	√
Giullaume Urvoy-Keller	EURECOM		
Giovanni Vigna	Associate Professor, Department of Computer Science, University of California Santa Barbara	√	
Ken Watson	Head of Information Assurance Services, CISCO Systems		

Table 6 lists attendees to the first workshop on the 7th February 2006, held in Cambridge.

Table 6: Attendees to the first workshop, Cambridge, 7th February 2006

Name	Affiliation
Danilo Bruschi	Professor, Computer Science, State University of Milan
Ian Brown	Co-ordinator, Security Working Group, Communication Research Network, Cambridge MIT Institute
Jon Crowcroft	Marconi Professor of Computer Science, University of Cambridge
Yves Le Roux	Security Strategist, Comptuer Associates
John Madelin	Business Development Director, RSA Security EMEA
Tyler Moore	Doctoral Fellow, Department of Computer Science, University of Cambridge
Phillip Nobles	Senior Lecturer, Cranfield University
George Polk	Chief Executive Officer, Cloudnet Wireless Service
Martin Sadler	Director, Security Research, HP Bristol
Angela Sasse	Professor of Human Computer Interface and Security, University College London

Appendix B: Case Study Interviewees

Table 7: Case study interviewees

Interviewee	Job Title	Date	Organisation
VoIP			
Tim Cureton	Head, HSBC Group Telecoms	12/04	HSBC Group
Nick Granger	Head, HSBC Technology Services Europe, IT Security	20/04	HSBC Group
James Traill	Systems Security Officer, HSBC Technology Services Europe, IT Security	20/04	HSBC Group
Jon Widdup	Deputy Head, HSBC Technology Services Europe, IT Security	20/04	HSBC Group
ARM			
Tim Thornton	Technical Marketer	13/03	ARM Holdings plc
Peter Harris	Technical Marketer	13/03	ARM Holdings plc
Tiego Alvers	Product Manager, TrustZone	07/04	ARM Holdings plc
WiMAX			
Graham Currier	Managing Director,	06/03	PIPEX
Paul Senior	Vice President of Marketing	06/03	Airspan Networks
RFID			
Jens Heitmann	Senior Manager, System/Equipment Standardisation Process and Methods	27/04	Airbus
Paul Stam de Jonge	Group Director, RFID Solutions	20/03	LogicaCMG
Phillipe Chenevier	Head of Research and Technology	20/04	Airbus Customer Services
Friz Obers	International Consulting & Project	21/04	Kortenburg

	management		
IPv6			
Ron Broersma		25/04	DREN
Alan Welday	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
Ken Renard	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
John Baird	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
Thomas Kendall	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
Bill Whittaker	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
Jim Matthews	Technical Officer, IPv6 Transition Team	25/04	High Performance Computing Modernization Program, DREN
Brent Rowe		10/02	DREN
Rodger Johnson		18/04	DREN

Appendix C – Terms of Reference for Final Workshop: Assessing the security challenges to the Deployment and Use of Disruptive Technologies

30th June 2006, 10.00 – 16.00, European Commission, Room BU30-0/58, Brussels

RAND Europe has completed a six-month project aimed at examining the security challenges associated with the implementation of the following five technologies: WIMAX, VoIP, IPv6, RFID and Trusted Computing. In particular, the project aimed to provide robust evidence to assist the European Commission in their activities and actions associated with the implementation of its i2010 initiative. In undertaking this project, RAND Europe has directed particular attention to the exploration and description of the way each one of the five technologies has been implemented and its security challenges addressed by undertaking specific case-studies.

In order to present the findings of the study and its suggestions for policy options, RAND Europe is organising a one-day workshop in Brussels. The workshop will be attended by representatives from industry, the public policy community, research and academia in order to bring to the table different perspectives.

In order to facilitate workshop discussions, RAND Europe distributes a draft of the project final report prior to the workshop. For more detailed information on the project and the workshop, please visit www.security-challenges.org or email Neil_Robinson@rand.org

Agenda

10.00	Welcome Introduction	Robert Henkel, European Commission Maarten Botterman, RAND Europe
10.15	Why study disruptive technologies and their security challenges?	Pete Bramhall, HP Invent
10.30	The impact of disruptive technology on the marketplace	Jonathan Cave, Warwick University

11.15	Introduction to the case studies, IPv6: DREN Voice over IP: HSBC WiMAX: Pipex and Airspan RFID: Airbus and Logica Trusted Computing: ARM	Neil Robinson, RAND Europe David Ortiz, RAND Corporation Richard Hackworth, HSBC Neil Robinson, RAND Europe Paul Stam de Jonge, Logica CMG Tiago Alvers, ARM
13.15	Lessons from the five case studies and overview of the security challenges	Neil Robinson, RAND Europe
13.30	i2010 Policy recommendations	Andreas Ligtvoet, RAND Europe
13:45	Moderated Discussion	all
15.30	Conclusions	Maarten Botterman, RAND Europe Robert Henkel, European Commission

Appendix D: Final Workshop participants

The following list indicates those participants registered to attend the June 2006 final workshop to review the draft final report and conclusions of the study.

Table 8 Final workshop participants list

Name	Organisation
Tiago Alves	ARM
Maarten Botterman	RAND Europe
Jeremy Hilton	University of Cardiff
Danilo Bruschi	University of Milan
Jonathan Cave	RAND Europe
Neil Fisher	Unisys
Richard Hackworth	HSBC
Yves Le Roux	Computer Associates, Paris
Andreas Ligtvoet	RAND Europe
Chris Marsden	RAND Europe
Stephen McGibbon	Microsoft
David Ortiz	RAND Corporation
Kai Rannenberg	University of Frankfurt
Neil Robinson	RAND Europe
Rebecca Shoob	RAND Europe
Lara Srivastava	International Telecommunication Union
Roberto Tavano	Unisys
Reka Bernat	DG INFSO (Unit C3)
Pete Bramhall	HP Labs
Andrea Servida	DG INFSO (Unit A3)
Anna Buchta	DG INFSO (Unit A3)
Leo Koolen	DG INFSO (Unit A3)
Robert Henkel	DG INFSO (Unit A3)
Merijn Schik	DG INFSO (Unit B1)
Philippe Gérard	DG INFSO (Unit B1)
Yves Paindaveine	DG INFSO (Unit D4)

Appendix E: Glossary

API – Application Programming Interface: A set of discrete instructions for a specific piece of software

ATA – Analogue Terminal Adaptor – a device allowing the connection of an analogue node (e.g. a telephone handset) into a digital network

ATA Spec 2000 - aerospace industry documentation standard

Blackberry – A form of Personal Digital Assistant where emails are sent directly to the device, instead of being downloaded by the user

Boot Loader - a piece of software that 'boots' the Operating System, network drivers, hardware etc

Codec – software codes that are used to compress content, usually audio-visual in nature

Common Criteria – a set of technical security specificaitons

CPE – Customer Premises Equipment – the devices installed at the end user or customers site

CPU – Central Processing Unit – the 'brains of any IT system'

DARPA - Defense Advanced Research Projects Agency, U.S. Department of Defense

DHCP – Dynamic Host Control Protocol

DoD - U.S. Department of Defense

DoS – Denial of Service

DREN - Defense Research and Engineering Network, U.S. Department of Defense

DRENv6 - DREN IPv6 test bed

Driver – a software program that allows the operating system to talk to hardware e.g. soundcard, video card

DRM – Digital Rights Management: the management of digital content under copyright

DSL – Digital Subscriber Line - a class of broadband digital network inferface

EASA - European Aviation Safety Agency

EMI – Electro Magnetic Interference

ERP – Enterprise Resource Planning software

FAA – Federal Aviation Authority

FTP - File Transfer Protocol

Foundry – a company that adds Intellectual Property into pre-built semiconductors

GNU/Linux – a form of Open Source software

HAL – Hardware Abstraction Layer – the means by which software can interact with hardware

HPCMP - High Performance Computing Modernization Program

HTTP - Hypertext Transport Protocol

I/O - Input / Output – the process of managing the input and output of data into memory and CPU cycles

IETF - Internet Engineering Task Force

IMEI – International Mobile Equipment Identifier

IP – Internet Protocol

IPR – Intellectual Property Rights

IPv4 - Internet Protocol Version 4

IPv6 - Internet Protocol Version 6

IPSec - Internet Protocol Security

ISP - Internet Service Provider

Kernel – the central part of the operating system that manages access to memory

LAN – Local Area Network

LBA - German Airworthiness Authority

Middleware – software designed to link two other software applications that cannot easily be connected together in an enterprise setting

NAT - Network Address Translation – a technical means to extend the use of IP addresses

NIST - U.S. National Institute for Standards and Technology

O/S – Operating System

Off Shoring – the placement of enterprise facilities in a location other than where the business is being conducted

OSI - Open Systems Interconnection

OTA – Over The Air

Outsourcing – the use of a third party to conduct part of a business operations

QoS – Quality of Service

QSIG – An internationally standardised signalling protocol designed to operate between Private Automatic Branch Exchanges (PABX)

PARC - Palo Alto Research Center, Xerox Corporation

PBX – Private Branch Exchange

PDA – Personal Digital Assistant

PSTN – Public Switched Telephone Network

RAM – Random Access Memory – volatile memory

RFID – Radio Frequency IDentification

ROM – Read Only Memory – non-volatile or read only memory

SCEM - Supply Chain Event Manager

SoC – System on Chip – a entire computing system etched onto one semi-conductor chip, containing (for example) video display logic, camera logic, sound production logic

SSL - Secure Sockets Layer

SIM – Subscriber Identification Module

TCG - Trusted Computing Group

TCB – Trusted Computing Base

TCP - Transport Control Protocol

TDM – Time Division Multiplexing

TPM – Trusted Platform Module

UDP - User Datagram Protocol

USB – Universal Serial Bus

URL - Uniform Resource Locators

Virtualisation – the process of creating two logical instantiations of a system, residing on only one physical instance

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

War Driving – the process of moving around (usually in a vehicle) trying to locate unsecured wireless networks

WCDMA - Wideband Code Division Multiple Access

WiFi – A conformity standard based on the IEEE 802.11 specification, for short range wireless radio interface, with speeds up to 54M/bps.

WiMAX - Worldwide Interoperability for Microwave Access specification IEEE 802.16 allowing the high speed transmission of data over medium to long distance

WWW - World Wide Web

XML – eXtensible Markup Language