Chapter 1

ON THE SECURITY IMPLICATIONS OF DISRUPTIVE TECHNOLOGIES

Neil Robinson and Lorenzo Valeri

Abstract This paper summarizes the results of a study that explored the security implications of the use of "disruptive technologies" in various economic sectors. Robust evidence of the security challenges associated with deploying advanced technologies was gathered by bringing together internationally-renowned experts with firsthand experience involving major case studies. Policy recommendations in the context of the European i2010 strategy were also articulated. This paper focuses on three technologies: Voice over Internet Protocol (VoIP), Radio Frequency Identification (RFID) and Internet Protocol version 6 (IPv6). It examines the security challenges related to the three technologies, and analyzes security issues that apply more generally to disruptive technologies.

Keywords: Disruptive technologies, security implications, VoIP, RFID, IPv6

1. Introduction

This paper summarizes the main results of a study undertaken by RAND Europe for the Information Society and Media Directorate-General of the European Commission. The goal of the study was to collect and analyze robust evidence on the security challenges involving the deployment and use of disruptive technologies.

Information and communication technologies (ICTs) are seen as the engine for sustainable growth and employment in Europe. This is the central message of the "i2010 Strategy" put forward by the European Commission in 2005. Its push for a "Single European Information Space" is based on faster broadband connections, seamless interoperability, and rich content and applications. The European Commission's communication that detailed the i2010 Strategy emphasized that "trustworthy, secure and reliable ICTs are crucial for the wide take-up of converging technologies" [10].

Coined by Harvard professor Clayton Christensen, the phrase "disruptive technology" refers to new technologies that unexpectedly displace the position of established technologies [5, 6]. An important element of these technologies is their potential for "creative destruction" and the resulting market impact [19]. Disruptive technologies displace leading technologies even though they may initially perform worse than existing technologies. Organizations often tend to focus on established technologies because they know the market, and have mechanisms in place to develop services and applications. Many organizations initially dismiss disruptive technologies, only to be surprised when the same technologies mature and gain massive market share. A good example is telephony, which was originally conceived as a short-range application. But it evolved and expanded, and completely disrupted the incumbent telegraph industry.

Given the ramifications that the successful deployment of disruptive technologies can have on global society, there is the need for appropriate awareness activities, self-protection mechanisms, and effective responses to attacks and system failures. Consequently, the RAND study focused mainly on the security challenges faced by organizations during the deployment of disruptive technologies and the steps taken by them to address the challenges. Five technologies were investigated. Of these, three were already stipulated by the European Commission: Voice over Internet Protocol (VoIP), trusted computing and Internet Protocol version 6 (IPv6). The remaining two technologies, Radio Frequency Identification (RFID) and wireless microwave access (WiMAX), were selected by RAND as good examples of disruptive technologies.

The study employed a multi-stage approach to investigate and identify security challenges for the five technologies. It involved a Delphi exercise, literature review, case studies and expert workshops. This was done to overcome the limited historical evidence base regarding the implementation of these technologies. The multiple case study approach was used as the primary research method to allow for the provision of more compelling evidence which would help support the conclusions and policy recommendations. This paper presents the results for three of the five technologies examined in the RAND study: VoIP, RFID and IPv6. It discusses the security challenges related to these three technologies as well as the security issues that apply more generally to disruptive technologies.

2. Voice over Internet Protocol Case Study

This case study considered the implementation of VoIP in the U.K. network of HSBC Bank, one of the world's largest financial institutions. Any new ICT implementation in HSBC, such as VoIP, must satisfy the key tenets of HSBC's technology strategy: standardization, self sufficiency, centralization and careful timing of technology adoption [17]. The VoIP implementation initiated with a pilot effort involving approximately 40 HSBC branches. The effort was undertaken by a corporate technology implementation team, which included two security experts. Key characteristics of the implementation were the creation of

virtual local area networks (VLANs) and the use of a consistent, organization-wide IP traffic allocation plan.

2.1 Risk Assessment

A formal risk assessment study was conducted by the IT security team and the overall project team early in the implementation effort. The study identified 23 risk areas. VoIP-related risks were categorized as follows:

- **Telephony End Point Attacks:** Eavesdropping on unencrypted network traffic, denial of service (DoS), Dynamic Host Control Protocol (DHCP) starvation, and attacks against IP handsets.
- **IP Telephony Server Attacks:** Viruses, worms and Trojans – typical attacks against servers connected to IP networks (Cisco Call Manager in this case).
- **Application Attacks:** Unauthorized access to the telephone system, toll fraud and telephony fraud using interfaces to the public switched telephone network. Other security issues included server organization, robustness, access control and vendor knowledge about voice communications, with a specific focus on QSIG signaling. QSIG is a signaling protocol used in enterprise voice and integrated services networks, typically between private branch exchanges (PBXs) [9].

The nature of the VoIP implementation with its separate VLANs for voice and data meant that other security considerations, especially those relating to availability, had to be met. Chief amongst these was the need for a contingency center capable of dealing with sites that were 100 km or more apart. Other availability issues came with the specific solution that was devised, e.g., managing the requirement for staff to make adjustments within the constraints of the solution.

HBSC also developed a traffic allocation plan to reduce congestion and mitigate the risk related to availability. As the VoIP implementation was carried out, HSBC staff began to appreciate that a higher level of security practices had to be undertaken with particular attention to servers, especially VoIP servers that carry both voice and data. HSBC staff were aware that users would not accept the same level of quality for voice communications as they did for e-mail communications, which suffers from occasional outages, low reliability and periodic non-availability. Finally, HSBC staff had to comply with various national and international regulations concerning the retention of communications data, which was possible with their new PBX solution.

2.2 Analysis

This case study illustrates that VoIP is a highly disruptive technology from the end-user and market perspectives, but at present is viewed less so within large corporations. In the case study, HSBC adopted a “wait and see” attitude;

it did not deploy the technology throughout its global organization as there was no clear business case.

VoIP deployment can act as a catalyst for important changes in numbering and addressing within an organization. However, by moving to a single technology other risks appear, especially those relating to reliability. Another challenge highlighted in the case study was meeting regulatory requirements across different legal jurisdictions. VoIP might be too secure in some cases, preventing regulators from undertaking the desired level of monitoring. Interoperability was also a large concern, particularly with regard to consumer use of VoIP software and applications. Security is a key element when addressing interoperability between different products.

3. Radio Frequency Identification Case Study

Airbus is a leading aircraft manufacturer with 434 deliveries and a turnover of 26 billion euros in 2006. The company maintains cooperative efforts and partnerships with major companies around the world; it has a network of more than 1,500 suppliers in 30 countries [2].

For this case study, Airbus collaborated with LogicaCMG, which operates the RFID Competency Center, and Kortenburg, which produced RFID chips to implement a fully-integrated solution for tracking and tracing of tools, instruments and spare parts. As a result, all Airbus tools and toolboxes are now equipped with RFID microchips, offering electronic support for tool loan and repair management. The microchips contain data about tools as well as shipping, routing and customs information.

The RFID solution was motivated by the desire to provide better, quicker service by improving the efficiency of the tool loan business. The tool loan business was chosen because it was a separate organizational division, and thus a relatively "safe" environment for experimenting with new technology [1, 18].

The RFID chips contain a variety of administrative data, including shipping information, serial numbers, receipt dates, last check numbers, check codes and original laboratory identifiers. The RFID solution is seamlessly integrated with Airbus' SAP business application software leading to the instant availability of data, which provides a great degree of transparency throughout the supply chain. Suppliers are able to verify that tools are genuine; this reduces the risk of unapproved tools entering the supply chain. Engineers do not need to delve through paperwork to discover the status of tools. The resulting optimization of the supply chain of repair tools has significantly reduced aircraft turnaround times.

3.1 Security Concerns

Data access and modification, and access to the backend system are possible only via authorized access by checking user rights. Only certain types of equipment can directly read and write to the RFID tags.

Data and system availability concerns were met by having the product serial number printed on the protective casing of the chip, allowing technicians to revert, if necessary, to manual handling. To maintain data integrity at the highest level, the complete destruction and revocation of a tag must be ensured if it is removed from a part or tool. Thus, counterfeit parts cannot be equipped with tags from scrapped components. Manufacturers check the tags to prevent unapproved parts entering the supply chain; therefore each tag must have a valid serial number.

Airbus performed extensive tests on the RFID tags to identify defects and evaluate interference during commercial aircraft operations. RFID devices used on aircraft must be of high integrity, and the radio frequencies must be stable. Tags were exposed to severe conditions followed by read-write tests. Safety tests included temperature changes, chemical and liquid exposure, humidity, lightning-induced transient susceptibility, electrostatic discharge, shock and vibration, and fire impact. None of the physical conditions had negative effects on the read-write functionality or data integrity; nor did the hostile test environment cause defects in the tags.

Government authorities are working on airworthiness approval and regulatory policy for passive RFID devices used in civil aircraft. In cooperation with a European airline, Airbus performed in-flight tests of RFID tags carried on Airbus A320 aircraft. No defects were encountered during 6,000 flight hours on 12 aircraft. The tags were approved by the German Airworthiness Authorities (LBA) after this successful test, paving the way for future approval and certification of the technology.

In 2005, the U.S. Federal Aviation Administration issued a policy memo on the safety aspects of passive RFID use in aircraft [11]. The memo suggested that data regarding parts should be accessible anytime, anywhere, by anyone and should respect data protection rights. Furthermore, round-the-clock verification of the information held on a tag must be possible from a secure central database.

The use of RFID accelerated goods receipt and quality inspection processes mainly due to the rapid availability of accurate data. 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. The technology was deemed to be reliable; nevertheless, additional reliability was achieved by adjusting the appearance and layout of the serial numbers on toolboxes.

3.2 Analysis

RFID is perceived as a controversial technology by the general public. The use of RFID in a supply chain environment is certainly not a controversial application, but one where the technology is being deployed very widely. In the case study, RFID was used only in a "safety-critical environment" in a relatively safe organizational area or "testbed."

In a logistics environment, the transmission of RFID data over open networks such as the Internet is of less concern than in an environment where the data

is of a personally identifiable nature. In Airbus' case, availability was the primary concern, not confidentiality. Clearly, as RFID applications increase, privacy issues associated with transmitting data over open networks will come to the fore.

Policy makers have an opportunity to promote appropriate and secure applications of RFID by encouraging research and development efforts related to security parameters for RFID infrastructures and by supporting efforts focused on addressing consumer perceptions related to RFID use. For example, initiatives such as the ongoing EU consultation on RFID should be encouraged and its results disseminated as widely as possible [13].

While the case study did not explicitly consider consumer concerns about RFID applications, other significant challenges were encountered. These included ensuring synchronization and concurrency of datasets (which are equally relevant to logistics and consumer applications of RFID). Obviously, failure to address these issues would wreak havoc on an RFID implementation. Another challenge deals with data being transmitted over open, potentially unreliable networks such as the Internet. The question is whether the data on a RFID chip ought to be complete or merely a serial number referencing a complete record held elsewhere.

Consideration of RFID as part of an open network (rather than a closed network as in the case study) is critical to identifying future challenges. The accessibility of the data in an RFID system is a key to realizing the benefits of the technology, with the caveat that such a system must be made as secure as possible to minimize data leakage.

4. Internet Protocol Version 6 Case Study

This case study investigated the deployment and use of IPv6 in a Defense Research and Education Network (DREN) trial. DREN is a U.S. Department of Defense (DoD) information network [8], which is part of the High Performance Computing Modernization Program (HPCMP), an effort to leverage cutting-edge technologies across the U.S. government. DREN connects 4,500 users across the U.S. It has ten core nodes and 100 smaller "service delivery points," all connected in a wide area network via high capacity optical links provided by Verizon [4].

The implementation of IPv6 in DREN was done to ease the DoD-wide transition to IPv6. HPCMP was not required to build a formal business case for its implementation, and there was no risk/reward threshold to be overcome before the decision to go ahead was taken. Undertaking the pilot effort was also seen as a way to identify best practices before the technology was rolled out more widely in DREN and within the DoD as a whole. It was crucial to understand the strengths and weaknesses of the technology, especially given the aggressive timetable for transition within the DoD. This was thrown into sharp relief by the need to identify the security risks inherent in a dual-stacked deployment of the technology. The DREN implementation operates two distinct IPv6 net-

works: a test network (DREN IPv6 Pilot) and DREN2, the rollout of IPv6 on the production network.

During the case study, emphasis was placed on having the most up-to-date equipment, which was critical to successfully deploying IPv6 on DREN. Experiments have shown that comparable performance is obtained for IPv4 and IPv6, despite claims of increased efficiency in IPv6's processing of datagrams. However, systems administrators must understand the complexities of operating in a dual-stack environment. Because of the requirements for either dual stacking or tunneling, the end-to-end paradigm is undermined during the transition period between IPv4 and IPv6. Another technical facet is that many IPv6 features (including its security benefits) will not have much of an impact until a significant portion of the Internet uses IPv6.

4.1 Security Concerns

The rollout of IPv6 in the DREN test network was simply a matter of enabling IPv6 on a new network. However, deploying IPv6 in the production network was more complicated and involved a significant planning effort. A team was formed to coordinate deployment across fifteen sites with the goals being to minimize workarounds and dual-protocol operations on the final dual-stack network – fewer tunnels and translators would make for a more robust and stable network. The well-known CMU SEI process for technology transition planning [15] was adopted by the project managers. 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.

Training sessions were conducted to assist staff during the transition; this also helped coordinate deployment and manage risk. The security of a dual-stacked environment is equal to that of an IPv4 network, and an IPv6 version of the IPv4 security strategy was deployed to manage risk. This case study is somewhat unique in that no cost-benefit study or risk assessment was undertaken. Network managers at HPCMP sites were responsible for carrying out the IPv6 plan for deployment. Ideally, the network protocol would be transparent to most network terminal users, so the term "user" in this case study refers to programmers who write applications to manage network resources or exploit protocol features.

Several general lessons were derived from the deployment. These included the importance of thorough planning, meaning that the margin for error was minimal or non-existent. The involvement of a broad range of stakeholders was crucial, especially those with security interests. Obtaining vendor support for IPv6 was also important; the demands placed on vendors by HPCMP for full IPv6 support was a significant motivator for them to upgrade their equipment and network management tools. However, some vendors offered less than complete support, and a number of tools and applications were incompatible with IPv6. The absence of a vendor schedule for delivering IPv6-ready applications along with new generations of equipment was a particular challenge, especially

concerning IPSec. More than 90% of the IPv6 products did not support IPSec. In fact, if systems are deployed inappropriately, IPSec communications can bypass traditional defenses, leading to the insertion of worms and viruses in secure links. Management of IPSec was difficult due to the absence of tools. Although HPCMP has not observed reduced security or an increase in attacks after deploying IPv6, it is clear that additional resources are required to maintain the security of DREN in a dual-stack environment.

4.2 Analysis

IPv6 can significantly increase the overall reliability and stability of public IP networks, and its DREN deployment was important as a precursor to the widespread use of IPv6 in U.S. government agencies. Lessons learned include the need to run a dual-stack environment with additional resources and the importance of engaging the vendor community, especially with regard to IPSec support. A heterogeneous network environment using both IPv4 and IPv6 during the transitioning from IPv4 to IPv6 may introduce other risks that undermine end-to-end security (e.g., tunneling between IPv4 and IPv6 affects IPSec). The need to maintain the same level of security during the transition period may also have second-order effects such as the need for additional resources.

The case study highlighted the narrow margin for error available to an organization deploying IPv6, and the need to effectively manage the transition, especially with respect to vendor expertise in IPSec.

The involvement of security personnel in the early stages of the IPv6 deployment eased the transition; this underscores the need to incorporate security in the core of any implementation or use of a disruptive technology. Organizations must be aware that vendor support for IPSec is limited, and must be prepared to negotiate with equipment suppliers to ensure that the appropriate security functionality is in place. Also, because the security benefits of IPv6 are realized more fully when it is used widely, it is important that policy makers encourage the pervasive use of the new protocol.

The case study did not consider the implementation of IPv6 in mobile environments. Given the DoD's massive investment in the area, it is extremely important to explore the challenges related to IPv6 in mobile environments. In addition to traditional security issues, it is critical to investigate the impact of IPv6 on the availability of applications and services in fast-moving mobile environments (e.g., command and control activities involving the use of 3G phones with wireless interfaces).

5. Analysis of Disruptive Technologies

The selected technologies are not inherently disruptive; rather, the disruption comes from how they are used [7]. This means that several of the lessons learned should apply to the larger set of emerging technologies.

A focus on "disruptive innovations" as a concept is recommended. More attention needs to be placed on defining what constitutes a "good" implementation. Effort also needs to be directed at attempting to pre-empt disruptions, for example, by exercising foresight, planning and evaluating scenarios, raising awareness, and engaging stakeholders [12].

Exploring the issues and impact of disruptive innovations based on one case study per innovation means that the results are a reflection of just a single application of the technology. Finding the right case studies to apply new technologies is not easy. Clearly, few, if any, mature applications exist of new technologies. Additionally, some case studies (e.g., RFID and IPv6), even if they are interesting and well motivated, do not represent the wider use of the technology in other applications. Positive experiences with new technologies lead to competitive advantages that are not always shared. Negative experiences for which solutions have not been found are often not shared by the affected organizations. Nevertheless, case studies are important because they help draw valuable insights on the disruptive effects of new technologies.

Recognizing the potential security challenges of disruptive technologies helps clarify what needs to be done to benefit from the new opportunities, and to avoid unnecessary risks. By considering the security challenges early, it is possible to move away from viewing security as an add-on. This ensures that all the issues, including the role of security, are fundamentally addressed from the outset.

6. Conclusions

Several observations can be made regarding the security challenges posed by the deployment of disruptive technologies in the case studies. The case studies show that it is important to include security in the business case when considering a new disruptive technology. In all three studies, the organizations involved did not make a business case either because the deployment was not mature enough or because a business case was not deemed necessary. In the case of VoIP, despite a business strategy of centralization and simplification, the organization did not elect to deploy the technology in a widespread fashion due to the absence of a clear business case. In the case of IPv6, it is questionable if a satisfactory business case could have been made given that none was required and that the deployment was mandated by the organization's heads.

This shows that doubt exists about the worth of disruptive technologies, despite the relative maturity of some of the technologies. But this is not entirely unexpected: organizations tend to favor the prevailing technology until an inescapable "tipping point" is reached. However, an organization's perception of a disruptive technology from a business perspective may parallel its view of how the technology contributes to the organization's overall security posture. Unfortunately, this could lead to a poor implementation of the disruptive technology, which translates to a poorer security posture.

The security implications of transitioning to a new technology must be considered very carefully. In the IPv6 case study, the security implications of an

organization's transitioning from one technology to another was highlighted. The need to keep IPv4 and IPv6 running together until the use of IPv6 was widespread enough to take full advantage of its security features undermined the end-to-end nature of the security mechanisms built into the IPv6 protocol.

Infrastructure reliability is a challenge when using disruptive technologies. With VoIP, reliability is a major concern in distributed geographies where the technology requires a massive degree of centralization to achieve economies of scale. Even in the case of privately-owned networks, reliability concerns are high and, although the economic possibilities offered by centralization of telecommunications at a regional level are attractive, the risks cannot be underestimated, particularly from denial of service attacks and natural disasters. Despite the hype, VoIP is regarded as suitable only for home-user communications where best-effort transmission is acceptable.

This challenge is also true for RFID when data is passed over the public Internet. The problem of ensuring that safety-critical data arrives when it should over a best-effort network is an important issue to any organization deciding to implement an RFID system using elements of public IP networks for data transmission. (The same concern has been raised for SCADA systems where electronic networks are used to transport control information for electric power stations, oil and gas pipelines, and public utilities.) Of course, with the increasing use of personal data in RFID systems, thorny security and privacy questions will no doubt arise.

Many security challenges are technology specific, but we can also conclude that some challenges apply to multiple (or all) disruptive technologies, even those not covered in this study. First, unexpected risks arise from "mission creep." As new technologies are implemented, their utility increases. This is unavoidable and, in a sense, is exactly what makes such technologies intrinsically disruptive. As applications of the technologies increase, new and unknown security issues often arise.

The convergence of nanotechnology, biotechnology, material science and information technology will surely have unexpected multi-disciplinary security consequences. For example, personal privacy could be infringed when implementing aspects of human genome research, or physical safety might be compromised by telemedicine-enabled applications.

Privacy may be even more at risk. Although privacy is often 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 network and information security principles). There could be a need for an effective ombudsman or trusted third party to act in cases where technology has breached privacy guidelines.

Network integrity and reliability are also critical issues. Many disruptive technologies rely on a global information infrastructure to one degree or another. Sensor networks built on a nanotech-enabled infrastructures will mean that networks will become ever "smarter," with the consequence of increasing frailty and fragility [14].

Finally, security challenges could also arise from social quarters not merely from technological vulnerabilities. Consider the case of genetically modified (GM) crops. The technology has existed for some time and the economic case is sound. But social and environmental factors will ultimately decide whether or not the technology will flourish.

References

[1] Airbus, Airbus applies RFID technology to supply of aircraft spare parts (www.airbus.com/en/presscentre/pressreleases/pressreleases_items/09_18_03_RFID_technology.html), 2003.

[2] Airbus, Airbus corporate website (www.airbus.com), 2007.

[3] T. Alves and D. Feldon, TrustZone: Integrated hardware and software security, White Paper, ARM, Cambridge, United Kingdom (www.arm.com/pdfs/TZ_Whitepaper.pdf), 2004.

[4] J. Baird, DREN IPv6 pilot network for HPC users, presented at the *Supercomputing 2004 Conference*, 2004.

[5] J. Bower and C. Christensen, Disruptive technologies: Catching the wave, *Harvard Business Review*, vol. 73(1), pp. 43–53, 1995.

[6] C. Christensen, *The Innovator's Dilemma*, Harvard Business School Press, Boston, Massachusetts, 1997.

[7] C. Christiansen and M. Overdorf, Meeting the challenge of disruptive change, *Harvard Business Review*, vol. 78(2), pp. 67–76, 2000.

[8] Department of Defense, Defense research and engineering network definition (www.hpcmo.hpc.mil/Htdocs/DREN/dren-def.html), 2004.

[9] ECMA International, QSIG home page (www.ecma-international.org/activities/Communications/QSIG_page.htm), 2006.

[10] European Commission, i2010: A European Information Society for Growth and Employment, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2005) 229 Final, Brussels, Belgium (europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0229en01.pdf), 2005.

[11] Federal Aviation Administration, Policy for passive-only radio frequency identification devices, U.S. Department of Transportation, Washington, DC (www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgPolicy.nsf/0/495367dd1bd773e18625715400718e2e?OpenDocument), 2005.

[12] Foresight Programme, Cyber Trust and Crime Prevention Project (www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html), 2005.

[13] P. Gabriel, RFID consultation website: Towards an RFID policy for Europe (www.rfidconsultation.eu), 2007.

[14] M. Handley, Why the Internet only just works, *BT Technology Journal*, vol. 24(3), pp. 119–129, 2006.

[15] L. Heinz, TransPlant: Helping organizations to make the transition, *News @ SEI*, vol. 4(4), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.sei.cmu.edu/news-at-sei/features/2001/4q01/feature-4-4q01.htm), 2001.

[16] M. Hines, Worried about Wi-Fi security? (news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html), 2005.

[17] HSBC Holdings, IT strategy (www.hsbc.com/1/PA_1_1_S5/content/assets/investor_relations/HSBC_Investor_day_6.pdf), 2003.

[18] Logica CMG, Case study: Airbus takes RFID into the spare parts supply chain (www.logicacmg.com/file/4017), 2005.

[19] J. Schumpeter, Creative destruction, in *Capitalism, Socialism and Democracy*, Harper, New York, pp. 82–85, 1975.