Risks in Networked Computer Systems

André N. Klingsheim

Thesis for the degree of Philosophiae Doctor (PhD)
at the University of Bergen, Norway

2008

ISBN 978-82-308-0632-6
Bergen, Norway 2008

Printed by Allkopi Tel: +47 55 54 49 40

Table of Contents

Abstract

Networked computer systems yield great value to businesses and governments, but also create risks. The eight papers in this thesis highlight vulnerabilities in computer systems that lead to security and privacy risks. A broad range of systems is discussed in this thesis: Norwegian online banking systems, the Norwegian Automated Teller Machine (ATM) system during the 90's, mobile phones, web applications, and wireless networks. One paper also comments on legal risks to bank customers.

Acknowledgements

I would first of all like to thank Kjell Jørgen Hole for his commitment and dedication as my supervisor, from which I have benefited since I first started working on my Master's thesis. With a fresh Master's degree, I spent a few months working in the private sector, before Kjell Jørgen made me an offer I couldn't refuse. Consequently, I returned to his research group as a PhD student, a decision never regretted. Thank you for putting in the effort necessary to assemble and run the group, and for letting me partake in the activities. You have invested time and effort way beyond your obligations as a supervisor, and have also been an excellent discussion partner in concerns other than those work-related. I am very grateful for the unbounded support and consideration you have shown.

Two fellow PhD students have earned my deepest respect: Lars-Helge Netland and Yngve Espelid. Your skills and personal qualities have significantly benefited our research group. We've spent many a night at work with paper deadlines approaching—arguing over the use of dashes, and discussing subtle differences between American and British English. You are henceforth relieved of such discussions, but I'll miss them. I'll remember our enjoyable conference trips, in particular the one were we went golfing amongst crocodiles. We've had great fun as PhD students, there are many hilarious stories to tell from our travels.

I would also like to thank my other co-authors: Thomas Tjøstheim, Kent Inge Fagerland Simonsen, and Vebjørn Moen.

Special thanks go to my wife Eli for her love and support throughout these years. You took care of all the domestic responsibilities when paper deadlines approached, and were patient when research challenges left me merely physically present at home. You've also given me two amazing girls, they are the light of my life.

Finally, I would like to thank my parents, Tor and Barbro, for motivating me, supporting me, and believing in me. I apologize for any frustration my varying focus on schoolwork may have caused you over the years. Things got a whole lot more interesting when I could study computer systems, as manifested by this thesis.

Risks in Networked Computer Systems

1 Introduction

Society depends on computer systems. Interactions in business and with the government are often carried out over the Internet, and even social networks are moving online. While people get convenient access to important services around the clock, great challenges also emerge in terms of security and privacy.

In computer systems, valuable assets are usually pieces of information. Information security, referred to as *security* for convenience, consists of three security goals: confidentiality, integrity, and availability [1, p. 10]. By achieving these goals, the value of the information can be sustained.

Large amounts of the information handled by computer systems is personal in nature, where personal information is defined as all information that identifies or describes an individual. When dealing with personal information, privacy concerns arise. Privacy is defined as the individual's interest in controlling the flow of his/her personal information [2], i.e. who has access to the information, how is it used, and is the information up to date.

The amount of valuable information managed in networked computer systems increases day by day. As more and more services become available, the overall attack surface—defined by Microsoft as the possible entry points to a system [3]—is growing. Furthermore, the 2007 threat reports from Symantec conclude that attackers are becoming more professional and their activities are increasingly driven by profit [4]. In short, the target is growing bigger, and the attackers are improving their aim.

In the near future, the odds seem to be shifting even more in favor of the attackers. There is an increasing interest in using "new" platforms—mobile phones and PDAs—for common Internet services such as online banking, e-commerce, e-mail, and web browsing. Although it can be convenient to use a mobile phone to fulfill tasks usually carried out on your home computer, there are several inherent drawbacks when relying on mobile devices. Most importantly, computational power and memory—in particular volatile memory—are limited and far from what is offered by desktop computers. Despite these constraints, modern phones resemble laptop computers in that they are networked, facilitate installation of third party applications, and support multitasking. Unfortunately, they usually lack defense mechanisms regarded mandatory for any "secure" computer, such as antivirus, antispyware, and firewall software. Taking into account the many security related bugs found in recent mobile devices [5], it is very challenging to offer both secure and widely available services on the mobile platform.

Security is a concern for anyone holding information valuable to an attacker. Small businesses can suffer the same attacks as large organizations. After an early version of our paper [6] was published on the Internet, large amounts of personal information (identification numbers, names, and addresses) were downloaded from Norwegian mobile operators' poorly designed web applications. The attackers targeted both small and large operators. Note that Norwegian newspapers uncovered that software tools to download personal information from the mobile operators had circulated on the Internet in advance of the public release of [6]. We merely uncovered and highlighted the problem.

Due to legal concerns, some of the work in this thesis focuses on Norwegian systems. Still, the insights should be relevant to other systems.

1.1 Overview

The remainder of this thesis is structured as follows. Section 2 discusses today's security challenges in light of insights achieved decades ago. Section 3 explains risk, and Section

4 goes on to discuss risk management. Section 5 outlines the thesis' contributions and impacts. Section 6 suggests further work, and Section 7 gives the thesis' conclusion. Section 8 summarizes the eight papers in the thesis.

2 Security in the past and the present

It is interesting (and devastating) to study today's security challenges in light of the classic 1975 paper by Saltzer and Schroeder [7]. They propose several design principles to achieve a high level of security in computer systems. To highlight a few, they recommend keeping the design as simple and small as possible to limit the complexity. The design should be open to external review, as it is unrealistic that the inner workings of a widely distributed system can remain secret over time. A third interesting principle is to assure psychological acceptability—which translates to usability—enabling the user to utilize the system and its security mechanisms correctly.

2.1 Complexity

In terms of complexity, our findings in [8] indicate that well-known vulnerabilities have a strong tendency to surface in large web applications. The mobile operator mentioned in [6] stated in an interview that their website consisted of several underlying systems, and that the resulting complexity made it difficult to change the system in order to stop the leakage of personal information. The new trend on the Internet, referred to as Web 2.0, is to build websites where users to a larger degree contribute the content. There is also a shift towards services that can be easily combined to create new services, and the storage of information is handled by central servers while computation is moved to users' web browsers. Although enabling new and interesting services, Web 2.0 also creates security challenges [9]. The trend seems to go in the direction of more complexity, not less.

2.2 Open design

Our findings on BankID—a security infrastructure owned by Norwegian banks—show that secrecy about a system is difficult to preserve over time [10]. By taking the role as an ordinary user of the system we got easy access to the client software, and were able to observe large parts of the application protocol, in addition to studying the details of the client software itself. With the momentum the BankID system is gaining in Norway, scrutiny by attackers and researchers should be expected by the BankID community. Furthermore, BankID is a candidate to become a national identity system. Public review of security and privacy implications for all stakeholders should be a prerequisite for sanctioning by the government [11].

2.3 Usability

There is still a long way to go before online systems reach a satisfactory level of usability. A Norwegian bank recently settled a long lasting dispute with a customer who entered an erroneous account number with an extra digit while transferring money in her online bank [12]. The client software truncated the account number, which the customer did not notice, and the money was transferred to the wrong person. The incident was partly caused by poor usability, a simple error message about the invalid account number would have avoided the accident. Another example is Canadian banks, requiring skills beyond the average customer's capabilities when offering secure online banking [13]. A final example, relevant to most e-commerce sites around the world, is users' limited understanding of certificates and their use in authentication with the Secure Sockets Layer (SSL) protocol [14], facilitating Man-in-the-Middle (MitM) attacks[1] [15]. Anderson discusses problems related to usability and psychology in [16].

2.4 Weak authentication

Authentication can be defined as the process of establishing an understood level of confidence that an identifier refers to an end-user [2]. The authentication is said to be strong if the level of confidence is high.

Apart from the design principles, Saltzer and Schroeder describe the inherent drawbacks of passwords—making password based authentication *weak.* They describe an attack where the attacker learns a user's password as it is typed in on a terminal, and then later misuses the credentials on another terminal. The same principle is used in phishing attacks, where users are lured into revealing their credentials to a malicious website.

At the time of writing, BankID stores end-users' private keys centrally, and a user supplies a password to remotely unlock his key. It seems the only requirement for the passwords is that they have a minimum of 6 characters. When testing the system we discovered that the user's birthdate—which equals the first six characters in the userid—was accepted when setting a new password. Despite the lax password policy, the BankID community claims that signatures generated by the system are legally binding. In addition to a password, customer authentication in BankID currently relies on one-time password generators. Schneier warned in 2005 that two-factor authentication did not solve well-known security challenges [17], and numerous news reports from the last few years discuss attacks on Scandinavian online banks, underscoring Schneier's point.

2.5 Cryptography is not enough

Our work is also interesting in light of earlier work by Anderson [18]. Although BankID uses a Public Key Infrastructure (PKI) [19], and employs two layers of encryption on the communication between the client software and BankID infrastructure—unchecked configuration parameters combined with session management issues opened the possibility for a MitM attack [10].

2.6 Improving the situation

So why are we still struggling with well-known security challenges? A new direction in security research has emerged in recent years shedding light on the problem, by looking at security from an economic perspective. Anderson and Moore have written a survey paper on the progress in the field of economics and security [20], and Anderson has devoted a chapter to the topic in [16]. Clearly, there has been a lack of incentives to produce secure computer systems. To improve the situation, either new business opportunities must emerge from more secure systems, or governments must enforce regulations that require improved systems. Anderson *et al.* [21] recently wrote a report for the European Network and Information Security Agency (ENISA) where they suggest regulatory measures to stimulate the creation of more secure computer systems.

System architects, designers, and programmers are the ones who have to create the secure systems of the future. Microsoft underscore the importance of security training of

[1] The politically correct term is "middleperson attack." For the sake of consistency, the preface uses the nomenclature from the thesis' papers.

their development staff [3]. Educational institutions have started to pick up on the challenge, but we need more initiatives. Security should be an integral part of any education related to development of computer systems.

The US National Research Council has released a comprehensive report on strategies for cybersecurity research that can contribute to more secure systems in the future [22].

3 Risk

Throughout the years there has been many risks related to computer systems [23], and there still are. This thesis touches upon several types of risks, namely security, privacy, and judicial risks.

Risk is often defined as a function of the likelihood and impact of an event, and comes in two categories: speculative and non-speculative. Speculative risk refers to risks where there is a potential gain from taking a risk. An example is gambling. You bet a certain amount of money, which you risk losing. Still there is a potential upside, you might win the bet and receive a larger amount of money in return. Non-speculative risks only carry a downside. Examples are natural disasters, or vulnerabilities in computer systems that can have a negative impact on business.

There are two main approaches to rate a risk, quantitative and qualitative. Consider the risk of a particular hardware component failing in a server. The vendor might supply numbers from their test lab stating that the component will work reliably for X hours. You might also have historical data on the components life expectancy. With high assurance, the likelihood of failure can be quantified. Furthermore, if the impact can be accurately quantified, i.e. the total cost of replacing the component, the risk can be quantitatively rated.

The problem with security risks is that the likelihood and impact of an attack can be very difficult to quantify. The qualitative approach can then prove useful [24]. Many models to rate risks exist, one is briefly discussed here to illustrate the qualitative approach. Microsoft created the DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) model to assess risks related to vulnerabilities in their software [25]. The idea behind the model is straight forward, when facing skilled and motivated attackers, how difficult is it for them to find and take advantage of a vulnerability, and what is the potential impact of an exploit. The five DREAD properties of a vulnerability are rated high/medium/low, which combined yields a total risk rating. Although Microsoft have further evolved their risk assessment methodology, they still follow the principles from DREAD [3].

This thesis focuses largely on vulnerabilities. However, when in presence of a motivated attacker, vulnerabilities create risks. To fully grasp the risk associated with a particular vulnerability, understanding the context of the vulnerability is very important. When a system lacks public documentation, researchers might discover vulnerabilities in the system but are unable to fully assess the associated risks. Furthermore, it is not uncommon that vulnerabilities are dismissed by system owners as unpractical to exploit. Proof-of-concept attacks may then play an important role in verifying a vulnerability, and can indicate the severity of the associated risk. At least, it will bring unarguable evidence into the discussion, and shed light on the vulnerability's context.

3.1 Stakeholders

For any risk, there are one or more stakeholders who may suffer an impact. Although companies and governments, are concerned with risks that may affect themselves, other stakeholders may be unaware of and/or unable to influence their exposure to a risk [26].

Recall the leaks of personal information from Norwegian mobile operators discussed in Section 1. In the aftermath of the information leaks, at least 180 000 Norwegian citizens were left uncertain about who had copied their personal information. They can all easily fall prey to identity thieves in the future. Another stakeholder, one of the mobile operators, had to pay for many worthless credit checks and was fined 150 000 NOK (approx. 30 000 USD). In addition, the operator had to deal with bad publicity. However, since victims to identity theft often can spend hundreds of hours clearing their name with different financial institutions, the total impact on the general public can easily exceed the impact on a single mobile operator.

Businesses can, intentionally or unintentionally, assign risk to stakeholders incapable of understanding the risk before they suffer the impact [6, 18, 27, 28]. Thus, it is important that a government provides and enforces laws and regulations that assign the risk to a party able to manage it.

Researchers, without commercial interests in a system, can play an important role in analyzing the risks on behalf of stakeholders incapable of detecting an unfair assignment of risks. This is particularly important for national systems, when at least one stakeholder has strong commercial interests. Several papers in this thesis highlight risks imposed on stakeholders other than the system owners, in particular the banking papers [10, 28, 29, 30] focus on the risks to banking customers, and [6] describes risks to most Norwegians.

4 Risk management

Risk management implies that exposure to risks should be a conscious decision. The starting point for a risk management process is to decide the risk acceptance criteria, reflecting how much risk one is willing to take. Figure 1 shows a high-level view of a qualitative risk management process containing two phases, *assessment* and *treatment* of risks [24, 31]. As computer systems and their threats tend to change over time, the process must be carried out periodically.

The first activity of the risk assessment stage aims to establish a good overview of the system. Second, threats and vulnerabilities are identified. The combination of a threat and a vulnerability constitute a risk to the system. Finally, the risks are evaluated by determining the likelihood and impact of each threat/vulnerability pair. A thorough assessment is of great importance to the success of the overall risk management process [31].

In the second phase, the determined risks are subject to risk treatment in light of the risk acceptance criteria. For each risk there are four approaches:

- **Accept** — The risk is acceptable, no action taken.
- **Control** — The risk is too high, measures are taken to reduce the likelihood and/or impact of the risk, thus making it acceptable.
- **Reject** — The risk is too high, the risk is avoided by e.g. dropping risky functionality or working around the risk.
- **Transfer** — The risk is transferred to another party, e.g. through insurance.

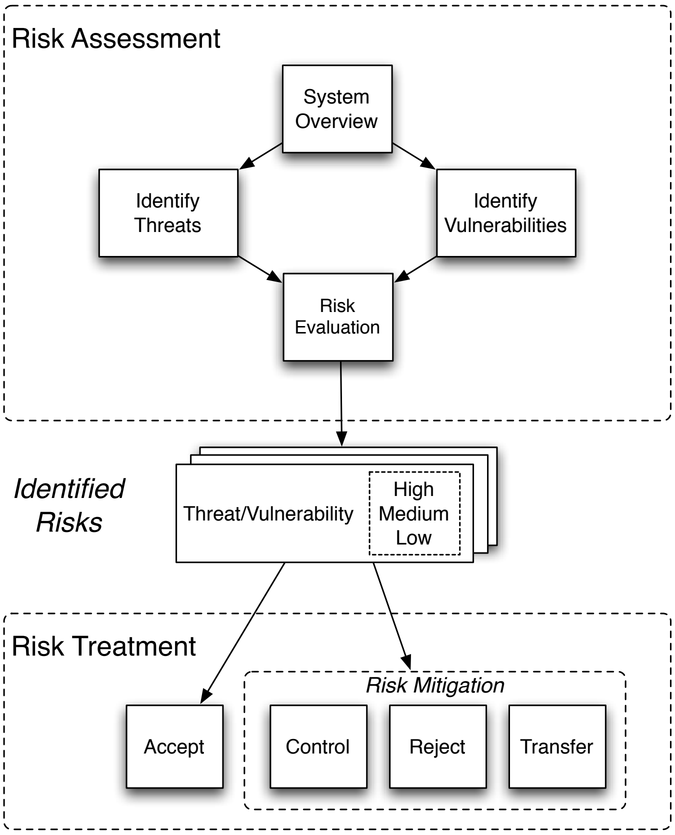

Figure 1: Risk Management Process

After the risk treatment phase there are remaining risks, referred to as residual risks, that satisfy the risk acceptance criteria.

In [32], we argue that universities should consider offering open wireless networks—meaning that users are relieved of authenticating themselves in order to use the network infrastructure. We further discuss controls that could mitigate apparent risks to open networks. In light of the advantages from open networks, universities should use risk management as a tool to decide whether to authenticate their wireless network users.

4.1 Software risk management

The advantages of using risk management as a tool to ensure the success of a software project in terms of project completion and software quality have been advocated for many years [33]. To manage software security, Verdon and McGraw argue that risk management should be an integral part of the software development life cycle [34]. In [35], McGraw names risk management as the first of three pillars in software security.

Microsoft changed their approach to software development after Bill Gates' Trustworthy Computing initiative, which resulted in the Trustworthy Computing Security Development Lifecycle (SDL) [3]. In [36], Microsoft give an overview of the SDL and conclude, based on early results, that the SDL has significantly improved the security of their software. Another interesting finding is that they highlight risk management (referred to as threat modeling in the paper) in the design phase as the most effective sub-process in the SDL.

5 Contributions and impacts

The work on BankID uncovered vulnerabilities in a (soon to be) critical national infrastructure, and spurred improvements to the security of the system [10]. However, the true level of security is still unknown to the public. The public debate following our proof-of-concept attack had an important outcome. Early in the process the BankID community questioned the lawfulness of our activity and stated publicly that their lawyers were looking into the issue. Later, a member of the Norwegian cabinet, and the Norwegian Data Inspectorate, declared that scrutiny by researchers was important and encouraged further review of the system. Their support silenced the debate on the legal implications, and paved the way for researchers to evaluate Norwegian systems of national importance. The Data Inspectorate states in their 2007 annual report the importance of independent researchers scrutinizing national systems, and specifically refers to our work on BankID [37]. One researcher has already responded to the challenge [38].

The paper on the Norwegian ATM system points out the seemingly weak legal protection bank customers have during a conflict with a bank [28], and provides arguments for more openness around security questions. If used by lawyers in future court cases, the paper may have a positive impact on bank customers' legal protection.

The paper on the potential for identity theft in Norway [6] ignited a public debate on privacy, and mobile operators consequently improved their authentication schemes on the Internet. After a live demonstration on national television of proof-of-concept software which determined a journalist's birth number, Norway Post closed down their online mail rerouting service—which had been used to commit identity theft on at least one occasion—and later relaunched the service with significantly improved authentication of individuals.

The security related shortcomings in Java 2 Micro Edition (J2ME) enabled devices are important input to mobile development projects [5]. The increasing interest in offering services on mobile devices indicates that the paper will remain relevant until flawed devices disappear from the market.

6 Further work

Although we have uncovered a series of vulnerabilities in the BankID system, the privacy aspects of the system have not been evaluated or debated. The fact that all digital signatures for individuals are created by the central infrastructure, raises the suspicion that the BankID community can keep a complete record of all communications between the end-users and BankID enabled websites. Privacy implications should definitely be evaluated and discussed before launching BankID, or any other system, as a national identity system.

More wide ranging research on how risk is shared among stakeholders in national systems would be interesting. The government could receive important insights that would let them enforce laws and regulations which assign risk in a fair manner.

The research on the economics of security shows promise, and can hopefully aid in introducing incentives for system developers to create more secure systems in the future. A team of skilled economic, computer science, and legal researchers could produce valuable results on how to reduce the problems of security and privacy in national computer systems.

7 Conclusions

Today's networked computer systems to a large degree fail to meet well-known security challenges. The key to change the situation lies within economics and law. Security researchers need to communicate security and privacy risks to business managers and policy makers, who in turn can affect the incentives for building secure systems.

In the future, security should be an integral part of educations in system engineering. If architects/designers and developers lack security training, they cannot make secure systems.

100% security is unachievable in complex computer systems. Vulnerabilities will exist that create risks, where some of them probably are acceptable. Risk management is the key to make well informed decisions on which risks to take.

8 Summary of Thesis

The papers herein consider security, privacy, and legal risks. The first four papers deal with security risks caused by vulnerabilities in both design and implementation of banking systems, and legal risks to banking customers. The fifth paper outlines risks faced when developing J2ME applications. The sixth paper describes security risks caused by vulnerabilities in the implementations of e-government web applications, and touches upon privacy risks caused by bad web application design. The seventh paper focuses on privacy risks following poorly designed web applications. The eighth paper assesses apparent risks in open wireless networks, and suggests controls to reduce these risks to an acceptable level.

Six of the papers [5, 6, 8, 28, 29, 32] have been published in international refereed journals or conferences, while the last two papers [10, 30] have been accepted for publication.

8.1 Paper I: Risk Assessment of Services in a National Security Infrastructure [30]

The NoWires Research Group carried out an extensive analysis of security aspects of BankID, a new security infrastructure developed by the Norwegian banking industry. BankID started out as a system to facilitate online banking, but is now on its way to be sanctioned by the Norwegian government as a national identity system. The banking community and relevant public authorities claim that BankID meets all requirements necessary to offer legally binding signature services. In [30], we assess the risks of Distributed Denial of Service (DDoS) attacks, and combined phishing/MitM attacks on the system, based on publicly available sources. In addition, we discuss the potential risk to BankID customers related to the weak and unfair non-repudiation process. Several more observations from our analysis can be found in a technical report [39].

8.2 Paper II: Lessons From the Norwegian ATM System [28]

The plaintiff's lawyer in a Norwegian court case on ATM card misuse brought the case to our attention and supplied us with legal documents for the case. During a trip to Spain the plaintiff's ATM cards were stolen and almost instantly misused. Expert witnesses from the Norwegian banking industry convinced the judge that the ATM system employed the Data Encryption Standard (DES) to secure the PIN-code, and that the ATM system was secure. No documentation was provided to back up the security claim. We argue that the bank's security-by-secrecy policy affects the security of their systems negatively over time—and is a threat to bank customers' legal protection during a conflict. The paper [28] was written together with an associate professor at the Faculty of Law, University of Bergen. More information on the security in ATM systems can be found in [16].

8.3 Paper III: A Proof of Concept Attack against Norwegian Internet Banking Systems [29]

In [39] we described an opportunity for a MitM attack on the BankID system. We explored this attack in more detail in [29], and succeeded in configuring the BankID client software to communicate with a specialized proxy, which relayed the traffic to the central BankID infrastructure. In the final steps of the BankID authentication protocol, we were able to seize control of the user's authorized session. The attack used the original, digitally signed BankID client software to carry out the user authentication.

8.4 Paper IV: Robbing Banks with Their Own Software—an Exploit against Norwegian Online Banks [10]

Following the findings in [29], we outline the details of the flawed BankID authentication protocol and the MitM attack in [10]. We also discuss the psychological aspects of our attack in more detail. We argue that—by misusing the customer's trust in BankID—our attack was more likely to succeed than the common phishing attacks plaguing online banking systems in recent years.

8.5 Paper V: Challenges in Securing Networked J2ME Applications [5]

Mobile devices are an emerging client platform for important services, such as online banking. During a commercial project, aiming to store medical information on mobile phones, we gained useful insights into the security challenges inherent in the software shipped with mobile phones. We tested a variety of J2ME enabled devices, and discovered that they behaved inconsistently and often contained bugs specific to a particular brand, or even a particular model. There were issues related to signature verification of signed applications, certificate management, and verification, and secure communication and storage.

Finally, we examine the Security and Trust Services API (SATSA) available on many mobile phones, which offers limited PKI client functionality and basic cryptographic services. Several shortcomings are highlighted.

8.6 Paper VI: Vulnerabilities in E-Governments [8]

We conducted a survey on governmental websites in 2005, seeking two well-known web application vulnerabilities: Susceptibility to Cross Site Scripting and SQL Injection attacks. More than 80% of the governmental sites we inspected were vulnerable to one or both of these attacks.

We also discovered the possibility of extracting Norwegian Birth Numbers (NBNs) (referred to as SSNs in the paper) from the website of a Norwegian pension fund, and were able to establish the NBNs of the ministers in the Norwegian cabinet at the time. Our findings show that the security of e-governments could be improved.

8.7 Paper VII: Identity Theft: Much too Easy? A Study of Online Systems in Norway [6]

Inspired by the findings in [8], we investigated the use of NBNs in national online systems in Norway. It turned out that personal information was easily available through various web applications. In particular, many Norwegian mobile operators leaked Norwegian citizens' NBNs, full names, and addresses. With this information at hand, an identity thief could e.g. reroute an individual's mail, order credit cards online, and order cell phone subscriptions on the individual's behalf. The paper pinpoints why systems leak, describes proof of concept software demonstrating the leakage, and suggests how to improve the situation. The interested reader can find more information in a technical report outlining how large scale identity theft can be prepared, and explaining the proof of concept software in more detail [40].

8.8 Paper VIII: Open Wireless Networks on University Campuses [32]

Wireless networks can give convenient access to a network infrastructure. We argue that universities should consider offering open wireless networks to their employees, students, and the general public. Open networks yield a higher degree of usability and privacy for their users than networks requiring authentication. Still, there are inevitable risks related to malicious use of open networks, such as illegal downloads and attacks both on and from the network. We analyze these risks and argue that they can be mitigated.

Bibliography

[1] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, Prentice Hall, fourth edition, 2007.

[2] S. T. Kent and L. I. Millett, editors, *Who Goes There? Authentication Through the Lens of Privacy*, The National Academies Press, 2003.

[3] M. Howard and S. Lipner, *The Security Development Lifecycle*, Microsoft Press, 2006.

[4] Symantec Inc., "Symantec Internet Security Threat Reports," `http://www.symantec.com/threatreport/`, 2007, last checked Feb. 20, 2008.

[5] A. N. Klingsheim, V. Moen, and K. J. Hole, "Challenges in Securing Networked J2ME Applications," *IEEE Computer*, 40(2):pp. 24–30, 2007.

[6] A. N. Klingsheim and K. J. Hole, "Identity Theft: Much too Easy? A Study of Online Systems in Norway," in *Proc. 12th International Conference on Financial Cryptography and Data Security (FC08)*, number 5143 in LNCS, pp. 192–196, Cozumel, Mexico, January 28–31 2008.

[7] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, 63(9):pp. 1278 – 1308, 1975.

[8] V. Moen, A. N. Klingsheim, K. I. F. Simonsen, and K. J. Hole, "Vulnerabilities in E-Governments," *International Journal of Electronic Security and Digital Forensics*, 1(1):pp. 89–100, 2007.

[9] G. Lawton, "Web 2.0 Creates Security Challenges," *IEEE Computer*, 40(10):pp. 13–16, 2007.

[10] Y. Espelid, L.-H. Netland, A. N. Klingsheim, and K. J. Hole, "Robbing Banks with Their Own Software—an Exploit against Norwegian Online Banks," in *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, pp. 63–77, Milan, Italy, September 8–10 2008.

[11] S. T. Kent and L. I. Millett, editors, *IDs—Not That Easy: Questions About Nationwide Identity Systems*, The National Academies Press, 2002.

[12] K. Olsen, "The $100,000 Keying Error," *IEEE Computer*, 41(4):pp. 108, 106–107, 2008.

[13] M. Mannan and P. C. van Oorschot, "Security and Usability: The Gap in Real-World Online Banking," in *NSPW '07: Proceedings of the 2007 workshop on New security paradigms*, 2008.

[14] S. A. Thomas, *SSL and TLS Essentials*, Wiley Publishing, 2000.

[15] R. Oppliger, R. Hauser, and D. Basin, “SSL/TLS Session-Aware User Authentication,” *IEEE Computer*, 41(3):pp. 59–65, 2008.

[16] R. Anderson, *Security Engineering*, Wiley Publishing, second edition, 2008.

[17] B. Schneier, “Two-Factor Authentication: Too Little, Too Late,” *Communications of the ACM*, 48(4):p. 136, 2005.

[18] R. Anderson, “Why Cryptosystems Fail,” in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 215–227, 1993.

[19] C. Adams and S. Lloyd, *Understanding PKI—Concepts, Standards, and Deployment Considerations*, Addison-Wesley, second edition, 2003.

[20] R. Anderson and T. Moore, “Information Security Economics—and Beyond,” in *Proc. of the 27th Annual International Cryptology Conference*, pp. 68–91, 2007.

[21] R. Anderson, R. Böhme, R. Clayton, and T. Moore, “Security Economics and the Internal Market,” European Network and Information Security Agency, 2008.

[22] S. E. Goodman and H. S. Lin, editors, *Toward a Safer and More Secure Cyberspace*, The National Academies Press, 2008.

[23] P. G. Neumann, *Computer Related Risks*, Addison-Wesley, 1995.

[24] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” 2002, NIST Special Publication 800-30.

[25] J. D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corporation, 2003.

[26] B. Schneier, “Risks of Third-Party Data,” *Communications of the ACM*, 48(5):p. 136, May 2005.

[27] N. Bohm, I. Brown, and B. Gladman, “Electronic Commerce: Who Carries the Risk of Fraud?” *The Journal of Information, Law and Technology (JILT)*, (3), 2000.

[28] K. J. Hole, V. Moen, A. N. Klingsheim, and K. M. Tande, “Lessons from the Norwegian ATM System,” *IEEE Security & Privacy*, 5(6):pp. 25–31, Nov/Dec 2007.

[29] Y. Espelid, L.-H. Netland, A. N. Klingsheim, and K. J. Hole, “A Proof of Concept Attack against Norwegian Internet Banking Systems,” in *Proc. 12th International Conference on Financial Cryptography and Data Security (FC08)*, number 5143 in LNCS, pp. 197–201, Cozumel, Mexico, January 28–31 2008.

[30] K. J. Hole, A. N. Klingsheim, L.-H. Netland, Y. Espelid, T. Tjøstheim, and V. Moen, “Risk Assessment of Services in a National Security Infrastructure,” *IEEE Security & Privacy*, accepted for publication.

[31] A. Calder and S. G. Watkins, *Information Security Risk Management for ISO27001/ISO17799*, IT Governance Publishing, 2007.

[32] K. J. Hole, L.-H. Netland, Y. Espelid, A. N. Klingsheim, H. Helleseth, and J. B. Henriksen, “Open Wireless Networks on University Campuses,” *IEEE Security & Privacy*, 6(4):pp. 14–20, July/August 2008.

[33] B. W. Boehm, “Software Risk Management: Principles and Practices,” *IEEE Software*, 8(1):pp. 32 – 41, 1991.

[34] D. Verdon and G. McGraw, “Risk Analysis in Software Design,” *IEEE Security & Privacy*, 2(4):pp. 79–84, 2004.

[35] G. McGraw, *Software Security*, Addison-Wesley, 2006.

[36] S. Lipner and M. Howard, “The Trustworthy Computing Security Development Lifecycle,” `http://msdn2.microsoft.com/en-us/library/ms995349.aspx`, March 2005.

[37] Datatilsynet, “Datatilsynets Årsmelding for 2007,” 2008, in Norwegian.

[38] K. Gjøsteen, “Weaknesses in BankID, a PKI-substitute Deployed by Norwegian Banks,” in *Proceedings of the 5th EuroPKI Workshop*, volume 5057 of *LNCS*, pp. 196–206, Trondheim, Norway, June 16–17 2008.

[39] K. J. Hole, T. Tjøstheim, V. Moen, L.-H. Netland, Y. Espelid, and A. N. Klingsheim, “Next Generation Internet Banking in Norway,” Technical Report 371, Institute of Informatics, University of Bergen, February 2008, available at: `http://www.ii.uib.no/publikasjoner/texrap/pdf/2008-371.pdf`.

[40] A. N. Klingsheim and K. J. Hole, “Personal Information Leakage: A Study of Online Systems in Norway,” Technical Report 370, Department of Informatics, University of Bergen, February 2008, available at: `http://www.ii.uib.no/publikasjoner/texrap/pdf/2008-370.pdf`.