CHAPTER 1

Introduction

This Ph.D. dissertation addresses the fundamental question: “How do you secure the shrinking computer?”.

In the old days (circa the 1970s), computers were unencumbered and free. Some may remember a young upstart named Richard Stallman who refused to password protect his MIT Media Lab user account for ideological reasons. His reasoning was simple – who would want to abuse such a useful and wonderful new technology? Let the access be free!

A lot has changed since then. Computer viruses now make regular headlines, Internet security is a booming business. Even the corner hairdresser will happily rant about the dangers of Internet banking. However, as computers get smaller and more pervasive, their security and privacy issues become less well understood.

Over the past few decades, the computer has been shrinking; room-sized mainframes and minicomputers evolved into a form that fits snugly onto a desk or a lap. Computers have been embedded into commonplace objects like cars, traffic lights, stereos, microwave ovens, and wrist watches, and at some point, these computers achieved wireless networking. Researchers then decided to build even tinier computers, that are equipped not only with wireless communications, but with “wireless power.” These millimeter-scale computers became known as Radio Frequency Identification (RFID) chips, and they are now used in all kinds of applications.

But the fundamental question remains: how do you secure the smallest and weakest of computers? How does one secure computers that can not perform cryptography? And what happens with computers that are so power limited that they can no longer control their own access? As illustrated since the 1970s, naive idealism is not enough.

This Ph.D. dissertation explores the security and privacy issues of Radio Frequency Identification technology. The first part of my thesis expounds upon the
security and privacy threats that RFID faces, and the second part proposes a solution that I call the RFID Guardian.

1.1. MOTIVATION FOR THIS WORK

Radio Frequency Identification (RFID) tags are remotely powered computer chips that augment everyday objects with computing capabilities. Corporate executives tout RFID technology as a technological means to achieve cost savings, efficiency gains, and unprecedented visibility into the supply chain. Scientific researchers consider RFID technology as nothing short of an embodiment of the paradigm shift towards low-cost ubiquitous computing. In both cases, RFID tags will blur the boundaries between the digital and physical worlds.

RFID automation will bring an unfathomable barrage of new applications. RFID proponents extol its professional uses for real-time asset management and supply chain management. RFID-based access passes help to police residential, commercial, and national borders; drivers have embraced RFID-based payment systems like EZ-Pass, FastPass, IPass, PayPass, and SpeedPass. RFID-based “feel good” personal applications are also proliferating, from automated dishwashers, to “smart rabbits”[115].

However, this pervasive computing utopia also has its dark side. Similar to other pervasive computing technologies (e.g., facial recognition, mobile phones), the same ease-of-use and pervasiveness that makes RFID technology so revolutionary offers less-than-ethical characters unprecedented opportunities for theft, covert tracking, and behavioral profiling. Without the appropriate controls, attackers can perform unauthorized tag reading and clandestine location tracking of people or objects (by correlating RFID tag “sightings”). Snooping is possible by eavesdropping on tag/reader communications. Criminals can also manipulate RFID-based systems (i.e. retail checkout systems) by either cloning RFID tags, modifying existing tag data, or by preventing RFID tags from being read in the first place.

Individuals need a means with which they can monitor and control access to their RFID tags (including the low-cost ones). Additionally, consumer privacy would be enhanced by an easy-to-use means of coordinating RFID security mechanisms, and should have fine-grained control over RFID-based auditing, key management, access control, and authentication capabilities.

RFID installations should also be subject to the same kinds of security auditing and “red teaming” like any other kind of computer system. Deployers have the responsibility to audit and test the security of their RFID installations, but they generally have no clue how to do this themselves. The computer security industry
can pick up the ball here, but security experts still lack the right tools to work in the RFID domain. Computer security professionals need tools to help them bridge the gap, and start attacking RFID.

1.2. CONTRIBUTIONS

The research presented in this Ph.D. dissertation has had a two-fold impact. The primary contribution is purely academic; but this research also had a surprisingly large impact on the “real-world.”

1.2.1. Academic

This dissertation presents the design, implementation, and evaluation of the RFID Guardian, the first-ever unified platform for RFID security and privacy administration.

For RFID privacy protection purposes, the RFID Guardian resembles an “RFID firewall”, enabling individuals to monitor and control access to their RFID tags by combining a standard-issue RFID reader with unique RFID tag emulation capabilities. Our system provides a platform for coordinated usage of RFID security mechanisms, offering fine-grained control over RFID-based auditing, key management, access control, and authentication capabilities. We have prototyped the RFID Guardian using off-the-shelf components, and our experience has shown that active mobile devices are a valuable tool for managing the security of RFID tags in a variety of applications, including protecting low-cost tags that are unable to regulate their own usage.

The RFID Guardian also aims to provide a “Swiss Army Knife” for RFID security, offering an integrated suite for the following kinds of RFID-based security testing: security diagnostics and monitoring, packet manipulation and filtering, penetration testing and side-channel attacks. Such a toolkit is essential for performing proper risk assessments of RFID systems, which can then enable deployers to make appropriate tradeoffs between security and RFID application requirements.

1.2.2. Real-World Impact

Much of computer science, while seemingly dry and technical at first blush, has an overwhelmingly fascinating human story behind it. Fortunately, the RFID security/privacy research presented in this Ph.D. dissertation is no exception. Here is a subjective first-hand account of the “real-world” events that unfolded in parallel to the scientific work described in the rest of this thesis.
The RFID Virus  On March 15, 2006, my co-authors and I published an article entitled 'Is Your Cat Infected with a Computer Virus?'[132] at the Fourth Annual IEEE International Conference for Pervasive Computing and Communications (IEEE PerCom) along with a companion website at http://www.rfidvirus.org. (This research is described in Chapter 4 of this dissertation.)

The first reaction to our paper was irrational exuberance from the press. They went wild upon hearing the words “RFID virus,” and the story was picked up by the New York Times, the Washington Post, Reuters, UPI, de Volkskrant, Computerworld, Computer Weekly, CNN, BBC, Fox News, MSNBC, and many other print, broadcast, and online news outlets, and blogs, which are listed at http://www.cs.vu.nl/~ast/rd/. However, while the original two news reports from the New York Times and Volkskrant kept a reasonably balanced perspective, the follow-up news reports one-upped each other with increasingly sensational reports, culminating in fictional “quotes” stating how RFID malware could cause a global infection within 24 hours.

Not surprisingly, shortly after the rapid spread of sensational press articles, the backlash began. RFID industry trade groups issued some statement downplaying the real-world value of our results, in an attempt to reassure nervous customers.[50] Other RFID industry sympathizers used less restraint in their choice of wording, attempting to discredit our research by calling it “rubbish,” “semi-academic,” and “bunk.” The antivirus industry released contradictory negative evaluations of our research. Sophos released a statement saying that our research results were rubbish and meaningless in the real world, while Kaspersky released a press release chiding us for releasing our findings, and calling our research “dangerous” and “immoral.” Some auto-id industry journalists and bloggers just blindly parroted the criticism.

In contrast, other parts of the RFID industry gave us an overwhelmingly positive response. Within 24 hours of release of the article, chief architects of large companies producing RFID middleware were quietly approaching us for help evaluating the security of their RFID middleware. RFID companies, consumer-rights organizations, and the antivirus industry were inviting us to do consultations and/or invited talks. We had to start turning down a number of the offers, due to the demands that all of this was placing on our time. Amidst the chaos, our research paper also received the Best Paper Award for High Impact at the IEEE PerCom conference.

In retrospect, according to Google Trends, our RFID malware research triggered the single largest news event that RFID technology ever had. If you type “RFID” into Google Trends[1], you will get the result that is shown in Figure 1.1. There is a noticeable peak in the “RFID” news reference volume in March 2006. Directly above the peak is label C, which says “RFID Tags Vulnerable”. This
links to a news article describing our RFID malware research.

That goes to show that regardless of whether (or not) the RFID industry agrees with the results of our research on RFID malware, there is no doubt that the research described in this Ph.D. dissertation has raised the awareness of RFID security and privacy issues on a massive global scale.

**RFID Guardian**  The RFID Guardian has had an impact of its own, separate from that of the RFID Virus. A vibrant open-source HW/SW project, the RFID Guardian was one of the first RFID tag emulators, and is the first-ever “RFID firewall”. For this reason, the RFID Guardian has received copious attention in the popular press (i.e. Popular Science and Scientific American). Also, our USENIX Lisa 2006 paper describing Version 2 of the RFID Guardian prototype won the Best Paper Award.

However, the relevance of the RFID Guardian’s tag emulation and security auditing abilities were underscored during the recent attacks on the RFID-based Dutch Public Transportation pass, the “OV Chipkaart.” The OV Chipkaart system
has been successfully attacked four times so far:

1. In July 2007, two University of Amsterdam students, Pieter Siekerman and Maurits van der Schee, used the single-use MIFARE Ultralight cards to exploit a back-end server bug. (I provided these two students with advice during the early stages of their project)

2. In December 2007, three German hackers, Karsten Nohl, Hendryk Plotz, and Starbug reverse engineered the proprietary MIFARE Classic Crypto-1 algorithm. This threatened the security of the multiple-use MIFARE 1K and 4K cards used for OV Chipkaart subscriptions.

3. In January 2008, Roel Verdult, an MSc. student from the Raboud University of Nijmegen, used an RFID tag emulator to conduct a simple but successful replay attack on the single-use MIFARE Ultralight cards. (This type of attack is also possible using the RFID Guardian.)

4. In March 2008, researchers from the Raboud University of Nijmegen conducted a purely cryptographic attack against the MIFARE Classic Crypto-1 algorithm (partially based upon the German hackers’ results), leading to the demonstrated cloning of MIFARE 1K/4K cards.

The OV Chipkaart system cost $2 billion, and the rapid sequence of attacks caused widespread media attention in the Netherlands. For that reason, immediately after the third attack, the Dutch Parliament (“Tweede Kamer”) called an emergency plenary session to discuss the OV Chipkaart hack, during which Tineke Huizinga, the Dutch Secretary of Transport and Public Works (“Verkeer en Waterstaat”) almost lost her job.

On the day prior to the plenary session, a small group of us (Roel Verdult and Wouter Teepe from Raboud Universiteit, Dutch hacker Rop Gonggrijp, and I) were invited to testify at a Dutch parliamentary hearing, regarding the cause of the problems and future of the OV Chipkaart system. (We also had similar meetings with Translink, the deployers of the OV Chipkaart system, and Secretary Huizinga at the Dutch Ministry of Transport.)

We explained to the Parliament members why “security by obscurity” does not work, and discussed how the situation is largely a result of closed-source HW/SW and a closed design processes. (Thus preventing timely advice about the system architecture, and a proper security audit.) We suggested that the Dutch Parliament look to the National Institute of Standards and Technology (NIST) in the USA as an example of how to incorporate open standards and peer review into the design of critical national infrastructure.
Figure 1.2: Testifying at the Dutch Parliament

At least one of the Dutch parliament members took our message to heart. Parliament member Wijnand Duyvendak (GroenLinks) opened the “Tweede Kamer” session with the following words:[29]

... Het debat over de OV-chipcard staat ook symbool, zo ondervonden wij gisteren bij de hoorzitting letterlijk aan den lijve, voor de keuze: open of geheime software. Het failliet van de geheime gesloten software kwam gisteren scherp aan het licht. GroenLinks pleit er al heel lang voor dat de overheid moet gaan werken met open source-software. Gisteren werd pijnlijk duidelijk dat wij misschien een heel hoge prijs moeten betalen voor het feit dat deze raad bij de OV-chipcard niet is opgevolgd. Het lijkt erop dat alle verantwoordelijken zich de risico’s van de gesloten geheime software op geen enkele manier hebben gerealiseerd.

Which translates to:

... The debate about the OV-Chipcard is symbolic, as we discovered firsthand at yesterday’s hearing, for the choice: open or closed software. The bankruptcy of closed source software shone solidly in the limelight yesterday. GroenLinks (a Dutch political party) has urged for a long time that the government should work with open-source software. Yesterday it became painfully obvious that we may pay a high price due to the fact that this advice was not followed for the OV Chipcard. It seems like the responsibility for the risks surrounding the use of closed secret software has not been accepted in any fashion.”
We (the RU researchers, Rop Gonggrijp, and I) have follow-up meetings scheduled with both Translink and the Dutch Ministry of Transport. Our intention is to push the various parties towards independently auditing and patching the current OV Chipkaart system – but only as a means of buying time for the development of a new public transport payment system that will make use of open design processes, open-source HW/SW, and well-known open cryptographic algorithms. (Instead of the current “security by obscurity”).

Despite the fact that the Dutch Ministry of Transport and Translink are listening to us, I do not know if they will follow our advice. Only time will tell.

1.3. STRUCTURE OF THE DISSERTATION

The rest of this dissertation is structured as follows:

- **Chapter 1 - Introduction**
  This chapter introduces the primary themes and motivation for our work, and describes its academic and real-world impact.

- **Chapter 2 - Radio Frequency Identification**
  This chapter describes RFID technology, its infrastructure, and applications.

- **Chapter 3 - RFID Security and Privacy**
  This chapter gives both a historical and modern perspective on the security and privacy threats surrounding RFID technology, and briefly touches upon potential countermeasures.

- **Chapter 4 - RFID Malware**
  This chapter introduces the concept of RFID malware, offering proof-of-concept code for: RFID exploits, RFID worms, and RFID viruses.

- **Chapter 5 - RFID Guardian: Platform Overview**
  This chapter gives an overview of the prototyped RFID Guardian platform, including the HW, SW, and user interfaces.

- **Chapter 6 - RFID Guardian: Primitive Operations**
  This chapter describes the RFID Guardian’s most basic building blocks, including tag emulation, selective RFID query/response jamming, and Guardian Protocol.

- **Chapter 7 - Tools for RFID Privacy**
  This chapter discusses the design and implementation of the RFID Guardian’s main privacy features, including auditing, key management, access control, and authentication.
- **Chapter 8 - Tools for RFID Security**
  This chapter discusses the design and implementation of the RFID Guardian’s main security features, including diagnostics and monitoring, packet manipulation, and penetration testing.

- **Chapter 9 - Discussion**
  This chapter discusses possible attacks against the RFID Guardian, plus some relevant legal issues.

- **Chapter 10 - Related Work**
  This chapter provides a survey of RFID security and privacy research, including both offensive and defensive techniques. It also compares the most closely-related tools to the RFID Guardian.

- **Chapter 11 - Summary and Conclusions**
  This chapter gives a brief recap of this dissertation, and points out some future work and lessons learned.