Available online at www.sciencedirect.com
ScienceDirect
Pervasive and Mobile Computing 2 (2006) 405–426
pervasive and mobile computing
www.elsevier.com/locate/pmc

RFID malware: Design principles and examples☆

Melanie R. Rieback[a,*], Patrick N.D. Simpson[a], Bruno Crispo[a,b], Andrew S. Tanenbaum[a]

[a] *Department of Computer Science, Vrije Universiteit, De Boelelaan 1081a, 1081 HV, Amsterdam, Netherlands*
[b] *Department of Information and Communication Technology, University of Trento, Via Sommarive, 14, 38050, Trento, Italy*

Received 1 February 2006; received in revised form 5 June 2006; accepted 26 July 2006
Available online 6 October 2006

Abstract

This paper explores the concept of malware for Radio Frequency Identification (RFID) systems — including RFID exploits, RFID worms, and RFID viruses. We present RFID malware design principles together with concrete examples; the highlight is a fully illustrated example of a self-replicating RFID virus. The various RFID malware approaches are then analyzed for their effectiveness across a range of target platforms. This paper concludes by warning RFID middleware developers to build appropriate checks into their RFID middleware *before* it achieves wide-scale deployment in the real world.

Keywords: Radio Frequency Identification; RFID; Security; Malware; Exploit; Worm; Virus

1. Introduction

Radio Frequency Identification (RFID) is a contactless identification technology that promises to revolutionize our supply chains and customize our homes and office. By

☆ This is an extended version of the paper Is Your Cat Infected with a Computer Virus? Presented at IEEE PerCom in March 2006.

* Corresponding author. Tel.: +31 205987874; fax: +31 205987653.
E-mail address: melanie@cs.vu.nl (M.R. Rieback).

1574-1192/$ - see front matter
doi:10.1016/j.pmcj.2006.07.008

leveraging low-cost RFID tags, often containing <1–2 kb of memory, proponents of RFID technology aim to create an "Internet of Things"; however these well-meaning experts should be careful what they wish for. While modern RFID deployments are usually small and located in benevolent environments, the Internet is vast and unmanageable, bringing together commercial interests, inexperienced users, and computer hackers. Furthermore, by bringing the Internet to the "things", RFID tags could inadvertently extend digital mayhem into the physical world.

This paper will demonstrate that the security breaches that RFID deployers dread most — RFID malware, RFID worms, and RFID viruses — are right around the corner. RFID attacks are currently conceived as properly formatted but fake RFID data; however no one expects an RFID tag to send a SQL injection attack or a buffer overflow. Unfortunately, the trust that RFID tag data receives is unfounded. To prove our point, this paper will describe the basic design principles of RFID malware. We will provide concrete examples for several target platforms, featuring a fully illustrated specimen of a self-replicating RFID virus. Our main intention behind this paper is to encourage RFID middleware designers to adopt safe programming practices.

1.1. Introduction to RFID

Radio Frequency Identification (RFID) is the quintessential Pervasive Computing technology. Touted as the replacement for traditional barcodes, RFID's wireless identification capabilities promise to revolutionize our industrial, commercial, and medical experiences. The heart of the utility is that RFID makes gathering information about physical objects easy. Information about RFID-tagged objects can be transmitted for multiple objects simultaneously, through physical barriers, and from a distance. In line with Mark Weiser's concept of "ubiquitous computing" [1], RFID tags could turn our interactions with computing infrastructure into something subconscious and sublime.

This promise has led investors, inventors, and manufacturers to adopt RFID technology for a wide array of applications. RFID tags could help combat the counterfeiting of goods like designer sneakers, pharmaceutical drugs, and money. RFID-based automatic checkout systems might tally up and pay our bills at supermarkets, gas stations, and highways. We reaffirm our position as "top of the food chain" by RFID tagging cows, pigs, birds, and fish, thus enabling fine-grained quality control and infectious animal disease tracking. RFID technology also manages our supply chains, mediates our access to buildings, tracks our kids, and defends against grave robbers [2]. The family dog and cat even have RFID pet identification chips implanted in them; given the trend towards subdermal RFID use, their owner will be next in line.

1.2. Well-known RFID threats

This pervasive computing utopia also has its dark side. RFID automates information collection about individuals' locations and actions, and this data could be abused by hackers, retailers, and even the government. There are a number of well-established RFID security and privacy threats.