Is Your Cat Infected with a Computer Virus?

Melanie R. Rieback Bruno Crispo Andrew S. Tanenbaum
Vrije Universiteit Amsterdam
Computer Systems Group
De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands
{melanie,crispo,ast}@cs.vu.nl

Abstract

RFID systems as a whole are often treated with suspicion, but the input data received from individual RFID tags is implicitly trusted. 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. This paper is meant to serve as a warning that data from RFID tags can be used to exploit back-end software systems. RFID middleware writers must therefore build appropriate checks (bounds checking, special character filtering, etc..), to prevent RFID middleware from suffering all of the well-known vulnerabilities experienced by the Internet. Furthermore, as a proof of concept, this paper presents the first self-replicating RFID virus. This virus uses RFID tags as a vector to compromise backend RFID middleware systems, via a SQL injection attack.

1. Introduction

Years after the successful introduction of RFID-based pet tagging, Seth the veterinarian's pet identification system started displaying odd behavior. First, the RFID reader seemed to be reporting incorrect pet address data. A couple hours later, the system seemed to be erasing data from pets' RFID tags. Then the strangest thing of all happened: the LCD display on the pet identification computer froze and displayed the ominous message: "All your pet are belong to us."[1]

Input data can be used by hackers to exploit back-end software systems. This is old news, but it has not prevented RFID system designers from implicitly trusting the structural integrity of data provided by RFID tags. RFID attacks are commonly conceived as properly formatted but fake RFID data. However, no one currently expects an RFID tag to send a SQL injection attack or a buffer overflow. This paper will demonstrate that the trust that RFID tag data receives is unfounded. The security breaches that RFID deployers dread most – RFID malware, RFID worms, and RFID viruses – are right around the corner. To prove our point, this paper will present the first self-replicating RFID virus. Our main intention behind this paper is to encourage RFID middleware designers to adopt safe programming practices. In this early stage of RFID deployment, SW developers still have the opportunity to "lock down" their RFID systems, to prepare them for the attacks described in this paper.

[1] See: http://en.wikipedia.org/wiki/All_your_base_are_belong_to_us

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 simultanously, through physical barriers, and from a distance. In line with Mark Weiser's concept of "ubiquitous computing"[20], 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[6]. The family dog and cat even have RFID pet identification chips implanted in