

# Fragmented malware through RFID and its defenses

Madhu K. Shankarapani · Anthonius Sulaiman ·  
Srinivas Mukkamala

Received: 4 September 2008 / Revised: 2 October 2008 / Accepted: 2 November 2008  
© Springer-Verlag France 2008

**Abstract** Malware, in essence, is an infiltration to one's computer system. Malware is created to wreak havoc once it gets in through weakness in a computer's barricade. Anti-virus companies and operating system companies are working to patch weakness in systems and to detect infiltrators. However, with the advance of fragmentation, detection might even prove to be more difficult. Malware detection relies on signatures to identify malware of certain shapes. With fragmentation, functionality and size can change depending on how many fragments are used and how the fragments are created. In this paper we present a robust malware detection technique, with emphasis on detecting fragmentation malware attacks in RFID systems that can be extended to detect complex obfuscated and mutated malware. After a particular fragmented malware has been first identified, it can be analyzed to extract the signature, which provides a basis for detecting variants and mutants of similar types of malware in the future. Encouraging experimental results on a limited set of recent malware are presented.

## 1 Introduction

RFID usage has been increasing steadily as of late, mainly in retailing [1]. One example is Wal-Mart, the world's largest retailer. According to CBS Market watch, Wal-Mart insists

its top suppliers' package products with radio-frequency identification tags [2]. The RFID system represents the most sweeping supply-chain advancement since June 16, 1974, when Wm. Wrigley Co. scanned the world's first, official grocery-store bar code on a pack of spearmint chewing gum.

The main difference between RFID tags and bar code system is that the bar code system requires the item to be imprinted with a bar code. This bar code is then scanned. During this process, an item may be scanned twice. RFID tags do not require the RFID reader to actually see the bar code. The tags themselves are embedded in the packaging labels. These tags can be read by wireless scanners. However, the tags must be within an acceptable distance to be read by the scanner. Even with this drawback, an RFID system automates the inventory procedure more than bar codes.

Another advantage that RFID tags have over bar codes is that the tags can contain more information. The error of scanning an item multiple times is a thing of the past.

Of course, RFID system is not only the monopoly of retailers. Companies have started to use RFID in their employees ID cards. RFID may even be used in passports [3]. Some countries may already have done so. While RFID has myriads of benefits, it also has its downside. Beside privacy concerns over RFID-enabled passports, there are malwares that can infect via RFID tags as well.

In this paper, we are providing a few examples of what RFID malware can do to an RFID-enabled system. We are also providing defense mechanisms that can be put in place to thwart RFID-related malware. Our focus is on the RFID fragmentation attack that we developed in our laboratory. Our defense mechanism is also geared towards protection against fragmentation attacks.

Previous works that have been done on RFID will be discussed in Sect. 2. Section 3 provides an insight to an RFID system and attacks on RFID is provided in Sect. 4. Since our

---

M. K. Shankarapani · A. Sulaiman · S. Mukkamala (✉)  
Department of Computer Science,  
Institute for Complex Additive Systems Analysis,  
Computational Analysis and Network Enterprise Solutions,  
New Mexico Tech, Socorro, New Mexico 87801, Mexico  
e-mail: srinivas@cs.nmt.edu

M. K. Shankarapani  
e-mail: madhuk@cs.nmt.edu

A. Sulaiman  
e-mail: ais@cs.nmt.edu