IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Malware :RFID

Ankur Singh Bist
Govind Ballabh Pant University Of agriculture And Technology, India
ankur1990bist@gmail.com

Abstract

This paper presents various approaches and analysis that describes the terminology for RFID malware. There are various approaches used for RFID malware analysis and still lot of work is going on in this direction. Our purpose in this paper is to analyse the various basic terms and approaches that have been introduced in this particular domain.

Keywords: Computer worms, RFID.

Introduction

RFID radio frequency identification is the use of a wireless non contact system that uses radio frequency electromagnetic fields to transfer data from a tag attached to an object for the purpose of automatic identification and tracking.

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 [1]. 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" RFID tags could turn our interactions with computing infrastructure into something subconscious and sublime. Some tags read via electromagnetic induction and require battery no battery. The tag contain electronically stored information that can be sensed from a distance of few meters . The tag does not need line of sight as required by barcodes [1][2].

RFID tags may send the buffer overflow and SQL injection attacks generally his kind of behavior is typical to predict so middleware designer of RFID tags should take care about these type of situations and should use proper checks.

RFID tags used in libraries: square book tag, round CD/DVD tag and rectangular VHS tag.[1]

A sheep with an RFID tag.[1]

Designing

There are various security threats that occur in RFID [2] ---

1. Sniffing
2. Tracking
3. Spoofing
4. Replay attacks
5. Denial of service

Computer worms can be defined as a programs that can have the process of self propagation .RFID worm propagates by breaking security boundary in RFID services. There are various process that have been used in the direction of classification of worms from normal files that will finally lead to worm detection.

Figure . First RFID tag infected with computer virus[2]

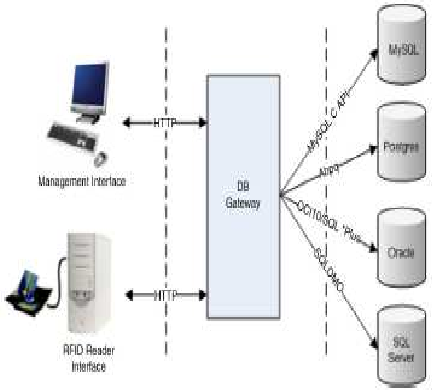

Figure ---RFID malware test platform[3]

There are various entities that are involved that are present in designing of RFID malware [3] —

1. **RFID exploits**
- SQL injection
- Code insertion
- Buffer overflow
- Payloads
2. **RFID middleware**
3. **RFID worm**
4. **RFID viruses**
- Viral self replication
- Self referential commands
- Quines
- Adding payload as introns
- Polymorphic RFID viruses
- Optimization

Security measures can be taken by adopting following methods [4] —

1. Bounds checking
2. Sanitize the input
3. Disable back end scripting language
4. Use parameter binding
5. Isolate the RFID middleware server
6. Review source code

Conclusion

In this paper basic terminology related to RFID malware is explained. There are various issues related to designing get reviewed with prevention methods at last. This study will be helpful for basic idea in this domain and for further research .

References

[1] www.wikipedia.com

[2] Melanie R. Rieback , Andrew\S. Tanenbaum ,” Is Your Cat Infected with computer virus ?”.

[3] Melanie R. Rieback , Andrew\S. Tanenbaum ,”RFID malware :Design principles and example “

[4] www.csharpcorner.com. ,”Advance concept o prevent SQL injection”