Fastcomcorp Research

White Paper

RFID Security Assessment

Introduction

In the drawing board one of the many things we looked into is RFID security and if we could apply it to a potential application, make RFID better, or come up with something better. This document is a summary of our research group notes on notepads, drawing board stuff in the conference room, and on many of our late nights when attempting to develop a higher level of abstraction.

Radio frequency identification (RFID) is a means of automatic identification that uses radio waves to detect, track, identify, and thus manage a variety of objects. You have one device sending the radio waves looking for a response. The other device is a tag. Each tag consists of an antenna constructed from a small coil of wires and a microchip used to store information electronically about the object.

RFID technology is everywhere, now in keycards to access a building, track packages, and now RFID tags are being distributed to pay for tolls in cities. One of the biggest surprises about RFID we found that this technology has been around for 60 years. It was developed by Great Britain known as the IFF system that was utilized to distinguish between friendly and enemy aircrafts in the 1940's.

Our group biggest question was could we utilize RFID as a security token like a key to secure something important such as a software application. So we took a look at the RFID spectrum.

	LF	**HF**	**UHF**	**MW**
Frequency	30 – 300 KHz	3-30 MHz	300 – 1000 MHz	2 -30 GHz
Data Transfer	Less 1Kbit/s per second	Up to 25Kbit/s per second	Up to 30Kibt/s per second	Up to 100 Kbit/s per second
Range	Up to 1m	Up to 1.5m	433 Mhz up to 100m 865 – 956 Mhz .5 – 5m	Active up to 15m Passive up to 3m
Application	Best for metal	Best for close proximity	Best for long range	Best for fast data transfer rates

Vulnerabilities We Found

Spoofing – We found that it is possible to spoof an RFID chip by capturing the data of the valid tag remotely or nearby proximity then unto an empty tag.

Cloning – Copy and Paste data of a valid tag.

Infection – We found a white paper from some researchers that successfully reported that a virus can be embedded in a RFID tag to take down an entire RFID system down.

Eavesdropping – A risk exists that the communication between tag and reader can be eavesdropped when interrogated by an RFID reader from an attacker due to the tag no matter what emits data and a unique identifier.

Tackling the Vulnerabilities

We came to the conclusion that it was not a safe bet to utilize RFID technology to secure something important because with great diligence of whatever counter measure was developed it could still be broken due to the tools available to break RFID security.

Safe Application of RFID Technology

Safe application of the technology is solutions such as consumer application in products instead of a bar code, supply chain, asset tracking, and access control in a building with cameras to track employee's access.

Fastcomcorp Research Team

Eric Gough

Francisco Pinochet

Kimlong Loung

Michael Thompson

Ryan Sema