RFID access control system, what it is and how to defeat it

Description

The presentation will consist of multiple parts.

The first part will break down the architecture of the average access control system, a high-level overview of the card, reader, communication with controller and controller, and a bit about electronic locks.

The second part will get into different types of cards and readers, including readers with backward compatibility and how that can be exploited.

The third part will talk about readers talking to controllers, and usual ways readers talk to controllers, and how that can be exploited.

The fourth part will discuss common mistakes integrators and equipment manufacturers make while producing RFID access control systems and how to exploit them.

Abstract

People attending the presentation will have the chance to try out some of the tools and see an example access control system.

While exploring the interesting world of RFID, witnessing a disappointing amount of improper implementations of access control systems, and dealing with shady vendors for backdoored cards, I realized there is a need for the proper education of people and making sure they know what to look for.

Prior knowledge about any of the topics of this presentation is optional, and it is appropriate for both beginners and someone who might already know something about this topic.

While some of the techniques and demos might look like some James Bond-level magic, most of the stuff I will be demoing and talking about can be done with pretty inexpensive equipment (you might need to spend some money if you decide to go deep into research equipment) and without much prior learning.

If you want to find more about some kind of credential, please,

Table of contents

- About me
- About presentation
- Access control system
- Card (ass grab tech)
  - Powering card - Electromagnetic induction
  - Data modulation - Load modulation
  - Command modulation
  - Figuring out the frequency
  - LF cards
    - LF card standards
    - Vulnerabilities and characteristics
    - Tools
  - HF cards
    - Vulnerabilities and characteristics
    - HF card standards
    - Tools
  - UHF cards
- Controller
- Attacks
  - Hardcoded/default credentials
  - Fuzzing attacks

About me

- nemanjan00
- I like to take things apart
- Sometimes put them back togetger
- Reverse Engineering, RND and DevOps @ Constallation

About presentation

Scope:

- RFID credentials
- RFID readers
- Highlevel controller overview
- Integrator mistakes and problems

Out of scope:

- Magnetic tape
- Biometrics
- Plate recognition
- OSDP
- Business logic

Access control system

```
Card -> Reader -> Controller -> Door
```

Card (ass grab tech)

Unique ID

- Different length
- Magic cards

Power supply:

- Active
- Passive

Frequency:

- LF (125kHz, 134khz)
- HF (13.56Mhz)
- UHF (300Mhz - 3Ghz) - Mostly for inventory systems, parking and tolls

Powering card - Electromagnetic induction

Current gets induced in one of these cases:

Controller

Input signal:

- Wiegand
- OSDP (out of scope)

Output signal:

- Control the relay
- Audiovisual feedback

Attacks

- Cloning credentials
- Hardcoded/default credentials
- Fuzzing attacks
- Downgrade attacks
- Crypto or PRNG implementation attacks (for example nested, hardnested and darkside attacks on Crypto1)
- Wiegand sniffing and replay
- Controller and reader combo attacks

Hardcoded/default credentials

- Some controllers come with default credentials hardcoded
- There are backdoor credentials
- Some of them have been leaked (No security by obscurity)

Fuzzing attacks

- There have been cases where readers did unlock for some

Extra - Privacy concerns with UHF RFID cards

Product identification by GS1 standards

- UPC
  - Company prefix
  - Item reference number
- EPC
  - Company prefix
  - Item reference number
  - Product serial number

About the community

- Iceman Discord (1$ donation)
- Abstract Security Discord
- RRG Github