---

title: “RFID access control system, what it is and how to defeat it”
author: “Nemanja Nedeljkovic”
theme: “Hannover”
colortheme: “beaver”
lang: en-US
classoption: “aspectratio=169”
fontsize: 10pt
colortheme: “dolphin”
mainfont: Noto Sans
toc: true

About me

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

About presentation

Scope:

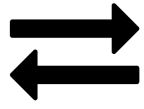
- RFID credentials
- RFID readers
- Highlevel controller overview
- Integrator and manufacturers mistakes and problems

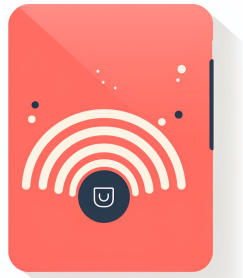
Out of scope:

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

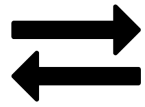
Access control system

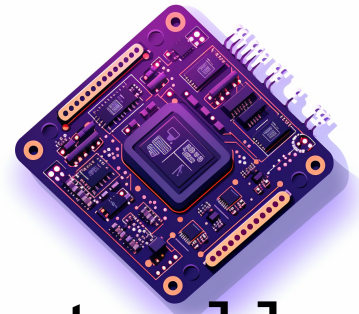
Card





Reader





Controller

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

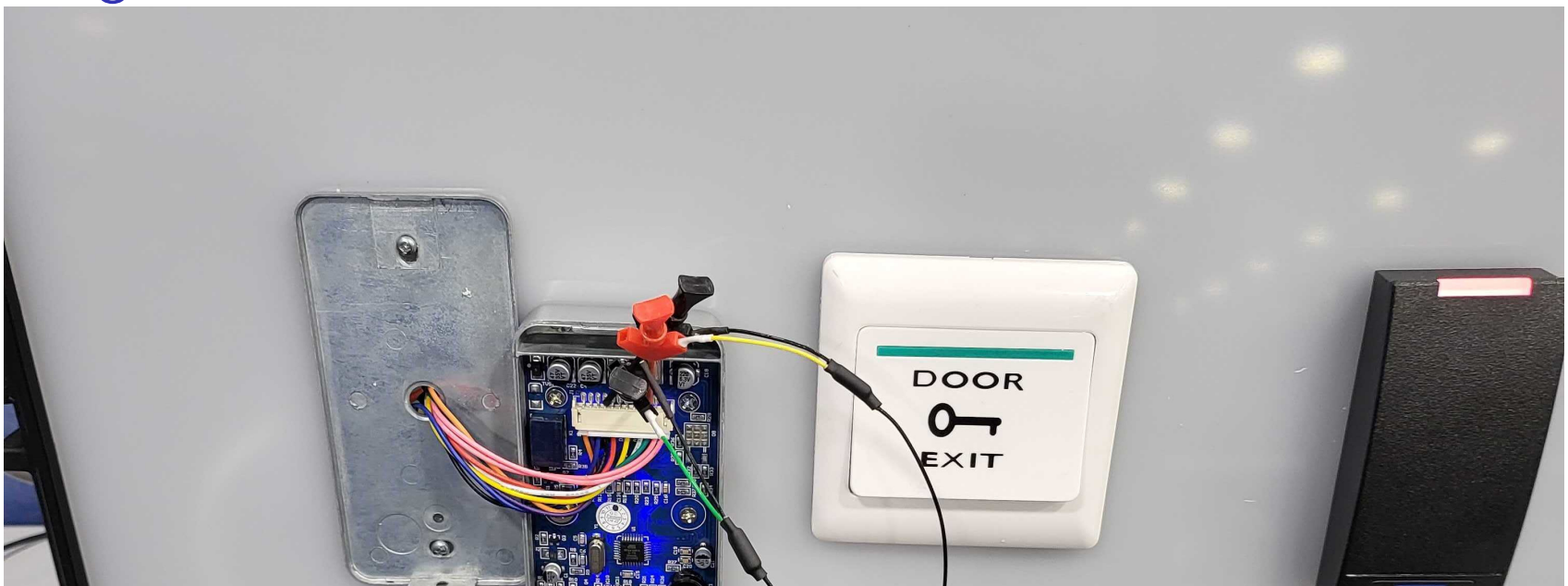
Input signal:

- Wiegand
- OSDP (out of scope)

Output signal:

- Control the relay
- Audiovisual feedback

Wiegand



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
- RRG Github