Behind Closed Doors

Bypassing RFID Readers

Julia Zduńczyk

$ whoami

Julia Zduńczyk

IT Security Specialist at securing

- Penetration Tester
- Red Teamer
- Horse archer, diver, caver, rock climber, hiker, gymnast…
- tl;dr – I like adrenaline rush :P

Disclaimer

Even though this version of slides contains additional notes that summarize topics discussed during actual live briefing, the original presentation included multiple live demos covering more topics. I encourage you to watch the recording of the session :)

RFID

Radio Frequency Identification

Source: www.nfcwork.com

Item tracking

Source: https://wallester.com

Contactless payments

Source: https://dicsan.com

Access Control

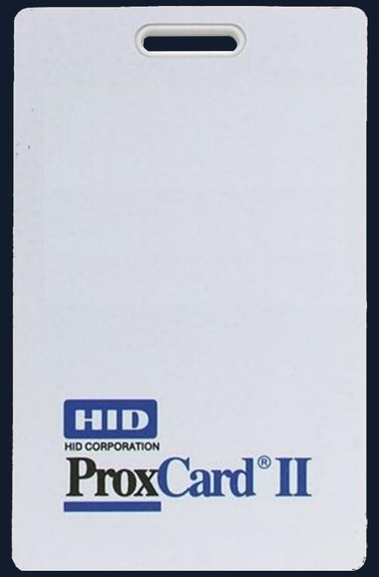
RFID

Other interesting use cases

Coffee filters

Road signs tracking…?

Card cloning



Sometimes it works…

In Red Teaming scenarios we must be quick and efficient. Access card cloning is easy when:

- the system in use is insecure
- employees don’t employ good card handling practices e.g. they leave their cards unattended in places accessible to unauthorized people

Card cloning

Sometimes it does not.

When an access system used in the facility is secure, e.g. employs proper encryption, it is very hard or expensive to clone access cards. In this case it is often not worth it for the attacker to try card cloning and risk being caught in the process.

Card cloning

Sometimes it does not.

And we will not always be so lucky to find cards permanently attached to readers as in this example ;)

How can we bypass RFID access control systems without card cloning?

Access control systems

Autonomous RFID locks

Reader is the decision-making unit, storing valid cards in its memory

Tag UID (via RF)

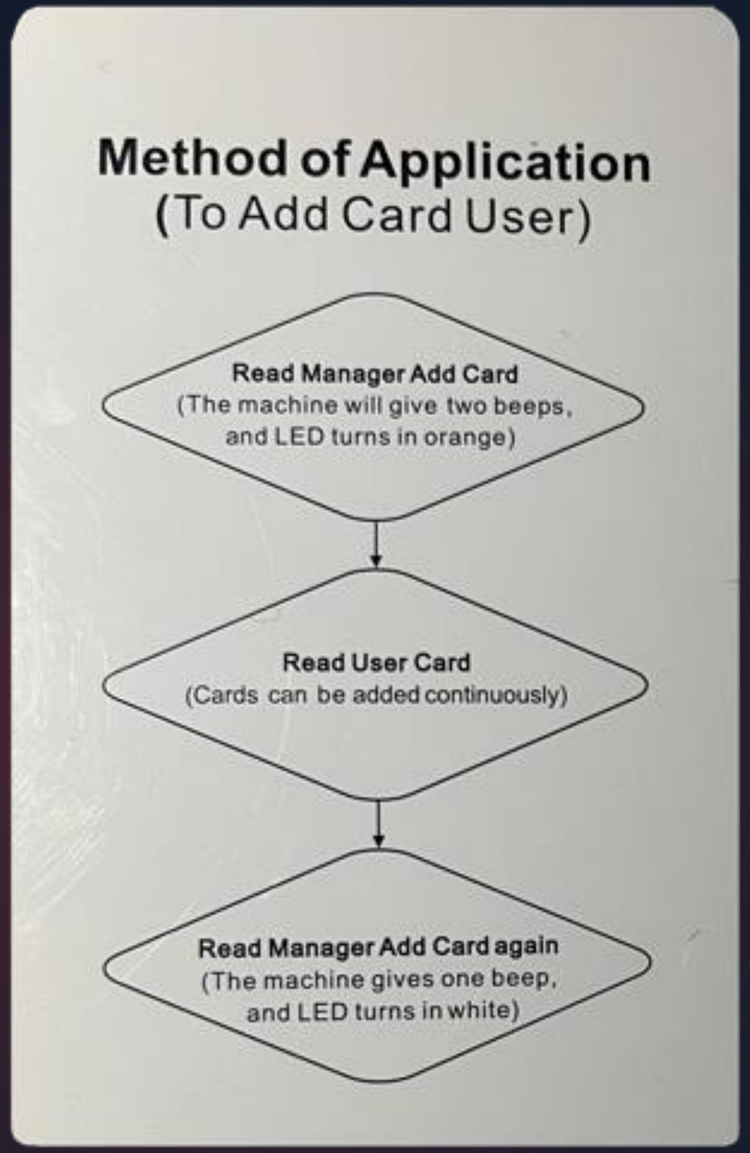
Open/Close command (via wires)

How this works?

Based on the Sebury reader example:

New cards can be added using:

- Manager Add and Delete cards



How this works?

New cards can be added using:

- Manager Add and Delete cards
- “administrator setting”

8. Detailed Programming Guide

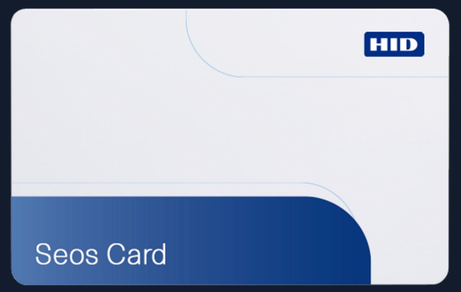
Standby	Master code	Start Menu	Sub Menu	Setting	Remarks
Logo LED Light indication					
White	Red	White Flash	Red	Orange	
Administrator setting					
*	Master code #	0	0	New master code # Repeat new master code # (Note: Code length:6~8 digits, factory default :888888)	
			1	Read Manager Add Card	
			2	Read Manager Delete Card	

What can go wrong?

- Leaving factory default PIN for admin settings
- Logic bypass of the lock operation – a card that would always open a lock (in this case card with UID ‘FFFFFFFF’ cannot be deleted from the system)
- Electromagnetic pulse generator? It can sometimes reset reader’s memory and open the lock (or it may fry the reader – don’t try it at home ;))
- Many other possible problems

Access control systems

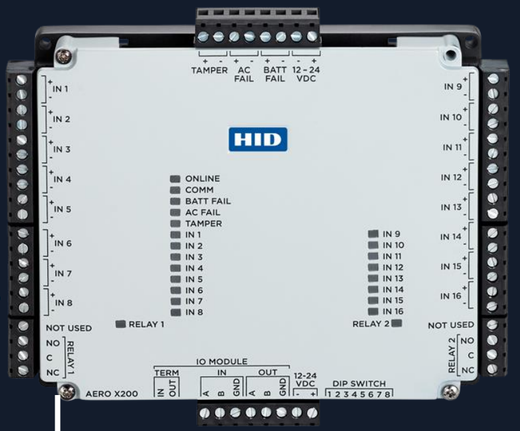
Reader + Controller



Card data
(via RF)

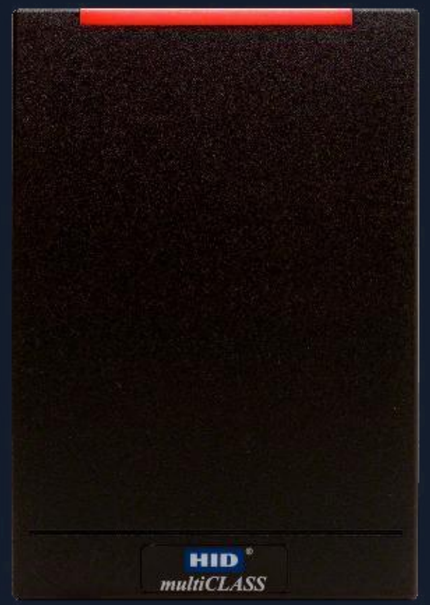
Card credential (via wires)

Open/Close
command

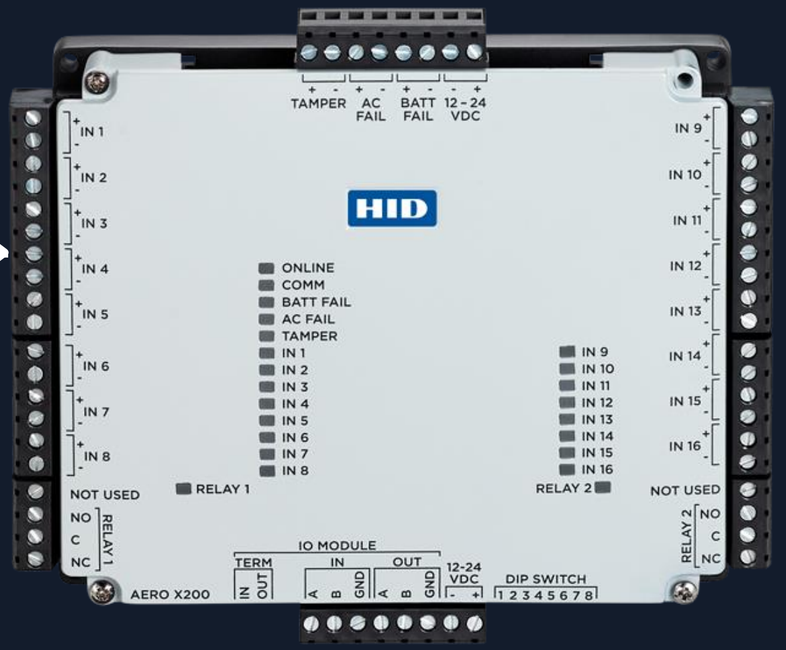


Controller

Communication protocol between the reader and the controller

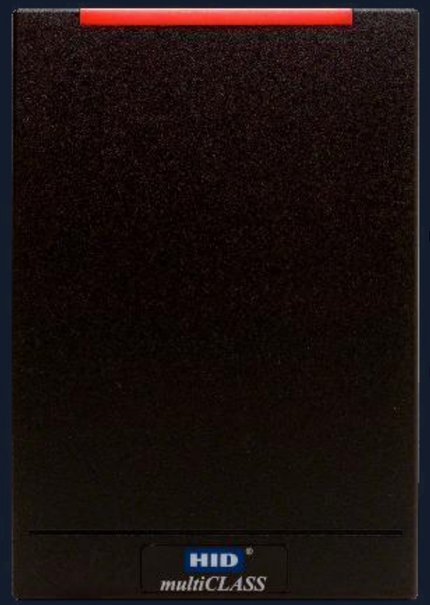


Wiegand



Controller

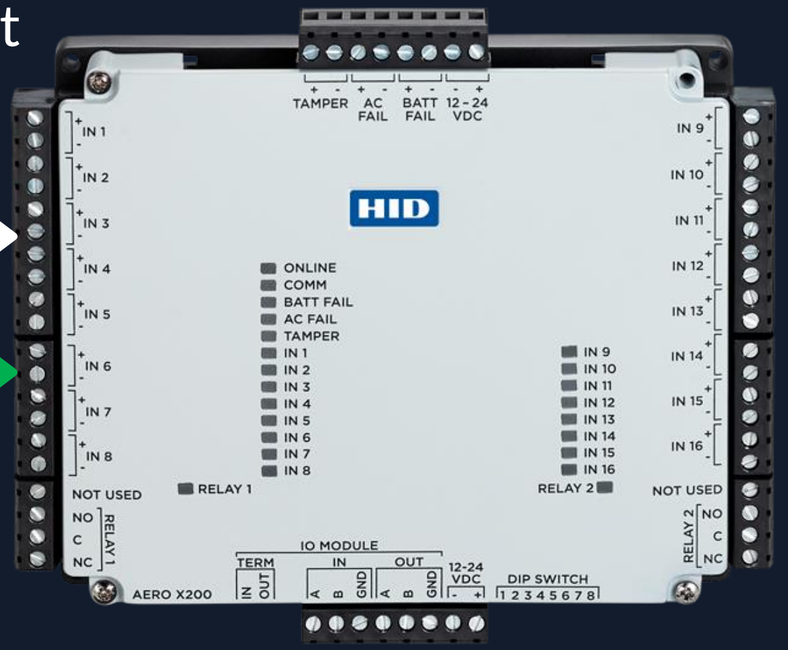
Wiegand



Wiegand uses two wires for data transfer. The data is sent in plaintext.
There is no encryption.

Data 1

Data 0



Controller

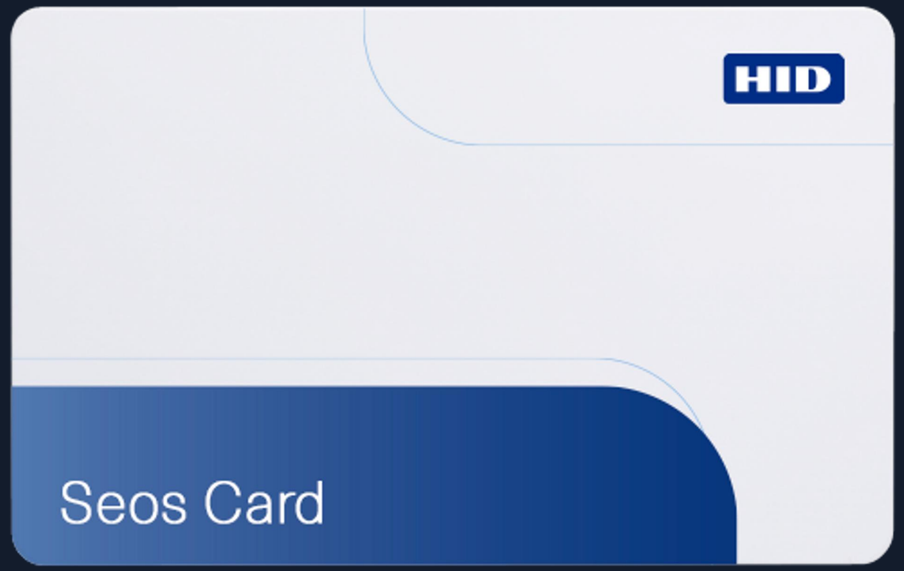
Red Team approach

How would we use that knowledge in a real physical Red Team assessment?

Red Team approach

- Step 1: learn what type of access system we are working with

Card used in the example



Seos Card

- Hard or expensive to clone
- Real credential is encrypted inside the card

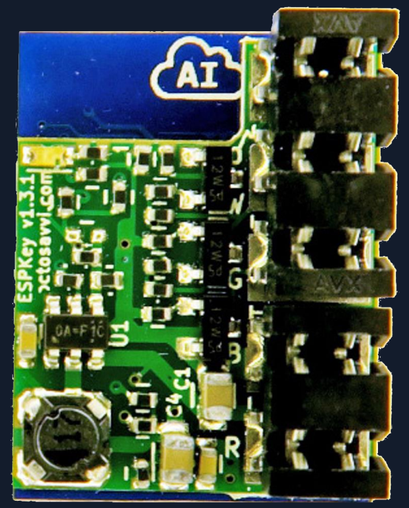
Red Team approach

- Step 1: learn what technology we are working with
- Step 2: decide which attack has high chance of success but does not pose a high risk of detection

Clone the cards? Attack Wiegand?

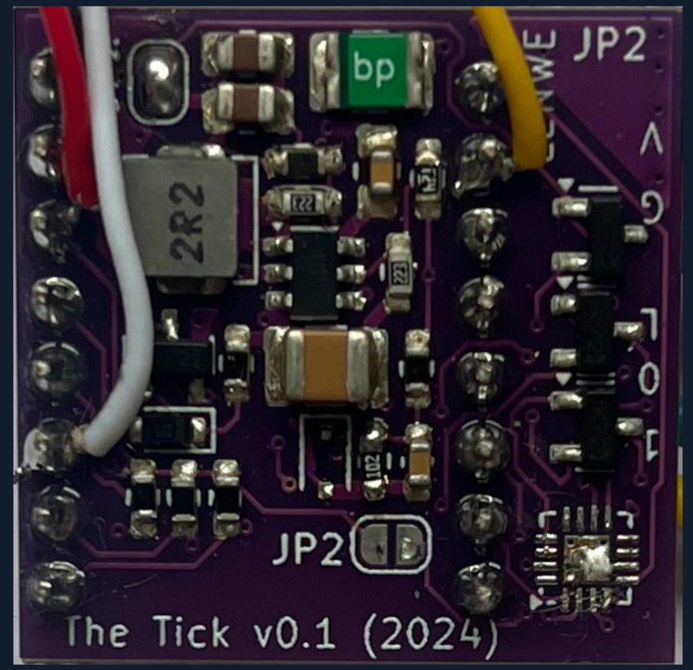
Wiegand Protocol Attack

Let’s sniff the communication



ESPkey
by Octosavvi

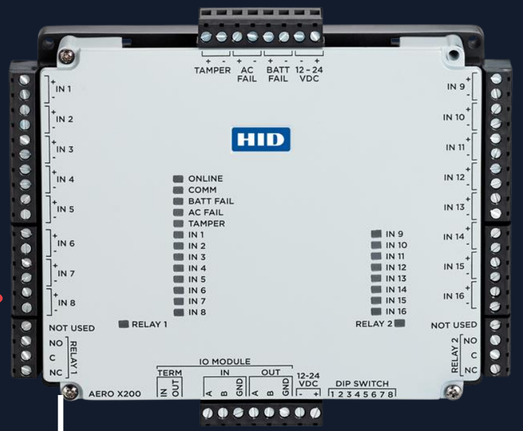
BLEkey
by Mark Baseggio and
Eric Evenchick



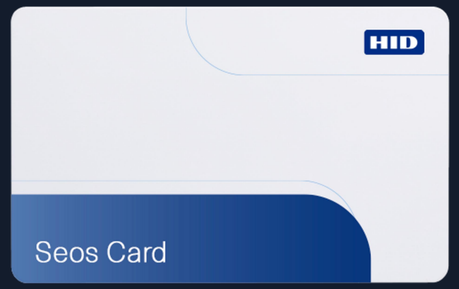
The Tick
by Jakub Kramarz
(with my small contributions ;)

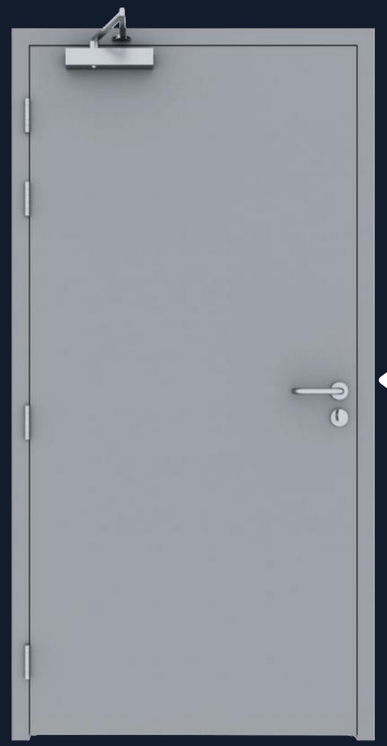
Access control systems

Reader + Controller



Controller





We can install the Tick on the Wiegand wires behind the reader and intercept the communication.

Success

After the Tick is implanted, we can connect to it via WiFi or Bluetooth and open the door remotely whenever we want – but we can only open the door where the Tick is installed.

Now, we want to make a clone of the card to get access to other areas protected by readers.
How?

SEOS cards

Real credential that is sent later via Wiegand is encrypted inside the card. Even though we have the unencrypted value, to make an exact clone we would still need the key to write data to the forged card. We have to find another way to clone this card.

Watch carefully

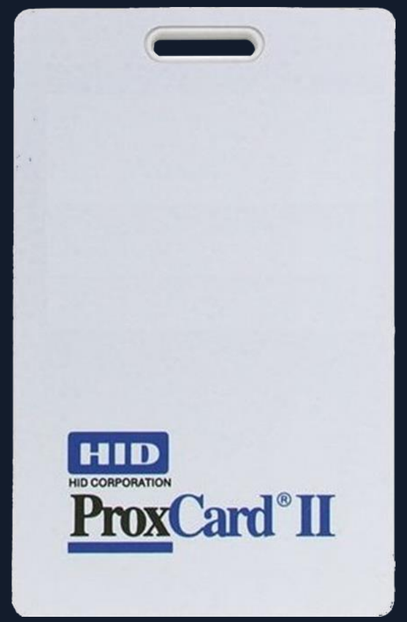
Let’s see once again which cards the reader supports. Maybe someone left some legacy settings turned on?

We can check that by putting different types of cards close to the reader and observing it’s reaction.

Cards used in the example

Seos Card

- More secure, way harder to clone
- Real auth data is encrypted inside the card

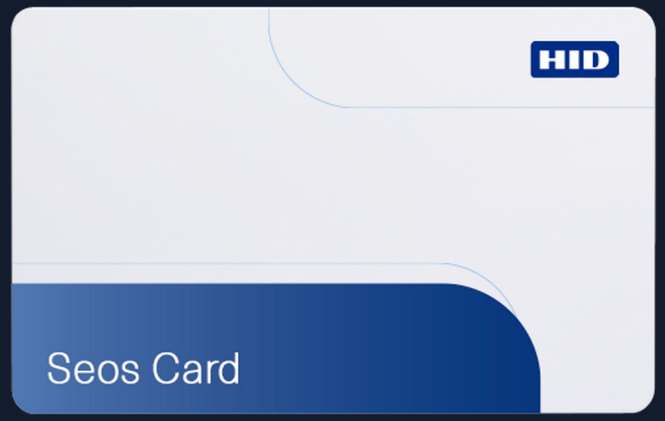


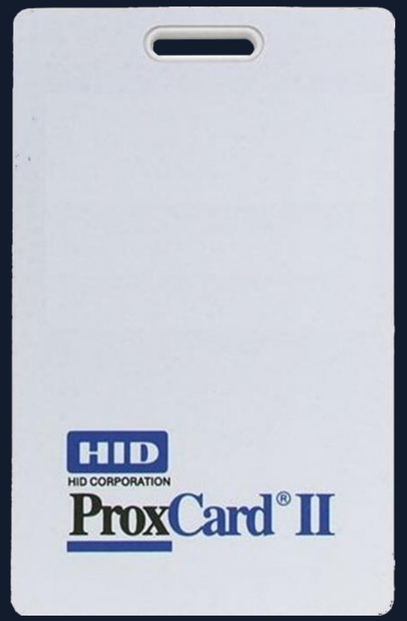
Prox Card

- Insecure
- Unencrypted data sent to the reader
- Easy to clone

Downgrade attack

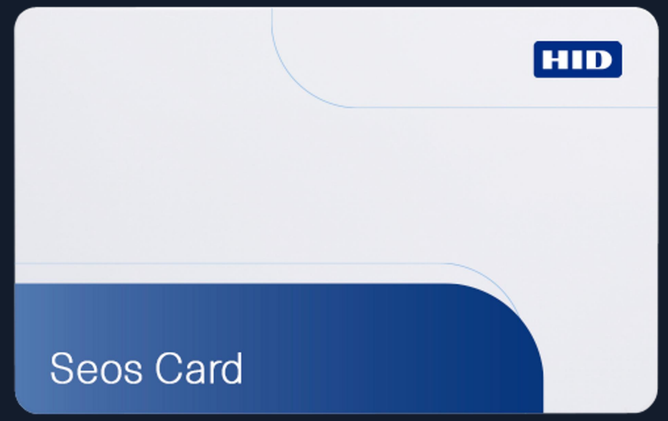
- Prerequisite:
  - The system must have legacy credentials enabled (e.g. Prox cards)
- The idea:
  - Obtain the decrypted data of the card that is not possible/easy to clone
  - Write this data to an old-type, less secure card that will send it to the reader directly in plaintext





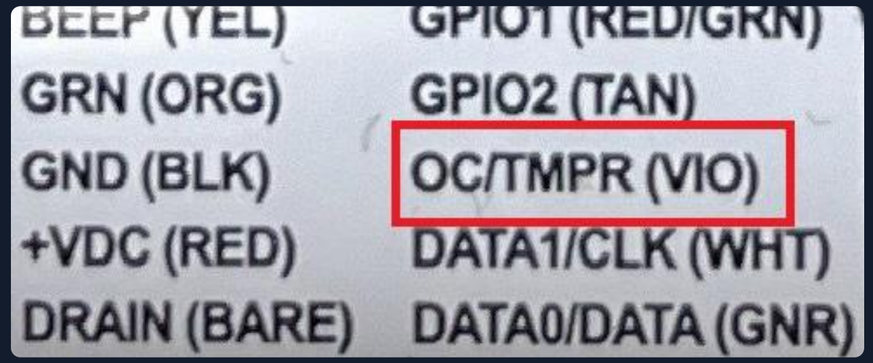
Downgrade attack

After successful downgrade attack, we obtain a new physical card that can be used on other readers in the facility with legacy credentials enabled. From the perspective of the controller, it will recognize it as a known, valid card, because the data sent over Wiegand will be exactly the same – even though it is a different card type.

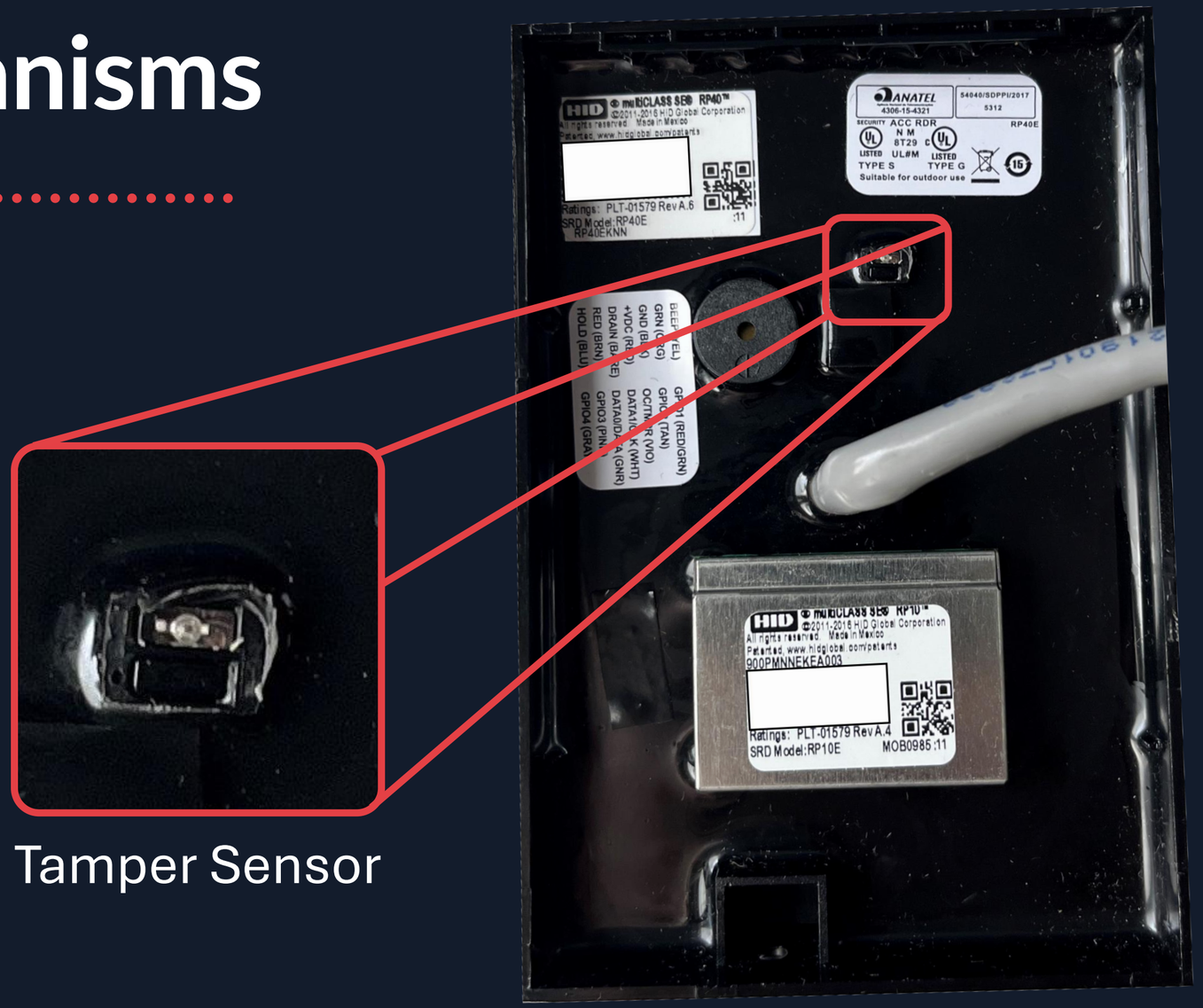


Anti-tamper mechanisms

The alarm triggers when the reader is taken off the wall, but it must be configured correctly – connected to a system that alerts security guards immediately.



Tamper detection wire label



Tamper Sensor

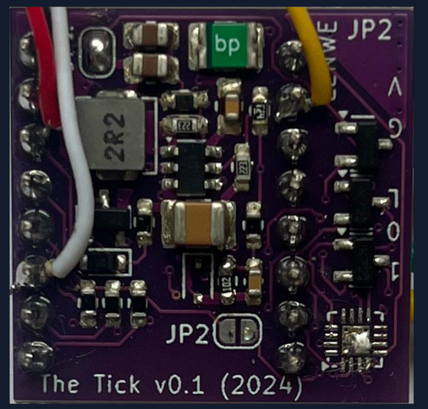
Open Supervised Device Protocol

- successor of Wiegand
- supports AES encryption
- bi-directional
- utilizes the RS485

Open Supervised Device Protocol

- supports AES encryption: when secure mode of operation is used

Interesting DEFCON talk:
“Badge of Shame”
by Dan Petro & David Vargas



See you in a year (maybe :P) with OSDP support

Cool, but how could we get inside to install the device in a real-life scenario?

Maybe try social engineering?

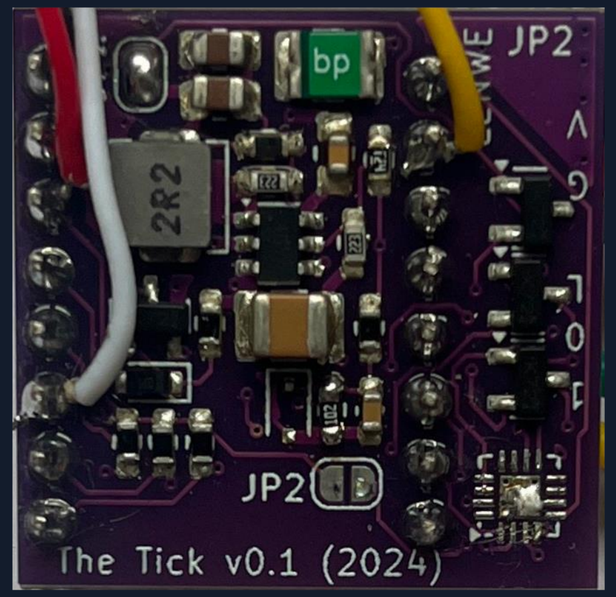
Trust me bro
I’m an engineer

Sometimes we may be able to get inside and install the device without rising suspicion with use of some kind of disguise. However, in most cases all you really need is a lot of confidence – if you act as if you belong and know what you are doing, in many places you will be able to get away with a lot – e.g. opening server-room doors with metal hangers (true story ;))

Reader Denial of Service

And how to make it useful

Let’s say we want to install some malicious devices inside the server-room, but we don’t want to get caught while doing it. We can run a DoS attack e.g. with the use of the Tick installed behind the reader to stop the reader from accepting cards thus denying access to the room.

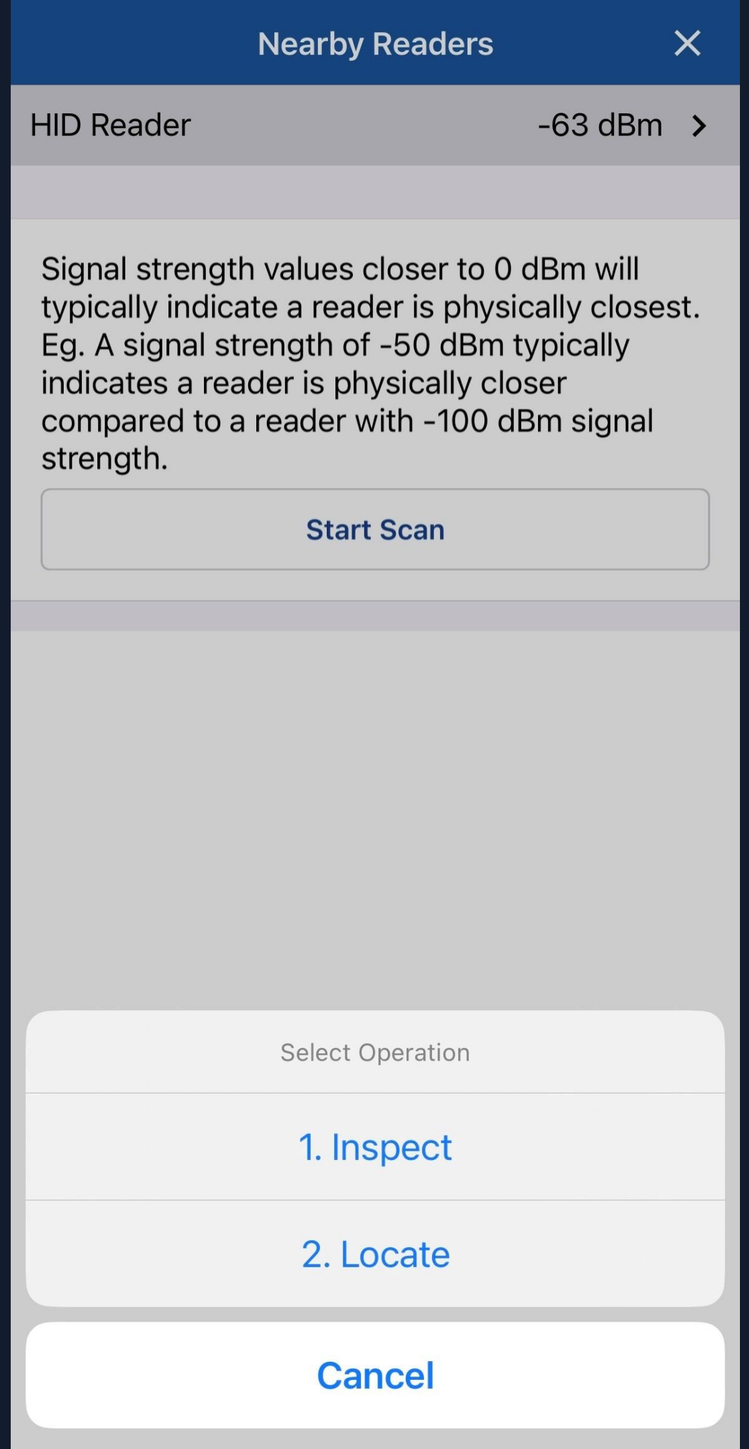


DoS mode – flooding data lines with random bits

Reader DoS

And how to make it useful

We can also use a vulnerability in some unpatched, Bluetooth-enabled HID Readers. With the use of the HID Reader Manager app, we can scan for nearby readers and then “Inspect” or “Locate” them. Using one of these options in a loop allows us to ‘block’ the reader. In case of “Inspect” mode, the reader’s LED will blink, and it won’t accept any cards…



Reader DoS

And how to make it useful

…and in case of “Locate” mode the reader will blink and beep loudly – we could use it as a decoy, making a lot of noise and chaos in one part of the target building while we perform some tests/attacks in other part.

How to secure access control systems against these attacks?

- Always place access controllers in secure areas
- Use a more advanced solution – OSDP over Wiegand
- Configure the protocol correctly (secure mode)
- Use proper tamper detection, collect and monitor logs
- Keep reader firmware up to date
- Disable legacy credentials
- ...

Black Hat Asia Sound Bytes – Key Takeaways

- Physical Access Control Systems are oftentimes insecure
- Physical Red Teaming is a service deigned to check for these vulnerabilities that are otherwise often overlooked
- Raise awareness, educate, learn

Special thanks

- Sławomir Jasek - https://smartlockpicking.com
- Jakub Kramarz - https://github.com/jkramarz/TheTick
- Maciej Mionskowski
- My dad :)
- Everyone who puts their time and effort into PACS research

securing

Thank you

I AM

Julia Zduńczyk

FIND ME ON LINKEDIN

www.linkedin.com/in/jzdunczyk

WEBSITE

www.securing.pl