HID CARD HACKING

Larry Pesce
Director of Research / InGuardians
Twitter: @haxorthematrix

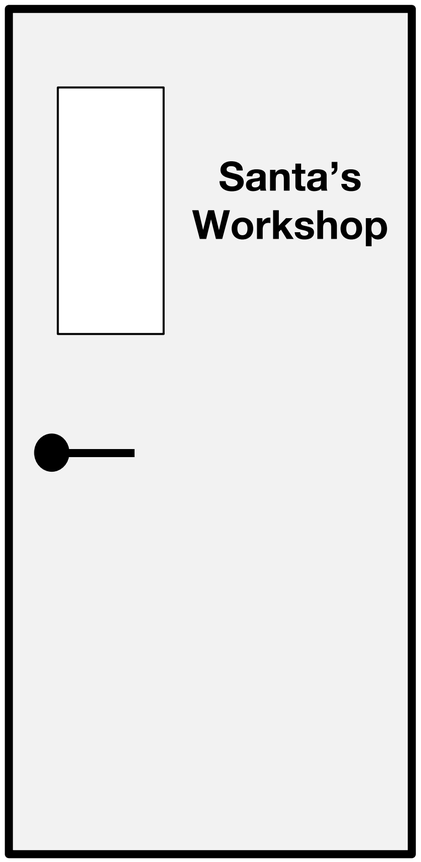
HID ProxCard II

- Very popular system for access control
  - Exterior doors to buildings
  - Interior doors to secure facilities
  - Parking garages, gated locations, etc.
- Low-cost solution for flexible access control

Legacy 125-kilohertz proximity technology is still in place at around 70% to 80% of all physical access control deployments in the U.S. and it will be a long time before that changes.
Stephane Ardiley, product manager at HID Global

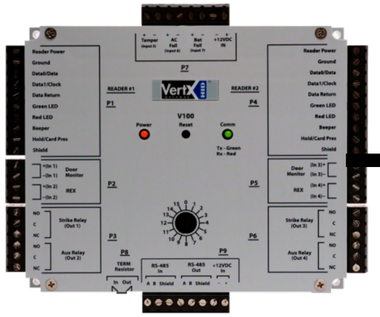
HID Proximity Lock

HID Prox II Reader



Wiegand Protocol

HID VertX Controller



Third-Party Access Policy Software

EXAMPLE

The reader converts the card data to the Wiegand protocol; the controller authorizes or denies the unlock event based on third-party software access policies.

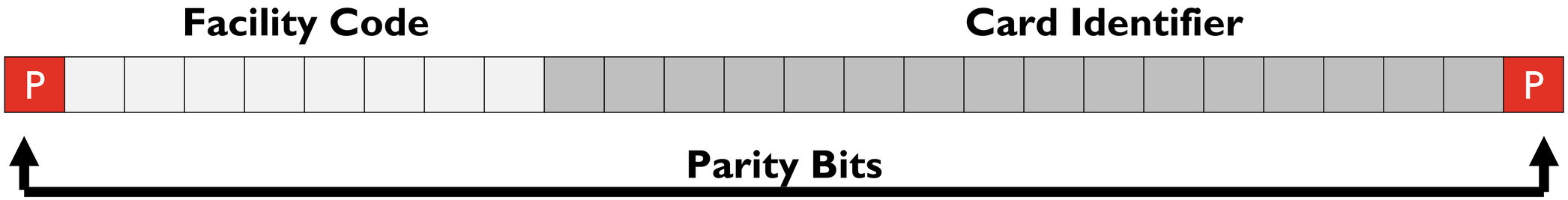
HID ProxCard II Format

WHAT'S INSIDE

The HID ProxCard II PICC is based on an Atmel T5557 RFID chip design. The T5557 is commercially available for other purposes.

HID ProxCard II Data Format

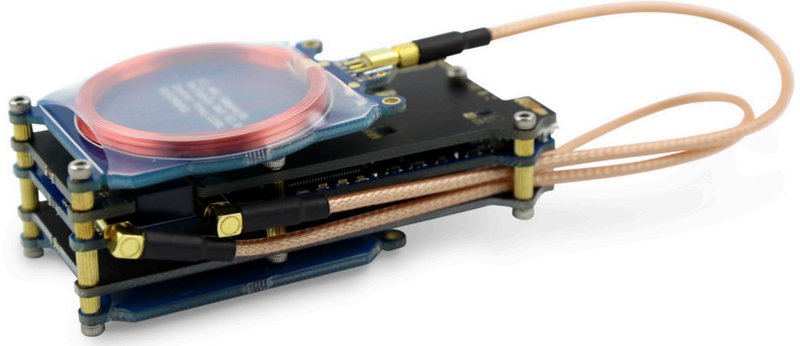
- RFID card read returns a facility code and the card ID value
  - Facility code is 1-255 (0 is reserved)
  - Card ID is 1-65,535 (0 is reserved)
- Data is encoded in the Weigand protocol 26-bit data format at reader and sent to controller

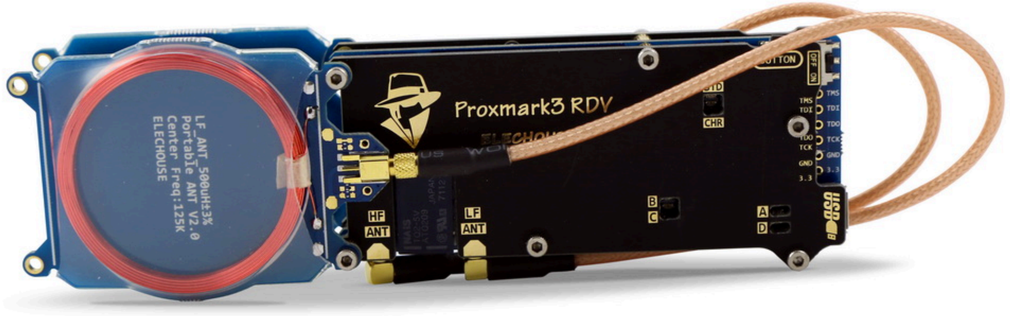


HID Corporate 1000 formats also support combinations of 34–37 bits, have no added protection against cloning attacks.

Proxmark 3 RDV2

- General-purpose RFID research and analysis tool
  - Hardware design by Jonathan Westhues, software by Gerhard de Koning Gans et al.
- Supports HF and LF tags
  - Can also sniff and analyze low-level activity
- Support to interrogate and emulate tags
- Support for Linux and Windows over USB
- Multiple firmware options (Iceman, Proxbrute, HHC, etc.)



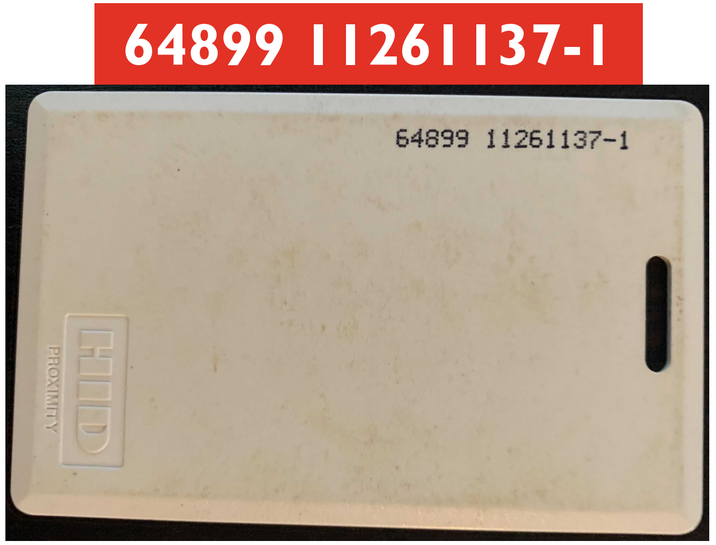


HID ProxCard II Read and Simulate

- No Protection against cloning attacks
- Read event against card with Proxmark is sufficient to clone and replay facility and card ID values

```
[usb] pm3 --> lf hid read
[+] [H10301] - HID H10301 26-bit; FC: 149
CN: 64899 parity: valid
[=] raw: 0000000000000024012bfb06
```

```
[usb] pm3 --> lf hid sim -r 24012bfb06
[=] Simulating HID tag using raw 24012bfb06
[=] Press pm3-button to abort simulation
```



Clone HID ProxCard

- Standard HID ProxCard II tags are not writable: Facility/ID code cannot be changed
  - Third-party "magic" writable cards
- Not typically sold in the US, available overseas
  - eBay, Amazon: "writable t5557 RFID"

```
[usb] pm3 --> lf search
...<trimmed for brevity>...
[=] Checking for known tags...
[+] [H10301] - HID H10301 26-bit; FC: 149 CN: 64899 parity: valid
[=] raw: 00000000000024012bfb06
```

```
[usb] pm3 --> lf hid clone 24012bfb06
[=] Preparing to clone HID tag with ID 24012bfb06
```

Standalone HID ProxCard Cloning

- Hard to be stealthy cloning HID ProxCard with a laptop
- Proxmark 3 can also perform untethered cloning
  - Using the single button and LEDs for status
- Requires battery source for Proxmark 3
  - Portable USB phone charger or optional RDV2 battery

ProxCard ID Numbers

When you purchase a new set of cards, you're asked to provide a facility/site code and a starting number or range for the card numbers. Cards are issued to the organization with nearly sequential numbering.

HOLIDAYHACKCHALLENGE.COM

SANS

HOLIDAY HACK CHALLENGE 2020

#HOLIDAYHACK

@KRINGLECON

THANK YOU!