SPIRENT

Breaking Bad: Stealing Patient Data Through Medical Devices

Saurabh Harit [0xsauby]
Spirent SecurityLabs

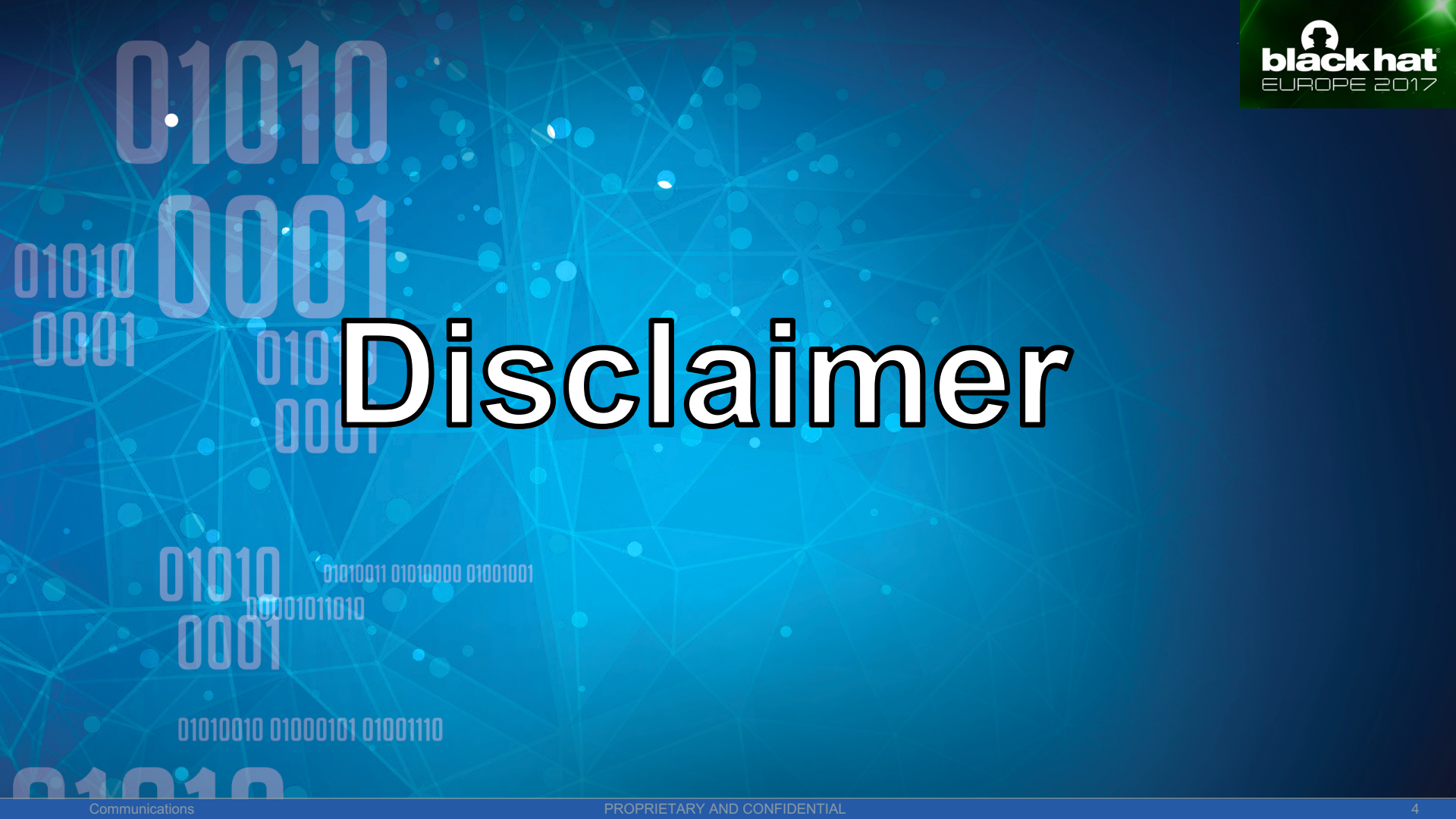
notroot@spirent:~$>getuid

Saurabh Harit [0xsauby]

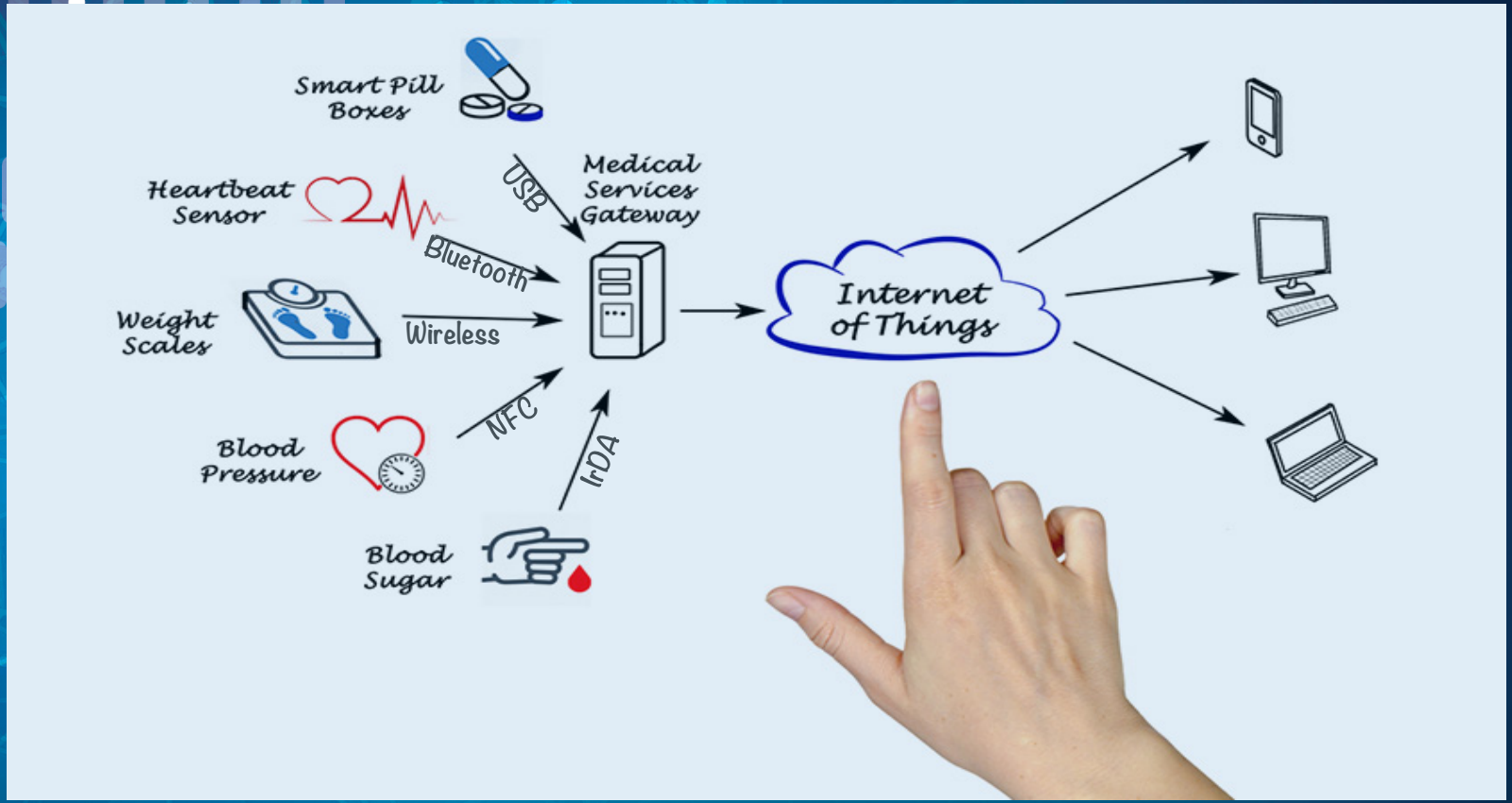
- Managing consultant @Spirent SecurityLabs
- Pentester / Domain Admin Everywhere
- Security Researcher
- Trainer, Speaker
- Wannabe Reverse Engineer
- Developer of Yasuo

tl;dr

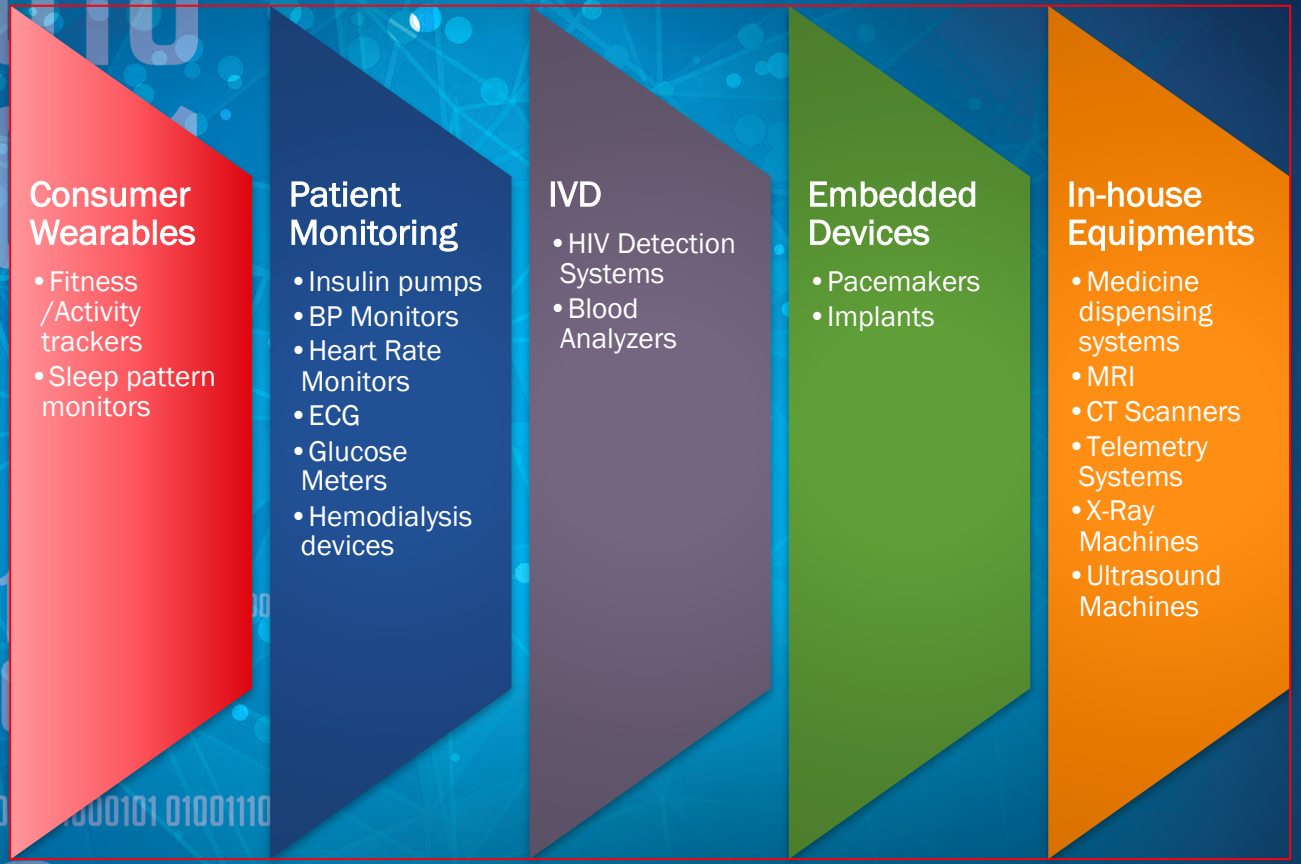
- Introduction to Internet-connected healthcare devices
- Architecture & Workflow
- Good, Bad & Ugly
- Medical records vs Financial data
- Threat surface of Connected healthcare devices – A pentester's perspective
- Real-world attacks against connected healthcare devices
- Case Study #1
- Case Study #2
- Closing Remarks


black hat
EUROPE 2017
Disclaimer

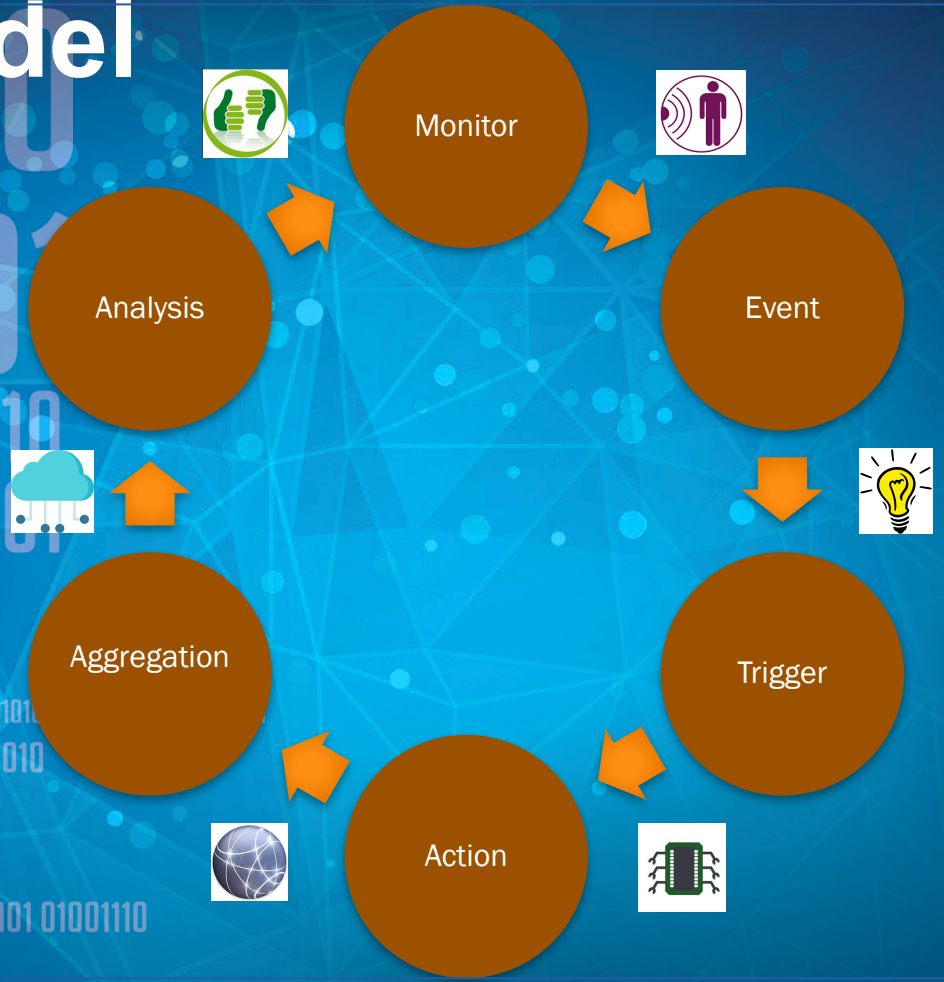
Connected Healthcare Devices



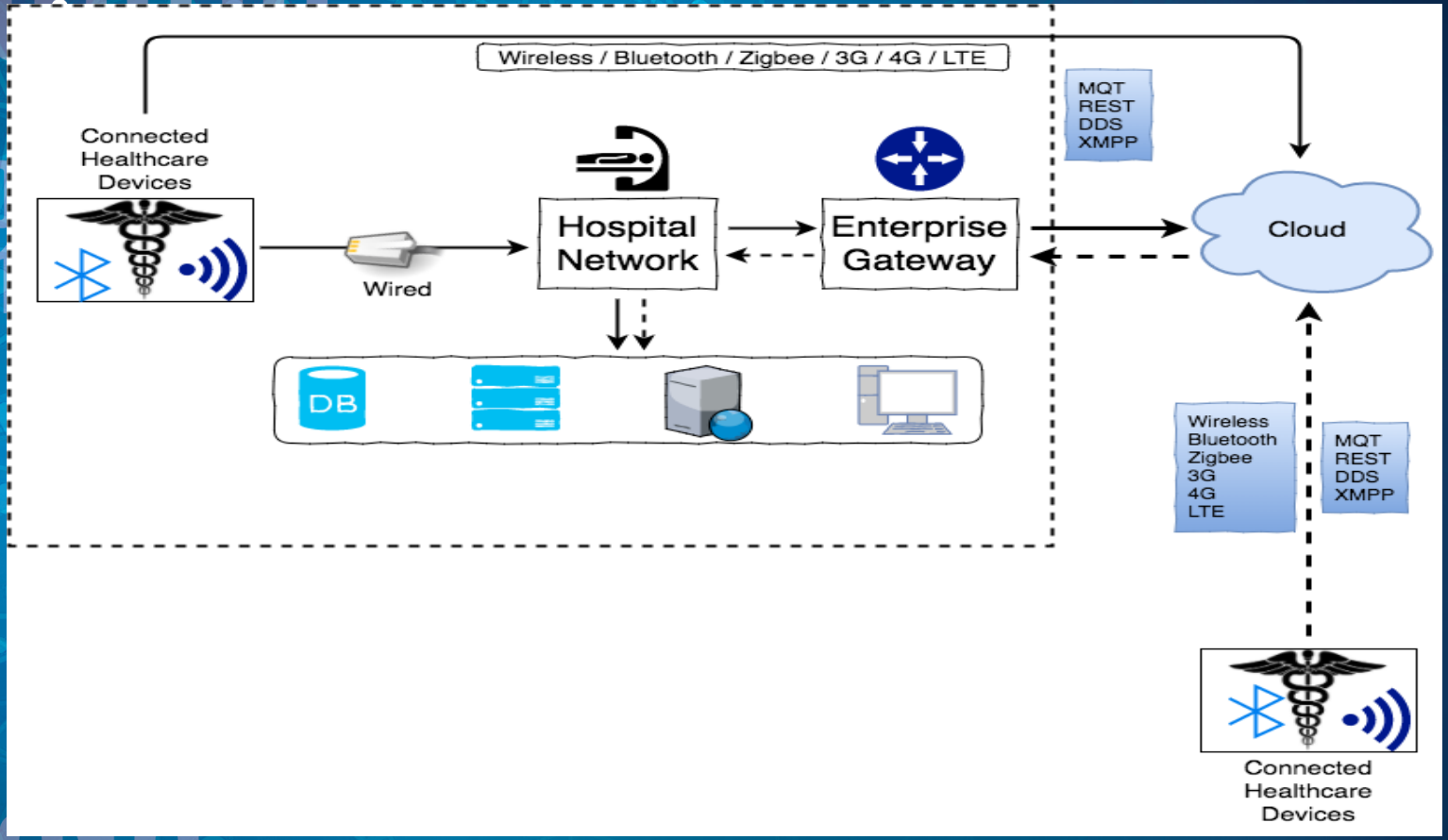
Medical Devices Classification



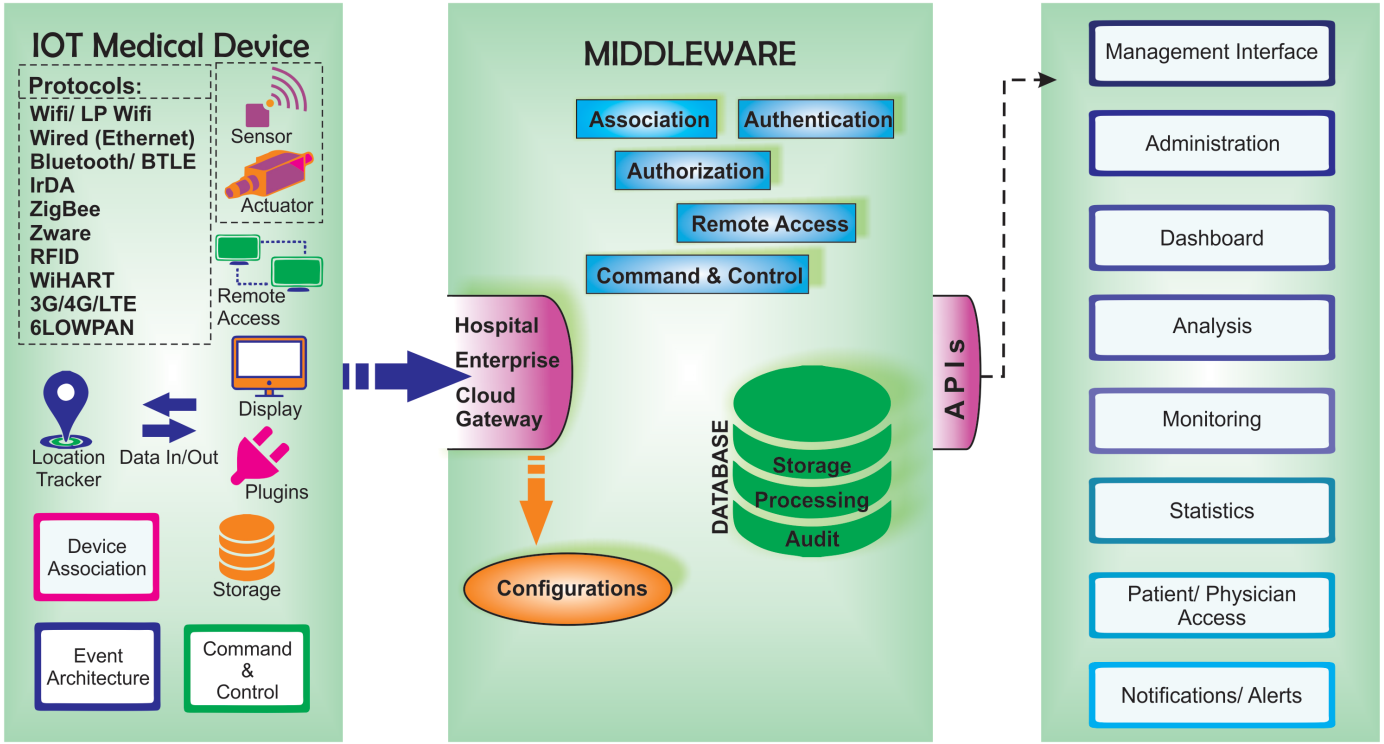
The Model



The Ecosystem / Architecture



The Ecosystem / Architecture



The Good

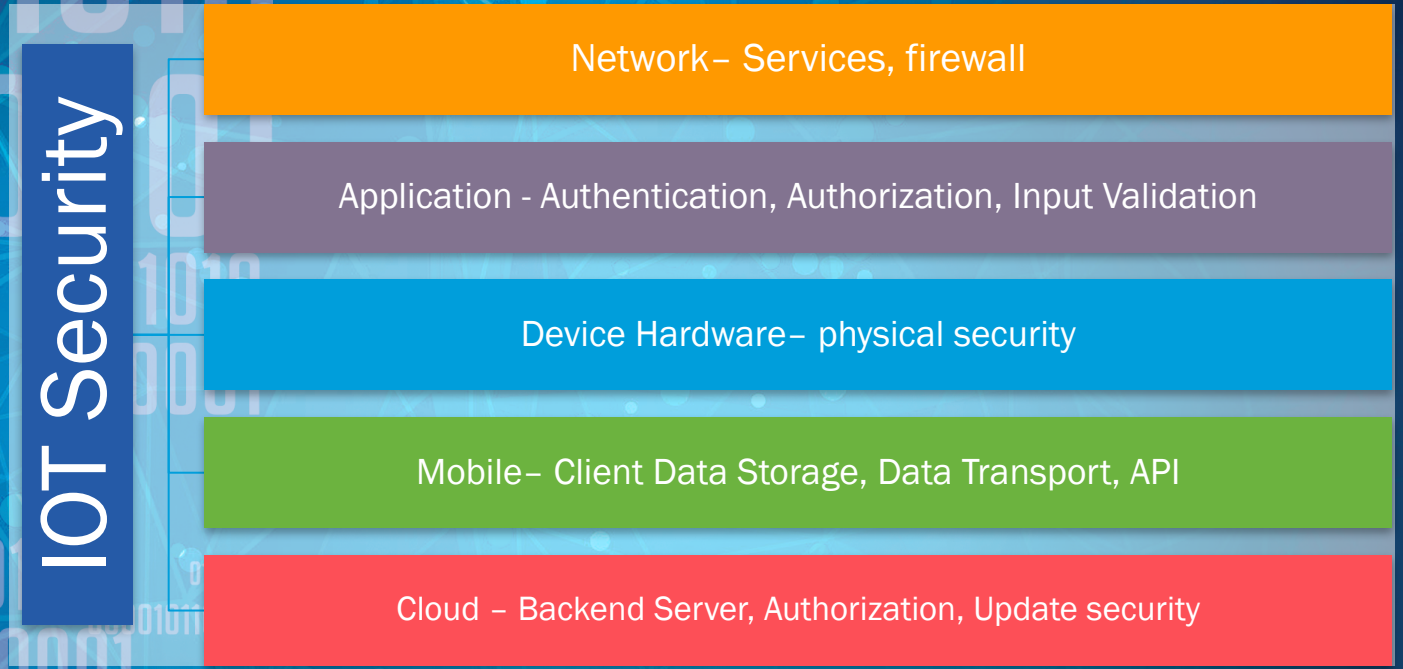
1. Remote health monitoring
2. Global health care
3. Less expenditure, better quality care
4. Faster response time
5. Efficient Asset Management & Maintenance
6. Alerts – Early Detection & Prevention
7. EHR (Electronic Healthcare Records)
8. RTHS (Real-Time Health Systems)

The Nightmare

1. Tons of new ”connected” medical devices
2. Numerous communication protocols
3. “Legacy” devices
4. Network Segregation
5. Robust WiFi infrastructure???
6. Monitoring, Automation & Analytics
7. Rogue Medical Devices
8. Operating Systems??? Think MedJack
9. Interoperability

Serial To Ethernet Converters

The Attack Surface



The Horror Stories – MEDJACK / MEDJACK.2

1. Medical Device Hijack
2. MEDJACK – 2015/2016
3. MEDJACK.2 – 2017
4. Attacked older operating systems
5. Affected devices: X-Ray machines, CT Scanners, Blood Gas analyzer, MRI systems etc.
6. Undetected by Endpoint security solutions

Financial vs Medical Data

	Financial Data	Medical Records
Attacks	▼	▲
Market Value	▼	▲
Detection Rate	▲	▼

Approach

1. OSINT
   - Previous Research
   - FCC Filings
   - Setup Guides
   - Help Forums
2. Passive Recon
3. Active Testing
4. Weaponize

Approach

1. OSINT
2. Passive Tests
   - Environment Setup
   - Regular User Interaction
3. Active Tests
4. Weaponize

Approach

1. OSINT
2. Passive Recon
3. Active Tests
   - Make controller changes
   - Observe & compare responses
   - Automate analysis where possible
4. Weaponize

Approach

1. OSINT
2. Passive Recon
3. Active Testing
4. Weaponize
   - Collect & Synthesize
   - Test, Extend & Refine
   - Automate & Optimize
   - Deploy & Exploit

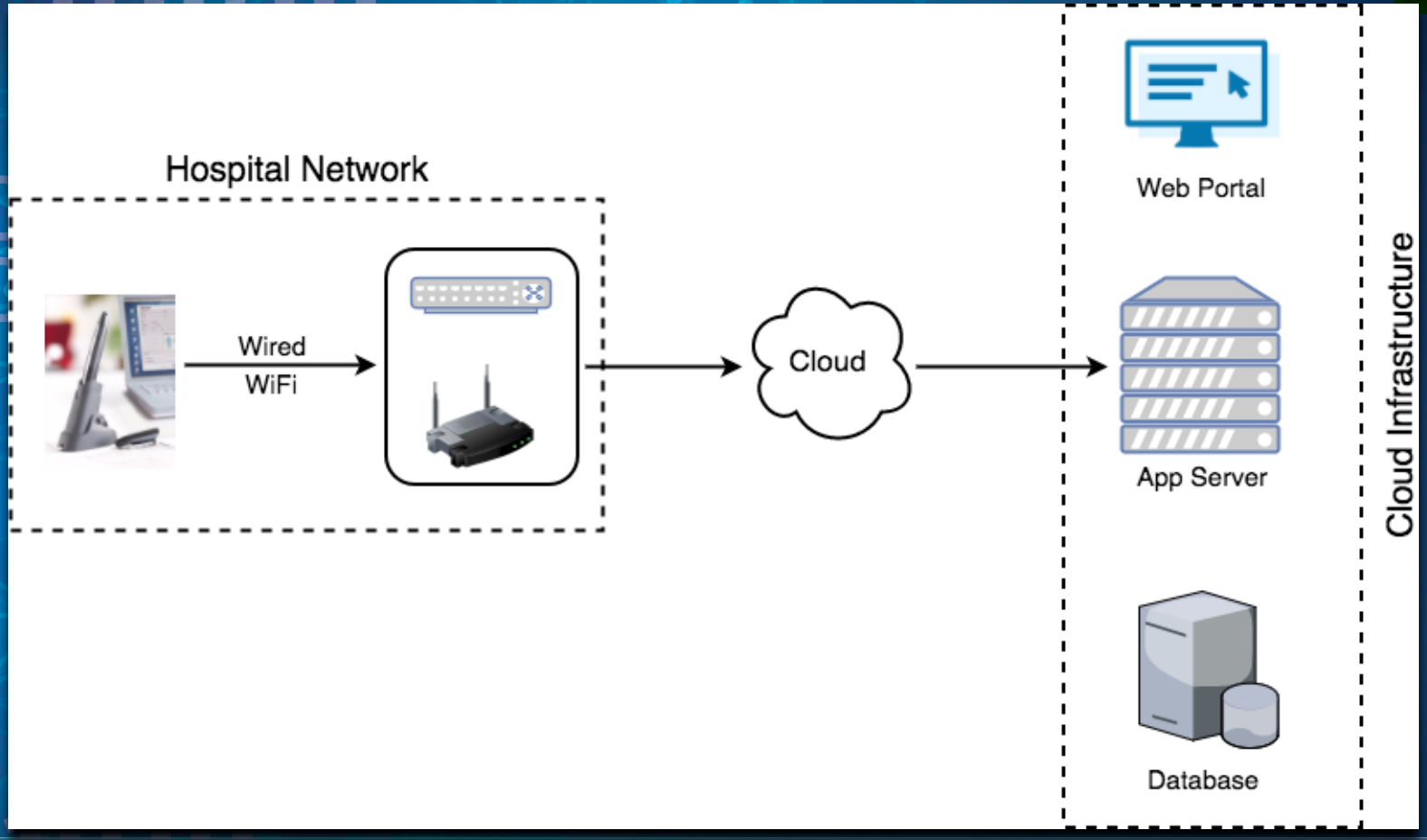

Case Study #1

About the Device

1. Digital Pen
2. Used for prescriptions
3. Electronic transmission to pharmacies
4. Many manufacturers
5. Random images, no point zooming in.

NOT THIS ONE!!!

Workflow


Hospital Network
Wired
WiFi
Cloud
Web Portal
App Server
Database
Cloud Infrastructure

Let's Break It Down

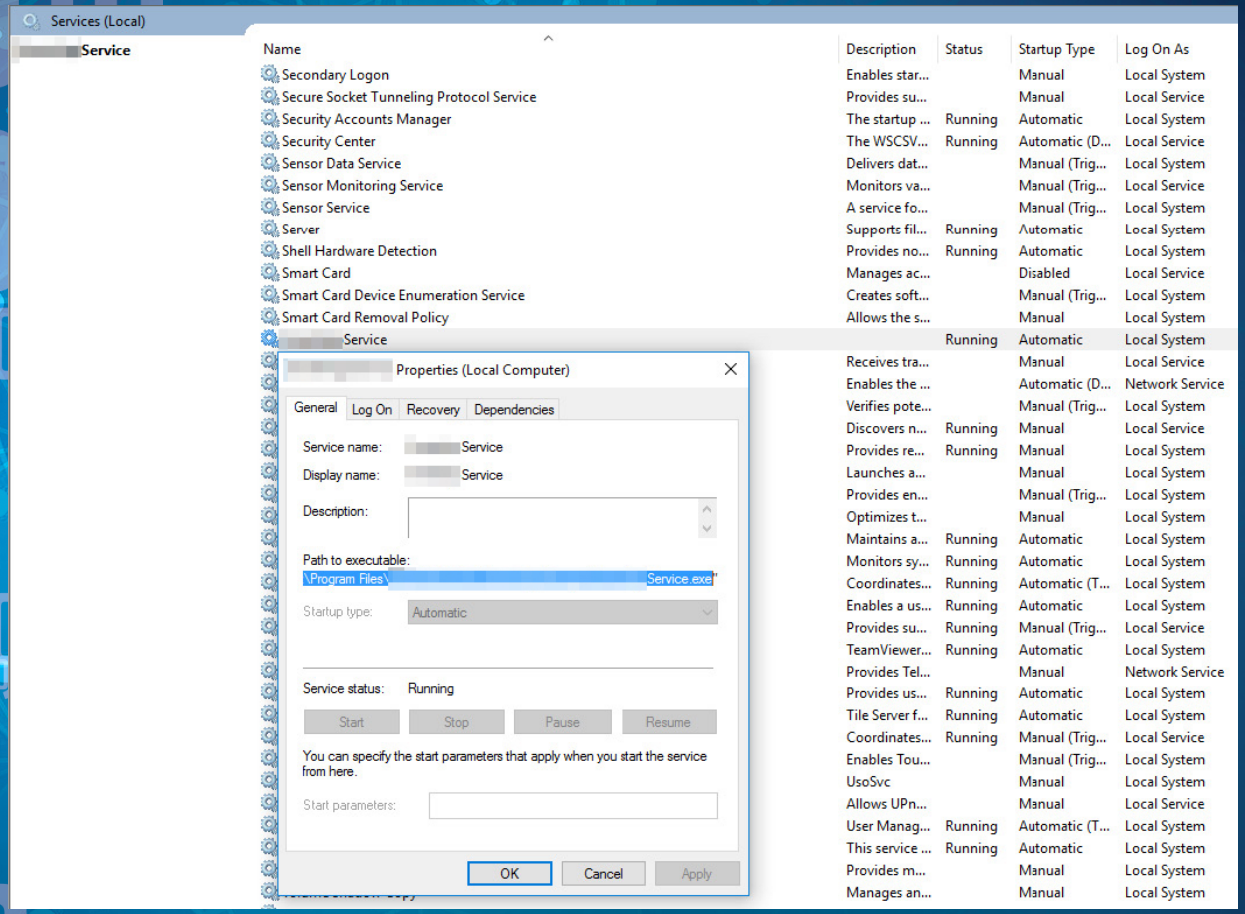
1. OS → Windows 10
   a) Nurse / Physician
   b) Administrator
2. USB
3. 802.11 b/g/n Integrated Wireless Network
4. 10/100M RJ45 Ethernet
5. HDMI, VGA
6. Digital Display
7. 3.5mm Audio Port
8. Windows Defender
9. Docking Station
10. Software Layer

Use Case Scenario

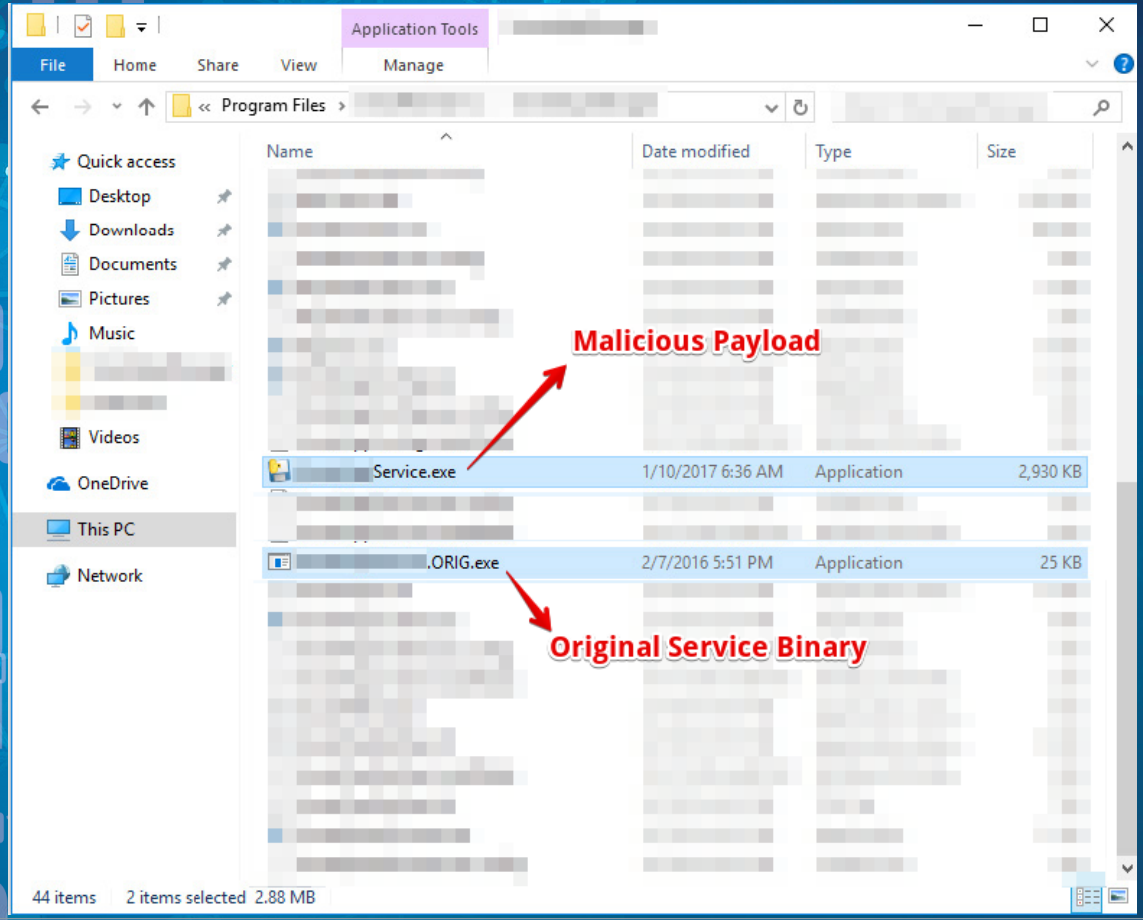
Initial Observations

1. Can connect a monitor, keyboard, mouse
2. Auto-login as Nurse (Total locked down mode)
3. Manufacturer software and services
4. Data capture via USB
5. Internet → Real-time data transfer
6. Offline → Stored encrypted
7. Over the wire → HTTPS (AES256)
8. Remote Access Component

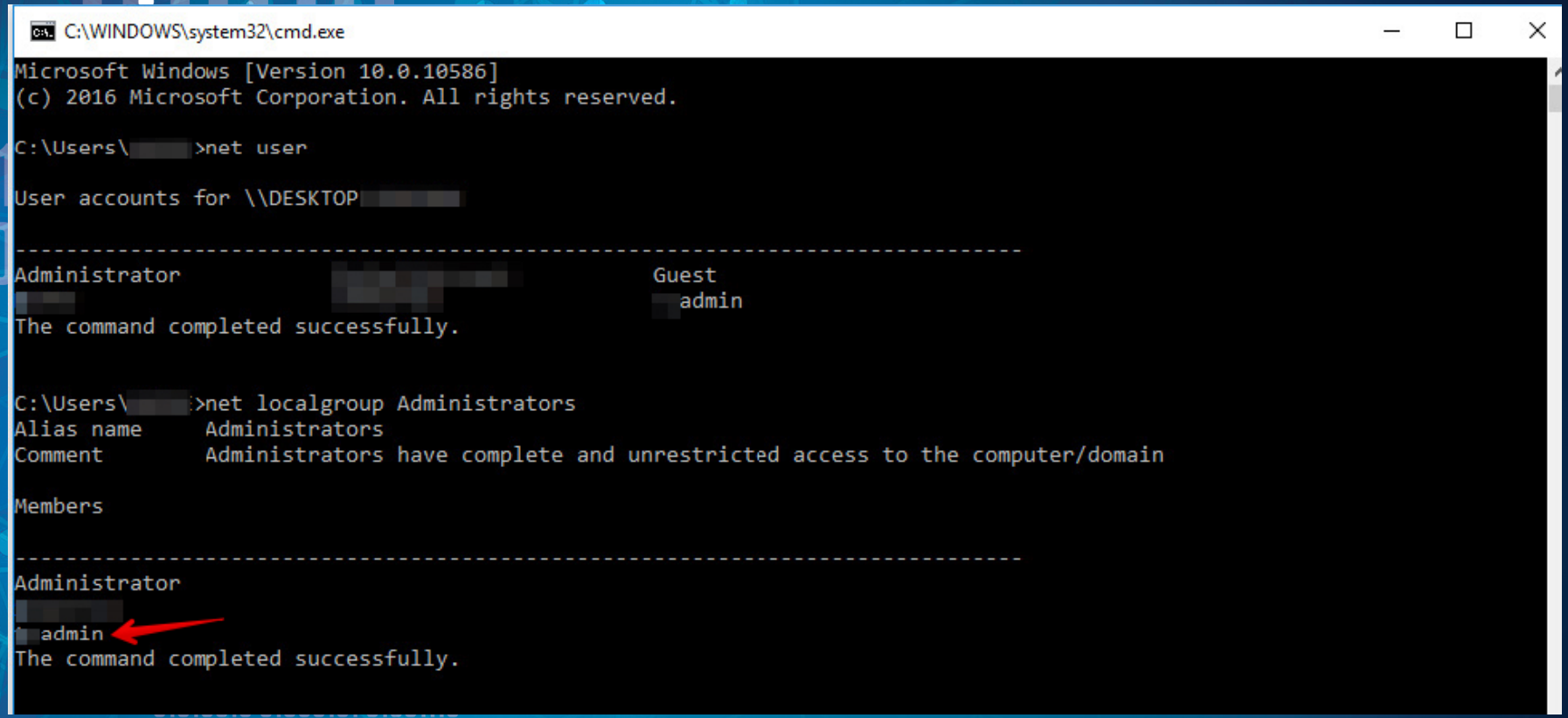
Privilege Escalation



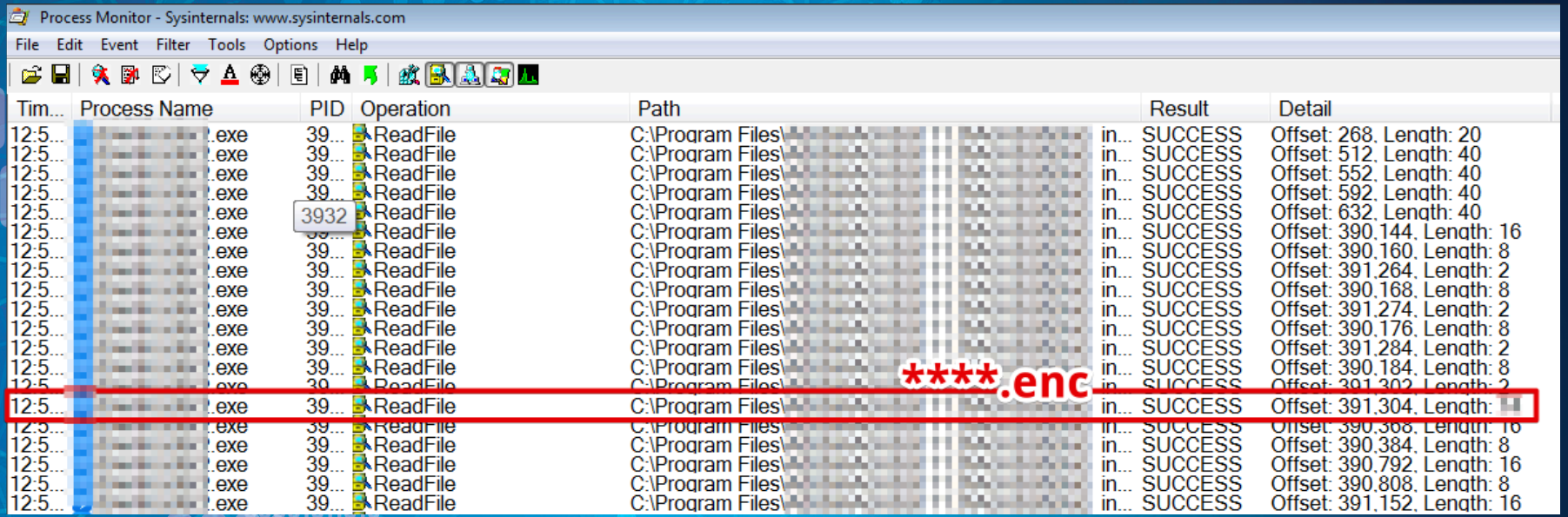
Privilege Escalation



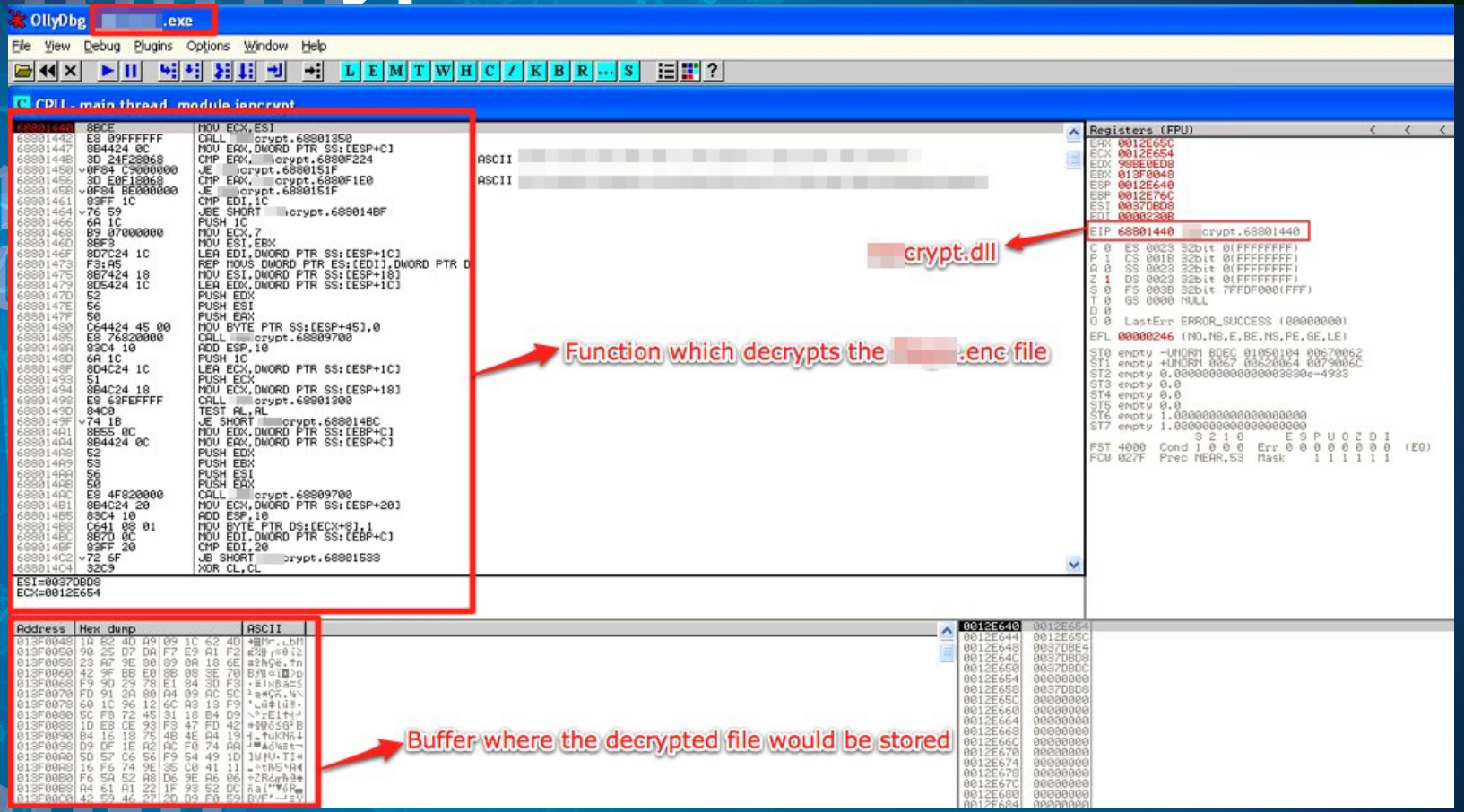
Privilege Escalation



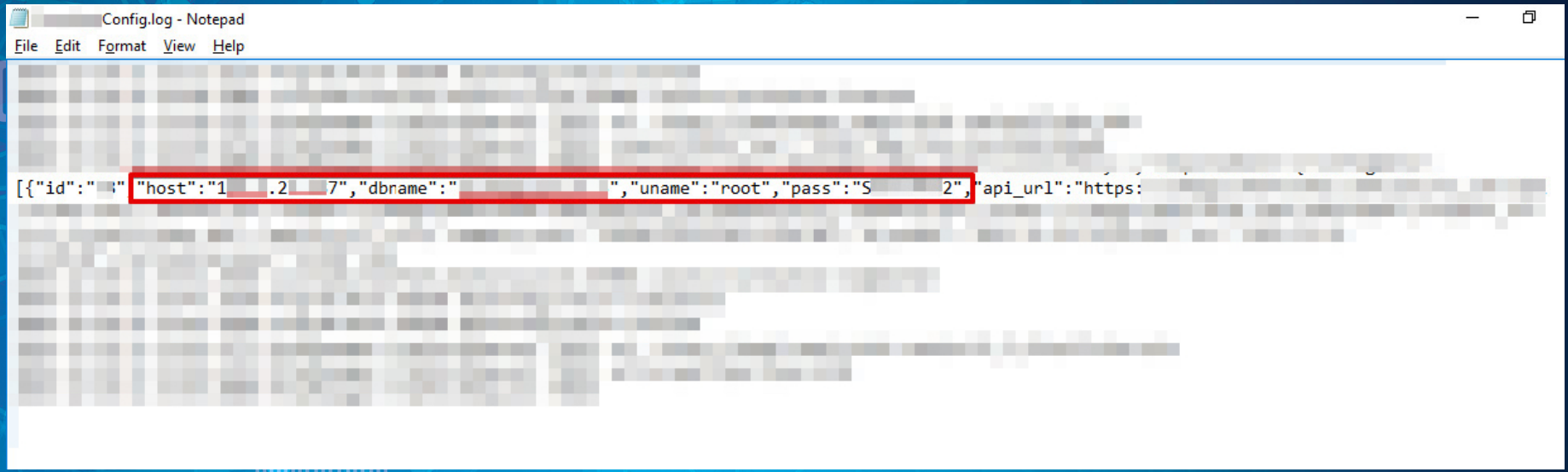
The Encrypted File



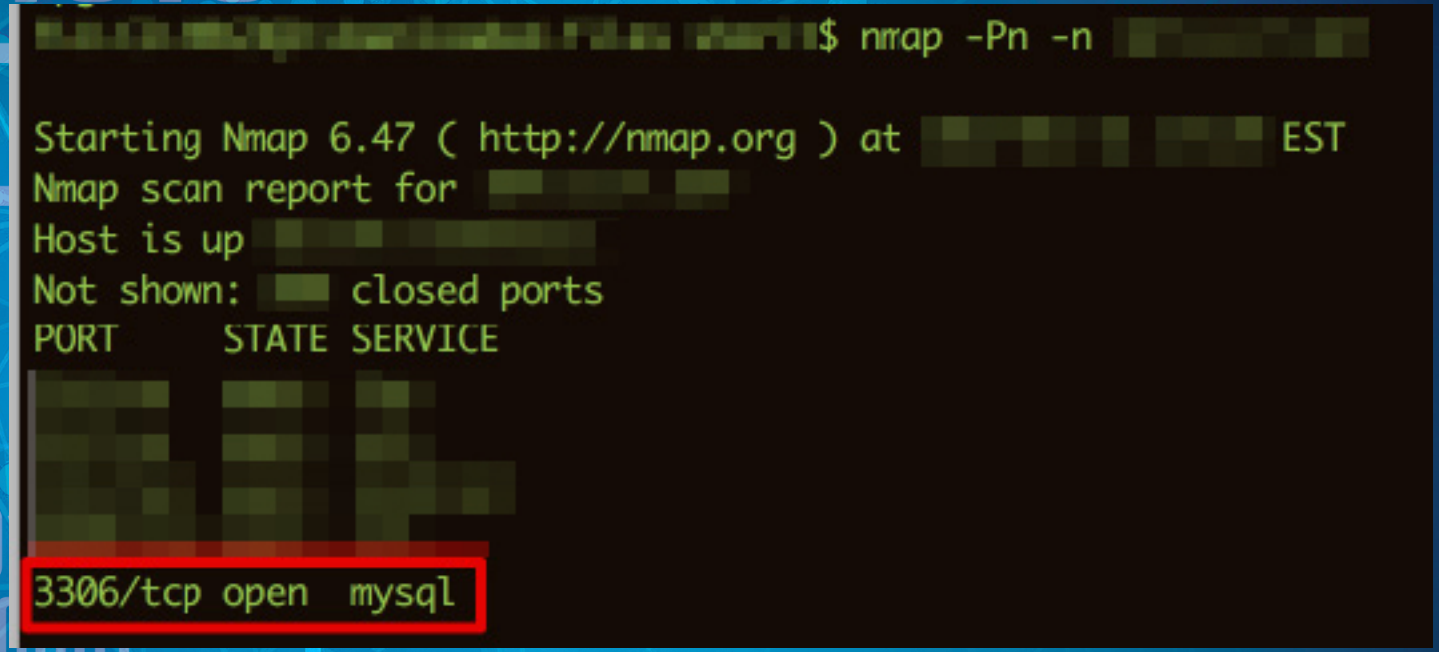
The Encrypted File



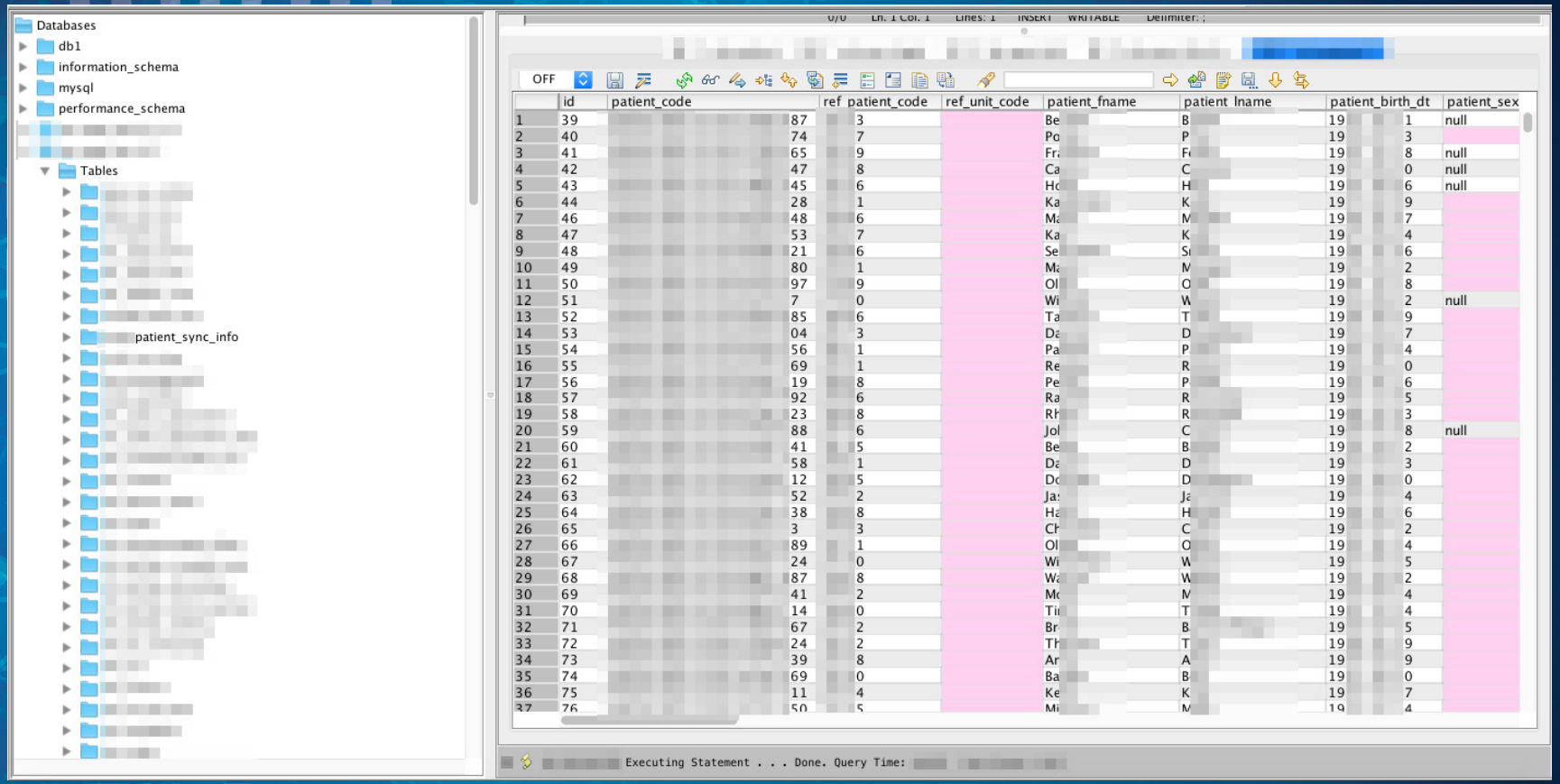
The Encrypted File – Win!!!



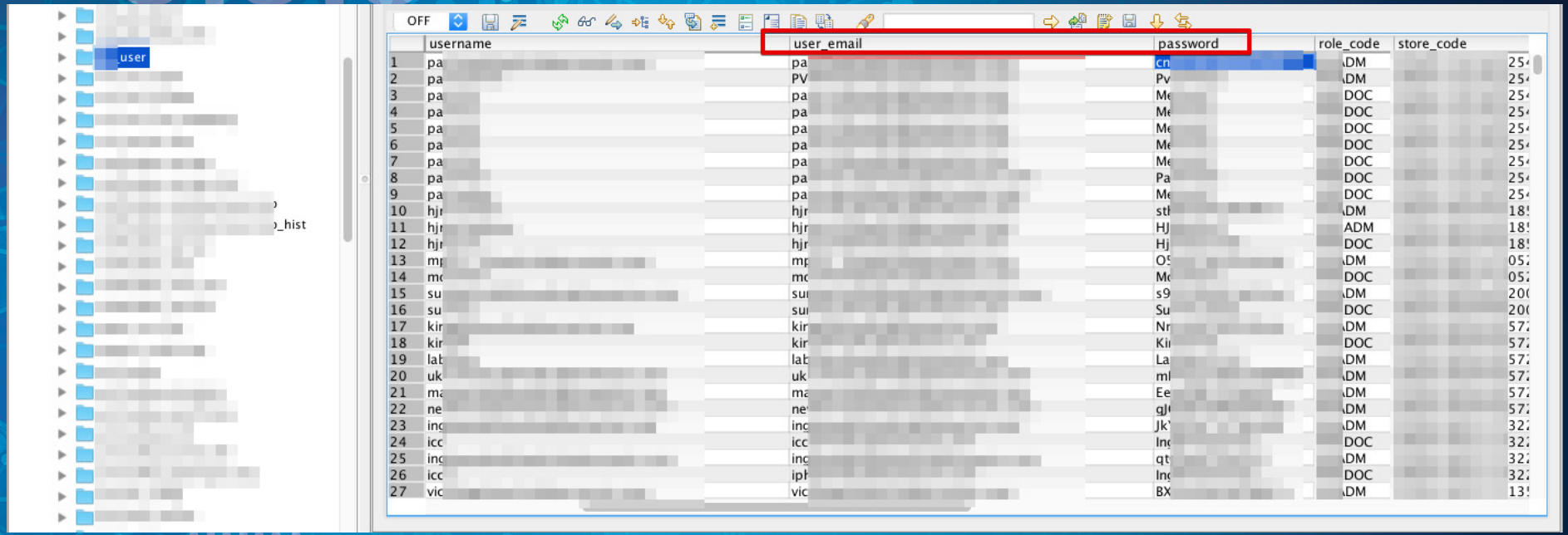
Another Crime



Access to Patient Data



Access to Patient Data



Access to Patient Data

Resident Name	Unit	Home	Room No	#HCN
At			2	369
At			2	639
Ba			8	978
Be			3	595
Be			3	230
Ca			2	247
Ch			0	293
De			1	452
El			0	682
Mc			2	391
Mi			1	985

Prescriptions

DIGITAL PRESCRIBER'S ORDERS

Facility: Pa Unit: Ma

Resident: Be ory Room: 2

Health Card#: E22 DOB (dd/mm/yyyy): 19/0 /19

Allergies: No Known Allergies

Date/Time	Clinical Indicator
T. o from Dr · Hold warfarin for 2days and me INR next week You taken by ☐ Start Today ☐ Start with Next Weekly Supply	

Prescriber's Signature / Registration#	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed			
			CarePlan	Consent	Mar/Tar	Lab
	Date / Time	Date / Time				

Date/Time	Clinical Indicator
17/11 17.30hrs T. o from Dr · Hold (days Ch me · order taken by ☐ Start Today ☐ Start with Next Weekly Supply	

Prescriber's Signature / Registration#	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed			
			CarePlan	Consent	Mar/Tar	Lab
	Date / Time 17/11/17	Date / Time				

Date/Time	Clinical Indicator

Let's Sum it Up

- Access to digital pen
- Privilege escalation
- A bit of reverse engineering
- Steal credentials
- Remote database and portal access from your basement

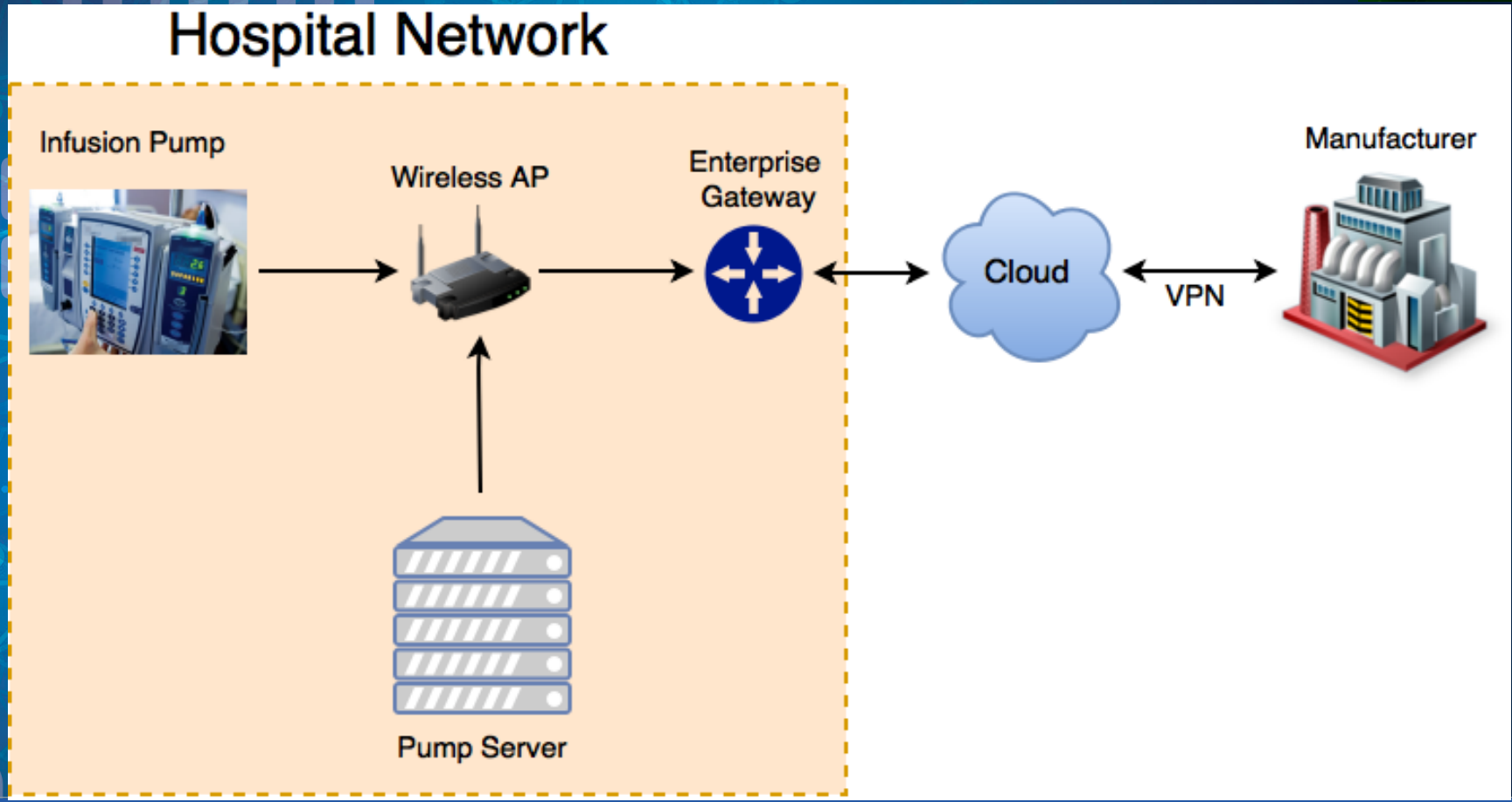
Case Study #2

About the Device

1. IV Infusion Pump
2. Injects nutrients & medication
3. Controlled dosage
4. Safety features
5. External or Implanted
6. Used to be standalone, not anymore
7. Once again, random images, no point zooming in.

NOT THIS ONE EITHER!!!

Workflow


Hospital Network
Infusion Pump
Wireless AP
Enterprise Gateway
Cloud
VPN
Manufacturer
Pump Server

Threat Vectors

Device

- Insecure Configurations
- Hardcoded Passwords
- No Tamper Detection
- Insufficient Patching
- Older Operating Systems
- Weak Access Control
- Insufficient Logging
- Unprotected BIOS
- Lack of AV

Data

- Weak Authentication / Authorization
- No Data Encryption
- Insufficient Data Validation
- Insufficient Data Integrity
- Insufficient Data Backup

Network

- Unencrypted Network Communication
- Insecure Network Configurations
- Insufficient Firewall Rules
- Lack of Segregation

Initial Lab Setup

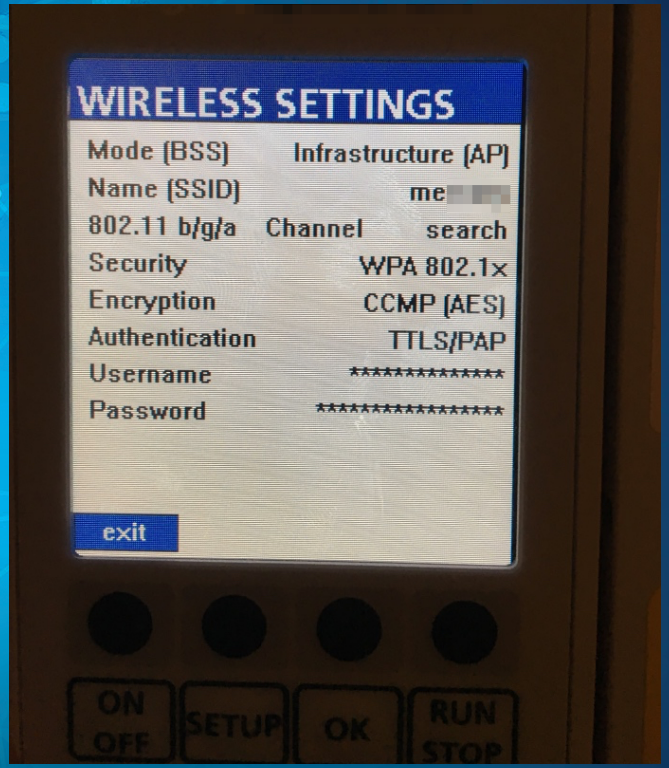
Standalone Infusion Pump

Initial Observations

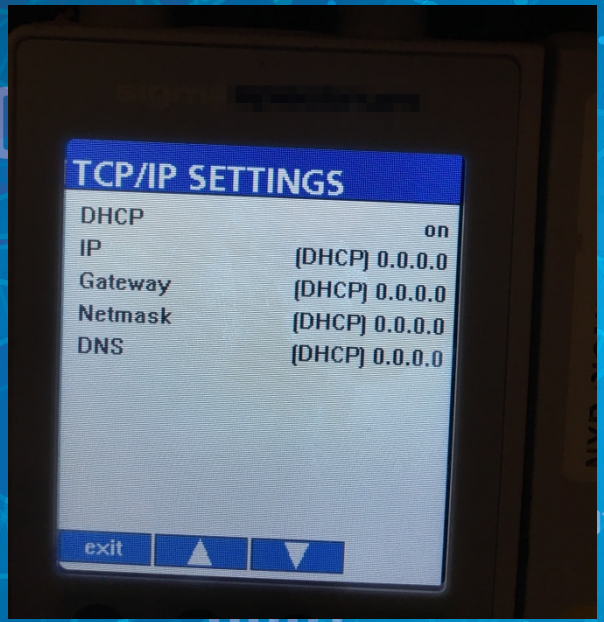
1. Ethernet (RS-232)
2. 802.11 b/g/a Integrated Wireless Network
3. USB Enabled
4. IrDA Port
5. Display – Touch Screen
6. Keypad
7. Maintenance Mode – Password Protected \o/

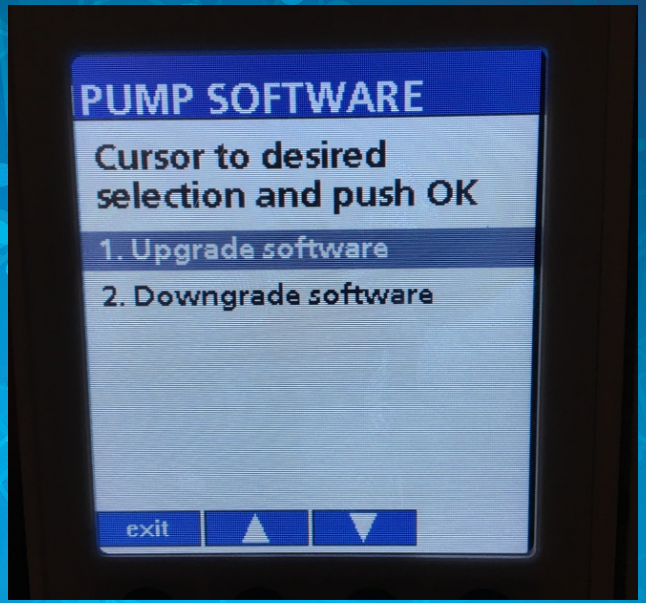
First Blood

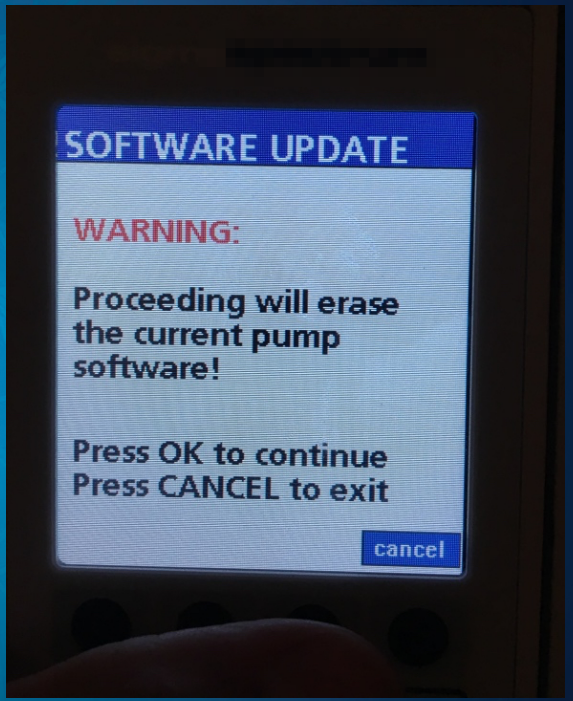
- Default Password
- Access to Network Config
- Change (some) Network Configs
- Upgrade/Downgrade Software



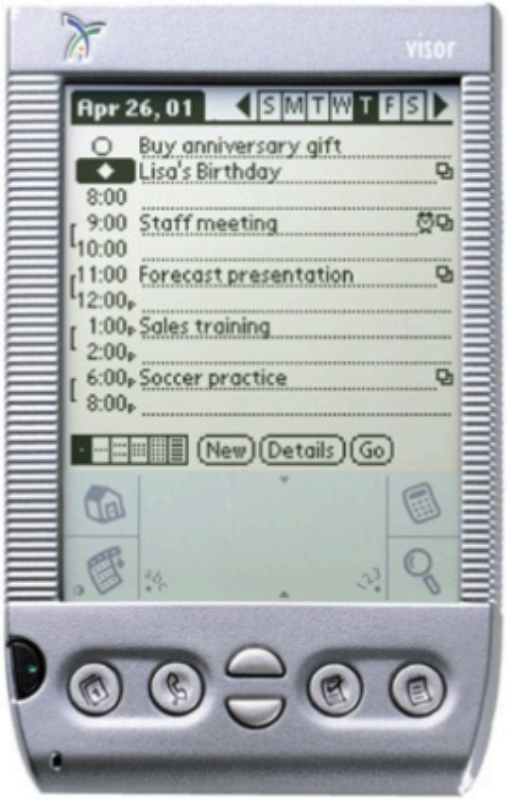
Configs


TCP/IP SETTINGS
DHCP on
IP (DHCP) 0.0.0.0
Gateway (DHCP) 0.0.0.0
Netmask (DHCP) 0.0.0.0
DNS (DHCP) 0.0.0.0
exit


PUMP SOFTWARE
Cursor to desired selection and push OK
1. Upgrade software
2. Downgrade software
exit


SOFTWARE UPDATE
WARNING:
Proceeding will erase the current pump software!
Press OK to continue
Press CANCEL to exit
cancel

We Bought a PDA



Handspring

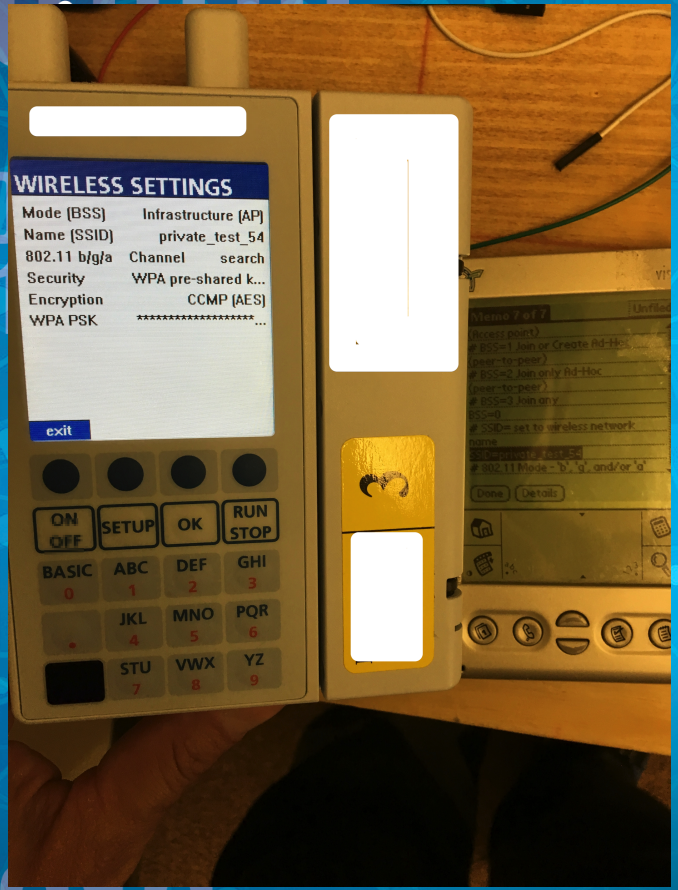
Handspring Visor Platinum (Silver)

78 customer reviews

Available from these sellers.

- 50 percent faster than Handspring Visor Deluxe
- 8 MB RAM stores thousands of addresses, appointments, to-do items, and more
- Features address book, to-do list, memo pad, date book, advanced calculator, and world clock
- Fully compatible with thousands of Palm OS applications
- What's in the box: Visor Platinum, Graphite HotSync cradle, 8 MB RAM, AAA batteries, Graphite snap cover, Leather case

Overwriting Wireless Settings

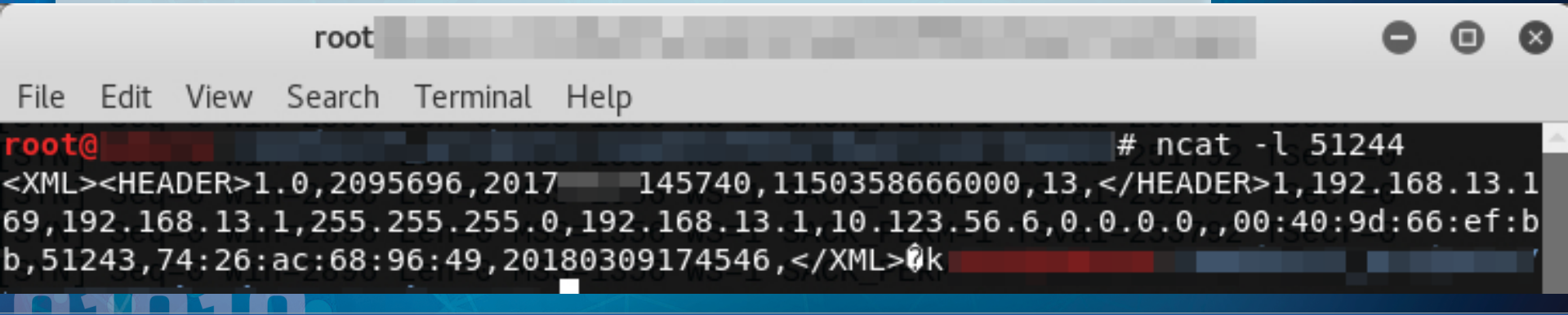


Additional Observations

- Telnet
- FTP
- SSH
- Connection attempt to pump server (****PUMPGW)

The Initial Traffic

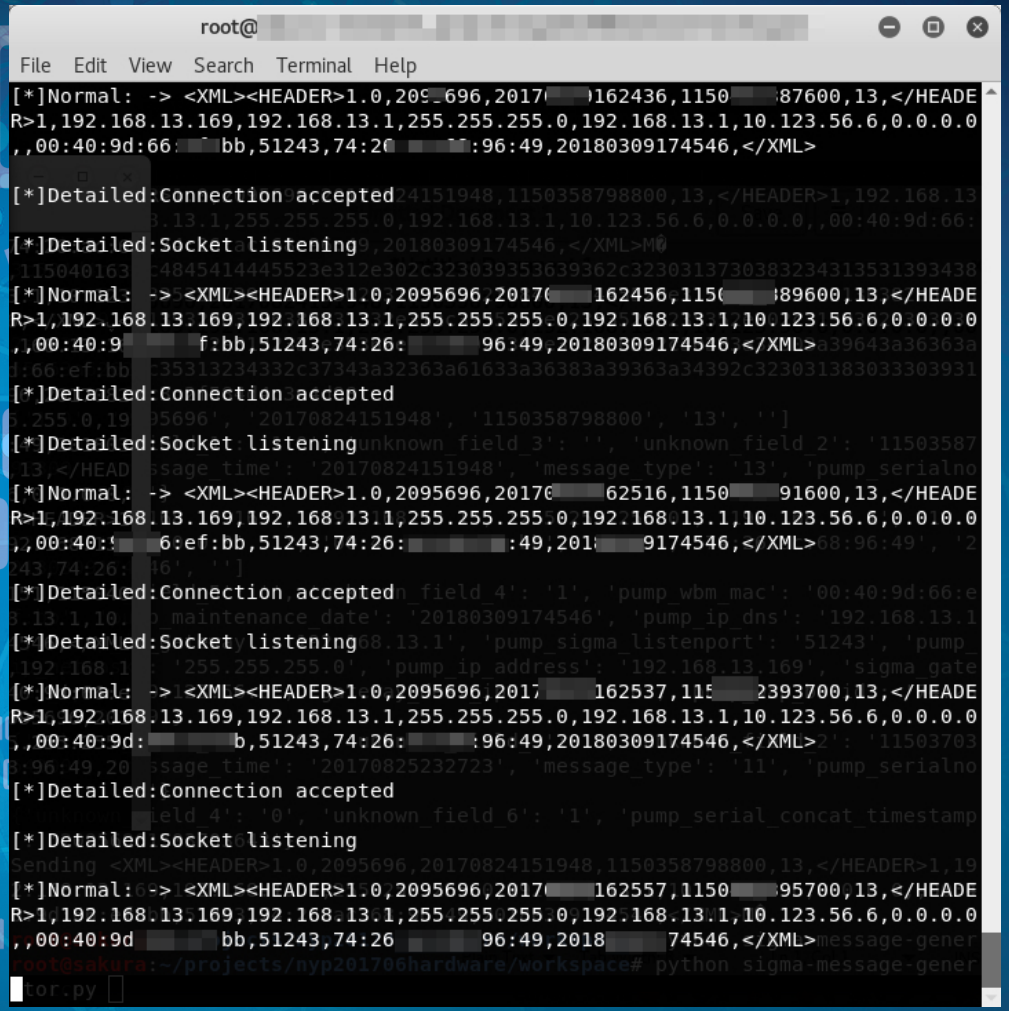
- Plain-text protocol loosely based on XML
- Contained pump description:
  - Pump Serial Number
  - Current Time
  - Wireless Access Point Data
  - IP/MAC Information
  - Maintenance Due Date
  - XMODEM checksum



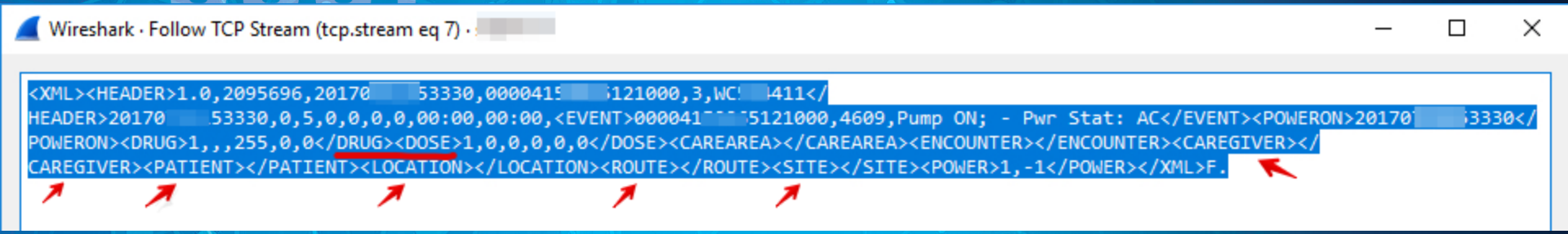
Time to Fuzz

- Communication with pump, both as client (tcp/51244) & server (tcp/51243)
- Created custom Python library to interact with pump
- Observed numeric header specifying Message types
  - Message Type 2 – Confirms pump to pump server connection
  - Message Type 7 & 31 – Not sure
  - Message Type 8 – Followed by Message Type 2. Updates pump status.
  - Message Type 20 – Network commands
  - Message Type 208 & 238 – Not sure

Fuzzing

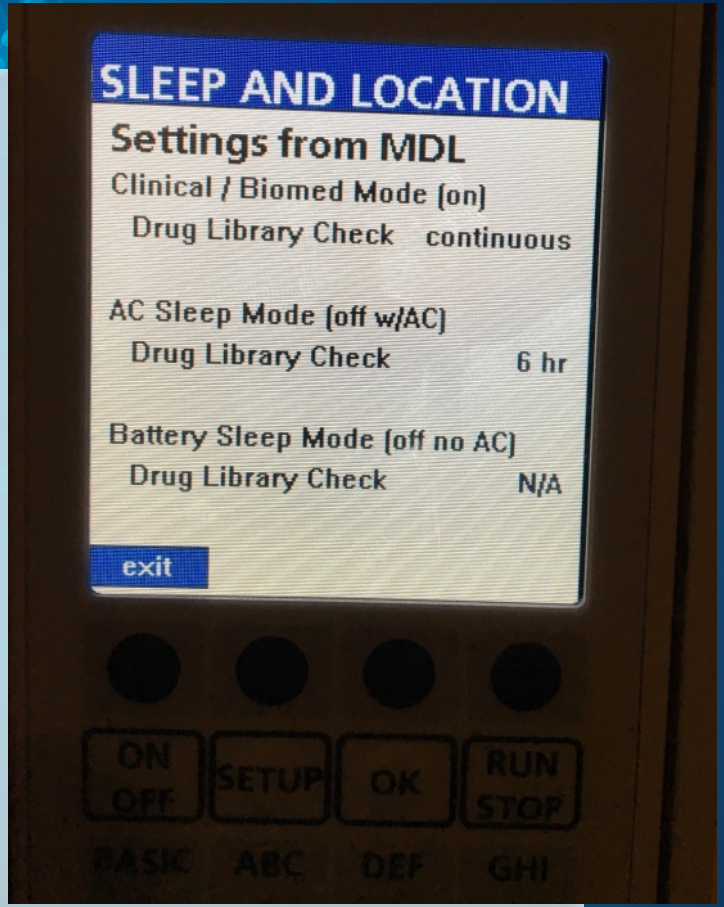

root@
File Edit View Search Terminal Help
[*]Normal: -> <XML><HEADER>1.0,209 696,2017 162436,1150 87600,13,</HEADE
R>1,192.168.13.169,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0
,,00:40:9d:66: bb,51243,74:2 :96:49,20180309174546,</XML>
[*]Detailed:Connection accepted
[*]Detailed:Socket listening
[*]Normal: -> <XML><HEADER>1.0,2095696,2017 162456,115 89600,13,</HEADE
R>1,192.168.13.169,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0
,,00:40:9 f:bb,51243,74:26: 96:49,20180309174546,</XML>
[*]Detailed:Connection accepted
[*]Detailed:Socket listening
[*]Normal: -> <XML><HEADER>1.0,2095696,2017 62516,1150 91600,13,</HEADE
R>1,192.168.13.169,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0
,,00:40: 6:ef:bb,51243,74:26: :49,201 9174546,</XML>
[*]Detailed:Connection accepted
[*]Detailed:Socket listening
[*]Normal: -> <XML><HEADER>1.0,2095696,2017 162537,115 2393700,13,</HEADE
R>1,192.168.13.169,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0
,,00:40:9d: b,51243,74:26: :96:49,20180309174546,</XML>
[*]Detailed:Connection accepted
[*]Detailed:Socket listening
[*]Normal: -> <XML><HEADER>1.0,2095696,2017 162557,1150 95700,13,</HEADE
R>1,192.168.13.169,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0
,,00:40:9d bb,51243,74:26 96:49,2018 74546,</XML>
tor.py

Winning Packet

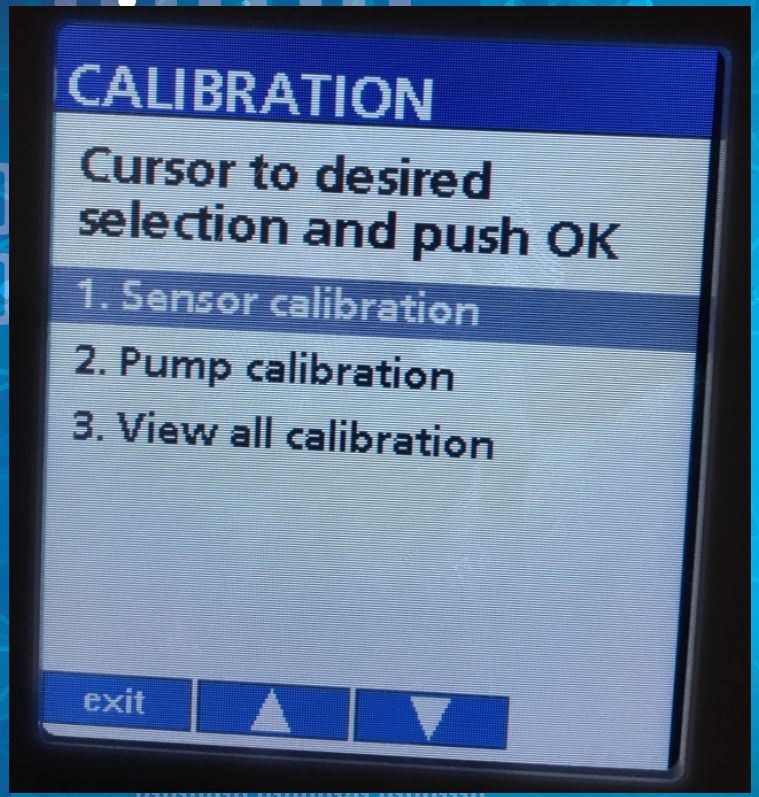


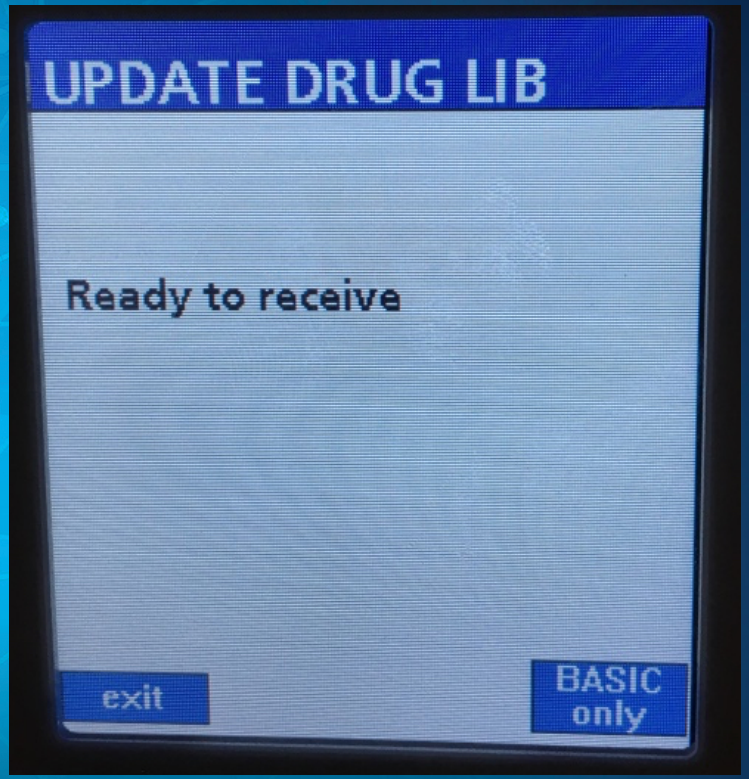
Master Drug List

- Used for drug administration
- Nutrients, Drugs, Blood etc.
- Maintains dosage, proportions
- Soft / Hard Limits



More Access


CALIBRATION
Cursor to desired selection and push OK
1. Sensor calibration
2. Pump calibration
3. View all calibration
exit


UPDATE DRUG LIB
Ready to receive
exit
BASIC only


QUESTIONS?

References

- Google Image Cache