



01010  
0001  
01010 0001  
0001 01010  
0001

# Breaking Bad: Stealing Patient Data Through Medical Devices

Saurabh Harit [0xsauby]  
Spirent SecurityLabs



DO GOOD *KNOW EVIL*

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

01010  
01010 0001  
0001

# Disclaimer

01010  
0001

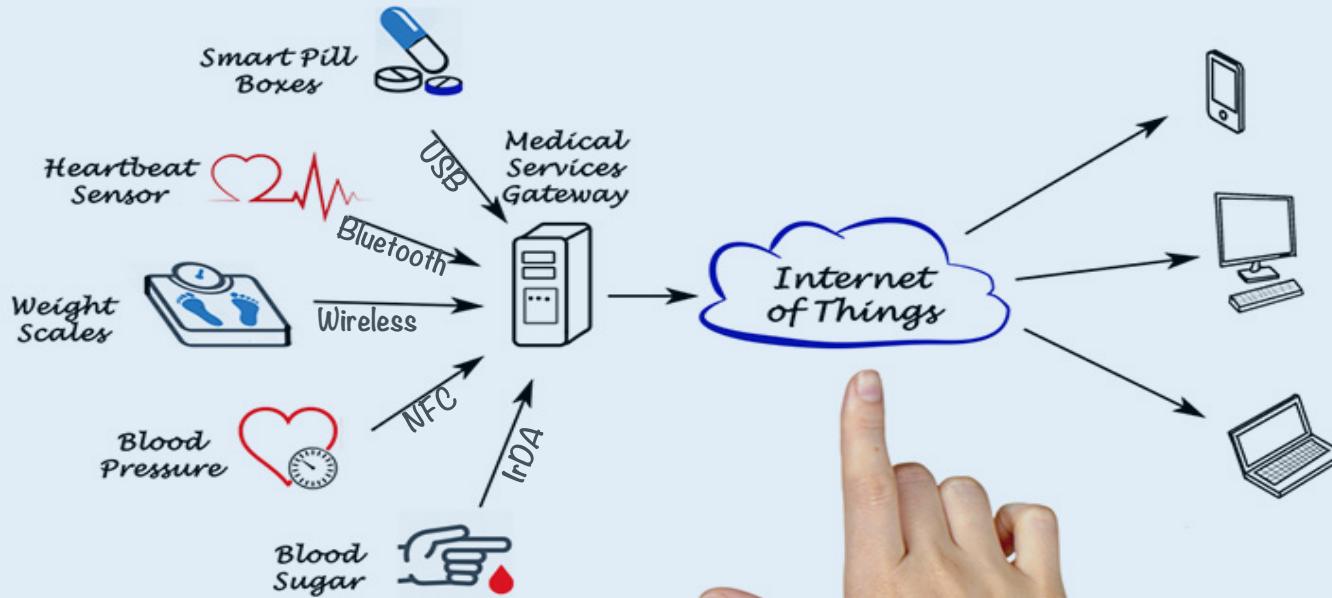
01010011 01010000 01001001

00001011010

01010010 01000101 01001110

01010

# Connected Healthcare Devices



# Medical Devices Classification

## Consumer Wearables

- Fitness /Activity trackers
- Sleep pattern monitors

## Patient Monitoring

- Insulin pumps
- BP Monitors
- Heart Rate Monitors
- ECG
- Glucose Meters
- Hemodialysis devices

## IVD

- HIV Detection Systems
- Blood Analyzers

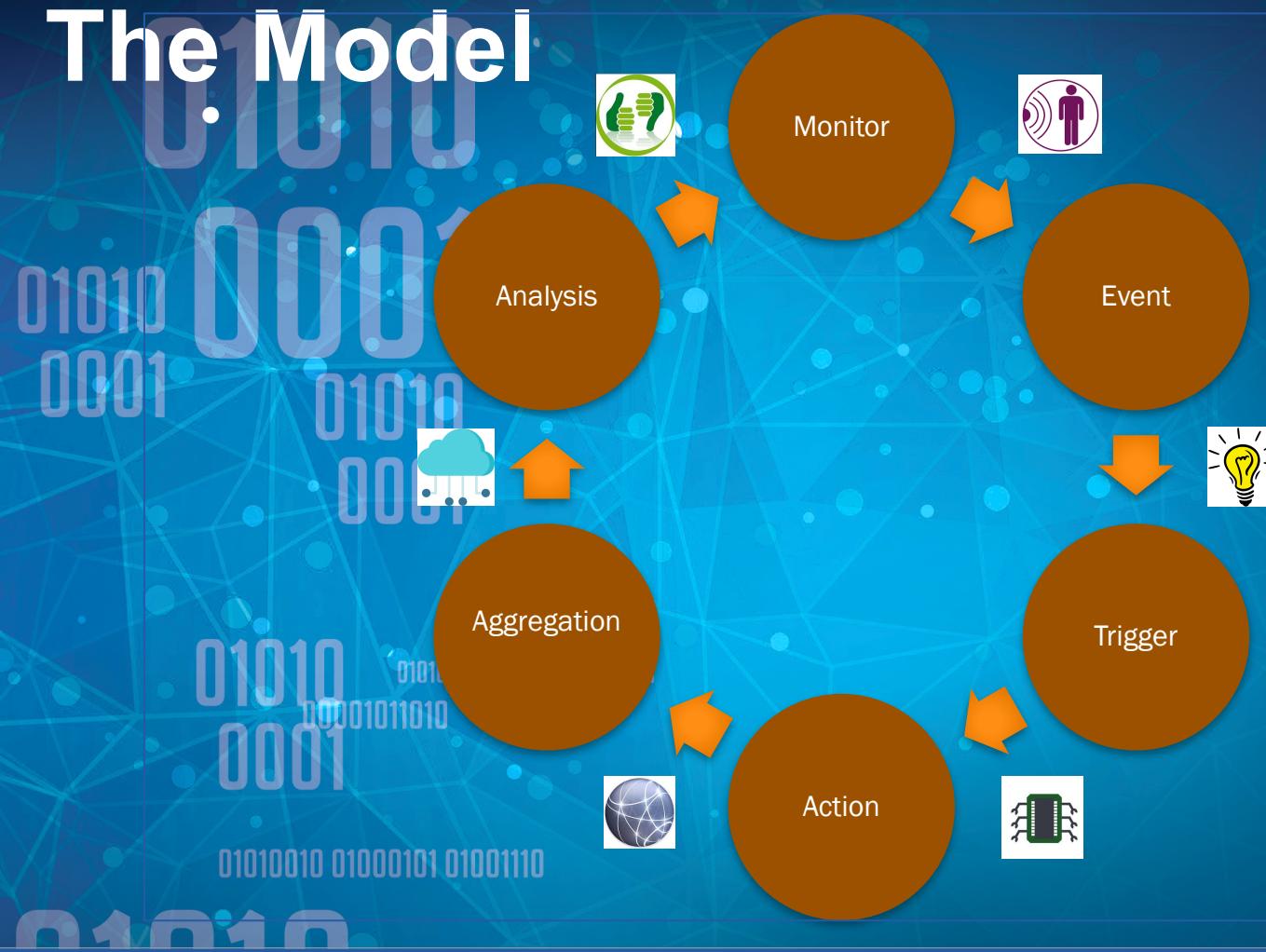
## Embedded Devices

- Pacemakers
- Implants

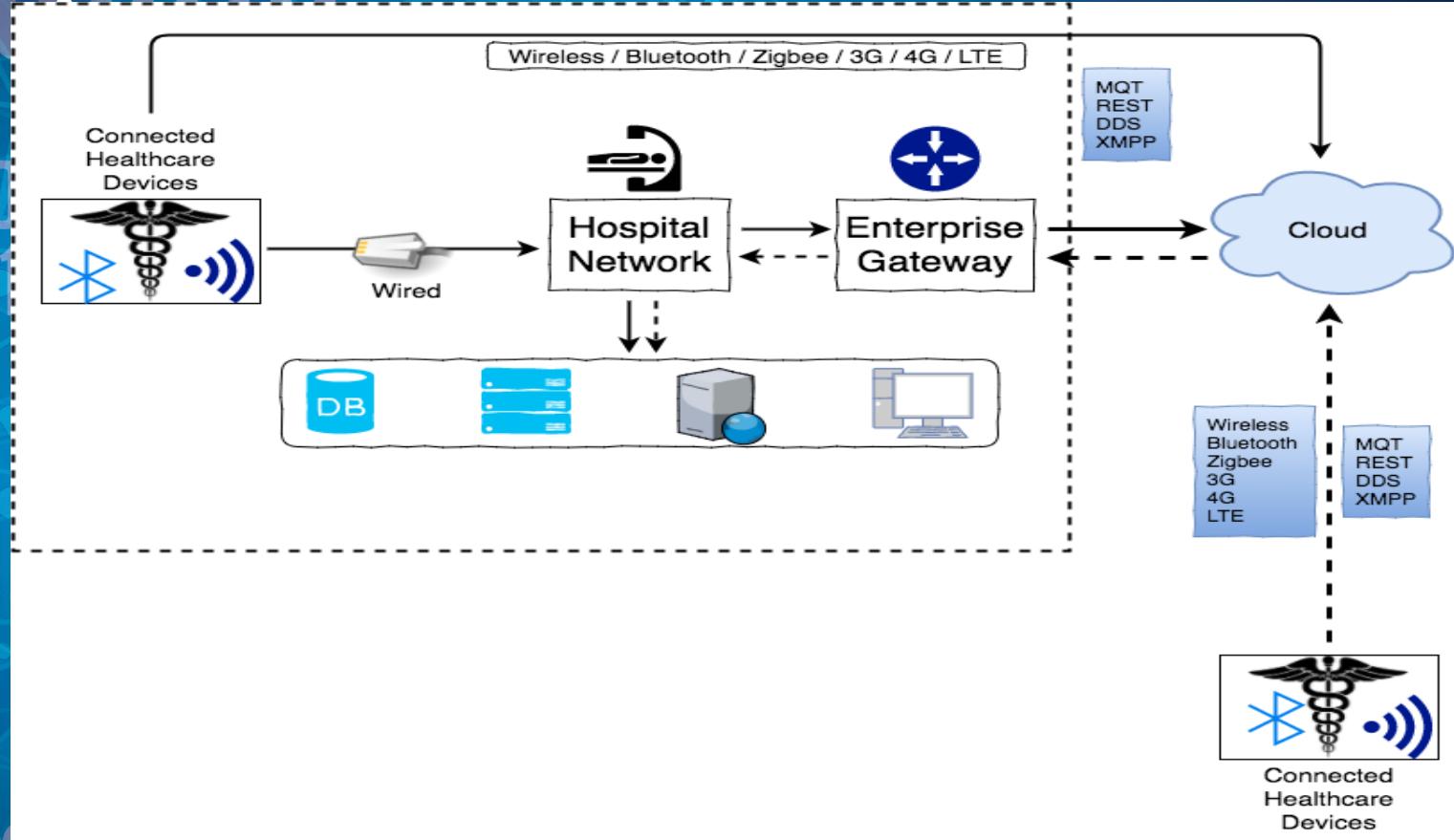
## In-house Equipments

- Medicine dispensing systems
- MRI
- CT Scanners
- Telemetry Systems
- X-Ray Machines
- Ultrasound Machines

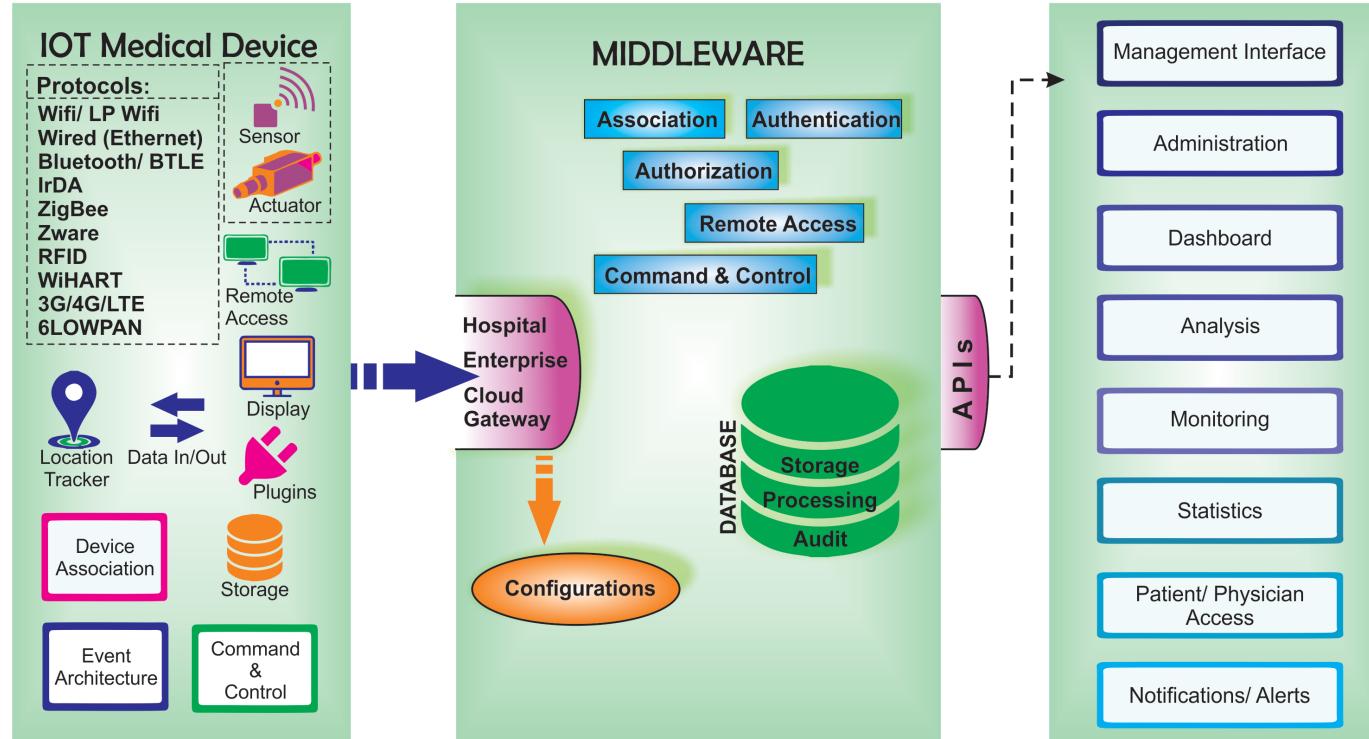
# The Model



# 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



# **JUST...**

# **JUST DON'T.**

# The Attack Surface

## IOT Security

- Network – Services, firewall
- Application - Authentication, Authorization, Input Validation
- Device Hardware – physical security
- Mobile – Client Data Storage, Data Transport, API
- Cloud – Backend Server, Authorization, Update security

# 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

OY VEY!!!



# 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

01010

01010 0001  
0001 01010

0001

01010

0001

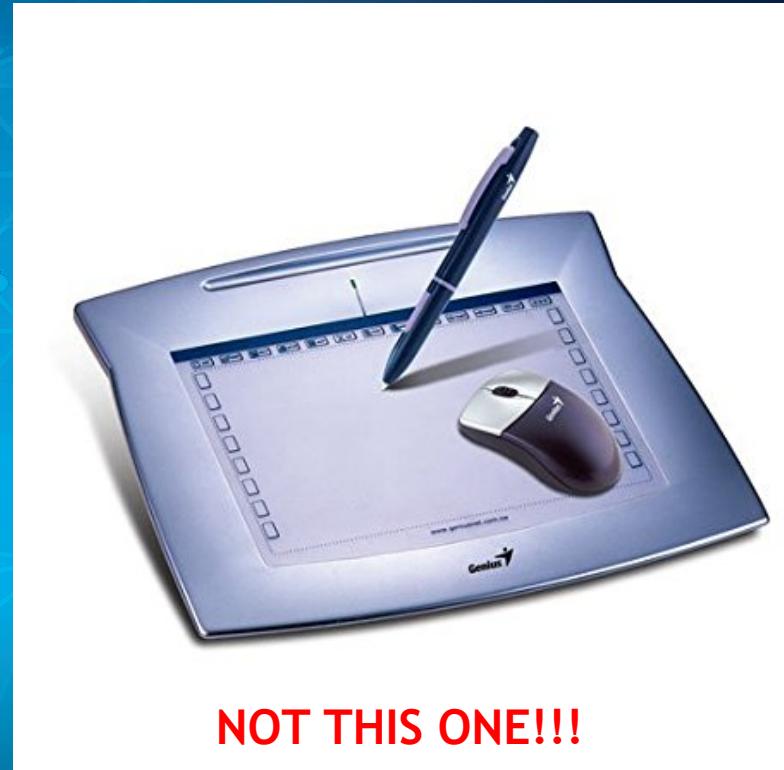
01010011 01010000 01001001

01010010 01000101 01001110

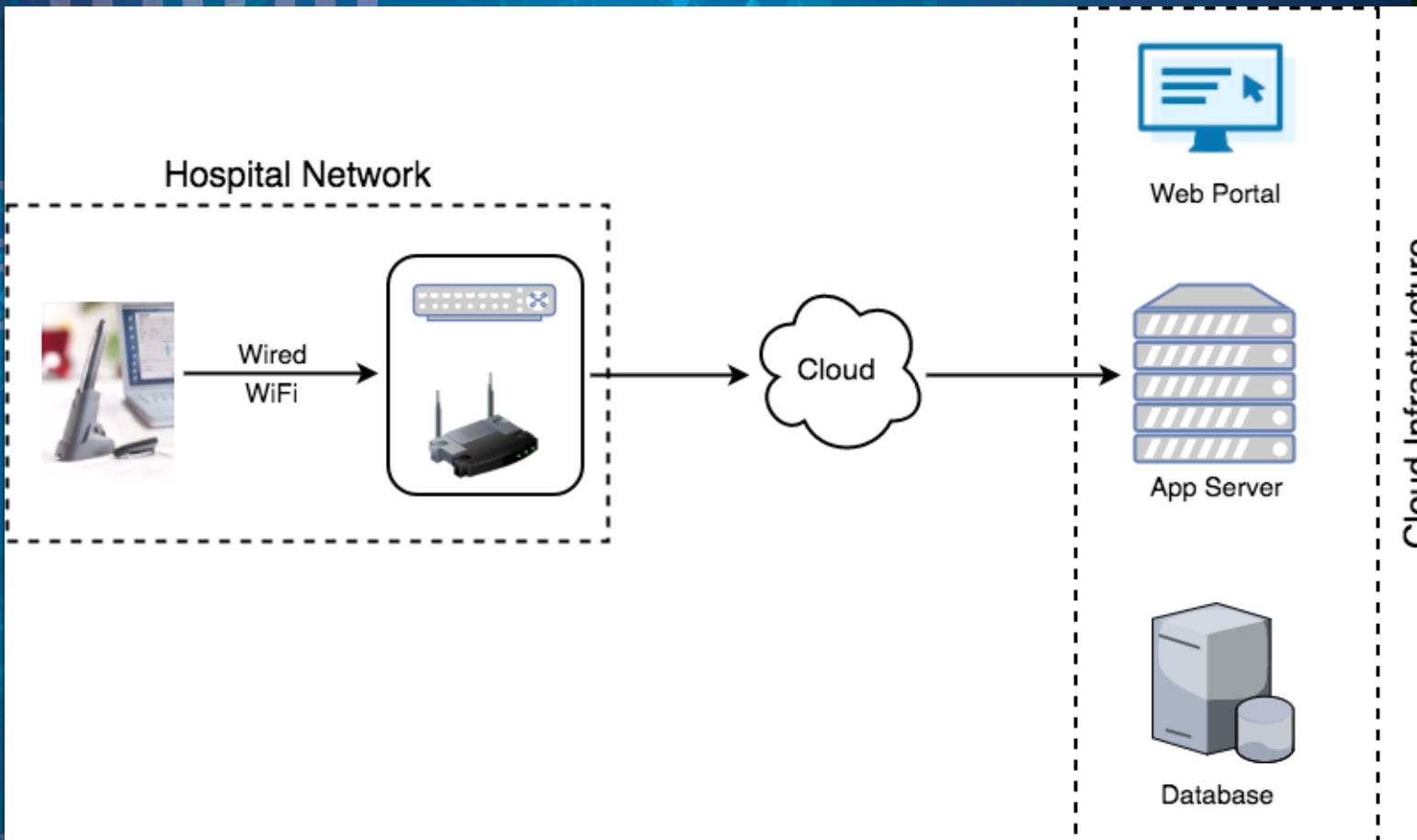
01010

# 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.



# Workflow



# 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

01010  
01010 0001  
0001 01010  
0001  
01010  
0001  
01010 0001  
0001 01010  
0001  
01010 0100011 010100000 01001001  
0001011010  
01010010 01000101 01001110  
01010

# 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  
  
01010011 01010000 01001001
7. Over the wire → HTTPS (AES256)
8. Remote Access Component  
  
01010010 01000101 01001110

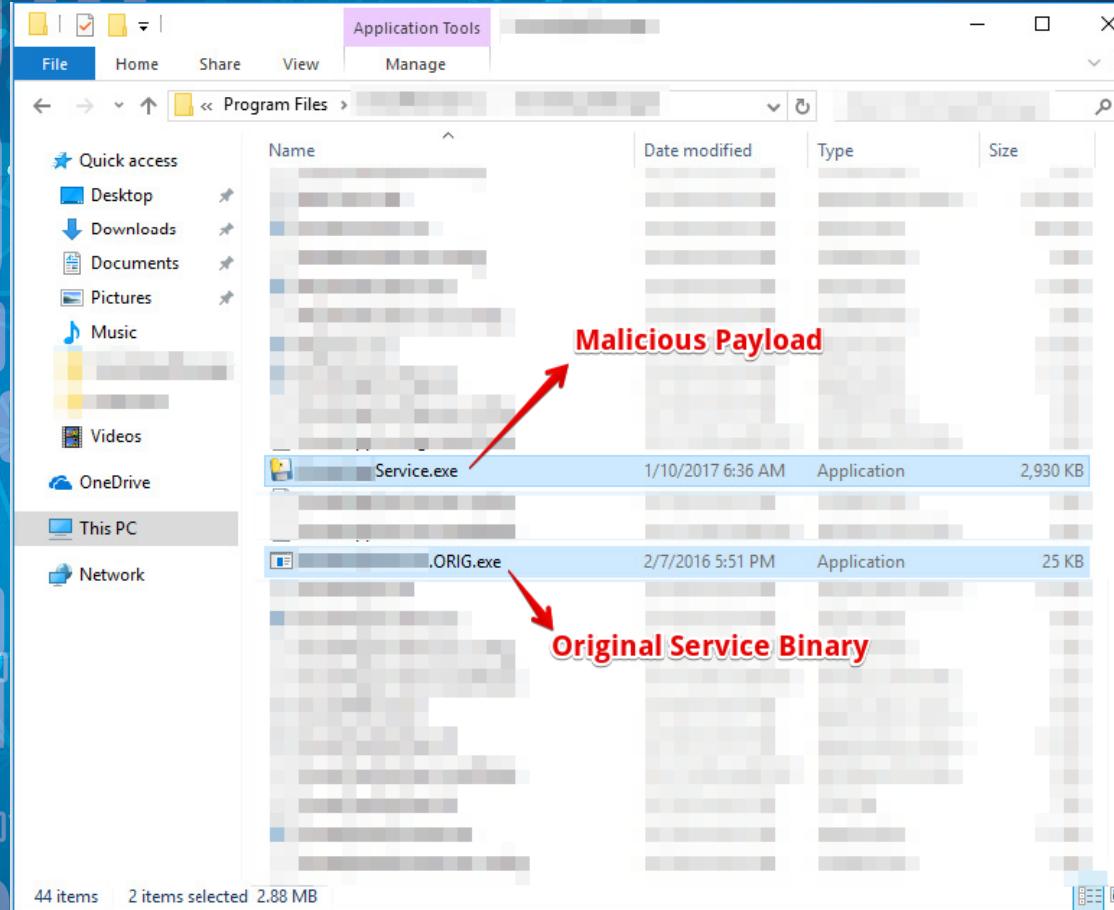


# Privilege Escalation

The image shows a Windows Services (Local) window. On the left, a tree view shows various service categories like Secondary Logon, Secure Socket Tunneling Protocol Service, Security Accounts Manager, etc. On the right, a detailed list of services is shown with columns for Name, Description, Status, Startup Type, and Log On As. A specific service, "Service", is selected and its properties are displayed in a modal dialog box. The modal dialog has tabs for General, Log On, Recovery, and Dependencies. The General tab shows the service name as "Service", display name as "Service", and path to executable as "\Program Files\Service.exe". The startup type is set to Automatic. The service status is listed as Running. Buttons for Start, Stop, Pause, and Resume are present. A note says "You can specify the start parameters that apply when you start the service from here." and there is a "Start parameters:" input field. At the bottom of the modal are OK, Cancel, and Apply buttons.

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables star...	Manual	Local System	
Secure Socket Tunneling Protocol Service	Provides su...	Manual	Local Service	
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSV...	Running	Automatic (D...	Local Service
Sensor Data Service	Delivers dat...	Manual (Trig...	Local System	
Sensor Monitoring Service	Monitors va...	Manual (Trig...	Local Service	
Sensor Service	A service fo...	Manual (Trig...	Local System	
Server	Supports fil...	Running	Automatic	Local System
Shell Hardware Detection	Provides no...	Running	Automatic	Local System
Smart Card	Manages ac...	Disabled	Local Service	
Smart Card Device Enumeration Service	Creates soft...	Manual (Trig...	Local System	
Smart Card Removal Policy	Allows the s...	Manual	Local System	
Service	Receives tra...	Running	Automatic	Local System
	Enables the ...	Manual	Network Service	
	Verifies pote...	Manual (Trig...	Local System	
	Discovers n...	Running	Manual	Local Service
	Provides re...	Running	Manual	Local System
	Launches a...	Manual	Local System	
	Provides en...	Manual (Trig...	Local System	
	Optimizes t...	Manual	Local System	
	Maintains a...	Running	Automatic	Local System
	Monitors sy...	Running	Automatic	Local System
	Coordinates...	Running	Automatic (T...	Local System
	Enables a us...	Running	Automatic	Local System
	Provides su...	Running	Manual (Trig...	Local Service
	TeamViewer...	Running	Automatic	Local System
	Provides Tel...	Manual	Network Service	
	Provides us...	Running	Automatic	Local System
	Tile Server f...	Running	Automatic	Local System
	Coordinates...	Running	Manual (Trig...	Local Service
	Enables Tou...	Manual (Trig...	Local System	
	UsoSvc	Manual	Local System	
	Allows UPn...	Manual	Local Service	
	User Manag...	Running	Automatic (T...	Local System
	This service ...	Running	Automatic	Local System
	Provides m...	Manual	Local System	
	Manages an...	Manual	Local System	

# Privilege Escalation



# Privilege Escalation

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\[REDACTED]>net user
User accounts for \\DESKTOP-[REDACTED]

-----
Administrator [REDACTED] Guest [REDACTED]
[REDACTED] admin

The command completed successfully.

C:\Users\[REDACTED]>net localgroup Administrators
Alias name      Administrators
Comment         Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator [REDACTED]
admin [REDACTED] ←
The command completed successfully.
```

# The Encrypted File

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 268, Length: 20
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 512, Length: 40
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 552, Length: 40
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 592, Length: 40
12:5...	[REDACTED]	3932	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 632, Length: 40
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,144, Length: 16
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,160, Length: 8
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,264, Length: 2
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,168, Length: 8
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,274, Length: 2
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,176, Length: 8
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,284, Length: 2
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,184, Length: 8
12:5...	[REDACTED]	20...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,302, Length: 2
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,304, Length: [REDACTED]
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,368, Length: 16
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,384, Length: 8
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,792, Length: 16
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 390,808, Length: 8
12:5...	[REDACTED]	39...	ReadFile	C:\Program Files\	in...	SUCCESS Offset: 391,152, Length: 16

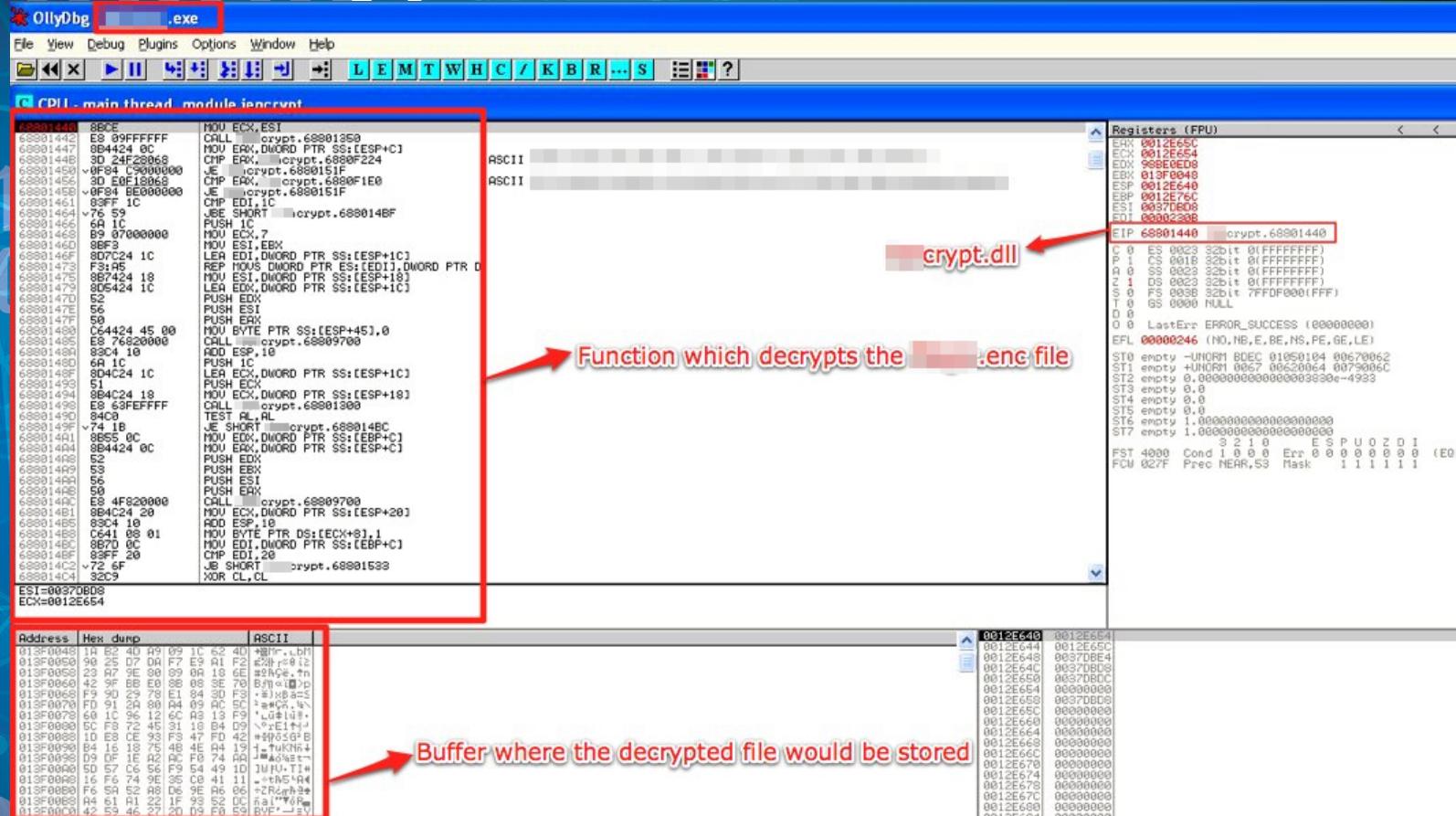
\*\*\*\*.enc

0001

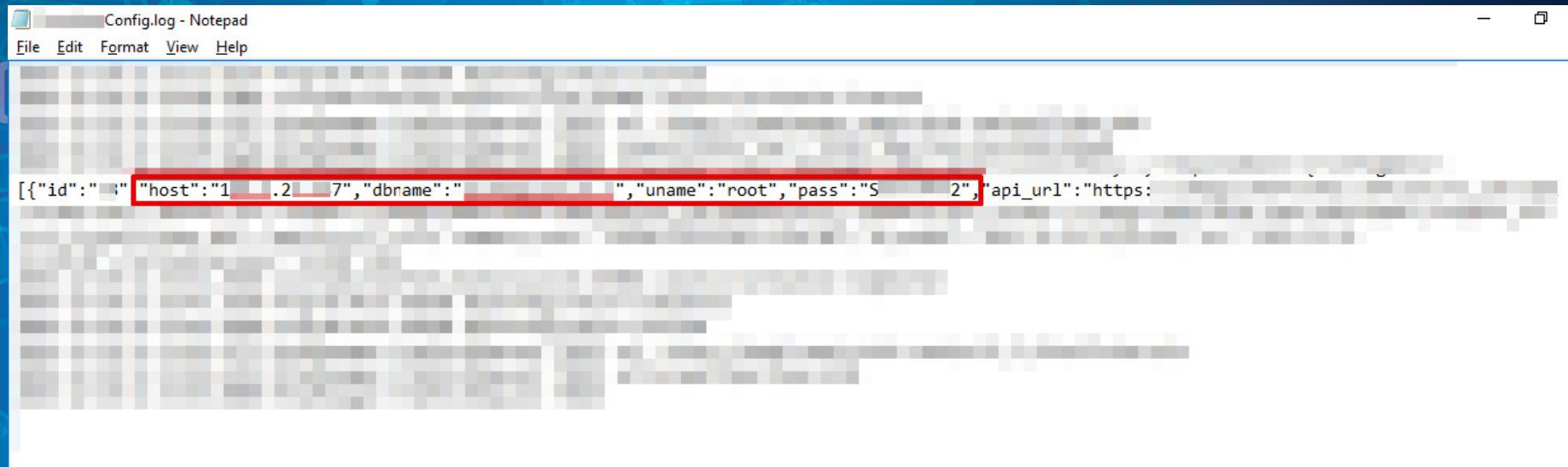
01010010 01000101 01001110

# The Encrypted File

010  
00



# The Encrypted File – Win!!!



A screenshot of a Windows Notepad window titled "Config.log - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The content of the file is a JSON array:

```
[{"id": "1", "host": "1.2.3.7", "dbname": "", "uname": "root", "pass": "S2", "api_url": "https://1.2.3.7/api"}]
```

The host, dbname, uname, pass, and api\_url fields are highlighted with a red rectangular box.



# Another Crime

# Access to Patient Data



The figure shows a MySQL Workbench interface. On the left, the 'Databases' tree view is open, showing the following structure:

- Databases
  - db1
  - information\_schema
  - mysql
  - performance\_schema
- Tables
  - patient\_sync\_info

The main area displays a table editor for the 'patient\_sync\_info' table. The table has the following columns and data:

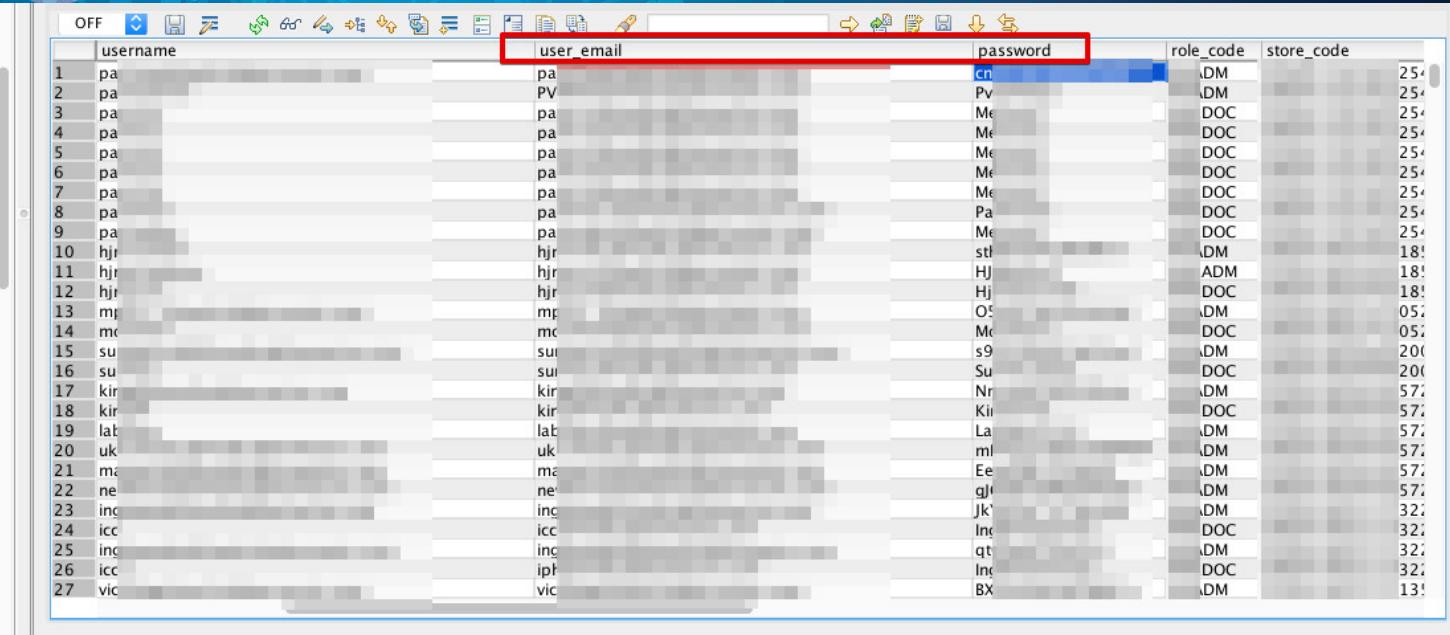
	id	patient_code	ref_patient_code	ref_unit_code	patient_fname	patient_lname	patient_birth_dt	patient_sex
1	39		87	3	Be	B	19	1
2	40		74	7	Po	P	19	3
3	41		65	9	Fr	F	19	8
4	42		47	8	Ca	C	19	0
5	43		45	6	Hc	H	19	6
6	44		28	1	Ka	K	19	9
7	46		48	6	Ma	M	19	7
8	47		53	7	Ka	K	19	4
9	48		21	6	Se	Si	19	6
10	49		80	1	Ma	N	19	2
11	50		97	9	Ol	O	19	8
12	51		7	0	Wi	W	19	2
13	52		85	6	Ta	T	19	9
14	53		04	3	Da	D	19	7
15	54		56	1	Pa	P	19	4
16	55		69	1	Re	R	19	0
17	56		19	8	Pe	P	19	6
18	57		92	6	Ra	R	19	5
19	58		23	8	Rh	R	19	3
20	59		88	6	Jol	C	19	8
21	60		41	5	Be	B	19	2
22	61		58	1	Da	D	19	3
23	62		12	5	Do	D	19	0
24	63		52	2	Ja	J	19	4
25	64		38	8	Ha	H	19	6
26	65		3	3	Ch	C	19	2
27	66		89	1	Ol	O	19	4
28	67		24	0	Wi	W	19	5
29	68		87	8	Wa	W	19	2
30	69		41	2	Mc	N	19	4
31	70		14	0	Ti	T	19	4
32	71		67	2	Br	B	19	5
33	72		24	2	Th	T	19	9
34	73		39	8	Ar	A	19	9
35	74		69	0	Ba	B	19	0
36	75		11	4	Ke	K	19	7
37	76		50	5	Mi	N	19	4

At the bottom, a status bar indicates: Executing Statement . . . Done. Query Time: [redacted]

## Communications

PROPRIETARY AND CONFIDENTIAL

# Access to Patient Data



	username	user_email	password	role_code	store_code
1	pa	pa	cn	ADM	254
2	pa	PV	Pv	ADM	254
3	pa	pa	Me	DOC	254
4	pa	pa	Me	DOC	254
5	pa	pa	Me	DOC	254
6	pa	pa	Me	DOC	254
7	pa	pa	Me	DOC	254
8	pa	pa	Pa	DOC	254
9	pa	pa	Me	DOC	254
10	hjr	hjr	stl	ADM	18!
11	hjr	hjr	HJ	ADM	18!
12	hjr	hjr	Hj	DOC	18!
13	mp	mp	O5	ADM	05!
14	mc	mc	Mc	DOC	05!
15	su	su	s9	ADM	200
16	su	su	Su	DOC	200
17	kir	kir	Nr	ADM	57!
18	kir	kir	Kir	DOC	57!
19	lab	lab	La	ADM	57!
20	uk	uk	ml	ADM	57!
21	ma	ma	Ee	ADM	57!
22	ne	ne	gl	ADM	57!
23	inc	inc	Jk	ADM	32!
24	icc	icc	In	DOC	32!
25	inc	inc	qt	ADM	32!
26	icc	ip	In	DOC	32!
27	vic	vic	BX	ADM	13!

01010010 01000101 01001110

# Access to Patient Data

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

# Prescriptions

01010 000 01010  
0001 01010 000  
01010 0001 01010  
0001011010  
01010010 01000101  
01010  
0001  
01010 0001 01010  
0001011010  
01010010 01000101  
01010

**DIGITAL PRESCRIBER'S ORDERS**

Facility: Pa \_\_\_\_\_ Unit: Ma \_\_\_\_\_  
Resident: Be \_\_\_\_\_ Room: 2 \_\_\_\_\_  
Health Card#: E22 \_\_\_\_\_ DOB (dd/mm/yyyy): 19/07/19 \_\_\_\_\_  
Allergies: No Known Allergies

Date/Time: T.O from Dr. [REDACTED]  
Hold warfarin for 2 days  
and [REDACTED] me  
INR next week  
order taken by [REDACTED]

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: 7/24/18 17:30:00 Date / Time: \_\_\_\_\_  
T.O from Dr. [REDACTED]  
Hold [REDACTED] days  
on [REDACTED] me.  
order taken by [REDACTED] Smith - Paul PW

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: 7/24/18 Date / Time: \_\_\_\_\_  
T.O from Dr. [REDACTED]  
Hold [REDACTED] days  
on [REDACTED] me.  
order taken by [REDACTED] Smith - Paul PW

Start Today  
 Start with Next Weekly Supply

Date/Time: \_\_\_\_\_ Clinical Indicator: \_\_\_\_\_

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

01010

01010 0001  
0001 01010

0001

01010

0001

01010011 01010000 01001001

01010010 01000101 01001110

01010

# 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.

01010010 01000101 01001110

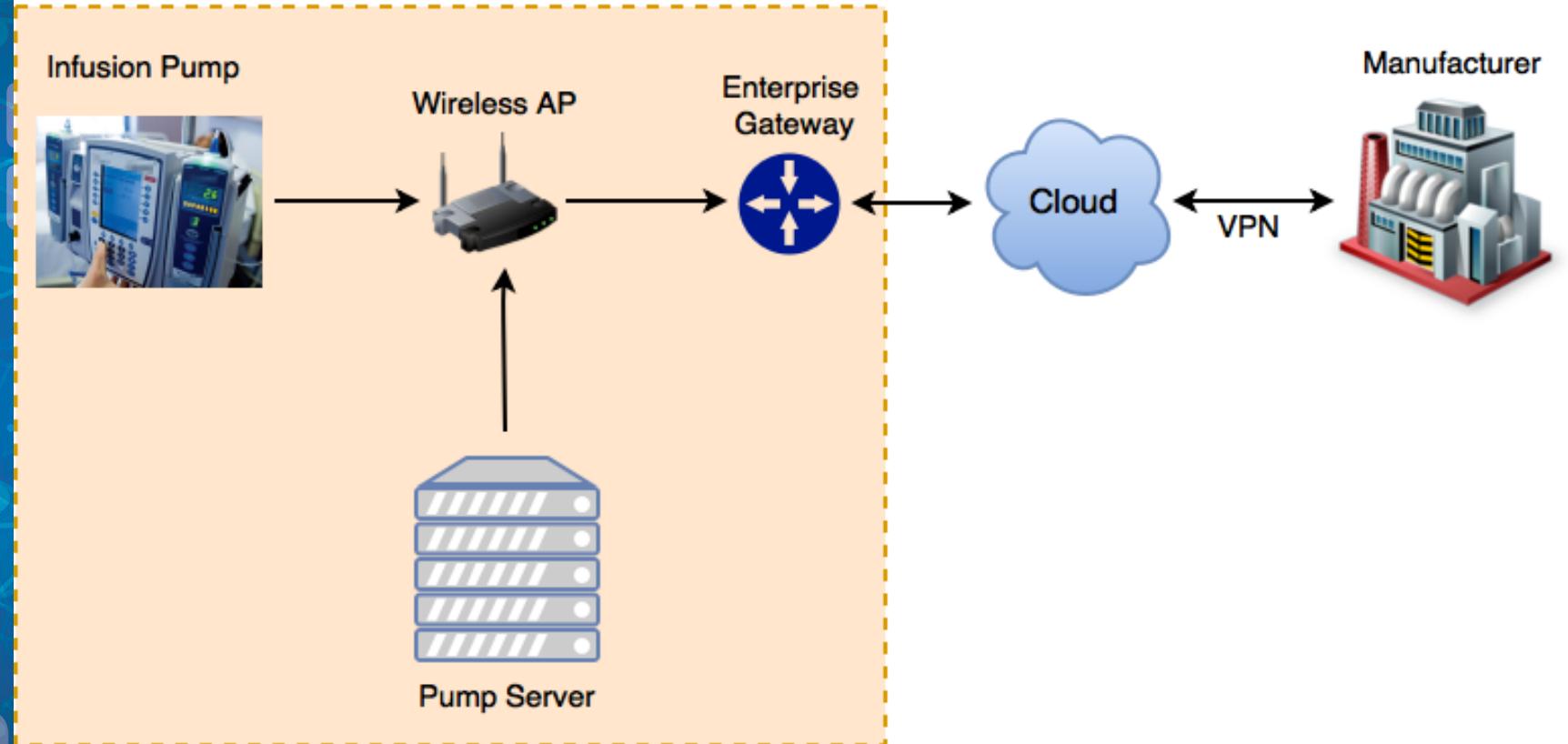


NOT THIS ONE  
EITHER!!!

# Workflow

## Hospital Network

01  
0



# 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

01010011 01010000 01001001

00001011010

01010010 01000101 01001110

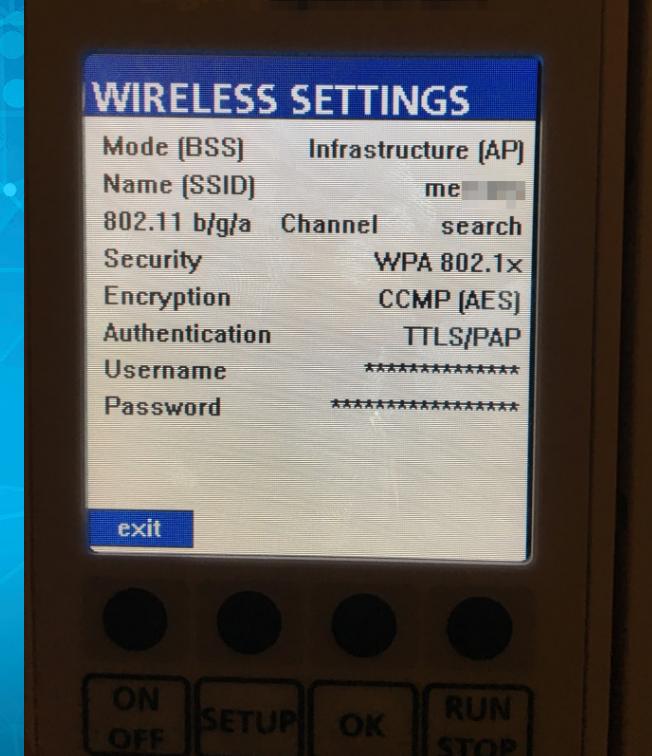
# Initial Observations

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/

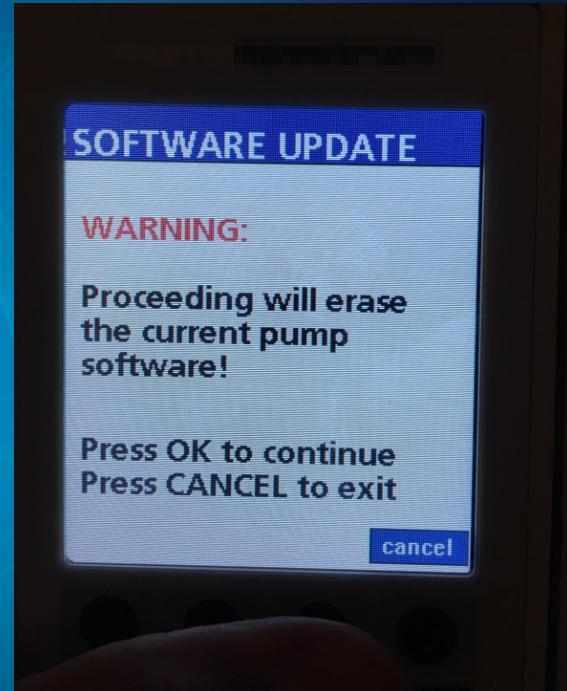
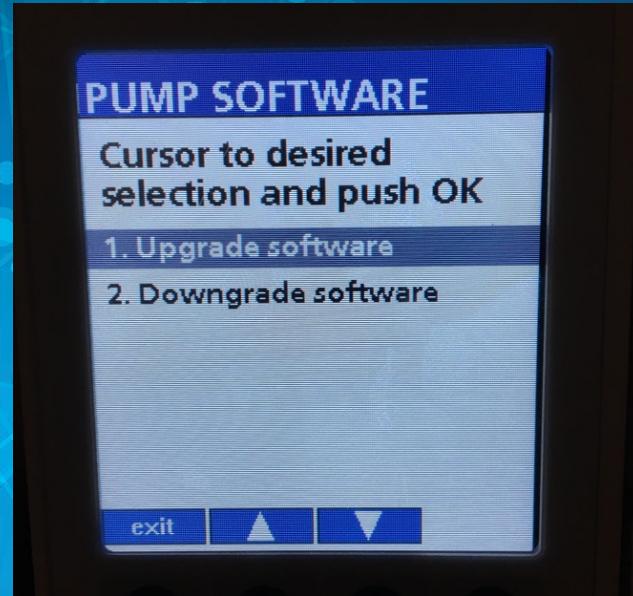
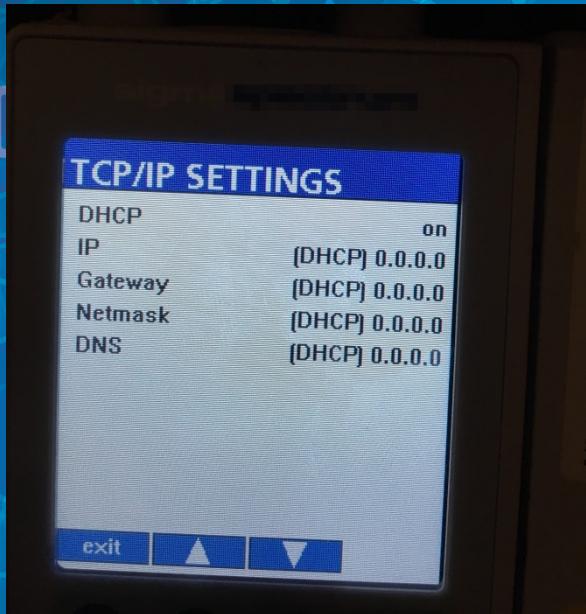


# First Blood

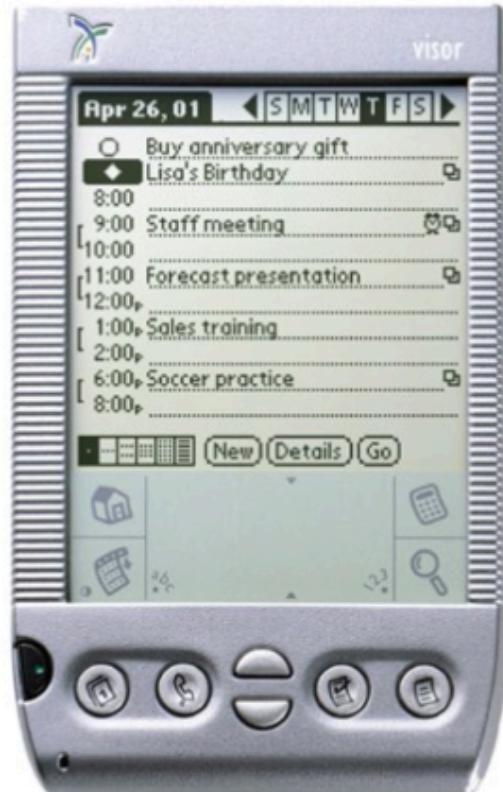
- Default Password
- Access to Network Config
- Change (some) Network Configs
- Upgrade/Downgrade Software



# Configs 01010



# We Bought a PDA



Handspring

## Handspring Visor Platinum (Silver)

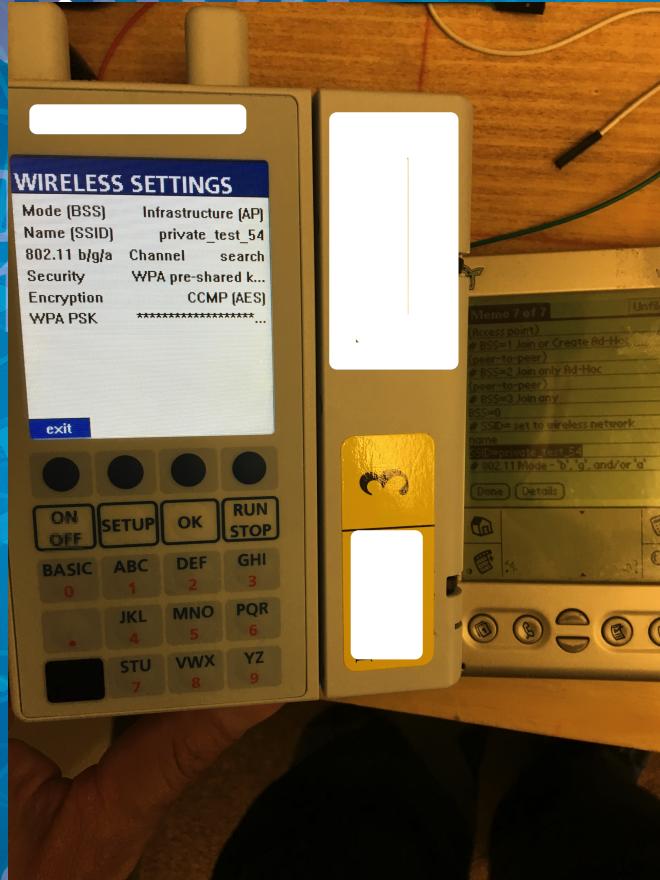


78 customer reviews

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

root



File Edit View Search Terminal Help

```
root@[REDACTED]# nc -l 51244
<XML><HEADER>1.0,2095696,2017    145740,1150358666000,13,</HEADER>1,192.168.13.1
69,192.168.13.1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0,,00:40:9d:66:ef:b
b,51243,74:26:ac:68:96:49,20180309174546,</XML>0k [REDACTED]
```

# 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

01010  
0001  
01010011 01010000 01001001  
10001011010  
01010010 01000101 01001110

# Fuzzing

01010 0000  
0001 0101  
000 000  
01010 01010  
0001 01010  
01010010 01000101  
01010 01010

```
root@[REDACTED] ~
File Edit View Search Terminal Help
[*]Normal: -> <XML><HEADER>1.0,2095696,2017[REDACTED] 162436,1150[REDACTED] 87600,13,</HEADER>
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:[REDACTED] bb,51243,74:20[REDACTED] 96:49,20180309174546,</XML>

[*]Detailed:Connection accepted 24151948,1150358798800,13,</HEADER>1,192.168.13.
1,255.255.255.0,192.168.13.1,10.123.56.6,0.0.0.0,,00:40:9d:66:
[*]Detailed:Socket listening 9,20180309174546,</XML>M0
,115040163[REDACTED] 4849414445523e312e302c323039353639362c3230313730383234313531393438
[*]Normal: -> <XML><HEADER>1.0,2095696,2017[REDACTED] 162456,1150[REDACTED] 89600,13,</HEADER>
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:ef:bb,51243,74:26:[REDACTED] 96:49,20180309174546,</XML>a39643a36363a
d:66:ef:bb,c35313234332c37343a32363a61633a3638a3a39363a34392c323031383033303931
[*]Detailed:Connection accepted
5,255.0,19205696,'20170824151948','1150358798800','13','')
[*]Detailed:Socket listening unknown field 3': '', 'unknown field 2': '11503587
,13,</HEADER> message_time': '20170824151948', 'message_type': '13', 'pump_serialno
[*]Normal: -> <XML><HEADER>1.0,2095696,2017[REDACTED] 62516,1150[REDACTED] 91600,13,</HEADER>
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:ef:bb,51243,74:26:[REDACTED] 96:49,20180309174546,</XML>68:96:49', '2
243,74:26:[REDACTED] 6', '')
[*]Detailed:Connection accepted _field_4': '1', 'pump_wbm_mac': '00:40:9d:66:e
3,13.1,10.1,0,maintenance_date': '20180309174546', 'pump_ip_dns': '192.168.13.1
[*]Detailed:Socket listening 68,13.1,'pump_sigma_listenport': '51243', 'pump_
,192.168.13.1,255.255.255.0', 'pump_ip_address': '192.168.13.169', 'sigma_gate
[*]Normal: -> 1<XML><HEADER>1.0,2095696,2017[REDACTED] 162537,1150[REDACTED] 2393700,13,</HEADER>
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:[REDACTED] b,51243,74:26:[REDACTED] 96:49,20180309174546,</XML>2': '11503703
8:96:49,20180309174546,'message_time': '20170825232723', 'message_type': '11', 'pump_serialno
[*]Detailed:Connection accepted
_field_4': '0', 'unknown_field_6': '1', 'pump_serial_concat_timestamp
[*]Detailed:Socket listening
Sending <XML><HEADER>1.0,2095696,20170824151948,1150358798800,13,</HEADER>1,19
[*]Normal: 68->1<XML><HEADER>1.0,2095696,2017[REDACTED] 162557,1150[REDACTED] 95700,13,</HEADER>
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:ef:bb,51243,74:26:[REDACTED] 96:49,20180309174546,</XML>message_gen
root@sakura:~/projects/nyp201706hardware/workspace# python sigma-message-gen
itor.py
```

# Winning Packet

01010 0001

Wireshark · Follow TCP Stream (tcp.stream eq 7) ·

```
<XML><HEADER>1.0,2095696,20170 53330,0000415 5121000,3,WCI 411</  
HEADER>20170 53330,0,5,0,0,0,0,0,00:00,00:00,<EVENT>0000415 5121000,4609,Pump ON; - Pwr Stat: AC</EVENT><POWERON>20170 53330</  
POWERON><DRUG>1,,,255,0,0</DRUG><DOSE>1,0,0,0,0</DOSE><CAREAREA></CAREAREA><ENCOUNTER></ENCOUNTER><CAREGIVER></  
CAREGIVER><PATIENT></PATIENT><LOCATION></LOCATION><ROUTE></ROUTE><SITE></SITE><POWER>1,-1</POWER></XML>F.
```

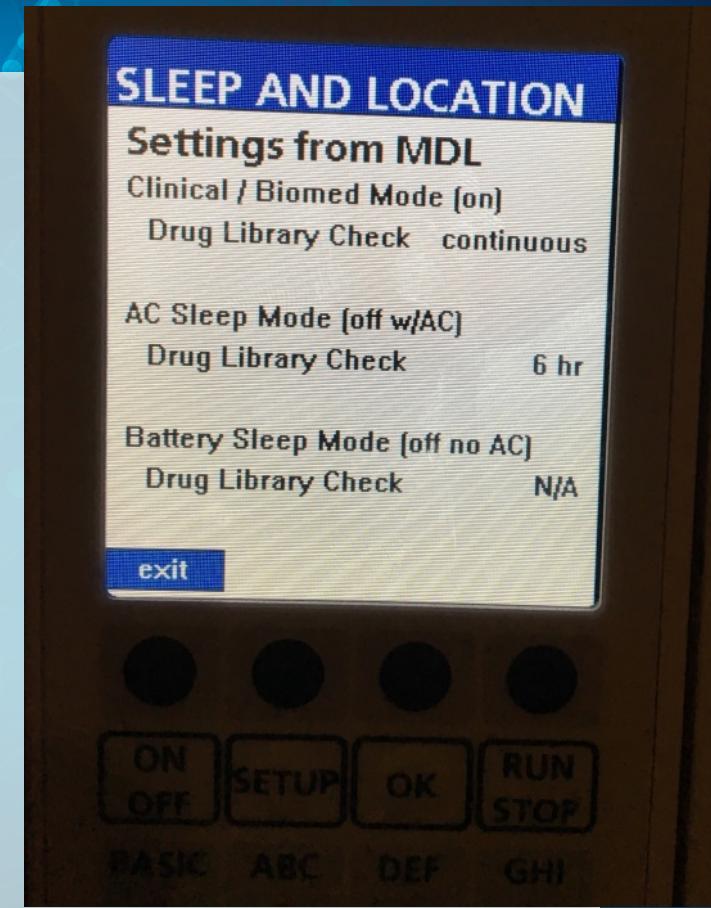


01010  
0001

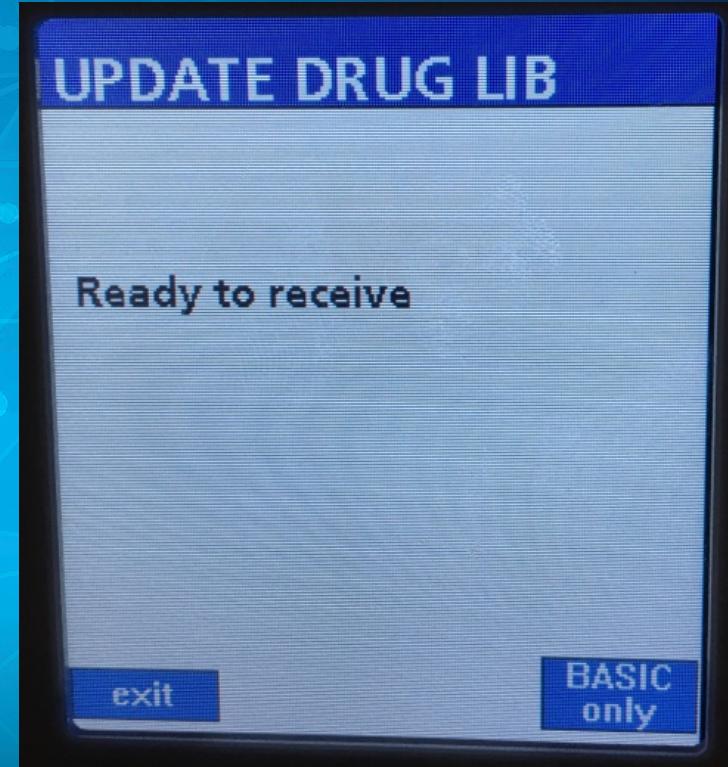
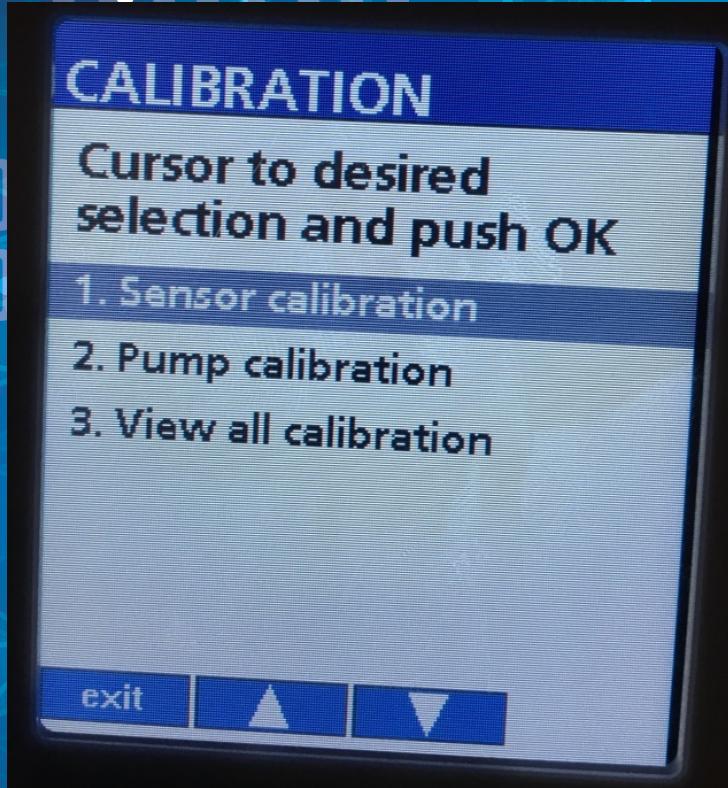
01010010 01000101 01001110

# Master Drug List

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



# More Access



# **QUESTIONS?**



# References

- Google Image Cache

0001  
01010  
0001

01010  
0001  
01010011 01010000 01001001  
0001011010  
01010010 01000101 01001110