

01010

0001

01010  
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 / Red Teamer / Domain Admin Everywhere
- Security Researcher
- Trainer, Speaker
- Wannabe Reverse Engineer
- Developer of Yasuo



- 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

# Disclaimer



# 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

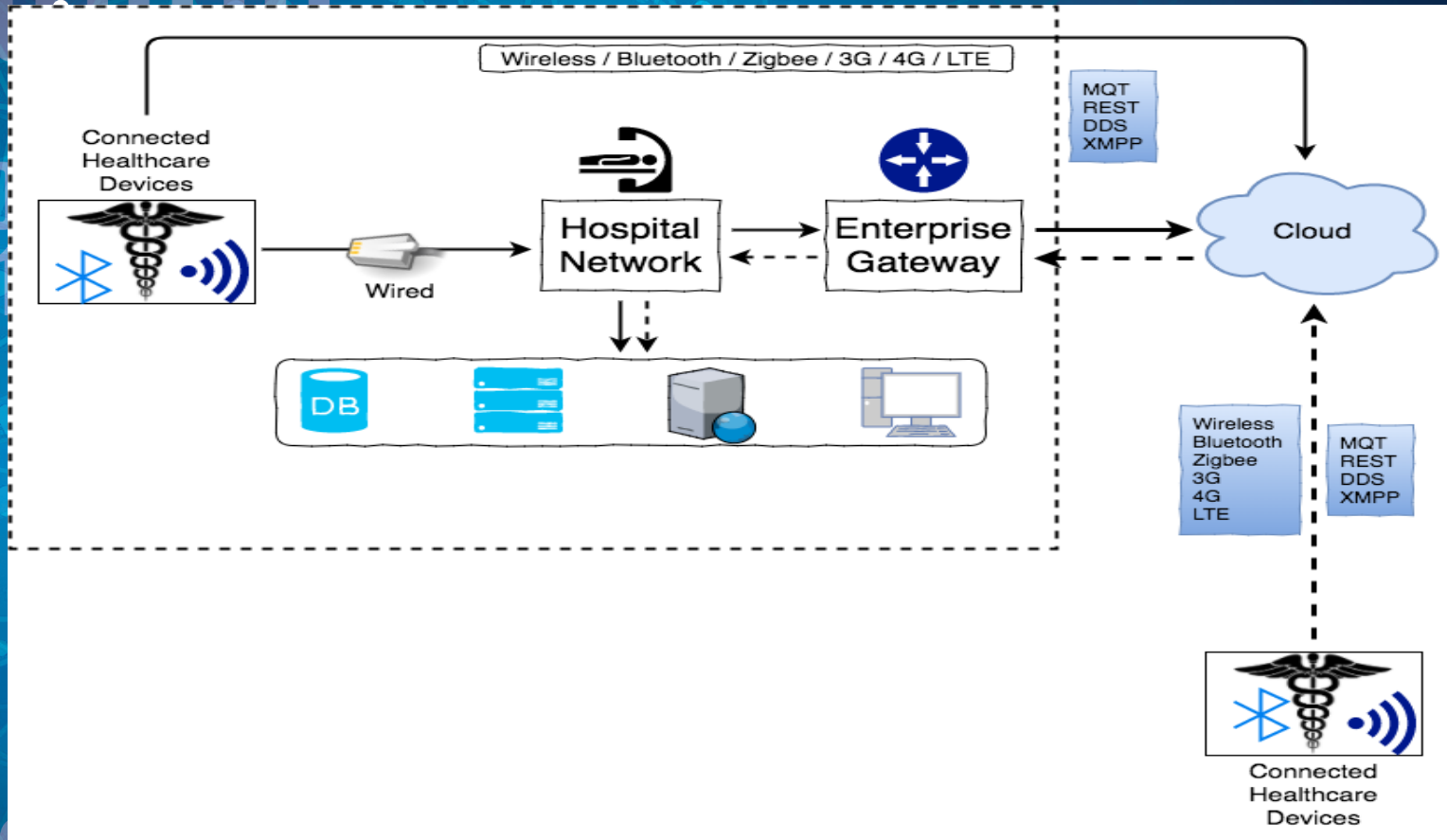
## In-house Equipments

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



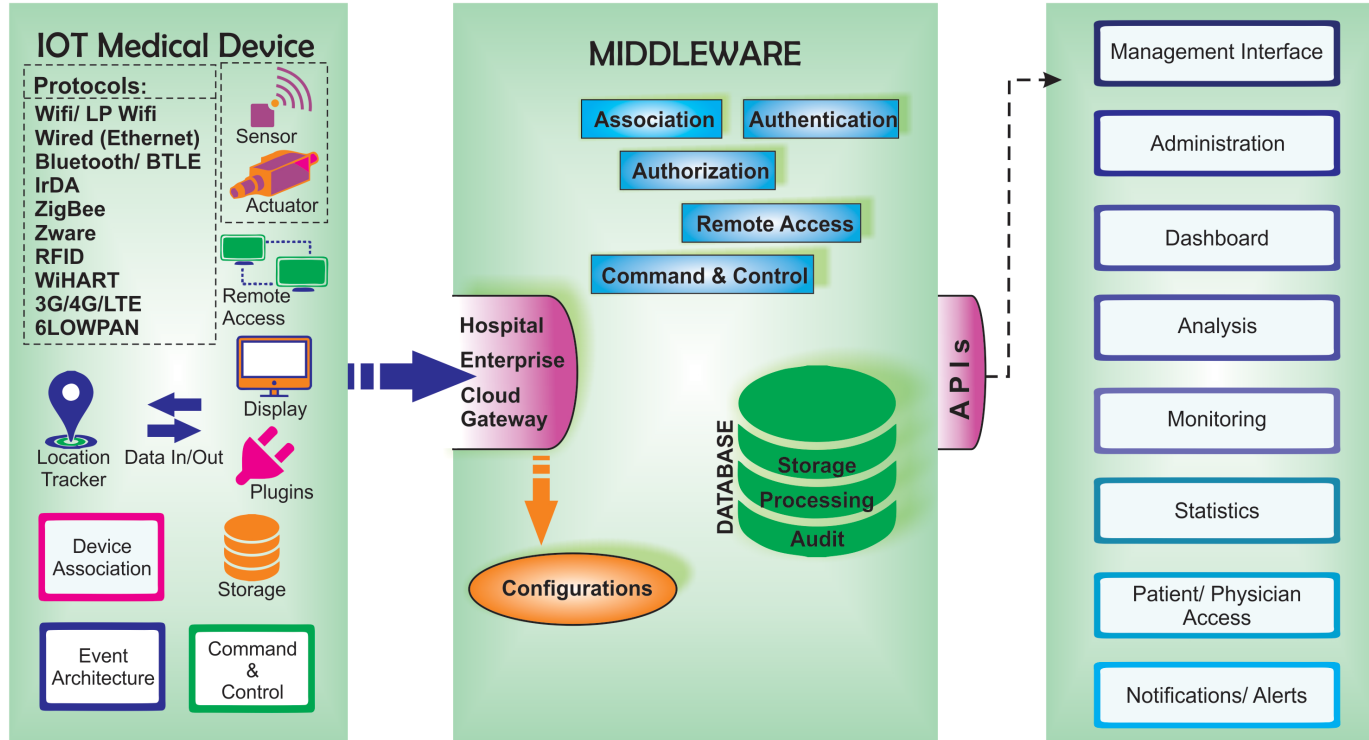


# The Ecosystem





# The Architecture



# The Good

1. Remote health monitoring
2. Less expenditure, better quality care
3. Faster response time
4. Global health care
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. Interoperability
7. Monitoring, Automation & Analytics
8. Rogue Medical Devices
9. Operating Systems???. Think MedJack

# Serial To Ethernet Converters



# 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



# Financial vs Medical Data



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



# Case Study #1



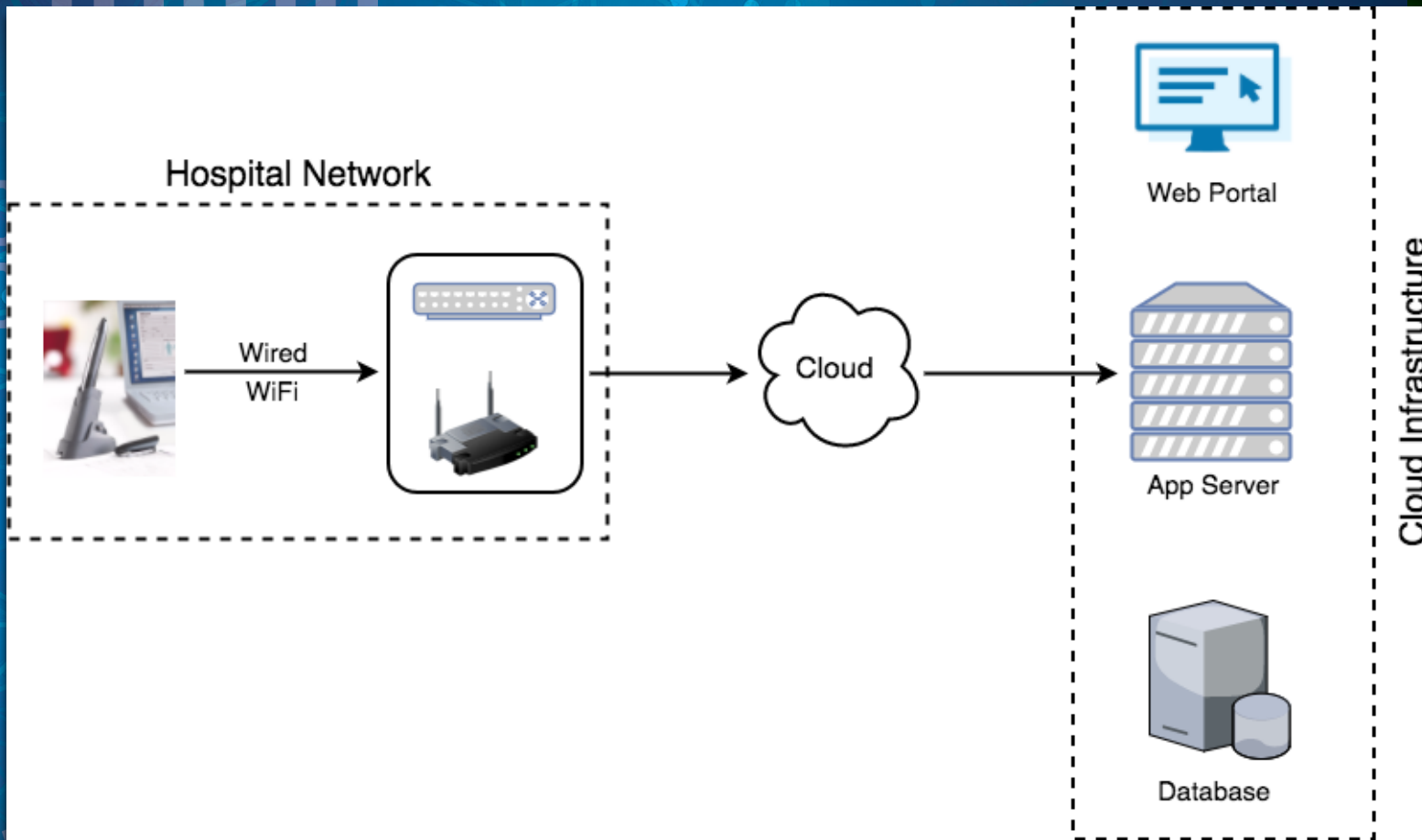
# About the Device

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





# 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

The screenshot shows the Windows Services console with a list of services and a Properties dialog box for a service named 'Service'.

**Services (Local)**

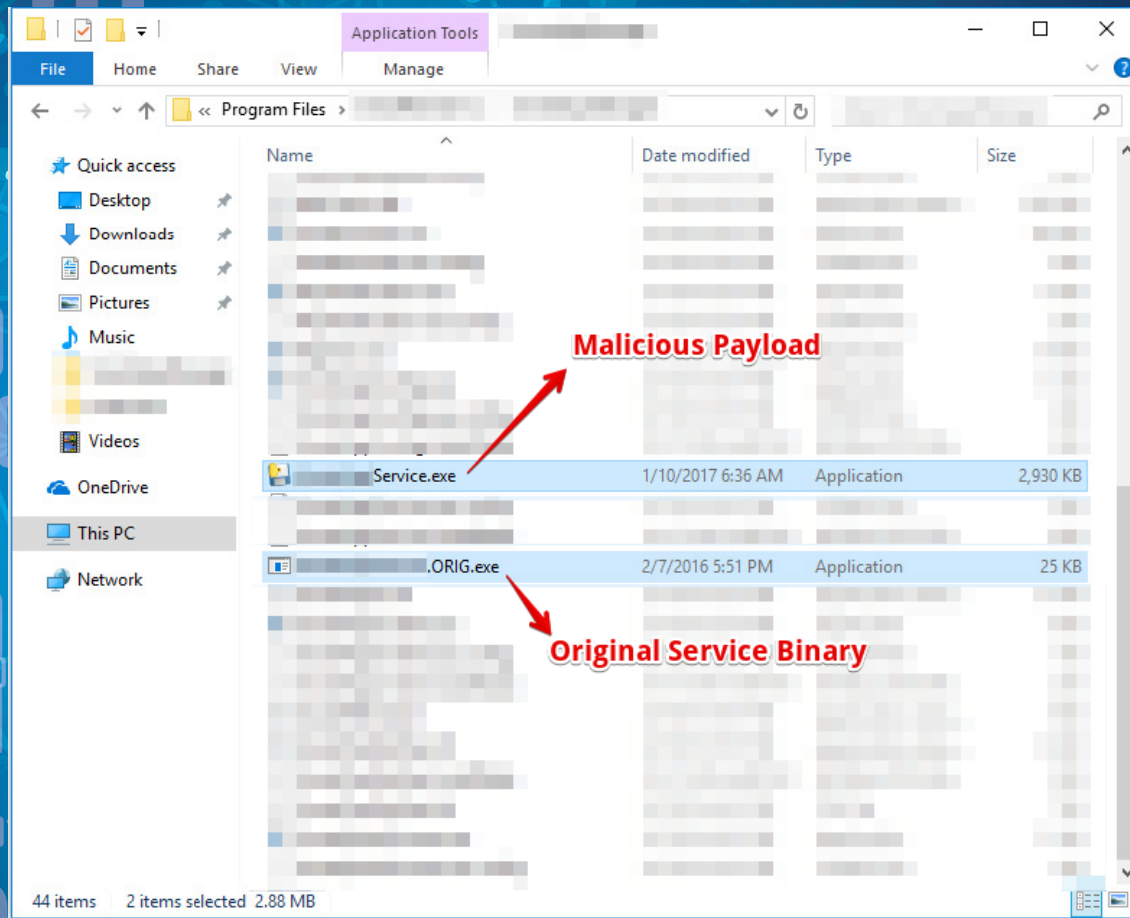
Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables star...		Manual	Local System
Secure Socket Tunneling Protocol Service	Provides su...		Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSV...	Running	Automatic (D...	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		Running	Automatic	Local System
	Receives tra...		Manual	Local Service
	Enables the ...		Automatic (D...	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

**Properties (Local Computer)**

General | Log On | Recovery | Dependencies

Service name: Service  
Display name: Service  
Description:  
Path to executable: Program Files\ \ Service.exe  
Startup type: Automatic  
Service status: Running  
Start Stop Pause Resume  
You can specify the start parameters that apply when you start the service from here.  
Start parameters:

# Privilege Escalation



# Privilege Escalation

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

C:\Users\>net user

User accounts for \\DESKTOP

-----
Administrator          Guest
                        admin
The command completed successfully.

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

Members

-----
Administrator
admin
The command completed successfully.
```



# The Encrypted File

Process Monitor - Sysinternals: www.sysinternals.com

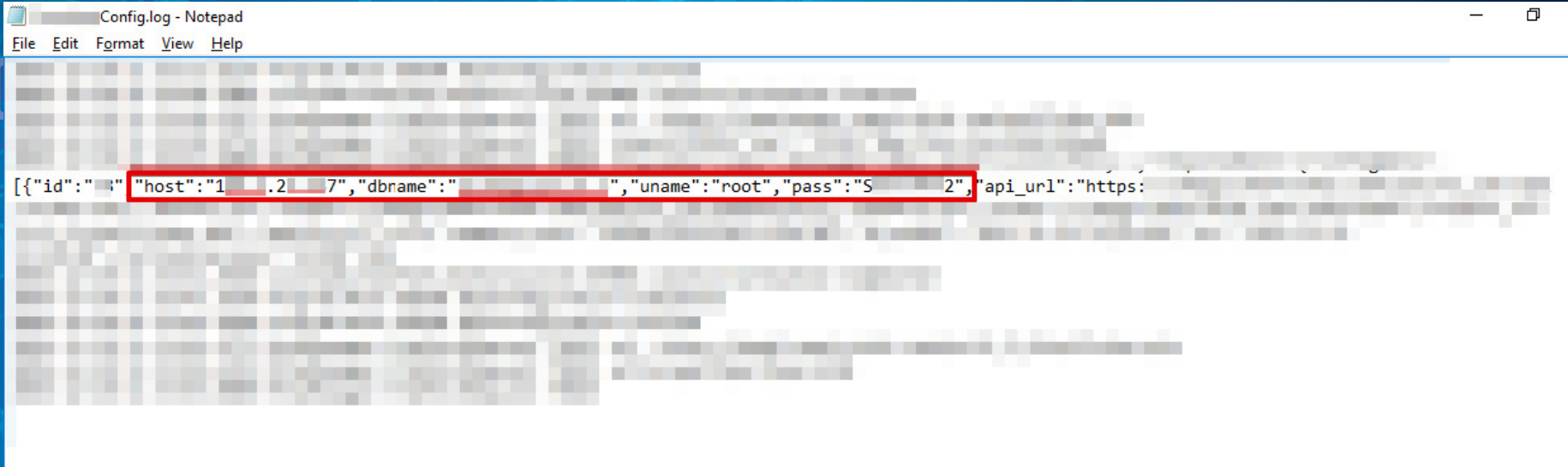
File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 268, Length: 20
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 512, Length: 40
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 552, Length: 40
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 592, Length: 40
12:5...	...exe	3932	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 632, Length: 40
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,144, Length: 16
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,160, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,264, Length: 2
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,168, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,274, Length: 2
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,176, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,284, Length: 2
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,184, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,302, Length: 2
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,304, Length: 16
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,308, Length: 16
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,384, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,792, Length: 16
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 390,808, Length: 8
12:5...	...exe	39...	ReadFile	C:\Program Files\...	in... SUCCESS	Offset: 391,152, Length: 16

\*\*\*.enc



# The Encrypted File – Win!!!



```
Config.log - Notepad
File Edit Format View Help

[{"id": "1", "host": "1.2.7", "dbname": "", "uname": "root", "pass": "S 2", "api_url": "https:"
```





# Access to Patient Data

The screenshot displays a database management interface. On the left, a tree view shows the database structure: Databases > db1 > information\_schema, mysql, performance\_schema, and Tables. The main window shows a table with the following columns: id, patient\_code, ref\_patient\_code, ref\_unit\_code, patient\_fname, patient\_lname, patient\_birth\_dt, and patient\_sex. The table contains 27 rows of data, with some cells highlighted in pink. The status bar at the bottom indicates 'Executing Statement . . . Done. Query Time: '.

	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 null
2	40		74	7	Po	P	19	3
3	41		65	9	Fr	Fr	19	8 null
4	42		47	8	Ca	C	19	0 null
5	43		45	6	Hc	H	19	6 null
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	Me	M	19	2
11	50		97	9	Ol	O	19	8
12	51		7	0	Wi	W	19	2 null
13	52		85	6	Ta	T	19	9
14	53		04	3	De	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 null
21	60		41	5	Be	B	19	2
22	61		58	1	De	D	19	3
23	62		12	5	Dc	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	M	19	4
31	70		14	0	Til	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	M	19	4

# Access to Patient Data

The screenshot shows a database management interface with a table of user data. The table has columns for 'username', 'user\_email', 'password', 'role\_code', and 'store\_code'. The 'user\_email' and 'password' columns are highlighted with a red box. The data is as follows:

	username	user_email	password	role_code	store_code
1	pa	pa	co	.DM	254
2	pa	PV	PV	.DM	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	.DM	18!
11	hjr	hjr	HJ	.ADM	18!
12	hjr	hjr	Hj	.DOC	18!
13	mp	mp	Os	.DM	05!
14	mc	mc	Mc	.DOC	05!
15	su	su	s9	.DM	20!
16	su	su	Su	.DOC	20!
17	kir	kir	Nr	.DM	57!
18	kir	kir	Kii	.DOC	57!
19	lab	lab	La	.DM	57!
20	uk	uk	ml	.DM	57!
21	ma	ma	Ee	.DM	57!
22	ne	ne	gj	.DM	57!
23	inc	inc	Jk	.DM	32!
24	icc	icc	Inc	.DOC	32!
25	inc	inc	qt	.DM	32!
26	icc	ipf	Inc	.DOC	32!
27	vic	vic	BX	.DM	13!

0001  
01010010 01000101 01001110

01010



# Access to Patient Data

Resident Name	Unit	Home	Room No	#HCN
At [REDACTED]	[REDACTED]	[REDACTED]	2	365 [REDACTED]
At [REDACTED]	[REDACTED]	[REDACTED]	2	635 [REDACTED]
Be [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]
Elv [REDACTED]	[REDACTED]	[REDACTED]	0	682 [REDACTED]
Mc [REDACTED]	[REDACTED]	[REDACTED]	2	391 [REDACTED]
Mi [REDACTED]	[REDACTED]	[REDACTED]	1	985 [REDACTED]

0001  
01010010 01000101 01001110

# 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																					
<p>T.O from Dr. _____            Hold warfarin for 2 days            and _____ me            INR next week            your taken by _____</p> <p style="text-align: right;"> <input type="checkbox"/> Start Today  <input type="checkbox"/> Start with Next Weekly Supply         </p>																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Prescriber's Signature / Registration #</td> <td style="width: 15%;">Nurse 1</td> <td style="width: 15%;">Nurse 2</td> <td colspan="4">Nurse: Please Initial The Documentation As Performed</td> </tr> <tr> <td></td> <td></td> <td></td> <td>Care Plan</td> <td>Consent</td> <td>Mar/Tar</td> <td>Lab</td> </tr> <tr> <td></td> <td>Date / Time</td> <td>Date / Time</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>		Prescriber's Signature / Registration #	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed							Care Plan	Consent	Mar/Tar	Lab		Date / Time	Date / Time				
Prescriber's Signature / Registration #	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed																			
			Care Plan	Consent	Mar/Tar	Lab																
	Date / Time	Date / Time																				
Date/Time	Clinical Indicator																					
<p>7/2/14 17:30m            T.O from Dr. _____            Hold _____ days            on _____ me            order taken by _____            Smith = Paul RN</p> <p style="text-align: right;"> <input type="checkbox"/> Start Today  <input type="checkbox"/> Start with Next Weekly Supply         </p>																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Prescriber's Signature / Registration #</td> <td style="width: 15%;">Nurse 1</td> <td style="width: 15%;">Nurse 2</td> <td colspan="4">Nurse: Please Initial The Documentation As Performed</td> </tr> <tr> <td></td> <td></td> <td></td> <td>Care Plan</td> <td>Consent</td> <td>Mar/Tar</td> <td>Lab</td> </tr> <tr> <td></td> <td>Date / Time</td> <td>Date / Time</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>		Prescriber's Signature / Registration #	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed							Care Plan	Consent	Mar/Tar	Lab		Date / Time	Date / Time				
Prescriber's Signature / Registration #	Nurse 1	Nurse 2	Nurse: Please Initial The Documentation As Performed																			
			Care Plan	Consent	Mar/Tar	Lab																
	Date / Time	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.



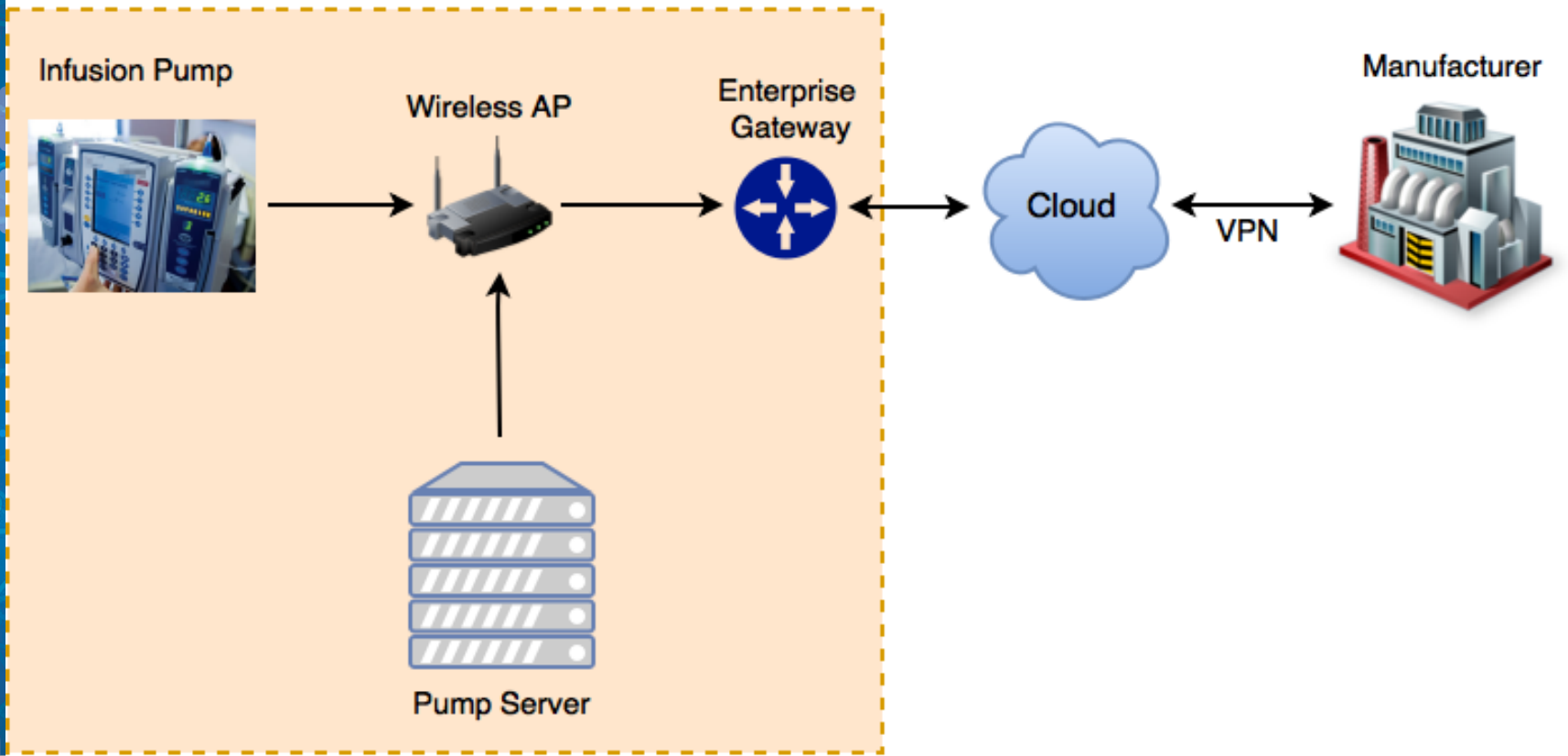
**NOT THIS ONE  
EITHER!!!**

01010010 01000101 01001110

01010

# Workflow

## Hospital Network





# Initial Lab Setup

Standalone Infusion Pump

# Initial Observations

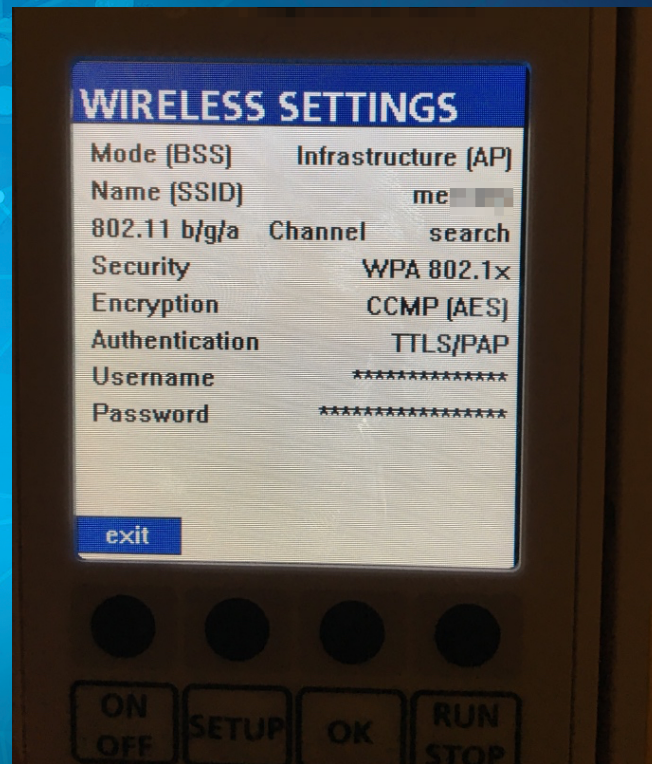
1. Ethernet (RS-232)
2. 802.11 b/g/a Integrated Wireless Network
3. USB Enabled
4. IrDA Port
5. Display – Touch Screen
6. Keypad
7. Maintenance Mode – Password Protected \o/





# First Blood

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





# We Bought a PDA

Handspring

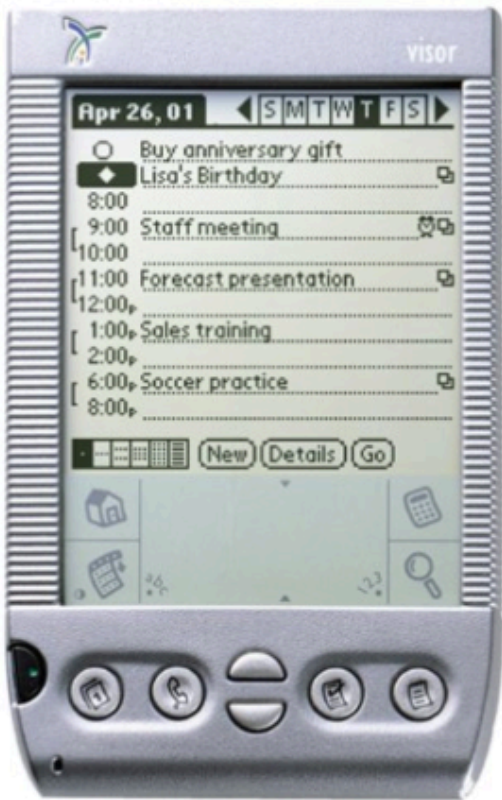
## Handspring Visor Platinum (Silver)



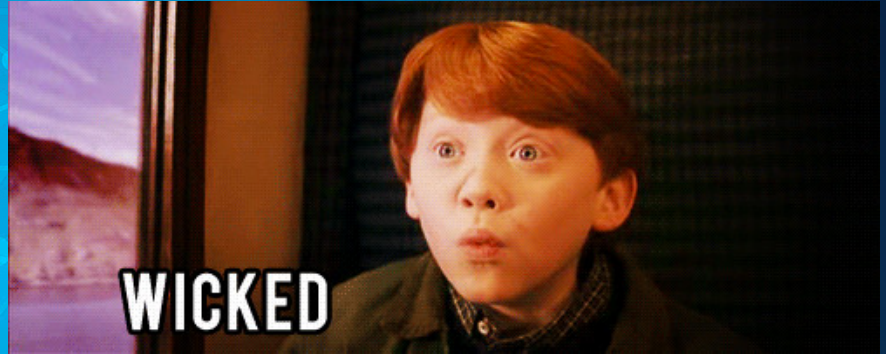
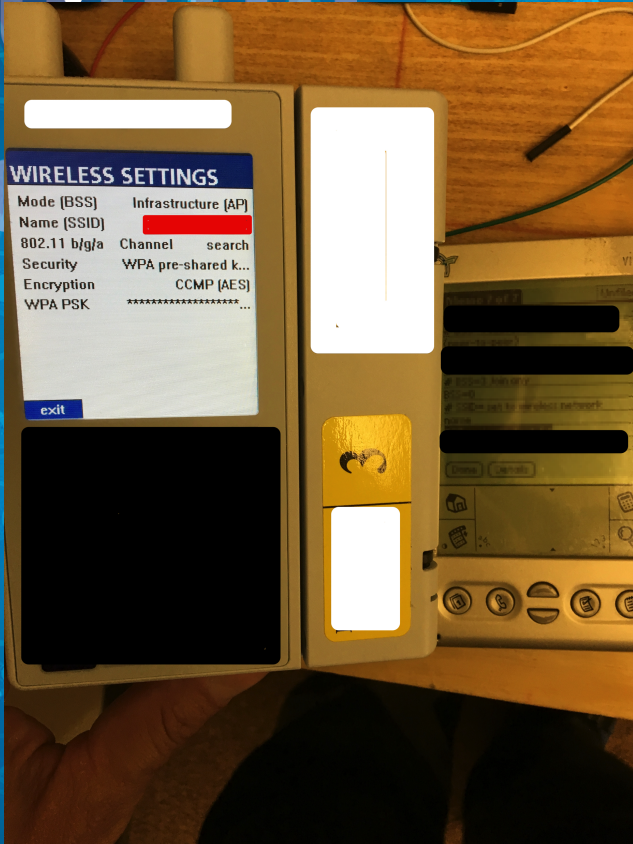
78 customer reviews

### 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 (\*\*\*\*PUMP\*\*)





# Time to Fuzz

- Communication with pump, both as client (tcp/11111) & server (tcp/22222)
- 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

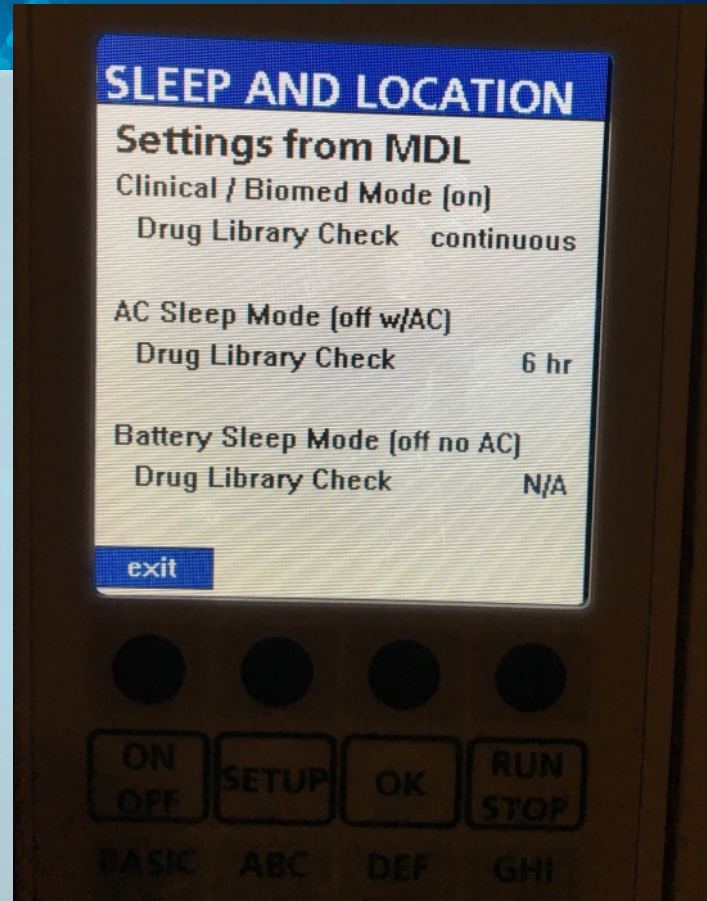






# Master Drug List

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



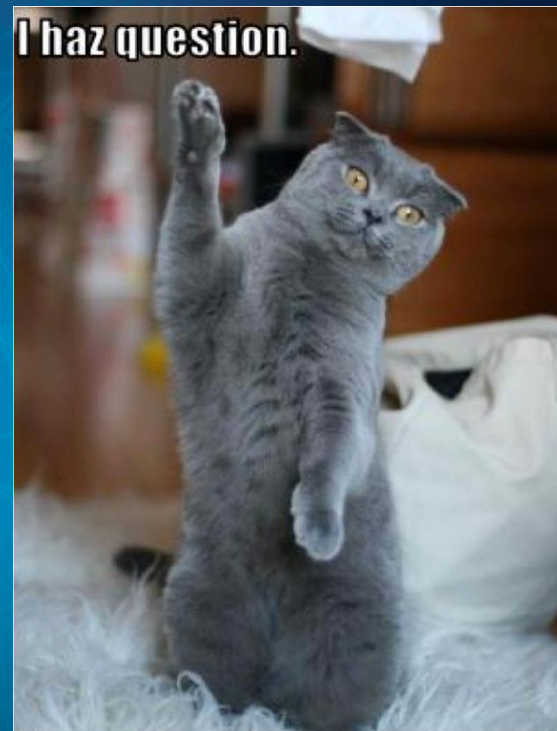
# Closing Remarks

- Built-in, not bolted on
- Trust no-one
- Better standards and regulations
- Beyond standards and regulations
- Learn from past mistakes
- Security Assessments



# Thank You

- Questions Anyone???
- Contact Info:
  - LinkedIn:  
<https://www.linkedin.com/in/saurabhharit/>
  - Email: Saurabh.Harit@spirent.com /  
SecurityLabs@spirent.com
  - Twitter: Oxsauby





# References

- Google Image Cache
- <https://www.cognizant.com/whitepapers/how-the-internet-of-things-is-transforming-medical-devices-codex1945.pdf>