

ThermoFisher
S C I E N T I F I C

Anatomy of a Hack

Jay Radcliffe, Director, Product Security Testing & Research

Twitter: @jradcliffe02

E-Mail: jay.radcliffe@thermofisher.com

Who Am I

- Jay Radcliffe
 - Undergrad: Criminal Justice/Pre-Law
 - Masters Degree: SANS Technology Institute
 - 20 years experience working in computer security
- Type I Diabetic
 - Published research in 2011 and 2016 on security weaknesses in Insulin Pumps



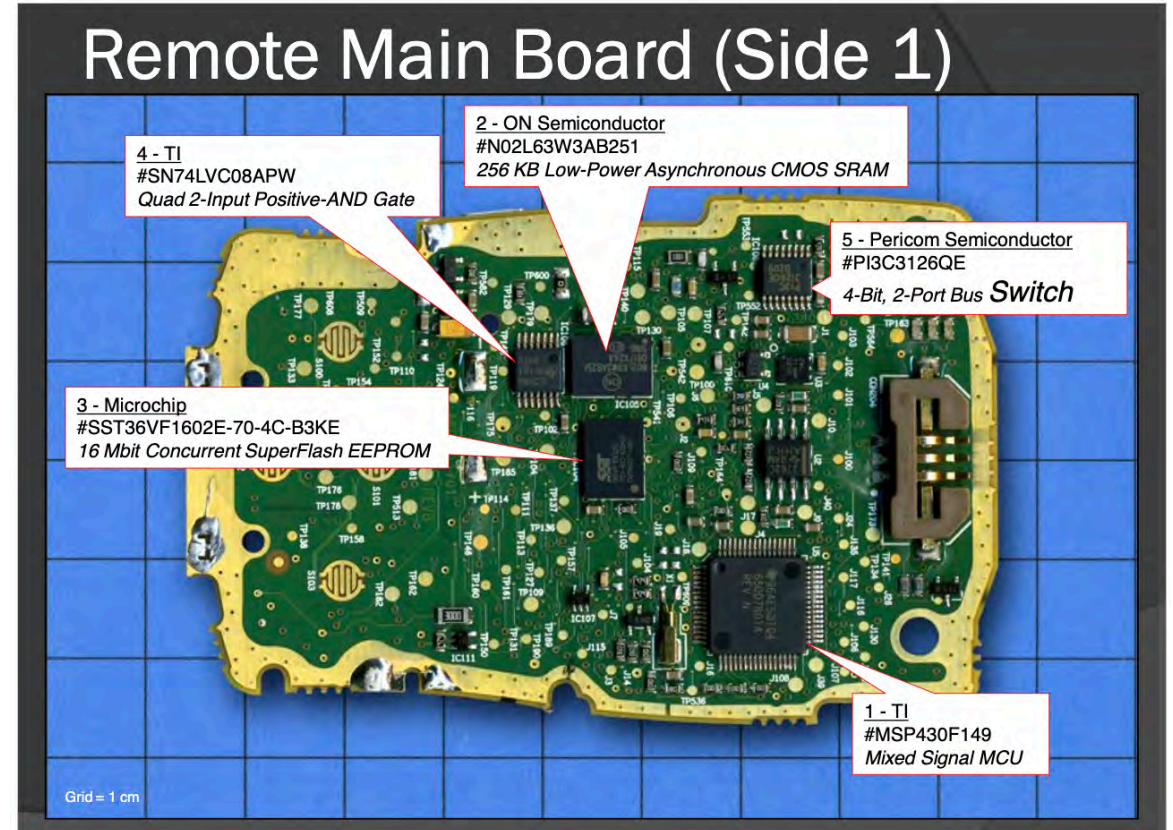
Step One: Information Gathering

- Crucial First Step in the process
- User Guides
- Patent Documents
- Pictures and Images
- Secondary Market Availability



Examples

- Animas Insulin Pump
 - Secondary Market: \$100
 - Google: Device Teardown
 - Multiple Patents on Communication Protocol



Look for Obvious Entry Points

- Network Communication Ports
 - Tools like nmap and massscan show what ports are open and communicating
 - Telnet (25), SSH (22), HTTP (80)
 - Shows Overall Attack Surface
- Trying obvious username/password
 - Sadly, this works too often
 - Admin/admin
 - Root/root



- Tools like nmap can tell you about the service(s)
 - What version of Apache/IIS is running
 - What Operating System is running
- Updates? Ha. Usually not.
- Example: URGENT/11
 - VxWorks easily ID'd from scanners
 - Can determine if vulnerable

```
31337
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    opn   smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Default Passwords

- California Law SB-327
 - Can't sell devices with a hardcoded default password
 - Has to be changed at first use OR be unique to the device
 - January 1st 2020
- Something that hackers are always looking at
- How are you storing your passwords?
 - Use strong hashing (bcrypt, SHA-512)



Patching and Long Term Support

- Patching is hard
 - Try and get into a regular cadence
 - Quarterly? Annually?
- Windows 7
 - EOL in 2020
- Android
 - Short support life
- Long Term Platforms
 - Windows 10 IoT
 - Ubuntu Core
 - Linux Zephyr



What the Future Holds

- Bluetooth
 - Low cost
 - Increased "default" security
- More Patient Questions
 - Patients are smarter
 - Cell Phone connectivity
- Legal
 - We'll see more laws like SB-327



Conclusion

- Focus on Basic Security Hygiene
 - Passwords
 - Patching/Updates
- Don't get cute
 - Changing what port number telnet runs on won't help
 - Same with Banners and Headers
- Be aware of what information is available
 - Google is your friend too





Thank You

Jay.Radcliffe@thermofisher.com

Twitter: @jradcliffe02