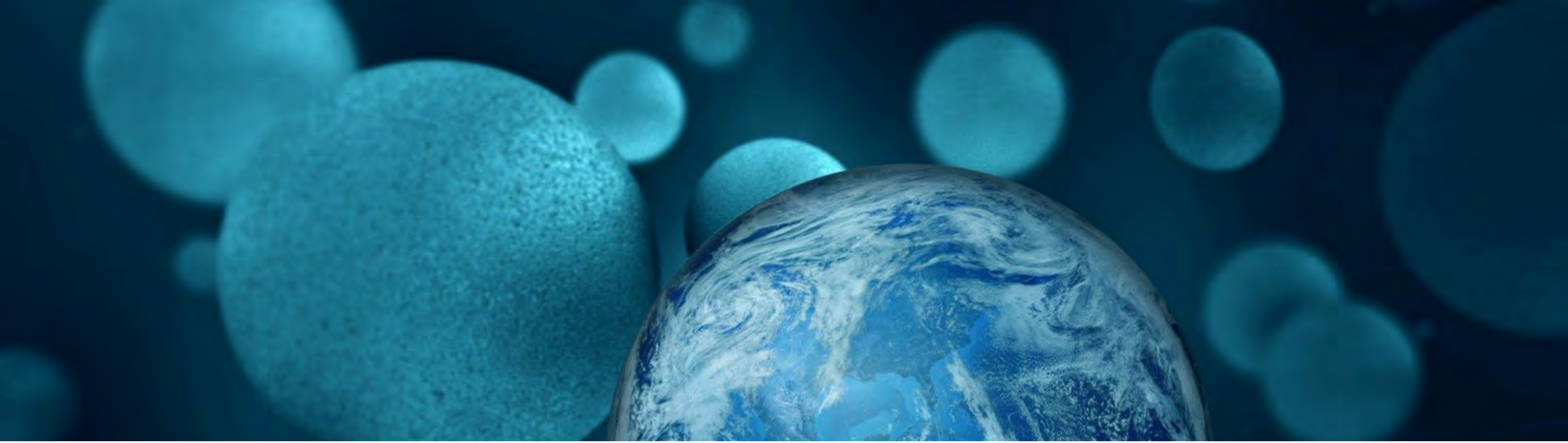


ThermoFisher SCIENTIFIC

Anatomy of a Hack

Jay Radcliffe, Director, Product Security Testing & Research
Twitter: @jradcliffe02
E-Mail: jay.radcliffe@thermofisher.com

Who Am I

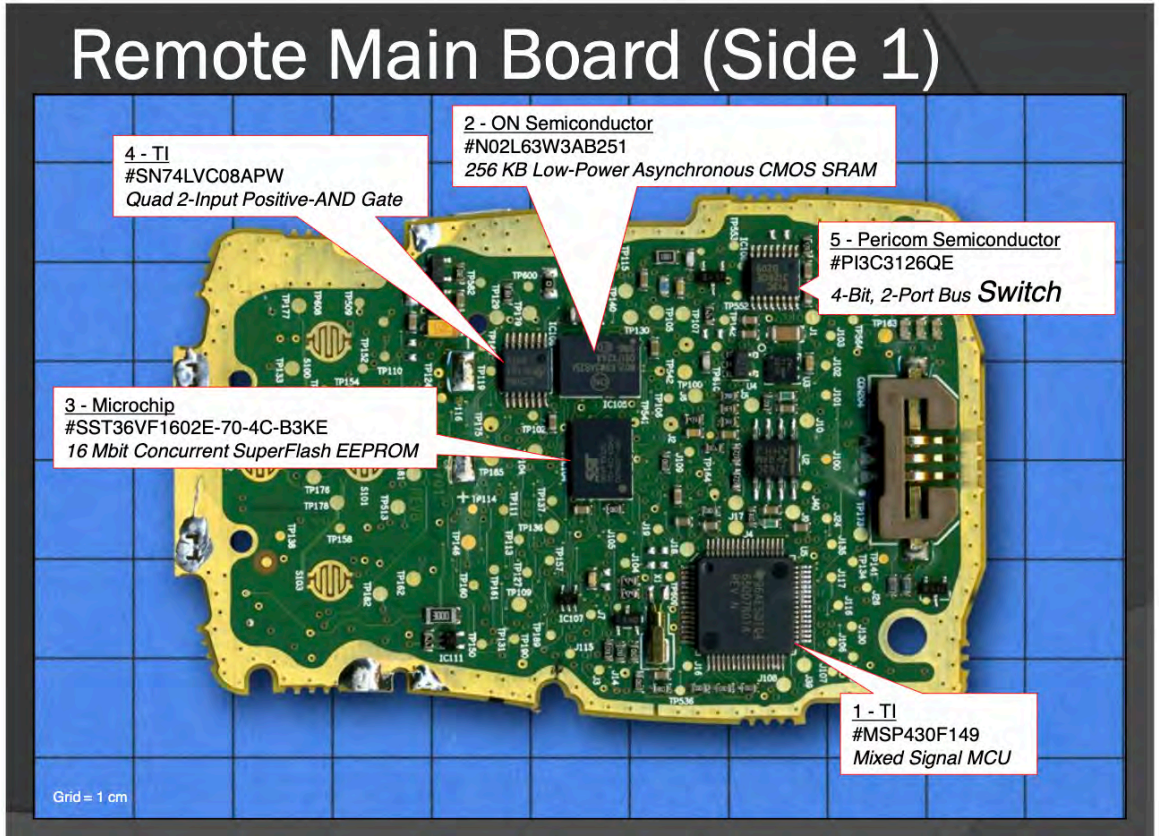
- Jay Radcliffe
  - Undergrad: Criminal Justice/Pre-Law
  - Masters Degree: SANS Technology Institute
  - 20 years experience working in computer security
- Type I Diabetic
  - Published research in 2011 and 2016 on security weaknesses in Insulin Pumps

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

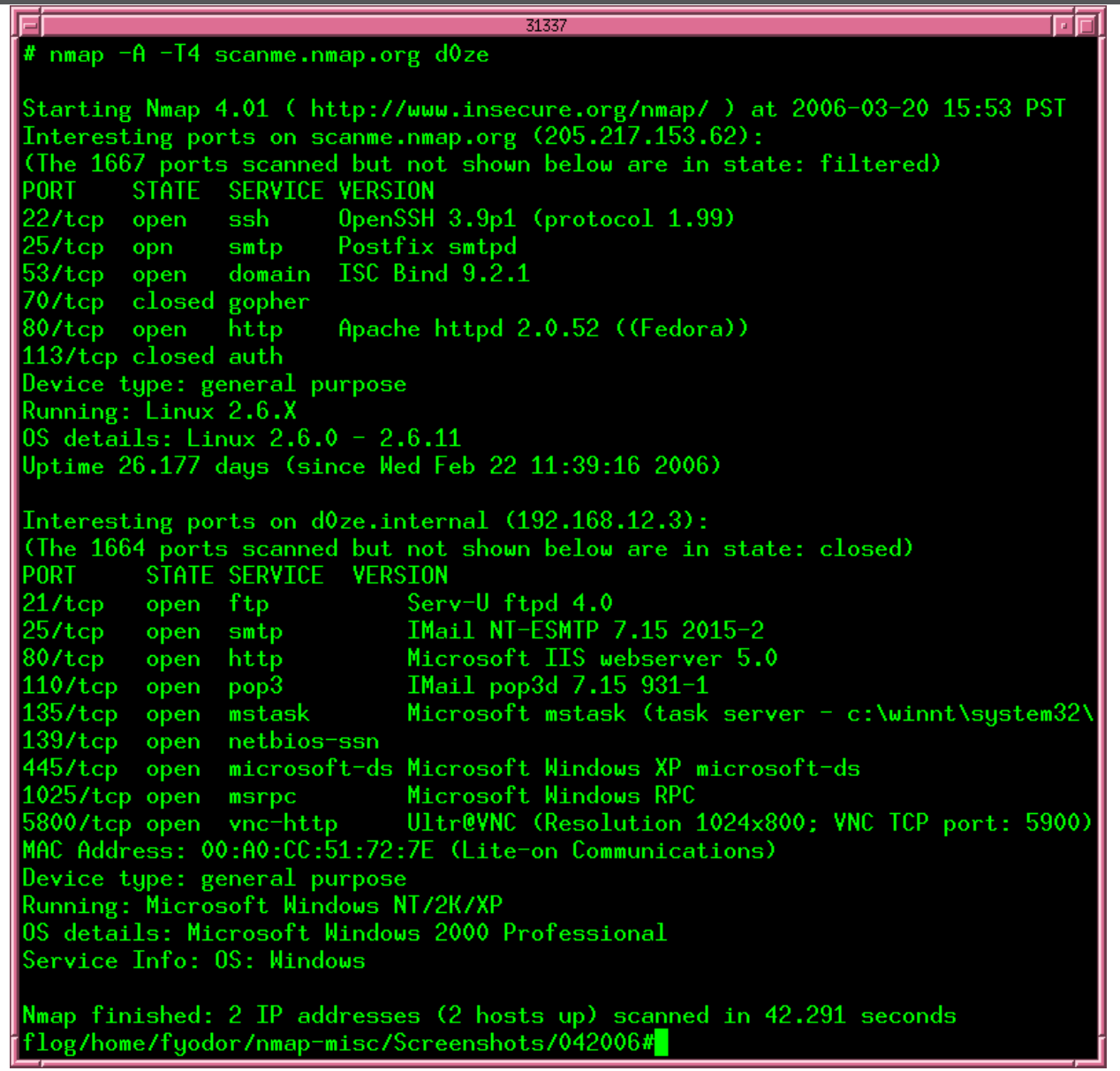


Look for Obvious Entry Points

- 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

Information to Research

- 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



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

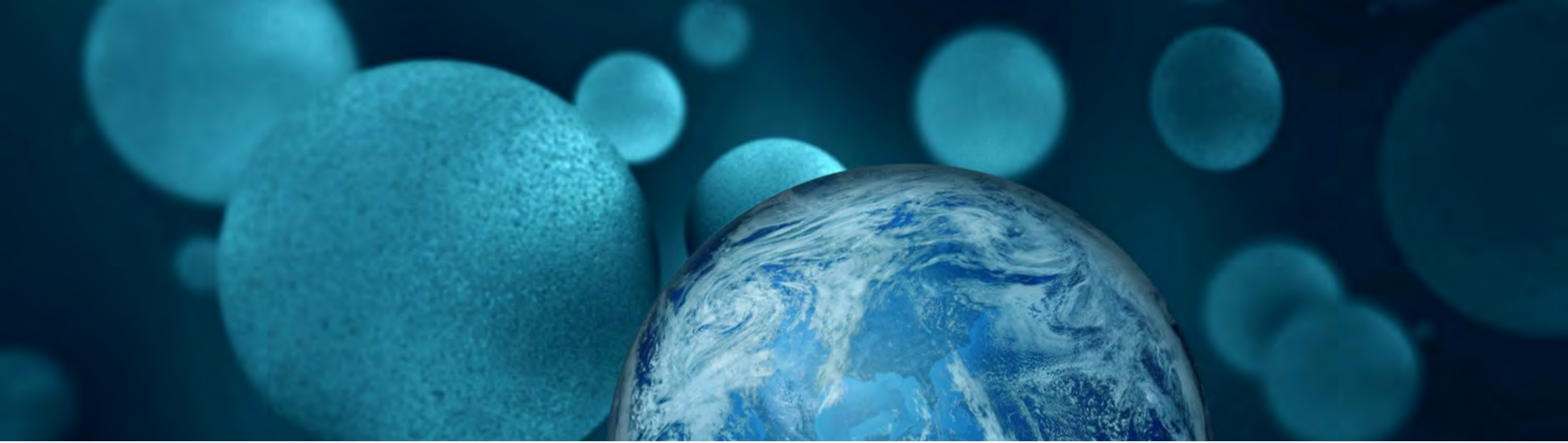
- Patching is hard
  - Try and get into a regular cadence
  - Quarterly? Annually?
- Windows 7
  - EOL in 2020
- Android
  - Short support life
- Long Term Platforms
  - Windows 10 IoT
  - Ubuntu Core
  - Linux Zephyr

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