MEDICAL DEVICE CYBERSECURITY

SETH D CARMODY PHD

CYBER SECURITY SUMMIT 2017
OCTOBER 23, 2017
Executive Orders (EO), Presidential Policy Directives, and Framework to Strengthen Critical Infrastructure Cybersecurity

- EO 13636 (Feb 2013) → NIST Voluntary Framework (Feb 2014) v1.1 in Draft Jan. 10, 2017
- PPD 21 (Feb 2013)
- EO 13691 (Feb 2015) – establishment of Information Sharing and Analysis Organizations (ISAO)
- EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” May 17, 2017
Informational Tech/Operational Tech

Operational Technology

IoT – Internet of Things

Internet-Connected Operational Technology

FDA’s Regulatory Scope

Center for Food Safety & Applied Nutrition
Center for Drug Evaluation & Research
Center for Biologics Evaluation & Research
Center for Tobacco Products
Center for Devices & Radiological Health (CDRH)
Center for Veterinary Medicine
National Center for Toxicological Research
Move over, Mirai

The attacks are a variation on those mounted by Mirai, a botnet made up of network cameras, digital video recorders, and other so-called Internet-of-things devices. The point of Mirai is to build an army of devices that

cripple prominent websites

with

record-setting distributed DoS attacks. The motivation for the PDoS attacks remains unclear, in part because BrickerBot.2 attacked a much wider variety of storage devices—including those used by servers—rather than storage used only by more limited IoT devices.
Intended Use + Misuse


Negative Requirements are *Infinite*!

**Features:**
What a Device MUST Do...
Get drug libraries from the Internet

**Safety:**
What a Device MUST NOT do

Thou, shall not under or over deliver therapy!
Postmarket Cybersecurity Risk Assessment

Severity of Patient Harm (if exploited)

Negligible  Minor  Serious  Critical  Catastrophic

Exploitability

High

Medium

Low

Uncontrolled Risk

Controlled Risk
Device Lifecycle: Ecosystem Challenges

[Diagram showing the lifecycle of medical devices with stages such as Premarket Decision, Postmarket Surveillance, Medical Device Manufacturers, Development, Procurement, Deployment, Operations and Maintenance, Disposal, and Health Delivery Organizations.]

www.fda.gov
Empathy and Collaboration

From EO 13636

“We can achieve these goals through a collaborative approach to improve cybersecurity information sharing and develop and implement risk-based standards.”
FDA’s Approach to Cybersecurity

- Executive Orders
- FDA Safety Communication
- Draft Premarket Guidance
- Begin Coordination with DHS
- Recognize Standards
- Establish Incident Response Team

2005: Issued guidance
2008: Halpern, et.al.
2009: Issued safety communication
2011: “Hacking” of implantable insulin pump (Radcliffe)
2012: First recall of vulnerable software (Roche - PC Anywhere)
2013: Recall of TNS-listener (Roche)
Questions?

Contacts:

CDRH mailbox, 
AskMedCyberWorkshop@fda.hhs.gov
Suzanne Schwartz, Suzanne.Schwartz@fda.hhs.gov
Aftin Ross, aftin.ross@fda.hhs.gov
Seth Carmody, seth.carmody@fda.hhs.gov