MEDICAL DEVICE CYBERSECURITY

SETH D CARMODY PHD

CYBER SECURITY SUMMIT 2017

OCTOBER 23, 2017

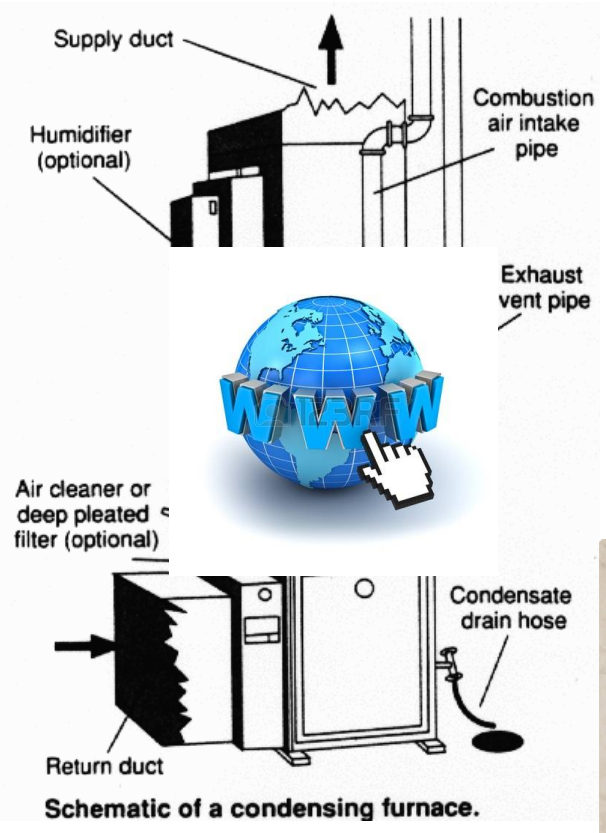
Executive Orders (EO), Presidential Policy Directives, and Framework to Strengthen Critical Infrastructure Cybersecurity

- 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

FDA

Operational Technology



Schematic of a condensing furnace.

Information Technology

IoT – Internet of Things

Internet-Connected Operational Technology

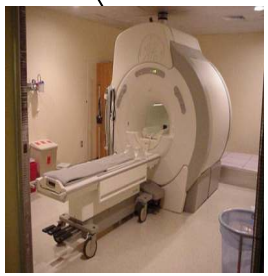
FDA's Regulatory Scope

Center for Food Safety & Applied Nutrition

Center for Drug Evaluation & Research

Center for Biologics Evaluation & Research

Center for Tobacco Products

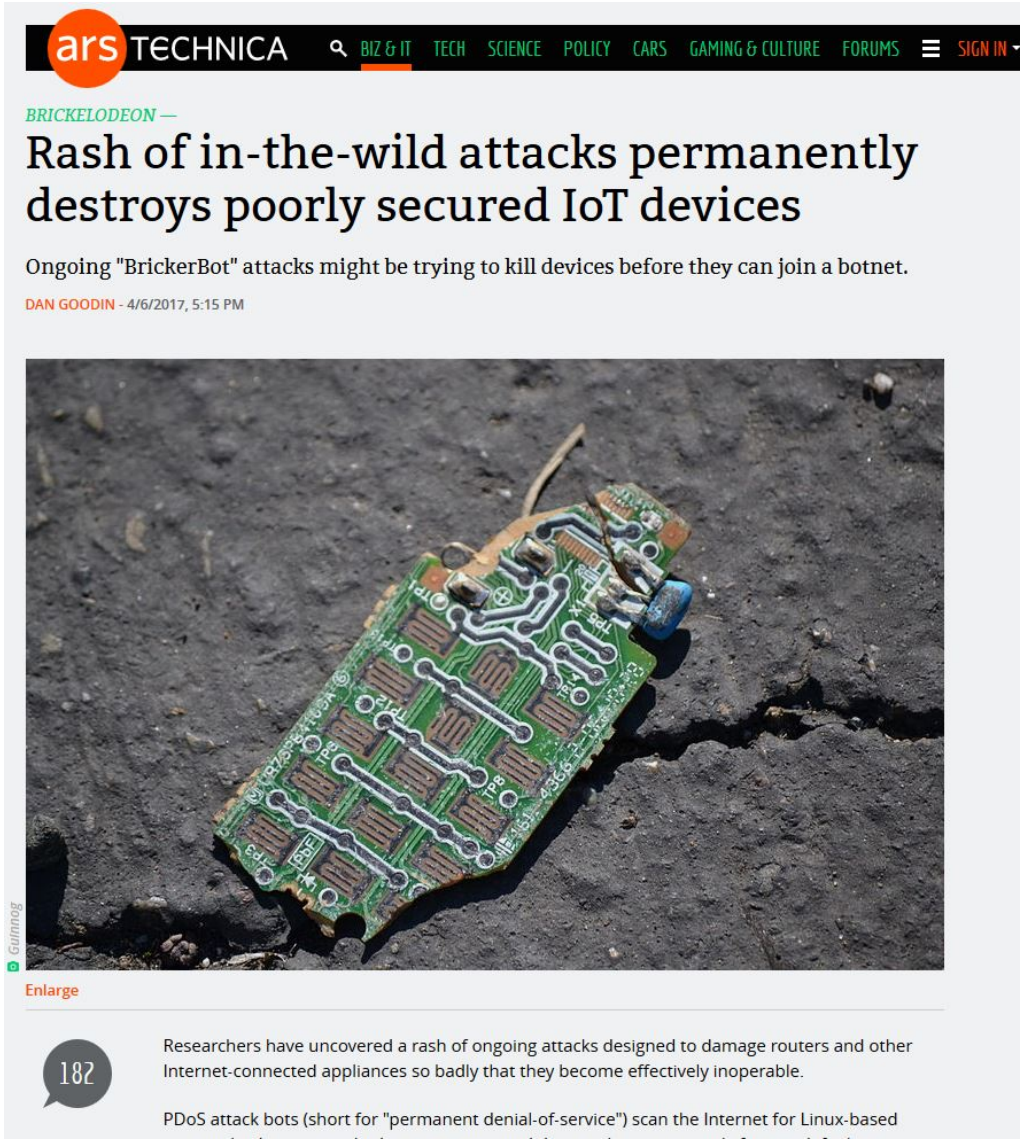


Center for Devices & Radiological Health (CDRH)

Center for Veterinary Medicine

National Center for Toxicological Research

The Active Adversary, A Fine Wine



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS SIGN IN

BRICKELODEON —

Rash of in-the-wild attacks permanently destroys poorly secured IoT devices

Ongoing "BrickerBot" attacks might be trying to kill devices before they can join a botnet.

DAN GOODIN - 4/6/2017, 5:15 PM

Enlarge

182

Researchers have uncovered a rash of ongoing attacks designed to damage routers and other Internet-connected appliances so badly that they become effectively inoperable.

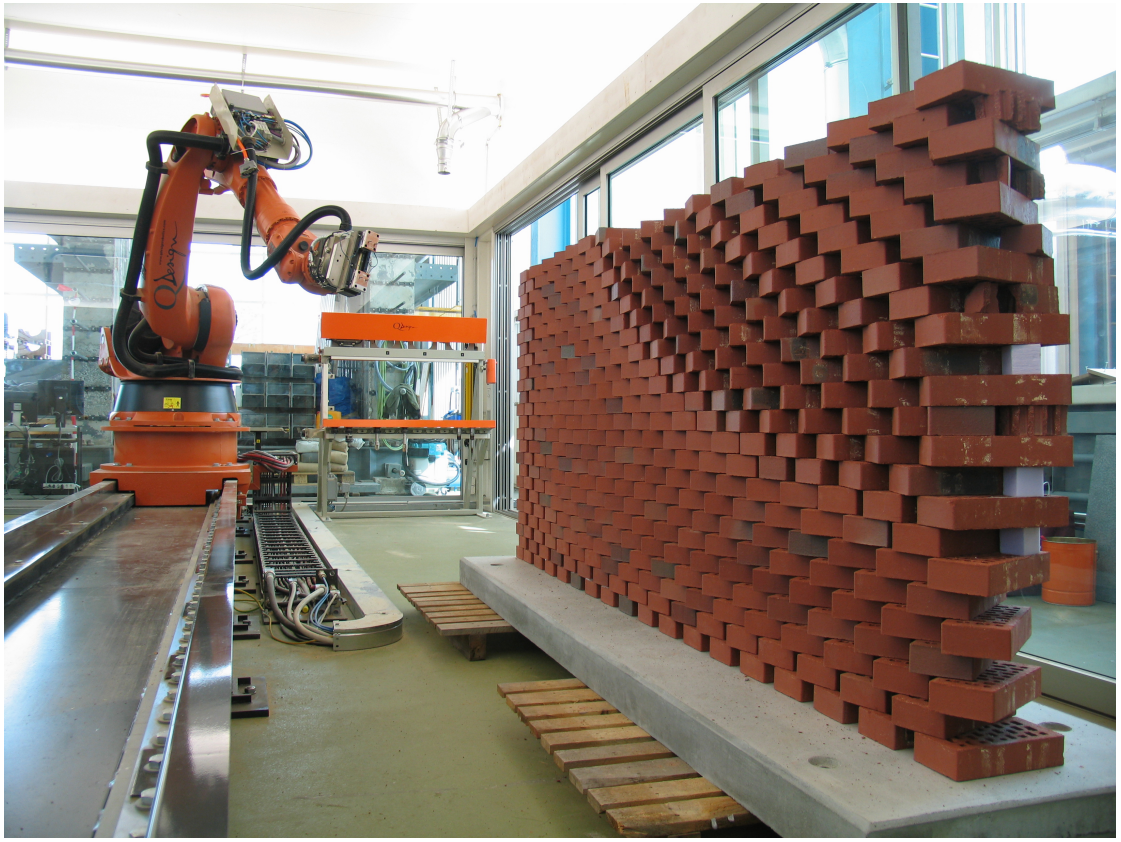
PDoS attack bots (short for "permanent denial-of-service") scan the Internet for Linux-based

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

Intended Use + Misuse

http://hackaday.com/2015/09/07/brick-laying-robot-does-it-better/

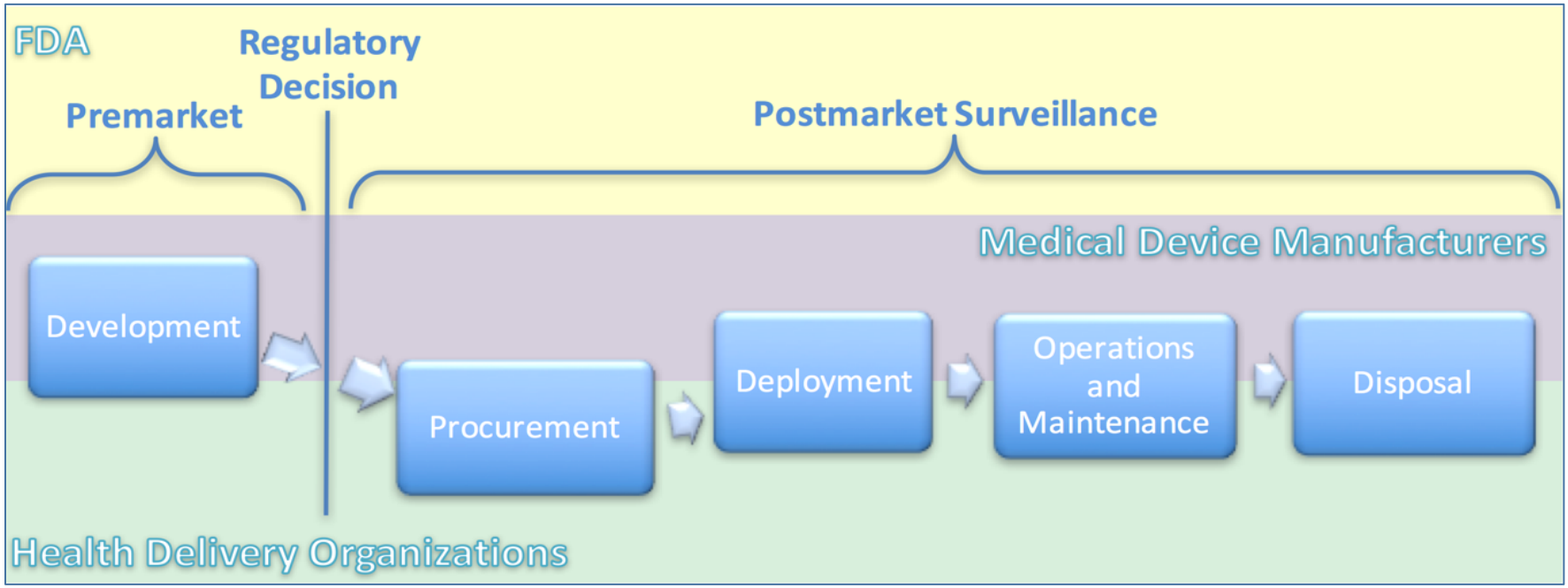


http://www.technologyvista.in/pin/here-comes-the-brick-laying-robot-to-make-buildings/

Negative Requirements are *Infinite*!

Postmarket Cybersecurity Risk Assessment

Device Lifecycle: Ecosystem Challenges

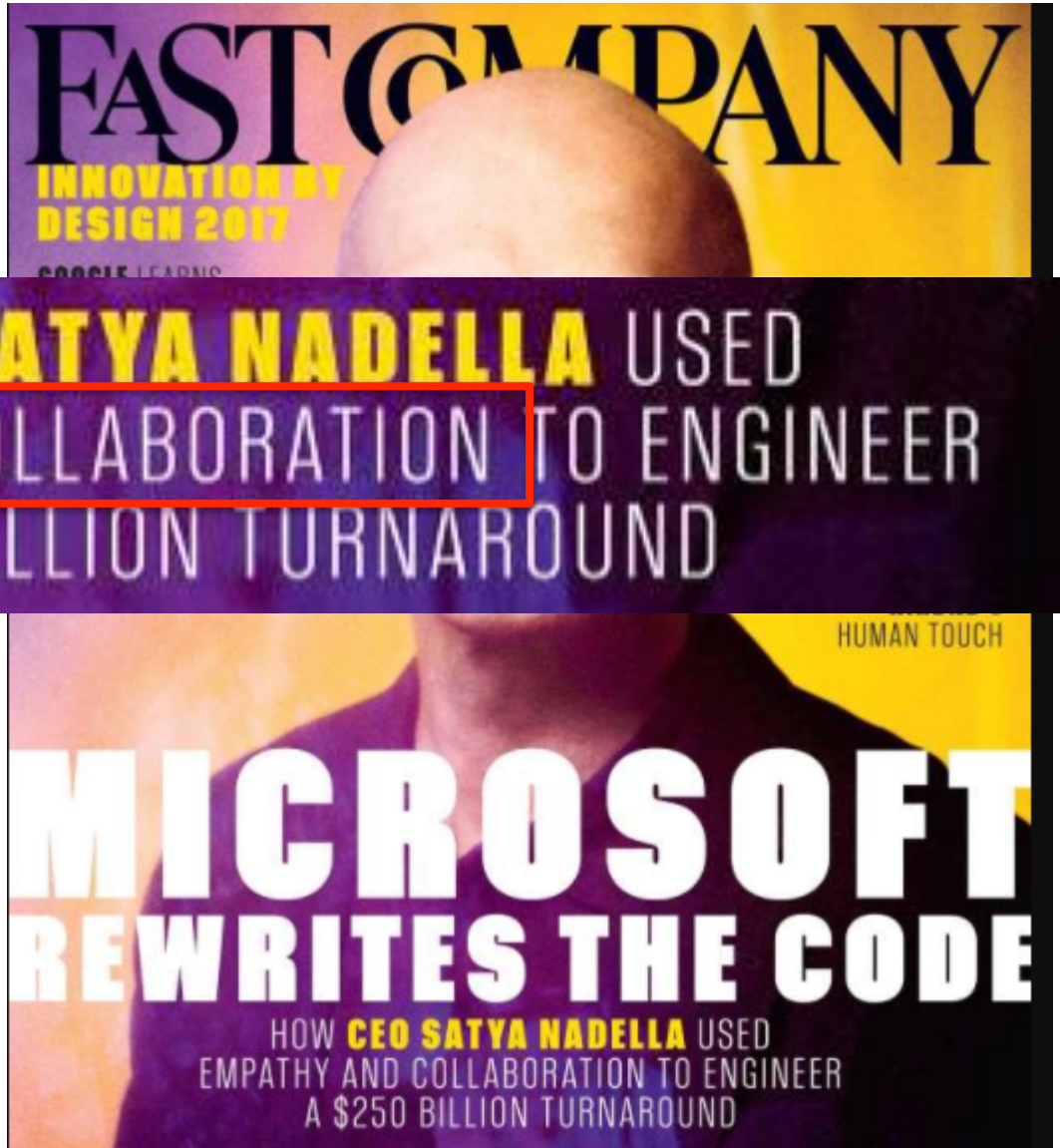


Empathy and Collaboration

From EO 13636

"We can achieve

improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."



FDA's Approach to Cybersecurity

2013

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

2014

Final Premarket Guidance
MOU with NH-ISAC
Public Workshop

2015

Product-Specific Safety Comm
Build Ecosystem/Collaboration

2016

Draft and Final Postmarket Guidance
Public Workshop
MOU with NH-ISAC/MDISS

2017

Product-Specific Safety Comm
1st Cybersecurity WL

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