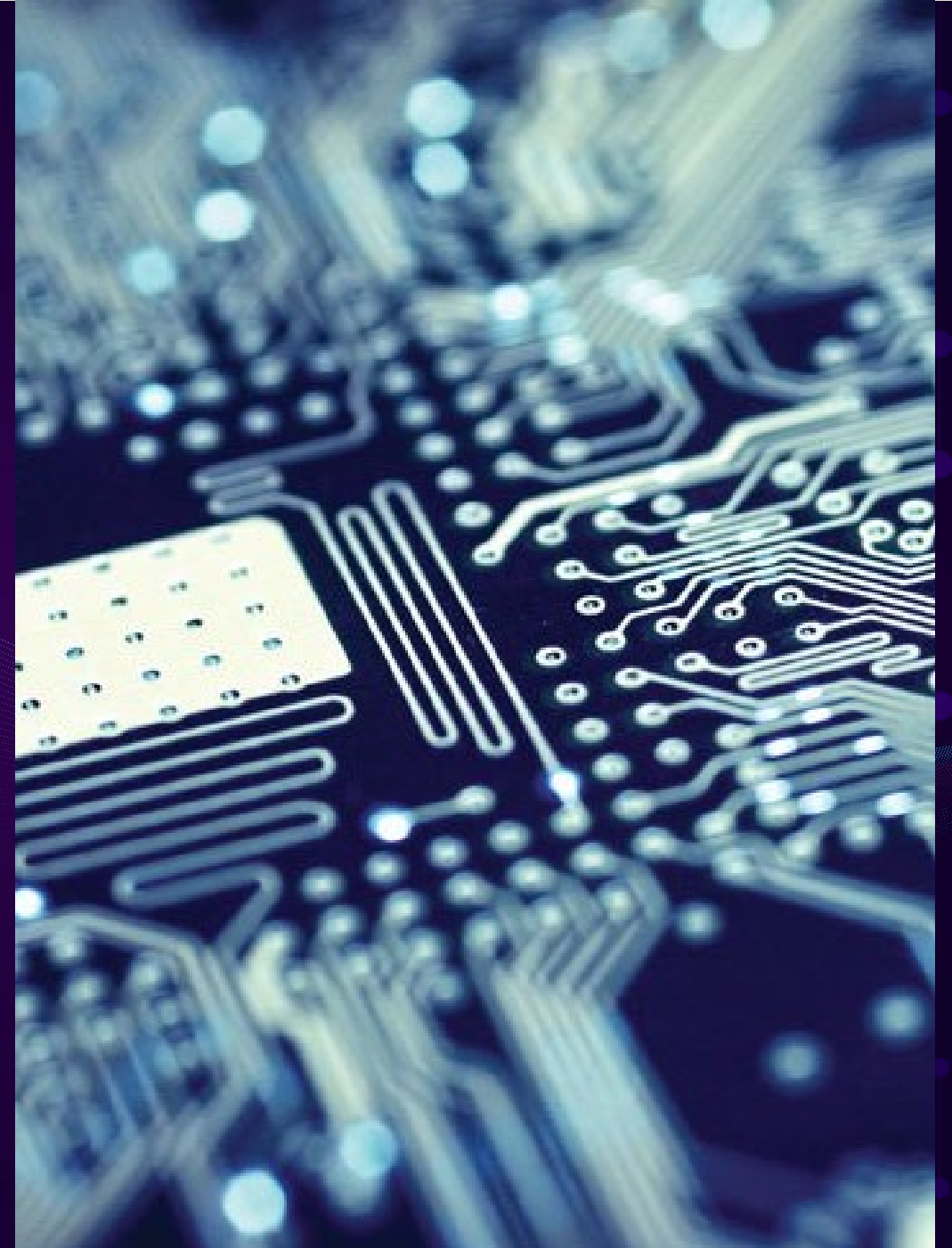


Security Challenges After Integration – Panel discussion

Dr. Kevin Fu
Ms. Cheri Caddy
Mr. Jason Williams
Dr. Lok Yan - Moderator



The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Distribution Statement A – Approved for public release. Distribution unlimited.

<https://www.nationaldefensemagazine.org/articles/2017/10/31/trusted-microelectronics-a-critical-defense-need>

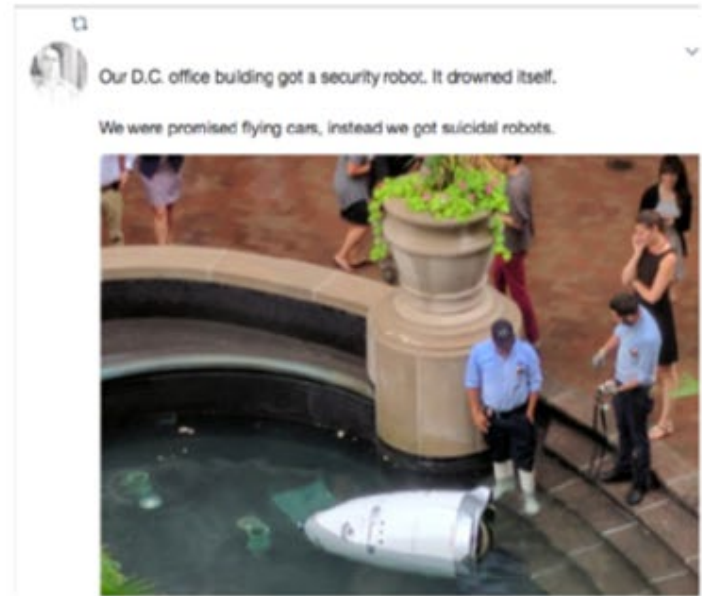
Security Challenges After Integration

Dr. Kevin Fu
Professor of Electrical and Computer Engineering,
Computer Sciences, and Bioengineering,
Northeastern University and KRI Kostas Research
Institute for Homeland Security

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

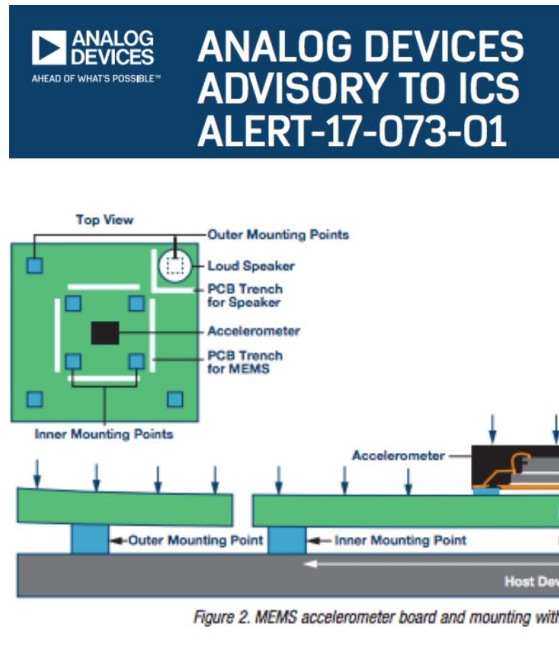
Sensors are everywhere



Wicked Bizarre Physics of Sensor Security • k.fu@northeastern.edu • [spqrlab1.github.io](https://github.com/spqrlab1)

Computers have always been vulnerable to analog cybersecurity threats

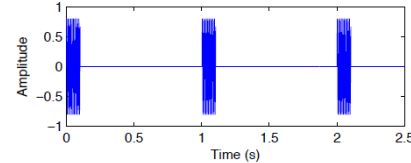
2017



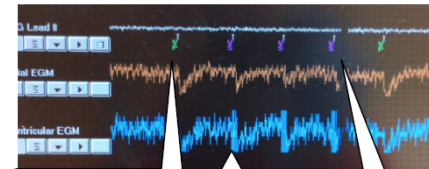
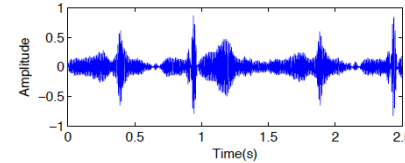
Results: Waveforms & Responses

2013

Pulsed sinusoid



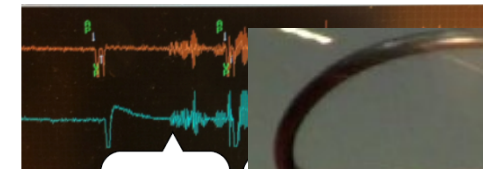
Modulated heart beat



Ventricular
pace

Signal
onset

Ventricular
sense



Signal
onset

t al., IEEE S&P 2013]

2008



Wicked Bizarre Physics of Sensor Security • k.fu@northeastern.edu

Novel medical devices are growing



Source <https://www.shutterstock.com/image-vector/doctors-researchers-using-innovative-technologies-medicine-1624377460>

2,011
DEDICATED CDRHRS



238,000
REGULATED DEVICES



18,800
SUBMISSIONS RECEIVED



27,000
DEVICE MANUFACTURING FIRMS



57
GUIDANCES/REVISIONS



<https://www.fda.gov/media/164837/download>

Medical device security guidance

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on October 2, 2014.
The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-0100 or Office of Communication, Outreach and Development (OCOD) at 1-800-635-4700 or 202-462-7000.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of Cyber Security and Radiological Health
Center for Biologics Evaluation and Research

2014


Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.
The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Human Factors, Center for Devices and Radiological Health, Food and Drug Administration, 1390 New Hampshire Ave., RM 3B, Silver Spring, MD 20910-0001, or 301-796-0177. For questions regarding the document or related to device registration to FDA, contact the Office of Communication, Outreach and Development (OCOD) at 1-800-635-4700 or 202-462-8000 or ocd@fda.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Cyber Director
Center for Biologics Evaluation and Research

2016

Contains Nonbinding Recommendations

Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on April 8, 2022.

You should submit comments and suggestions regarding this draft document within 90 days of publication in the Federal Register at the notice announcing the availability of the draft guidance. Submit electronic comments to <https://www.fda.gov/oc>. Submit written comments to the Drafts Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (01 A-1061), Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the Federal Register.

For questions about this document regarding CDRL regulated devices, Suzanne Schwartz, Office of Strategic Partnerships and Technology Innovations at (301) 796-0977 or email CyberMed@fda.hhs.gov. For questions about this document regarding CDRH regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-635-4700 or 240-462-8000, or by email at ocod@fda.gov.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

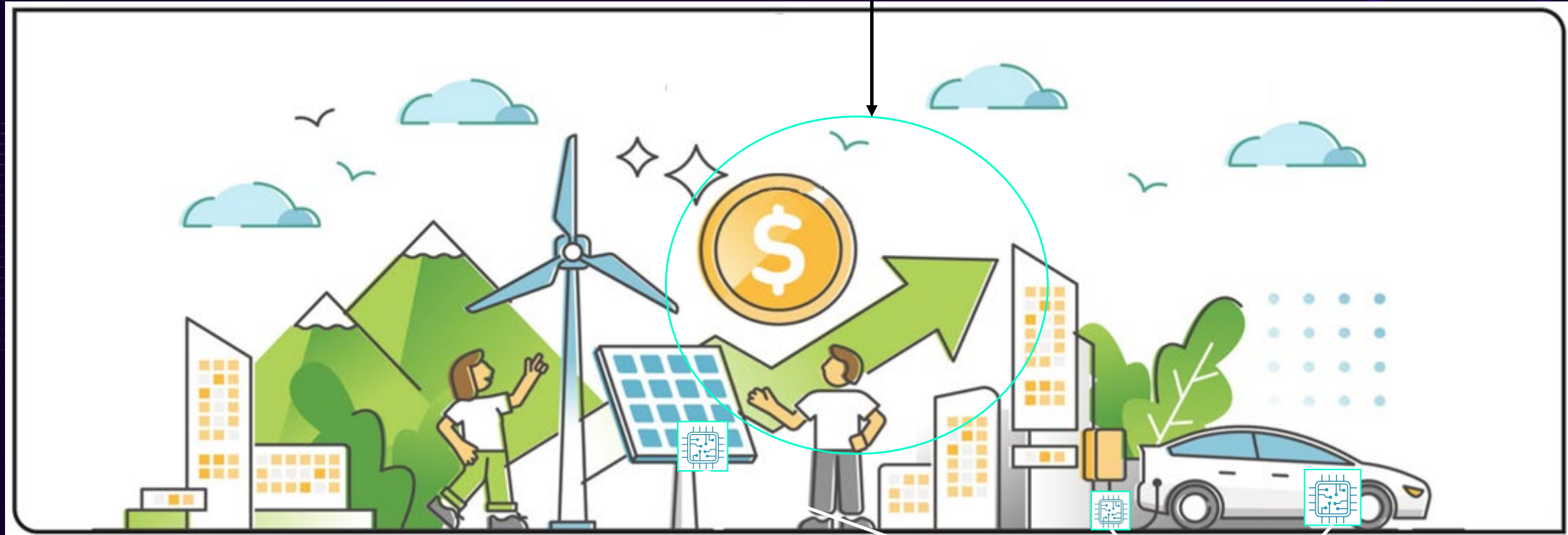
2022

Security Challenges After Integration

Ms. Cheri Caddy
Deputy Assistant National Cyber Director, Office of
the National Cyber Director (ONCD)

\$3.5T once-in-generation public investment

Inflation Reduction Act



Bipartisan Infrastructure Law

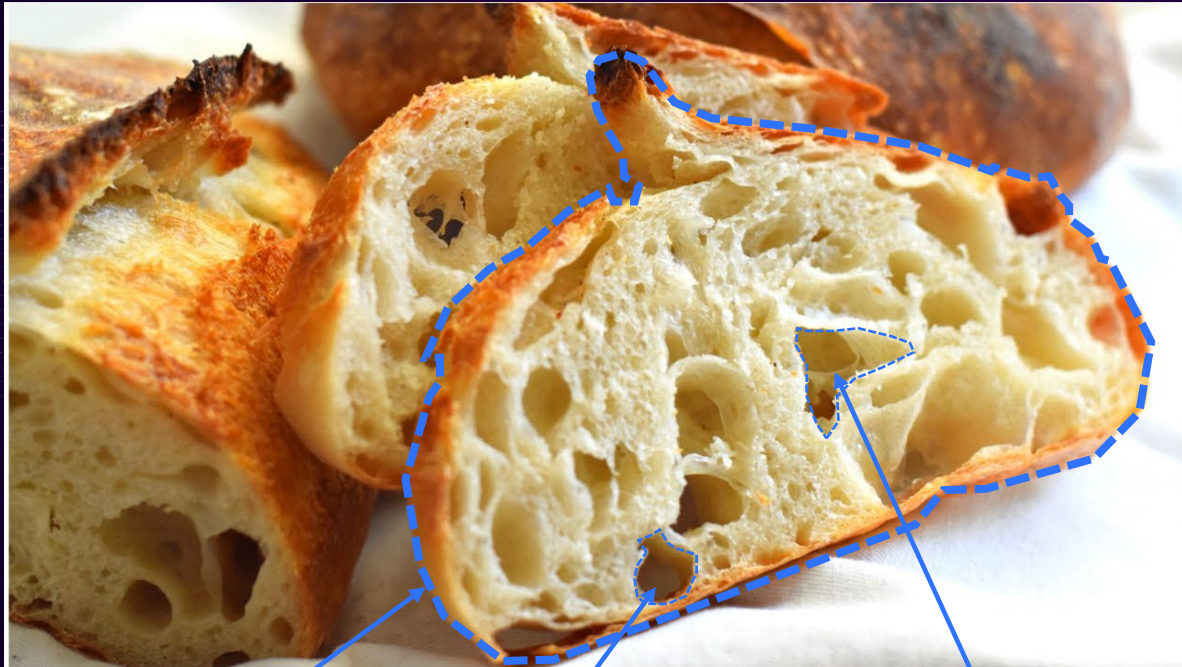
Source: <https://read.nhbr.com/nh-business-review/2022/08/26/#?article=4013034>

CHIPS and Science Act

Office of the National Cyber Director's perspective

Baked-in Security

Partnerships



Security-by-design

Hardware bill of materials

Software bill of materials

- Standards and requirements
 - 2022 National Cyber-Informed Engineering Strategy
 - 2023 National Cybersecurity Strategy
- Incentives (grants, funding, etc.)

Example focus area: Securing the Clean Energy Transition



Security Challenges After Integration

Mr. Jason Wilson
Co-Founder and Chief Executive Officer,
Cromulence, LLC

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Background



<https://www.darpa.mil/program/cyber-grand-challenge>

Designer vs. security perspectives



Well protected front door



Easily broken window



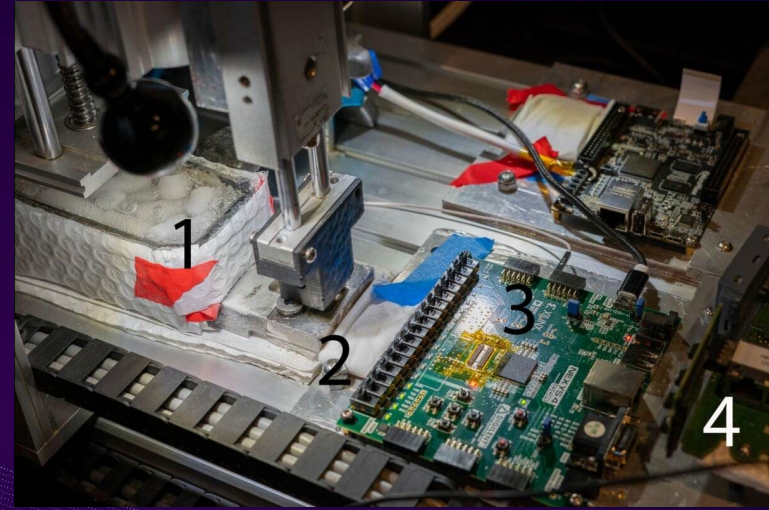
You will open door for us

Attackers, ever resourceful



Cold boot attack
2008

Old is still new?



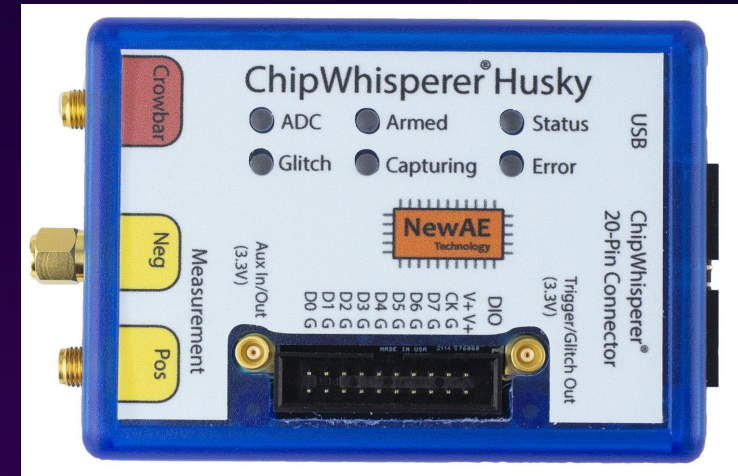
Cold boot attack
2022 (with robots)

Commoditization of attacks

\$100



\$549



\$35



\$300

