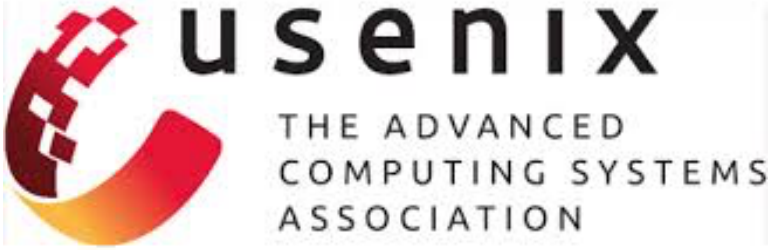


Hacking Health

Professor Avi Rubin

Computer Science

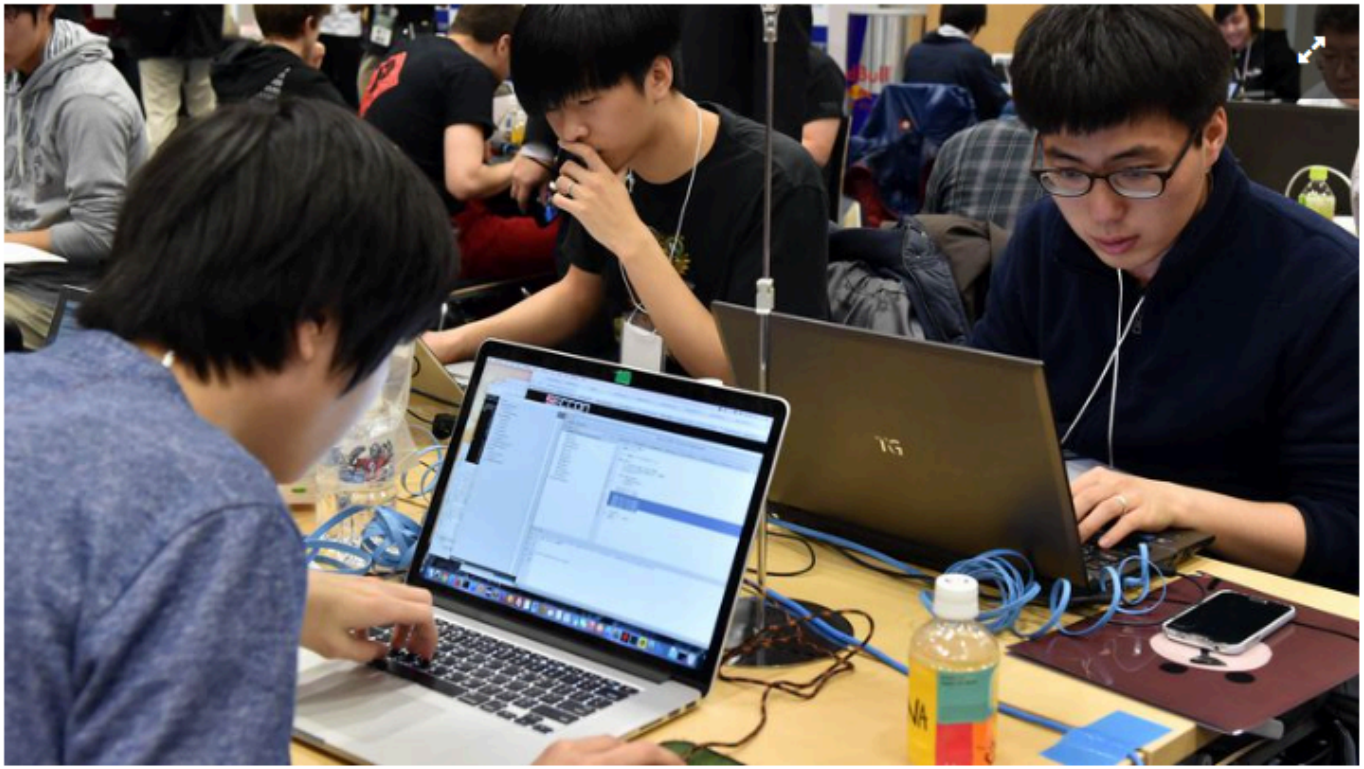
Johns Hopkins University

ENIGMA

China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF
October 26, 2015

VOL 51 ISSUE 43
News · Technology · World · China



My first security evaluation, 2003

- Rental receipt with printed CC #
- Easy access to consumer data
- Poor data security practices
- Weak authentication, if any

Founded security evaluation company

Getting to know Health IT Security

- In 2009, transitioned from e-voting security
  - To healthcare IT security

- Began with IT-focused tours of several hospitals
  - Radiology, Pathology, Children's hospital, etc.
  - About 6 visits

  - Security situation was abysmal
    - 8,000 hospital employees 100% access
    - Nurse w/ "special task"
    - Home VPN as bridge
    - Desktop EHR access

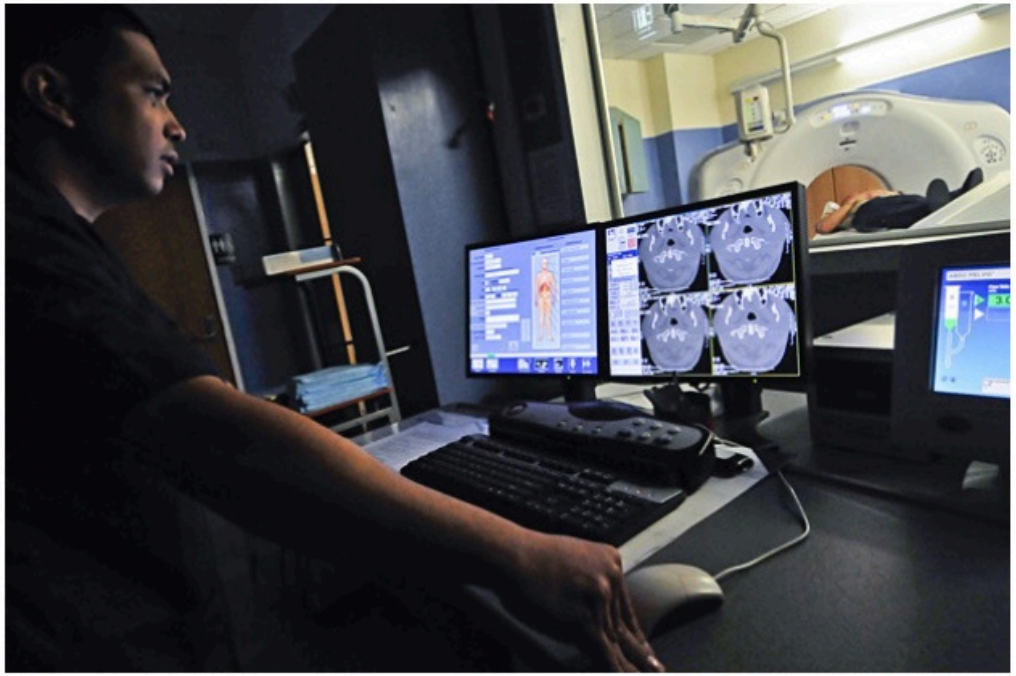
Example: X-rays

Old way:

New way:

NEWS

Attackers targeting medical devices to bypass hospital security



Credit: U.S. Navy

Other important devices remain neglected on the hospital's network

CSO | Jun 4, 2015 3:49 AM PT

- Blood Gas Analyzers (BGA) compromised
- PACS system compromised

NEWS

Cyberattacks will compromise 1-in-3 healthcare records next year

Credit: Shutterstock

MORE LIKE THIS

Hospital tests lag time robotic surgery 1,200 r away from doctor

Penn Medicine's big da system triggers early d of life-threatening...

Intel to pilot cloud tecl for sharing personalize treatment

on IDG Answers

How to turn on Windows 10's 'Find M Device' feature?

Healthcare is Unique

- The players:
  - Doctors
    - (God complex; don't like new ways of doing things)
  - Patients
    - (often not tech savvy; don't follow instructions)
    - Includes all of us
  - Nurses & other Clinical staff
  - Regulators: Congress, FDA
    - (well meaning; may not understand implications)
  - Insurance companies
  - Medical device manufacturers
  - Entrepreneurs
    - Mobile, Wearables,
    - Internet of Things

Healthcare applications

- Connectivity
  - Modern devices, always connected, always on
  - Databases always online
- Mobile/cloud
  - Data in multiple places
  - Data owner not in possession of data
- Expectation that data is always available

Key point: most interaction with health data controlled by **SOFTWARE**

Controlled by software

- Radiation dosage
- Dosage of medication
- Stocking of supplies in ICU
- Shift schedule for Doctors & Nurses
- EHRs
- Drug dispensing robot
- Communications of devices

Threat model:

Anything controlled by software is potentially exploitable.

Hackers Can Wirelessly Upload Malware to a Fitbit in 10 Seconds

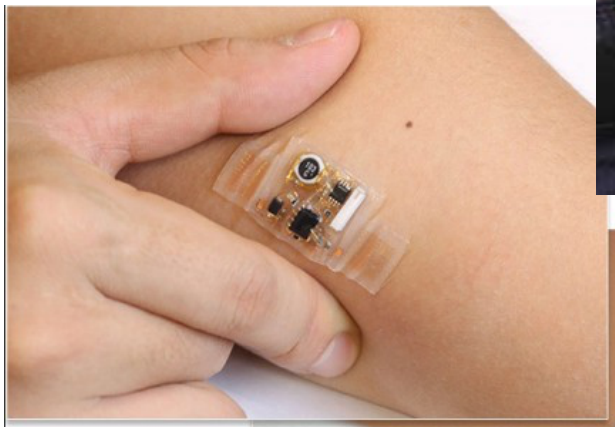
Adam Clark Estes
Filed to: SECURITY 10/21/15 5:05pm

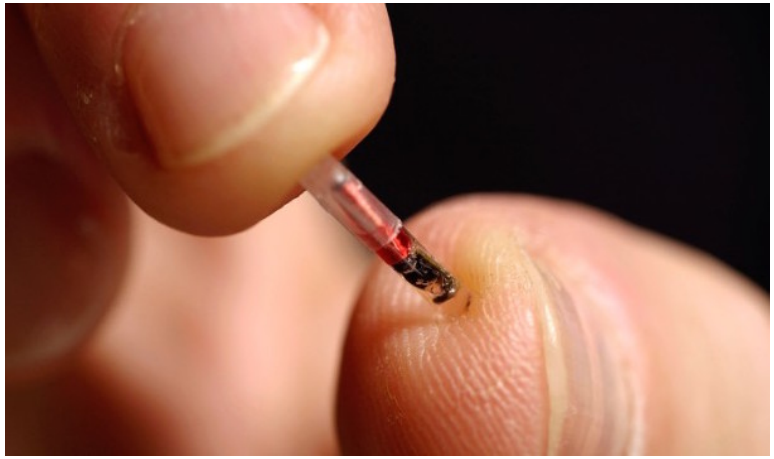
1

Wearables are like hacker candy. They represent a new category of technology that's capable of storing data—including malware—that people don't expect to get pwned. But that's exactly what just happened: Hackers figured out how to remotely upload malware to a Fitbit. It only takes ten seconds.


Blood Pressure
Blood Pressure reminder
SYS
121
mmHg
DIA
78
mmHg
HEART RATE
62
BPM
The measure is within the normal range.
Notes


MiniMed 508
sel
act





Biggest bang for the buck

1. Application whitelisting on medical devices
2. Hygiene for backend systems
3. Database Activity Monitoring – anomalous queries
4. Multifactor authentication for remote access
5. Virtualization for access to clinical data
6. Universal encryption of data
7. Terms of agreement with cloud service providers
8. Automated support for security in chart accesses
9. Privacy for self-identify data (e.g. genome sequences)
   - HIPAA safeguards inadequate
10. Authentication for clinical personnel

Final Thoughts

- Healthcare Sector has unique security challenges due to:
  - regulatory environment
  - Stakeholders
  - Dependence on software
  - Availability requirements for data
  - Affects us all personally!
  - Trend towards cloud/mobile

- Need to consider security implications of new technologies, e.g. network-connected infusion pumps

Speaker information

Professor Avi Rubin
Dept. of Computer Science
Johns Hopkins University
Email: rubin@jhu.edu
Web: avirubin.com
: @avirubin