Medical Device Cybersecurity

CY 7790 / CY 4973
Spring 2026
https://spqrlab1.github.io/medcybersecurity/
Thursday, January 8, 2026

Instructors:
Axel Wirth (primary)
Kevin Fu

TA:
Jiancong Cui

Today’s Learning Goal

- Course overview
- Re-introduction to security

About Kevin Fu

- Professor,
  Khoury College of Computer Sciences,
  Electrical and Computer Engineering,
  Bioengineering, Northeastern University
- Director, Archimedes Center for Healthcare and Medical Device Cybersecurity
- Former Acting Director, FDA Medical Device Security
- PhD in EECS, MIT
- Research
  - Medical device cybersecurity
  - Analog sensor security

Fu(n) facts

- ➡ Teaching security since 2001
- ➡ Former PC Chair, USENIX Security
- ➡ Certificate in artisanal bread making
- ➡ Due to disabilities, rely more on audio
- ➡ Teach mini courses in craft cocktail making, French pastries, Italian wood-fired pizza, and French cooking

About Axel Wirth

Passionate about Medical Device Cybersecurity

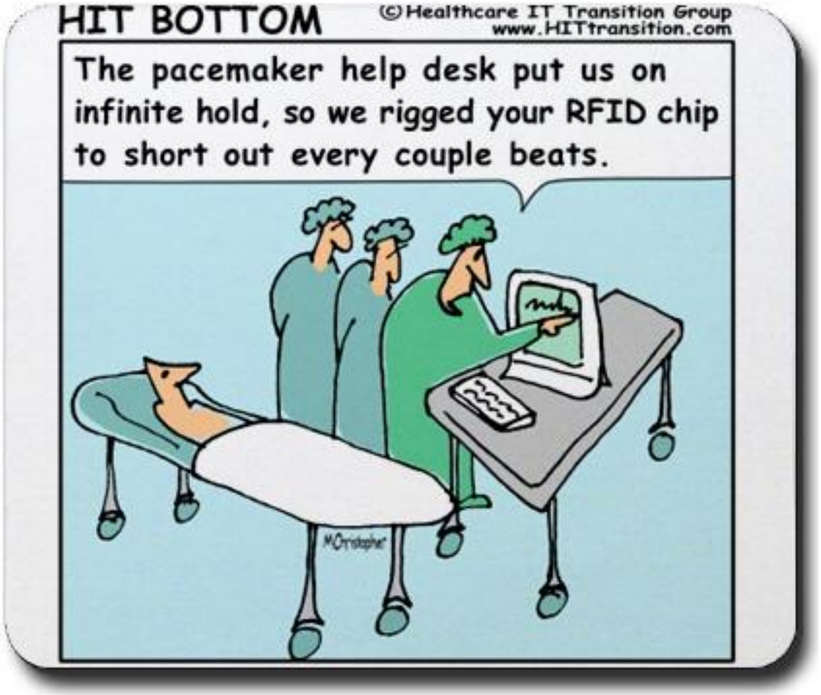
- BSEE / MSEM
- Author and speaker on the topic
- Adjunct Professor UConn – teaching Medical Device Cybersecurity for Clinical Engineers
- Worked in a variety of standards and industry organizations
- Recognized as Fellow by AAMI, HIMSS, and ACCE

Introduce Yourselves (2-minute exercise)

- What is your name?
- Why are you interested in medical device cybersecurity?
- How do you approach learning complicated subject materials?
- How do you like to use ChatGPT?

Course Topics

- Technical Proficiency: Apply security assessment techniques such as threat modeling, fuzz testing, software bill of materials (SBOM) generation and ingestion, and resilience testing to medical devices.
- Regulatory Knowledge: Understand and navigate regulatory affairs for medical device security, including U.S. FDA and international standards.
- Incident Management Skills: Engage in a simulated cybersecurity recall, working directly with FDA reviewers and device industry professionals.
- Ethics: Explore the ethical and privacy implications of cybersecurity in healthcare, especially concerning patient safety.
- Experiential Learning: Gain firsthand insights through hospital site visits, operating room observations, and interviews with medical device manufacturers and FDA regulators.
- Term Project Collaboration: Work in interdisciplinary teams to mirror real-world scenarios, balancing technical, legal, and regulatory considerations for a term paper on medical device cybersecurity.
- Technical Communication: In-class essay writing exercises combined with at-home editing will provide opportunities for students to learn how to convey complicated cybersecurity arguments with cogent and well organized prose to prepare them for skills needed in the workplace when reporting to future supervisors, as well as preparing students for future leadership roles in conveying technical subjects to hospitals, regulators, laypersons and the public.



Goals of Course

- ~~Be a hacker~~
- ~~Be a security expert~~

- Learn about a complex, interdisciplinary field mixing healthcare, medical device design, and cybersecurity
- Gain an appreciation for the culture of healthcare delivery
- Learn how to make technical and public policy arguments via essays
- Increase career opportunities in healthcare and medical device cybersecurity

Correctness is easy.

Security is hard.

Photo by Kevin Fu

Computer Security

- Computer Security (Informal Definition):

  Study of how to design systems that behave as intended in the presence of **determined, *malicious*** *third parties*

- Security is different from reliability
  - The malicious third party controls the **probability distribution** of malfunctions
  - Security researchers focus on understanding, modeling, anticipating, and defending against these malicious third parties

[This description drawn from the work of Prof. Yoshi Kohno with permission]

Monday Jan 18, 2015 in Australia

Royal Melbourne Hospital attacked by damaging computer virus

January 18, 2016

Julia Medew
Health Editor

THE AGE
Victoria

A virus has attacked the computer system of one of Melbourne's largest hospital networks, causing chaos for staff and patients who may face delays as a result.

Staff at Melbourne Health - the network which runs the Royal Melbourne Hospital - are urgently trying to repair damage to its IT system after a virus infected Windows XP computers.

An email sent to staff today said the virus had hit Melbourne Health's pathology department, causing staff to manually process specimens such as blood, tissue and urine samples instead of computers aiding the registration, testing and entry of results.

Wednesday Jan 20, 2015 in Texas

THE DAILY TRIBUNE

Virus hits TRMC computers

By MARCIA DAVIS Managing editor

TRMC CEO John Allen said the hospital experienced a network issue that was revealed about 7:30 p.m. Friday, Jan. 15.

TRMC public information officer Shannon Norfleet said a computer ransomware virus encrypted files on several of the TRMC database servers within the health system, which affects the TRMC access to the computer files.

Thursday Jan 21, 2015

Advisory (ICSA-15-337-02)

Hospira Multiple Products Buffer Overflow Vulnerability

Original release date: January 21, 2016

- Hospira manufactures networkable drug infusion pumps
- Remotely accessible buffer overflow via port 5000/TCP
- Difficulty: Low skill attacker

Friday Jan 22, 2015 in Michigan

Flint hospital confirms 'cyber attack,' Anonymous threatens action over water crisis

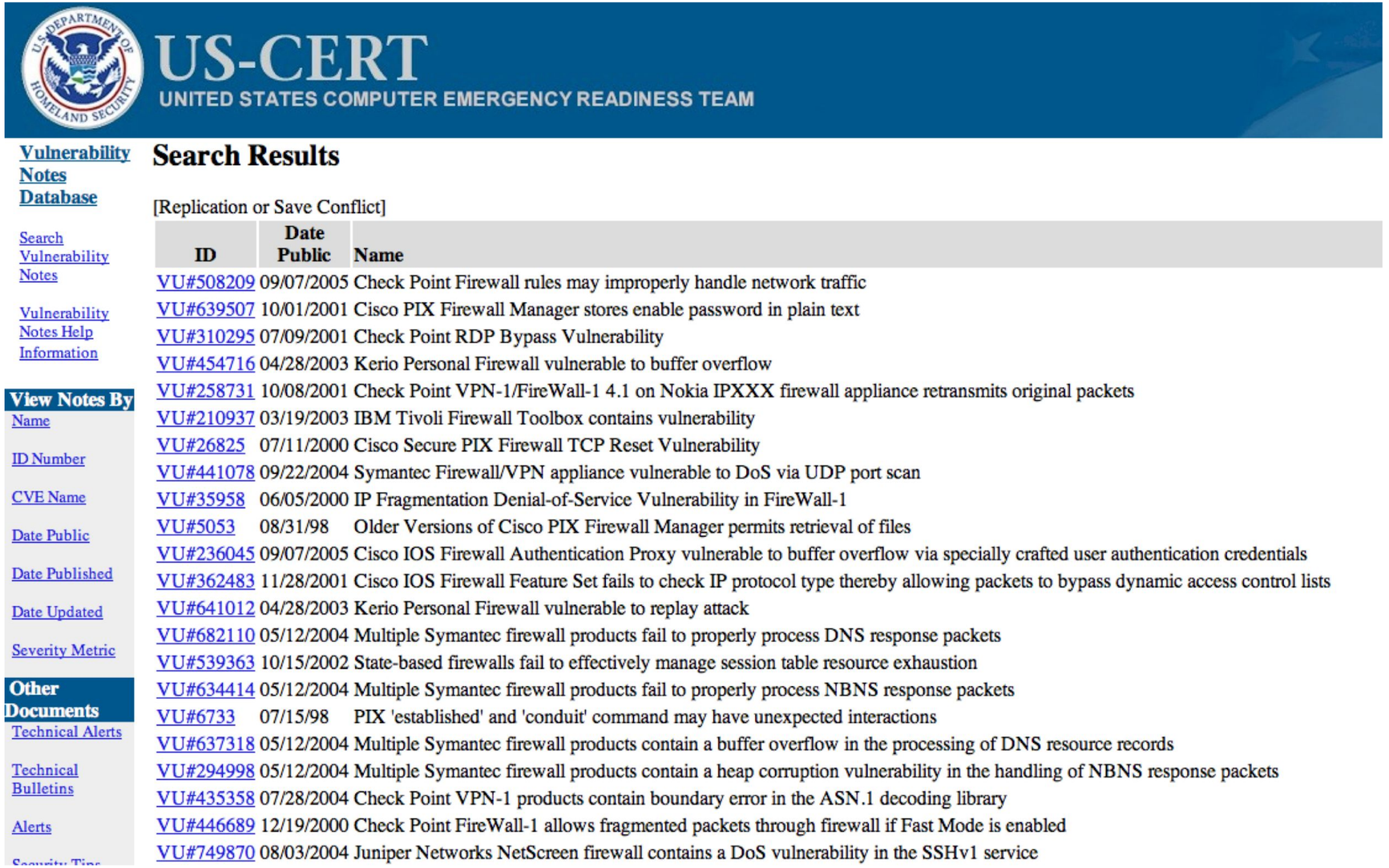
on January 21, 2016 at 9:43 PM, updated January 22, 2016 at 9:59 AM By Gary Ridley | gridley@mlive.com

FLINT, MI – Hurley Medical Center has confirmed it was the victim of a "cyber attack" a day after hacktivists threatened action over Flint's water crisis.

The hospital confirmed the attack Thursday, Jan. 21, but few details were released.

"Hurley Medical Center has IT systems in place, which aid in detecting a virus or cyber attack," hospital spokeswoman Ilene Cantor said. "As such, all policies and protocols were followed in relation to the most-recent cyber attack on our system. Patient care was not compromised and we are closely monitoring all systems to ensure IT security is consistently maintained."

Known Vulnerabilities in Firewalls



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By

Name

ID Number

CVE Name

Date Public

Date Published

Date Updated

Severity Metric

Other Documents

Technical Alerts

Technical Bulletins

Alerts

Security Tips

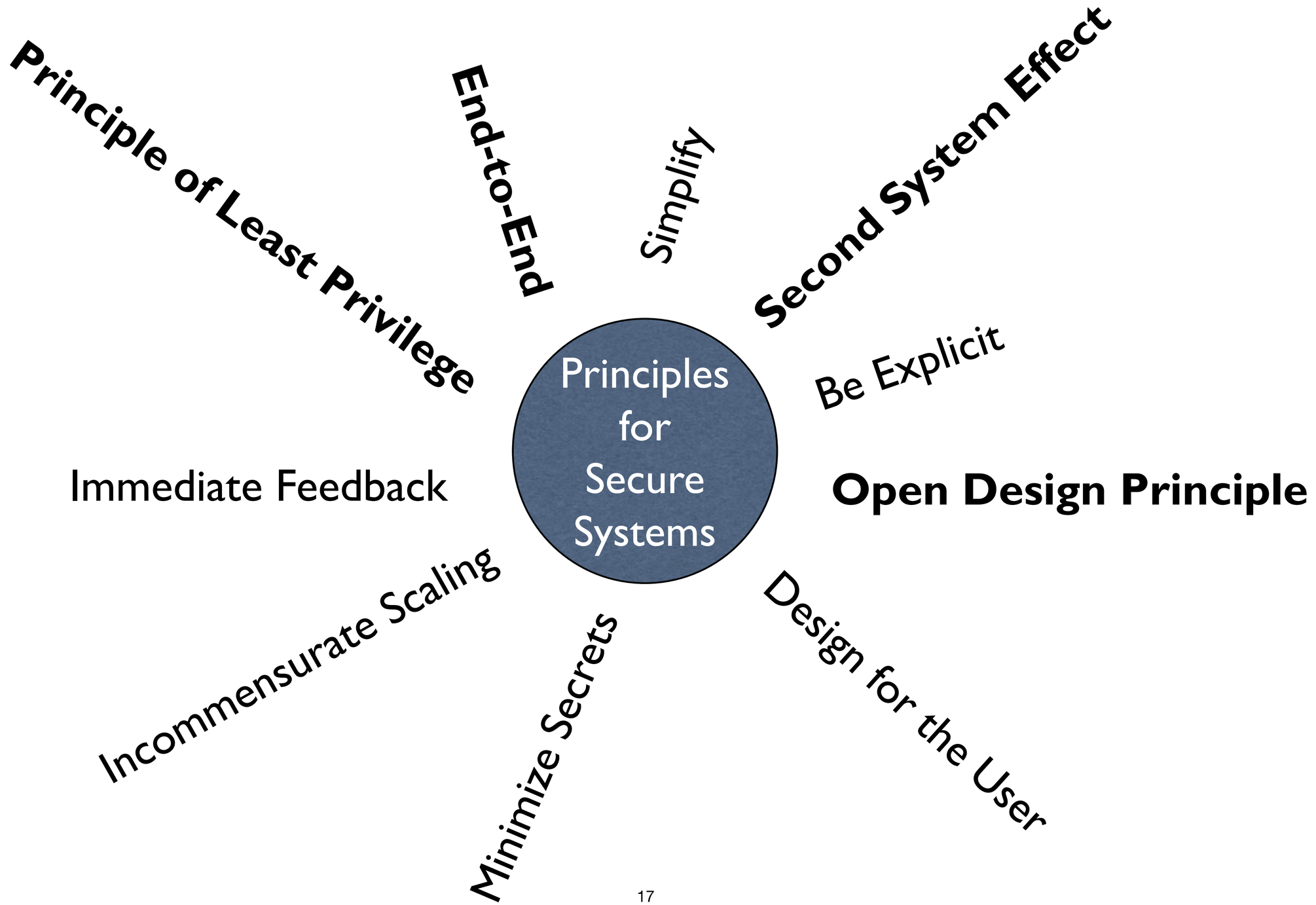
Search Results

[Replication or Save Conflict]

ID	Date Public	Name
VU#508209	09/07/2005	Check Point Firewall rules may improperly handle network traffic
VU#639507	10/01/2001	Cisco PIX Firewall Manager stores enable password in plain text
VU#310295	07/09/2001	Check Point RDP Bypass Vulnerability
VU#454716	04/28/2003	Kerio Personal Firewall vulnerable to buffer overflow
VU#258731	10/08/2001	Check Point VPN-1/FireWall-1 4.1 on Nokia IPXXX firewall appliance retransmits original packets
VU#210937	03/19/2003	IBM Tivoli Firewall Toolbox contains vulnerability
VU#26825	07/11/2000	Cisco Secure PIX Firewall TCP Reset Vulnerability
VU#441078	09/22/2004	Symantec Firewall/VPN appliance vulnerable to DoS via UDP port scan
VU#35958	06/05/2000	IP Fragmentation Denial-of-Service Vulnerability in FireWall-1
VU#5053	08/31/98	Older Versions of Cisco PIX Firewall Manager permits retrieval of files
VU#236045	09/07/2005	Cisco IOS Firewall Authentication Proxy vulnerable to buffer overflow via specially crafted user authentication credentials
VU#362483	11/28/2001	Cisco IOS Firewall Feature Set fails to check IP protocol type thereby allowing packets to bypass dynamic access control lists
VU#641012	04/28/2003	Kerio Personal Firewall vulnerable to replay attack
VU#682110	05/12/2004	Multiple Symantec firewall products fail to properly process DNS response packets
VU#539363	10/15/2002	State-based firewalls fail to effectively manage session table resource exhaustion
VU#634414	05/12/2004	Multiple Symantec firewall products fail to properly process NBNS response packets
VU#6733	07/15/98	PIX 'established' and 'conduit' command may have unexpected interactions
VU#637318	05/12/2004	Multiple Symantec firewall products contain a buffer overflow in the processing of DNS resource records
VU#294998	05/12/2004	Multiple Symantec firewall products contain a heap corruption vulnerability in the handling of NBNS response packets
VU#435358	07/28/2004	Check Point VPN-1 products contain boundary error in the ASN.1 decoding library
VU#446689	12/19/2000	Check Point FireWall-1 allows fragmented packets through firewall if Fast Mode is enabled
VU#749870	08/03/2004	Juniper Networks NetScreen firewall contains a DoS vulnerability in the SSHv1 service

Principles for Secure Computer Systems

Based on: Fredrick Brooks, Jerome Saltzer, Mike Schroeder, Butler Lampson, Frans Kaashoek, and the cumulative wisdom of many others


Principle of Least Privilege
End-to-End
Simplify
Second System Effect
Principles for Secure Systems
Be Explicit
Immediate Feedback
Open Design Principle
Incommensurate Scaling
Minimize Secrets
Design for the User

Open Design Principle

Credit: softwar.net

End-to-End Argument Saltzer, Reed, Clark (1981)

Whenever possible, communications protocol operations should be defined at the end-points of a communication system, or as close as possible to the resource being controlled.

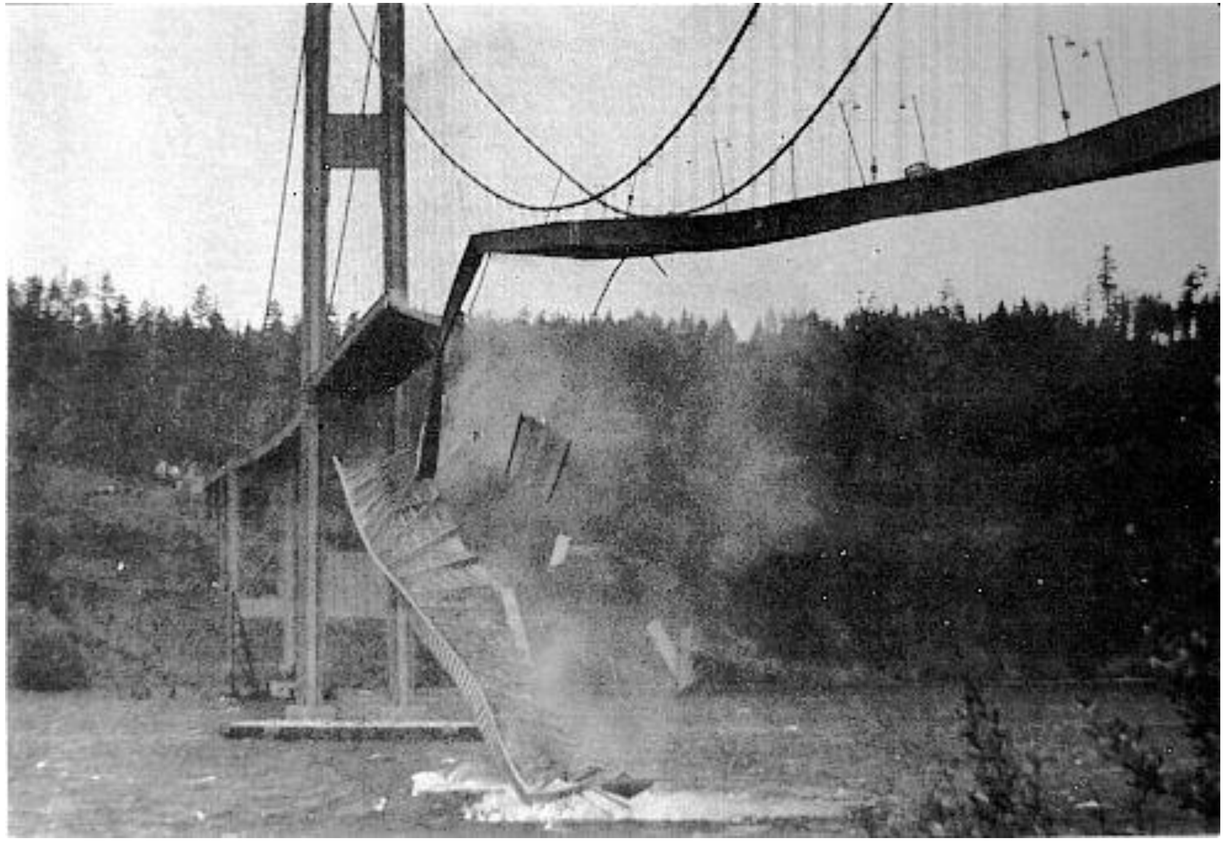
Secure device to monitor?
Secure device to database?
Secure device to device?

Find your end points.
Or you might implement an expensive approach.

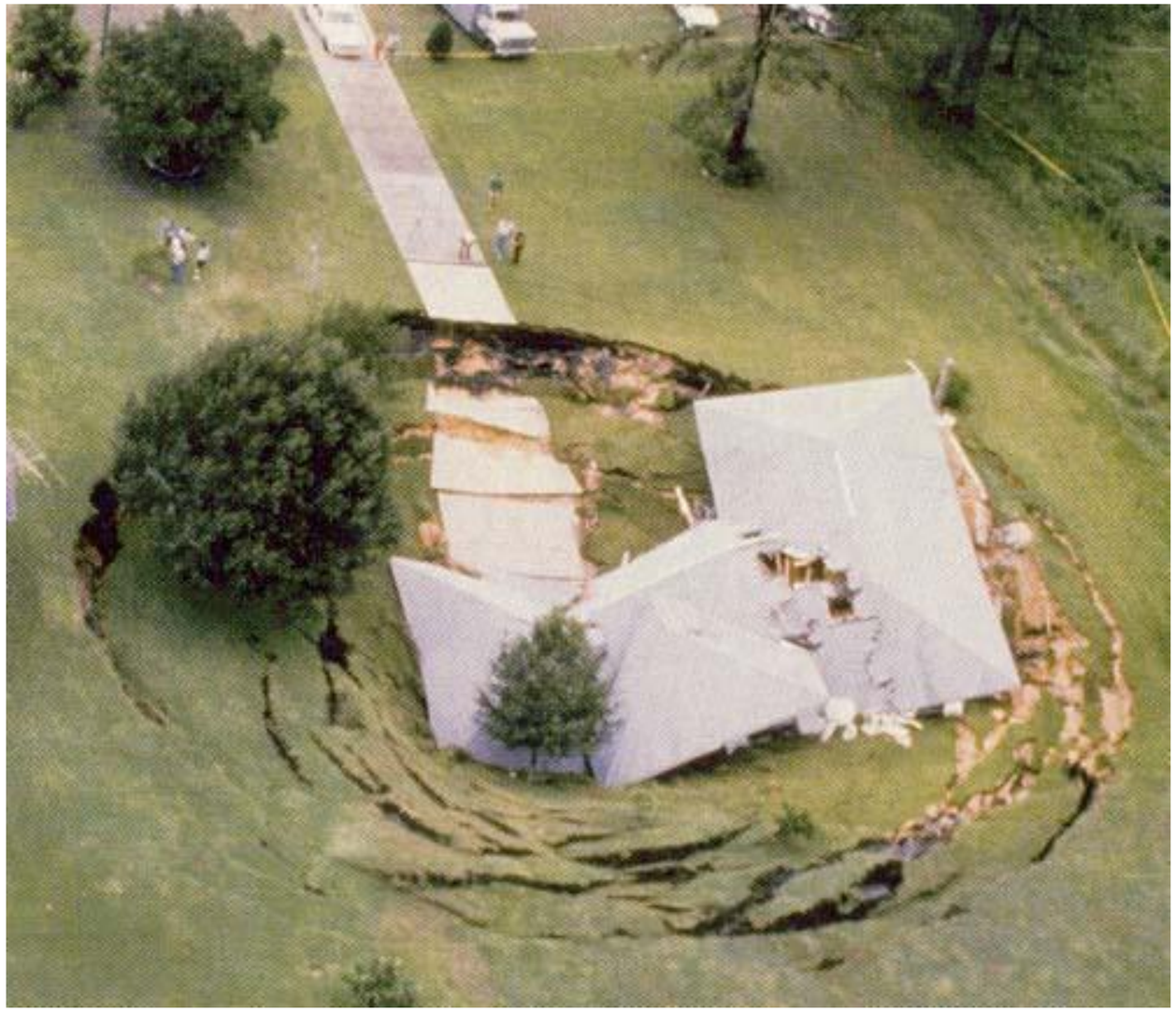
Corollary: if you think firewalls are the design solution to a problem, you don't understand the problem.

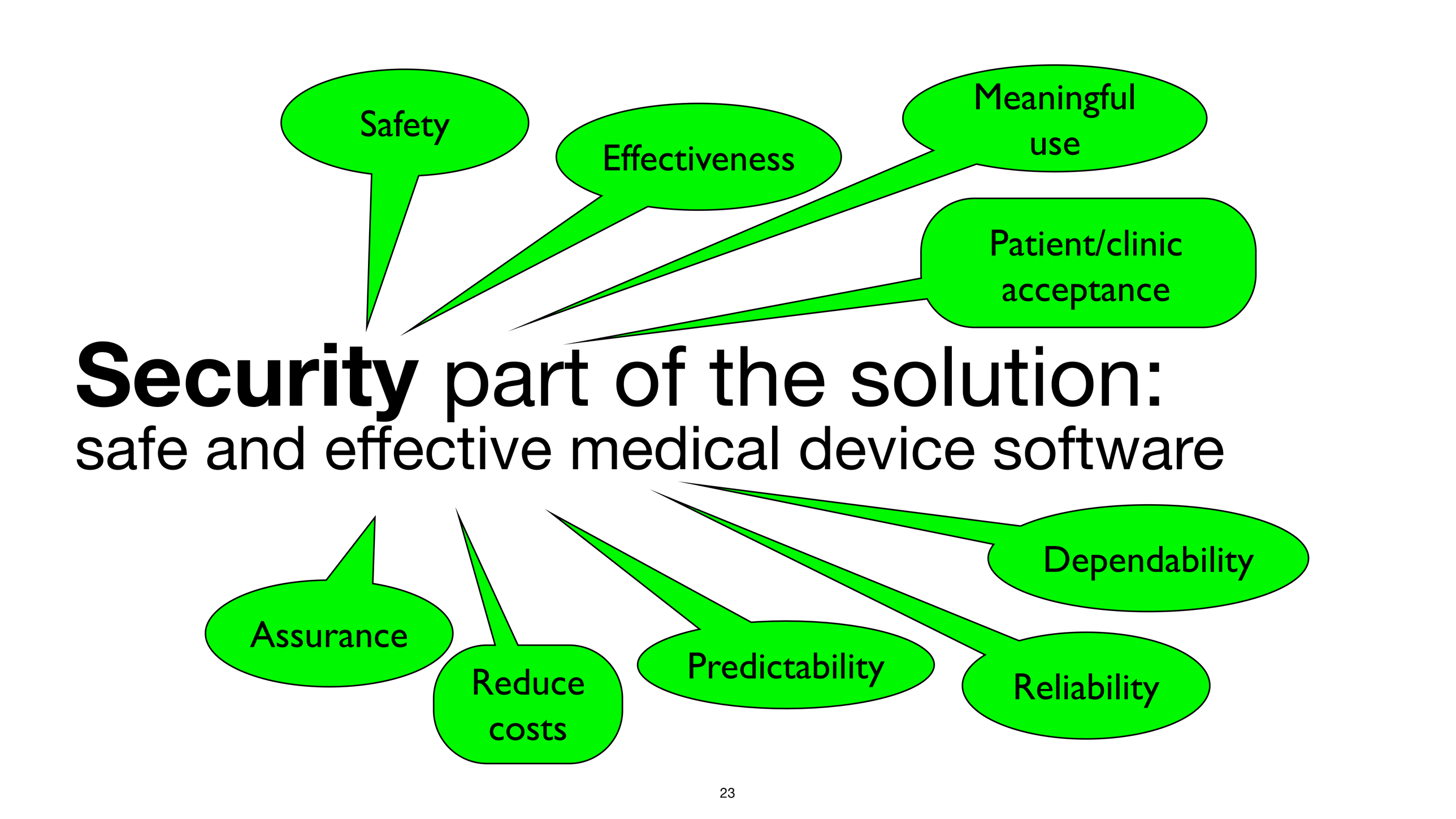
Humility

If you think you have a completely secure system, you are doomed.



Your application is as strong as...




Safety
Effectiveness
Meaningful use
Patient/clinic acceptance
Security part of the solution:
safe and effective medical device software
Assurance
Reduce costs
Predictability
Reliability
Dependability

Syllabus & Grading

- piazza.com
- spqrlab1.github.io/medcybersecurity/

Next

- Tuesday:
  Framing Medical Device Cybersecurity & Differentiating Stakeholders and Context

- Thursday Tour:
  Dr. Daniel Kramer's Cardiac Lab @ BIDMC near Longwood
  (Details TBA on Piazza)