

Security as an Issue for Medical- Device Software

Rance Cleaveland, PhD

Professor of Computer Science, University of Maryland
and

Executive & Scientific Director, Fraunhofer USA Center for
Experimental Software Engineering (CESE)

Fraunhofer CESE

- Applied-research institute in software engineering, founded 1998
- Located in U. Maryland research park
- Staff: 30 (~22 FTEs): 16 technical (10 PhDs), 12 students / visitors
- Annual budget: US \$4.5m
- Affiliated with U. Maryland, Fraunhofer USA, Fraunhofer Gesellschaft (€2bn non-profit research organization in all areas of applied science and engineering)



CESE Overview

- **Mission**

Better software-development technologies, practices and processes

- **Technical expertise**

Software design, verification and validation, project management

- **Target sectors**

Aerospace / defense, automotive, medical

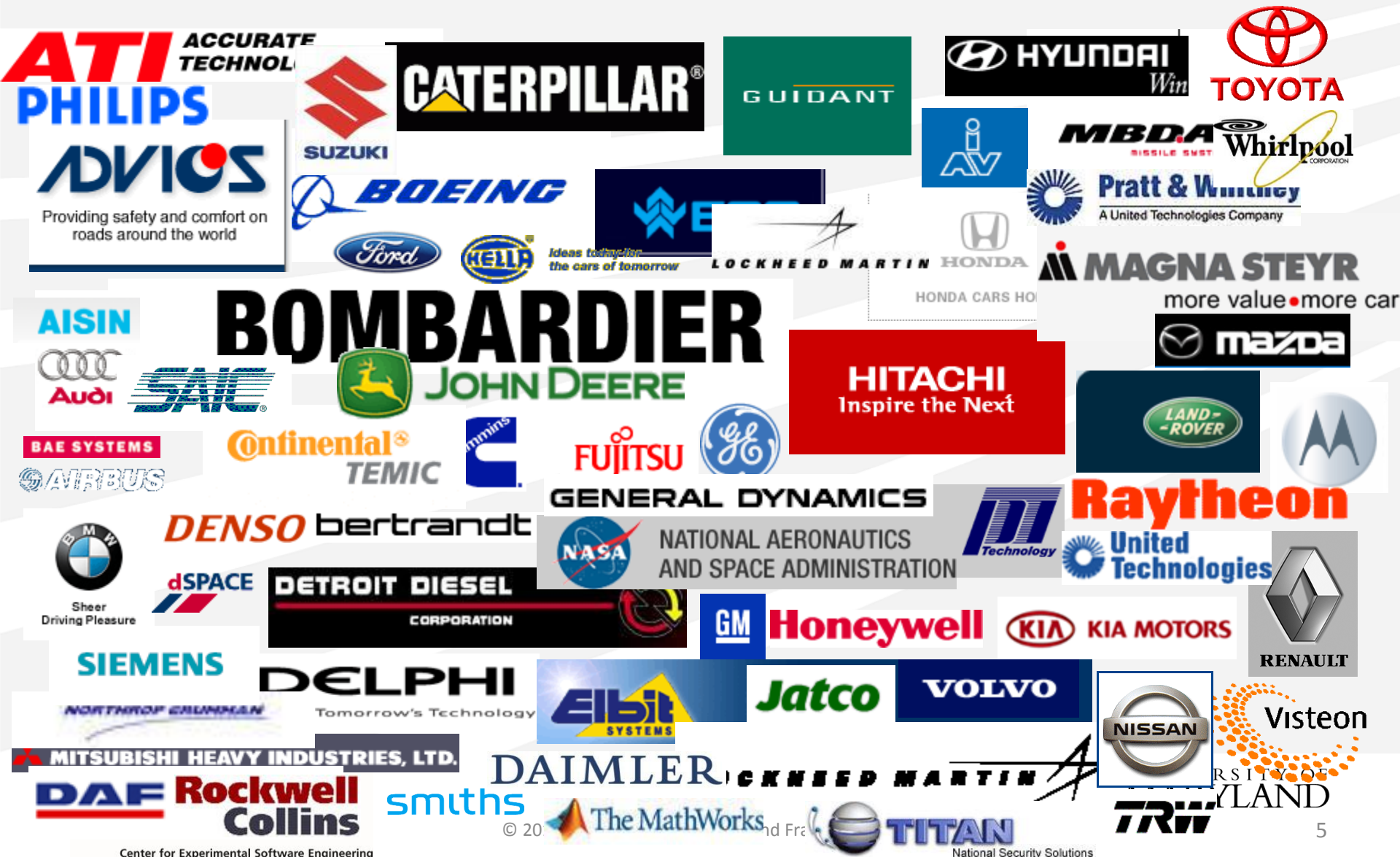
- **Biggest customer**



This Meeting vs. This Talk

- Is this talk about ...
 - Standards? No
 - Tools? No
- Why not? Because they don't exist for medical-device software security!
- Nevertheless
 - Security is a growing industrial concern for medical devices
 - Something has to be done
 - So: this talk talks about a method for security analysis of medical devices

Some Software Companies



Framing the Problem

Primary drivers for medical-device certification:

- Safety (“Is it possible for the device to harm the patient?”)
- Efficacy (“Will the device provide clinical benefit to the patient?”)



A Fundamental Assumption

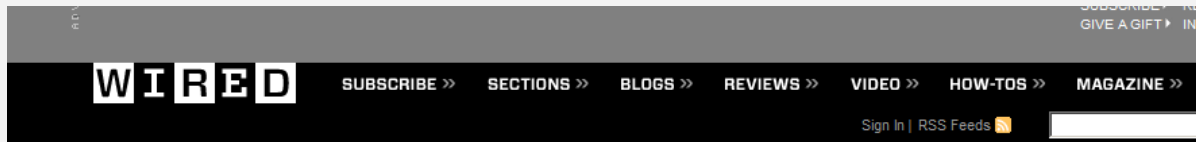
Hazards occur **accidentally**

- A power source blows out due to a random surge
- A wireless receiver accidentally picks up communication meant for someone else

What about “Malign Intent”?

- This assumption no longer holds!
 - An attacker who wants to deprive a patient of insulin could both run down the battery and deactivate the alarm on an insulin pump
 - Triggering conditions for hazards considered “independent” now have a common cause
 - Hazard-mitigation measures put into place under this assumption of independence”are no longer sufficient

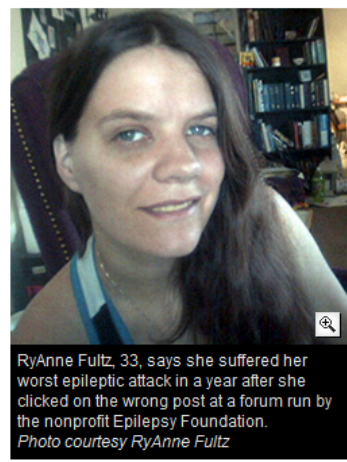
Malign Intent



POLITICS : SECURITY

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08



Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit [Epilepsy Foundation](#), which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs.

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.

RyAnne Fultz, a 33-year-old woman who suffers from pattern-sensitive epilepsy, says she clicked on a forum post with a legitimate-sounding title on Sunday. Her browser window resized to fill her screen, which was then taken over by a pattern of squares rapidly flashing in different colors.

[Email Article](#)

[Full Page](#)

[Comments](#)



WORLD

KFC fined \$8M for Australia salmonella case

4 of 9



60 MINUTES

Ex-CIA chief defends waterboarding of al Qaeda leader

5 of 9

August 5, 2011 10:14 AM

PRINT

TEXT

Black hat hacker can remotely attack insulin pumps and kill people

By [Chenda Ngak](#) Topics [Wired for Women](#)



(Credit: iStockphoto)

[said Radcliffe](#). He said that the devices turned him into a supervisory control and data acquisition (SCADA) system.

Out of fear for his own safety he wanted to see if he could hack into these wireless medical devices. As a [senior threat intelligence analyst](#) for a major computer security organization, it only made sense that he would test his own defense against hackers.

His presentation, "[Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA](#)

(CBS/AP) - As if we didn't already have enough to be neurotic about, a man at the [Black Hat Technical Security Conference](#) gave a presentation detailing how he could take control of insulin pumps from miles away and kill his victims.

Take a minute to panic. Now keep reading.

Jerome Radcliffe is a diabetic. The nefarious hack he presented at the conference Thursday was a response to his condition. "I have two devices attached to me at all times; an insulin pump and a continuous glucose monitor,"

Why Attack Medical Devices?

- Bloody-mindedness: “because you can”
- Desire to inflict harm on specific individuals
- Data harvesting
- Attacks difficult to detect and trace back to the perpetrator
 - A successful attack may be considered an accidental device mal-function

More..

- Researchers have shown how it is possible to **wirelessly induce fatal heart rhythms** (ventricular fibrillation) in an Implantable Cardioverter Defibrillator

[Halperin et al, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. IEEE Symposium on Security and Privacy. 2008]

CNET > News > Security & Privacy

Conficker infected critical hospital equipment, expert says

Hundreds of PCs and medical devices at hospitals in the U.S. were found to be infected with the Conficker worm recently, a security expert says.



by Elinor Mills | April 23, 2009 4:23 PM PDT



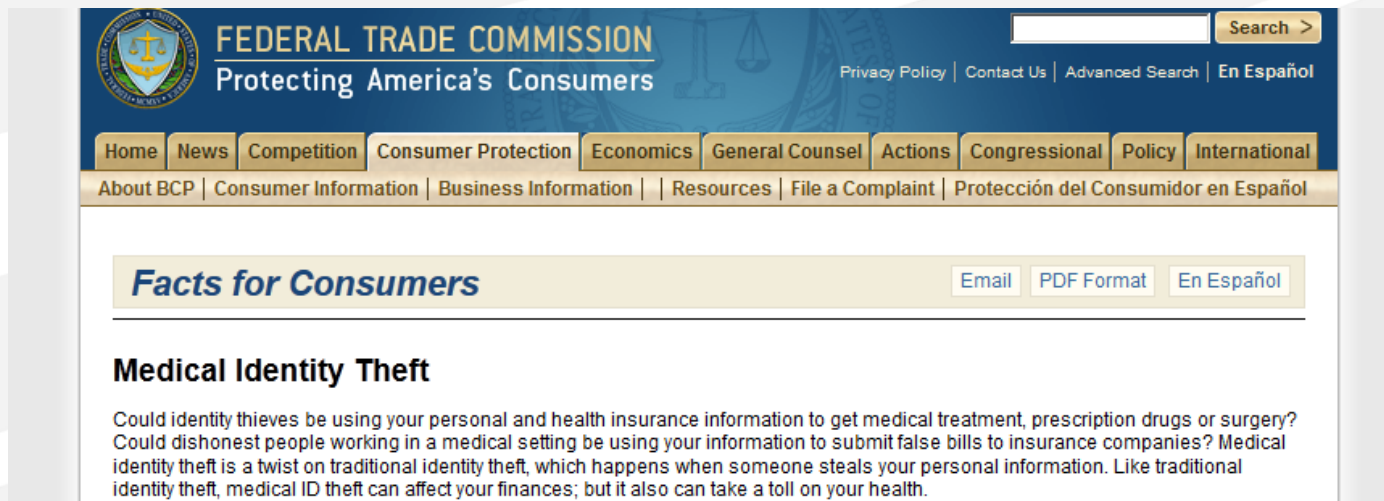
Updated 7:50 a.m. PDT April 24 to specify that the infection was in the U.S.

SAN FRANCISCO--The [Conficker](#) worm infected several hundred machines and critical medical equipment in an undisclosed number of U.S. hospitals recently, a security expert said on Thursday in a panel at the RSA security conference.

Generic,
non-device-
specific
attacks also
possible

Wait There Is More...

- So far we have looked at attacks where fraudulent control of device is sought to be imposed
- And then, there is medical identity theft



The screenshot shows the Federal Trade Commission (FTC) website. The header includes the FTC logo, the text "FEDERAL TRADE COMMISSION Protecting America's Consumers", a search bar, and links for "Privacy Policy", "Contact Us", "Advanced Search", and "En Español". Below the header is a navigation menu with buttons for "Home", "News", "Competition", "Consumer Protection", "Economics", "General Counsel", "Actions", "Congressional", "Policy", and "International". A secondary menu includes "About BCP", "Consumer Information", "Business Information", "Resources", "File a Complaint", and "Protección del Consumidor en Español". The main content area features a section titled "Facts for Consumers" with buttons for "Email", "PDF Format", and "En Español". Below this is a section titled "Medical Identity Theft" with the following text: "Could identity thieves be using your personal and health insurance information to get medical treatment, prescription drugs or surgery? Could dishonest people working in a medical setting be using your information to submit false bills to insurance companies? Medical identity theft is a twist on traditional identity theft, which happens when someone steals your personal information. Like traditional identity theft, medical ID theft can affect your finances; but it also can take a toll on your health."

Electronic Data On Medical Devices

- Treatment regimes
- Medication doses
- Values of vital parameters
- Personally identifiable information
 - Even when personally identifiable info is not there, the attacker may find it by other means



POLITICAL HOT SHEET
**Can Mitt Romney
make boring sexy?**

1 of 9



CRIMESIDER
**Rodney King reflects
on life since '92 LA
riots**

April 6, 2012 4:21 PM

PRINT TEXT

Utah: Medical records breach more extensive

SALT LAKE CITY — Health officials in Utah say hackers who downloaded thousands of medical files from state computers stole far more personal information than originally thought.

The Utah Department of Health said Friday that **nearly 182,000 recipients of Medicaid and the Children's Health Insurance Program had their personal information stolen.** The department estimates more than 25,000 Social Security numbers were compromised.



Health Blog

WSJ's blog on health and the business of health.

May 8, 2009, 8:52 AM

Hackers May Have Stolen Patient Data

Article

Comments (10)



Email



Print



Like



+ More



Text

By Jacob Goldstein

Hackers claimed they tapped into a Virginia database of patient records and said they would sell the records unless they were paid a ransom of \$10 million.

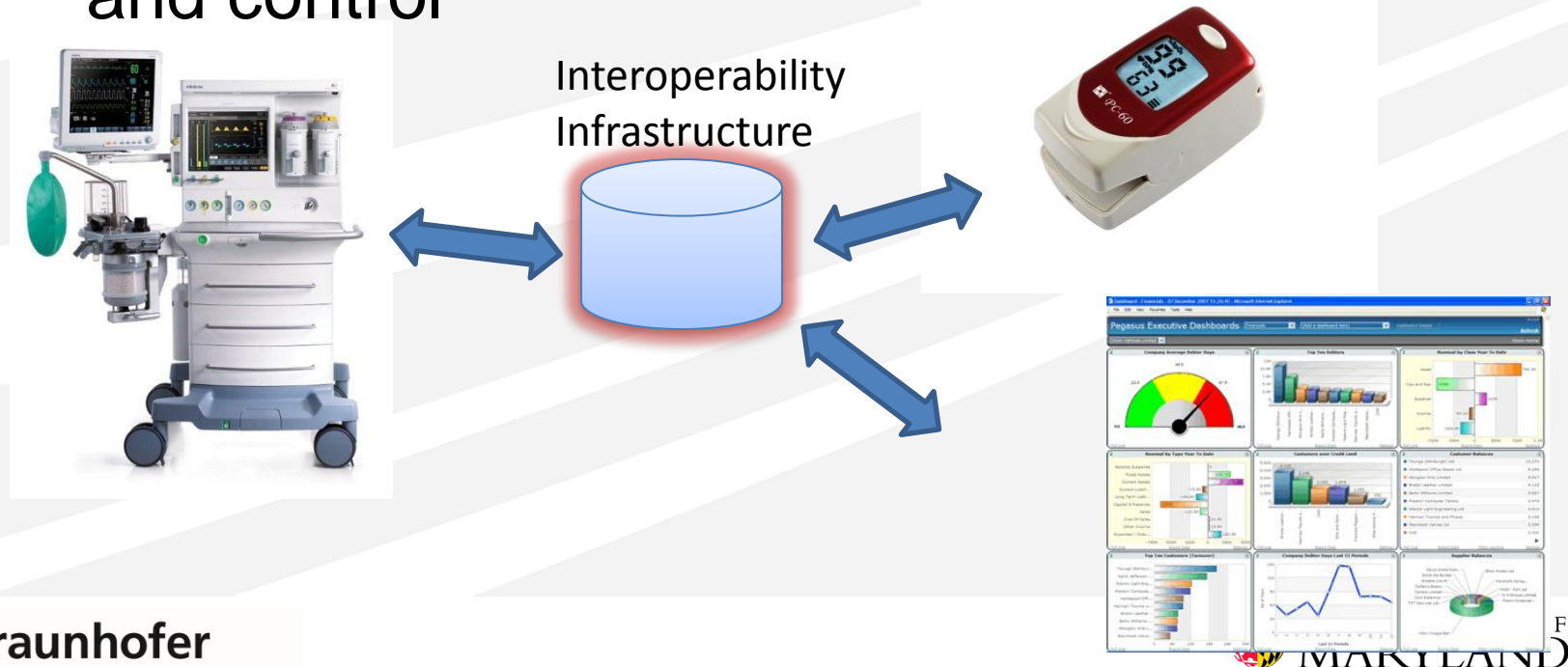
Timothy M. Kaine, the state's governor, has called the threat "an intentional criminal act against the commonwealth by somebody who was trying to harm others," the [Washington Post reports](#) this morning.



A single health record fetches \$50 on the black market [Digital Health Conference, New York City]

How It's Going To Get Worse

- Interoperability!
 - Different devices plugged into centralized communication infrastructure exchanging data and control



Why Things Are Going to Get Worse

- Connecting to an interoperability infrastructure provides new attack surfaces
 - These things were designed to be stand-alone devices. Not nodes on a network”
- The interoperability infrastructure will itself become a target for attack

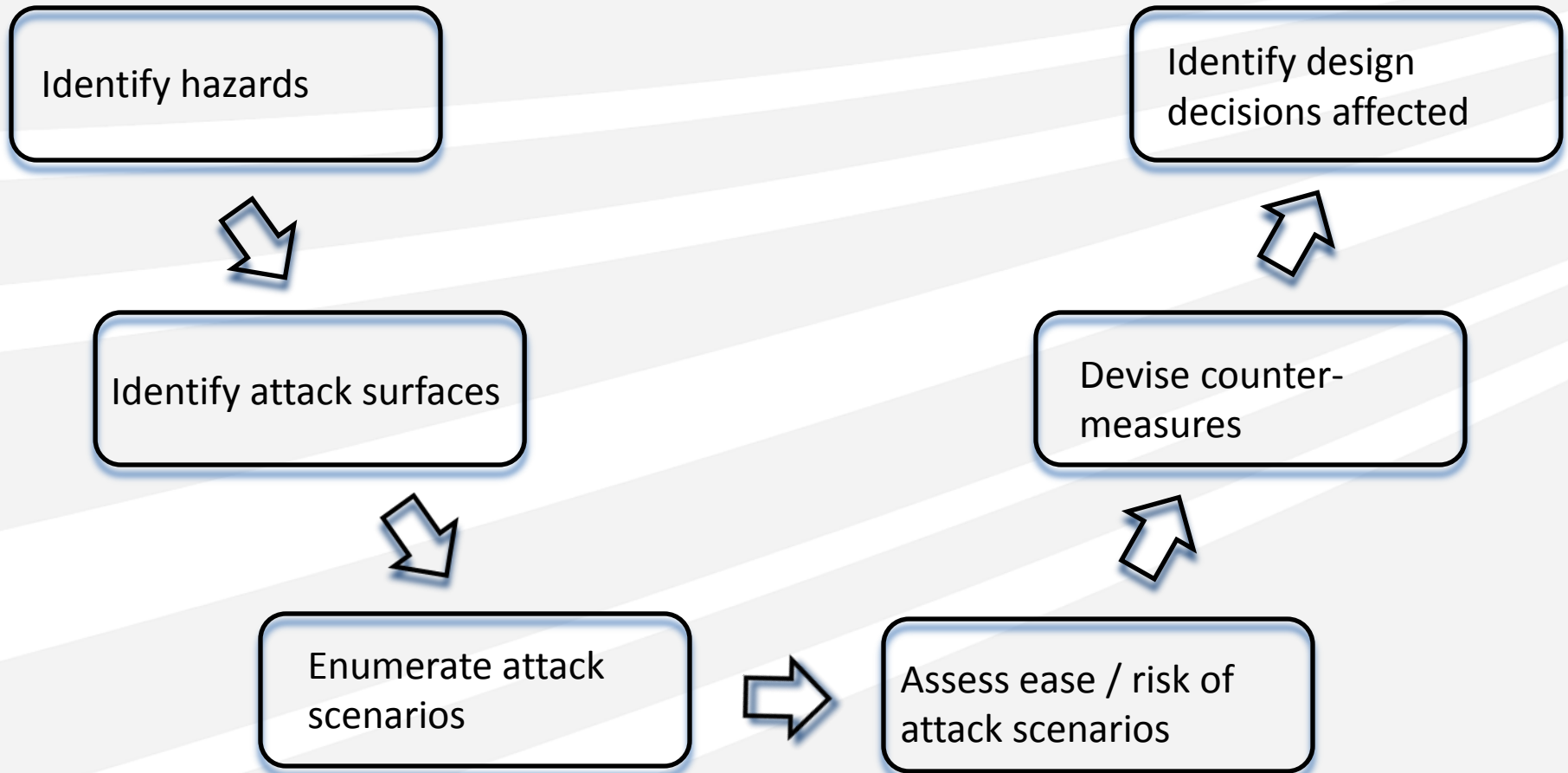
This All Came to a Head

- A large medical-device company approached Fraunhofer
 - They wanted security audits for different portable infusion pumps
 - They had \$\$\$
- What to do?
 - We “knew” security
 - We “knew” embedded software
 - We didn’t know security for embedded software ... but we are not alone!
 - No standards
 - No tools
 - No methods

So What To Do?

- We devised a “security by design” approach
 - Security vulnerability: use of an **interface** to trigger a **hazard**
 - Security analysis can build on hazard analysis, system design (for the interfaces)
 - No such thing as a “secure device”
- We applied it to three separate devices in late 2011 / early 2012

A Security By Design Methodology



Example – Wearable Infusion Pump

- Interfaces
 - Wireless (for remote control)
 - Infrared (for flashing software, upgrades)
 - Device keypad
- Hazards
 - Drug overdelivery
 - Drug underdelivery
 - Patient data compromise

Attack Scenarios

- Principle: use interfaces to trigger hazards
- How can attacker access interfaces?
 - Specialized equipment (RF / IR transceivers)
 - Internet
- “Internet”?
 - Pump includes software for storing data, changing pump settings on PC
 - If PC is connected to internet ...!

Kinds of Attacks

- Command injection / replay (capture commands sent to pump, replay latter to modify treatment regime)
- Denial-of-service (bombard pump with bogus commands to run down battery)
- Pump configuration changes (change maximum / minimum dosages, alter clock, etc.)
- Data compromise (steal treatment data from pump / PC)

Attack Ranking

- Protections incur costs
- Which should be invested in?
 - An economic question
 - Data to base decisions on are scarce
 - Our advice
 - Coarse guesses about ease of attack, level of reward
 - Use these guesses to guide decision-making

Typical Counter-Measures

- Time-stamping data
- Password-protection
- Data encryption
- Logging (“forensic dissuasion”)

What About...

- “Security by obscurity”?
 - “We use a proprietary protocol”
 - Issues
 - Single line of defense
 - Proprietary does not mean secret (cf. patent disclosures)
- Range of communication
 - Better
 - Beware of “range-extendors” (cf. Internet)!

Design Designs

- Security, like performance and usability, is a design dimension
- Strengthening one dimension may weaken the other
Requiring a user to input a password every-time he/she wants a bolus may strengthen security but will introduce human-factors safety risk
- Some security vulnerabilities may not be mitigated based on considerations on other design axes
- If so, document WHY the decision was taken
We could have user input password every time he wants a bolus but the safety implications are too severe

Now Over To Interoperability...

- The interoperability infrastructure may become the target of attacks
 - Spurious or compromised or spoofed devices exploit vulnerabilities in infrastructure software
- The interoperability infra-structure may become the source of attacks
 - Compromised interoperability infrastructure attacks devices connected to it

What We Need

- Prevent bad things from happening
 - Mutual authentication scheme for infrastructure and devices (“I am who I say I am”)
 - Signed behavioral guarantees (“I shall behave in this pre-defined way) at registration-time
 - Real-time compliance-checking (“I do what I said I would do”)
 - Mandatory encryption (“I don’t reveal data to sniffers”)

What We Need

- Be pro-active when bad things happen
 - Detect “bad” behavior of device
 - Quarantine it from network
 - Maintain secure logs of activities so that attacks can be forensically analyzed
 - Distributed logging and log-analysis is a challenge

What about “Standards / Methods / Tools, and Efficacy”?

- Standards document perceived best practices
- Standards lag practice as a result
 - Practices must first be identified
 - Consensus of sorts must be achieved
- Methods / tools precede, inform standards

Conclusions

- Security is a new concern in medical device (and other, cf. automotive) arenas
 - No standards
 - Not likely to be any soon
- Methods / tools needed in mean time
- Our approach: use hazards and interfaces to drive security analysis

Thank You!

Rance Cleaveland

University of Maryland / Fraunhofer USA CESE

rcleaveland@fc-md.umd.edu

+1 240-487-2905

www.fc-md.umd.edu