Security of Safety-Critical Devices

Frankie Catota and Adam Durity

April 8, 2014

Outline

- Introduction
- Medical devices
  - Risks
  - Defense Approaches
  - Perception
- Vehicle safety
- Other safety-critical areas
- Economics of safety-critical devices

Safety-Critical Devices

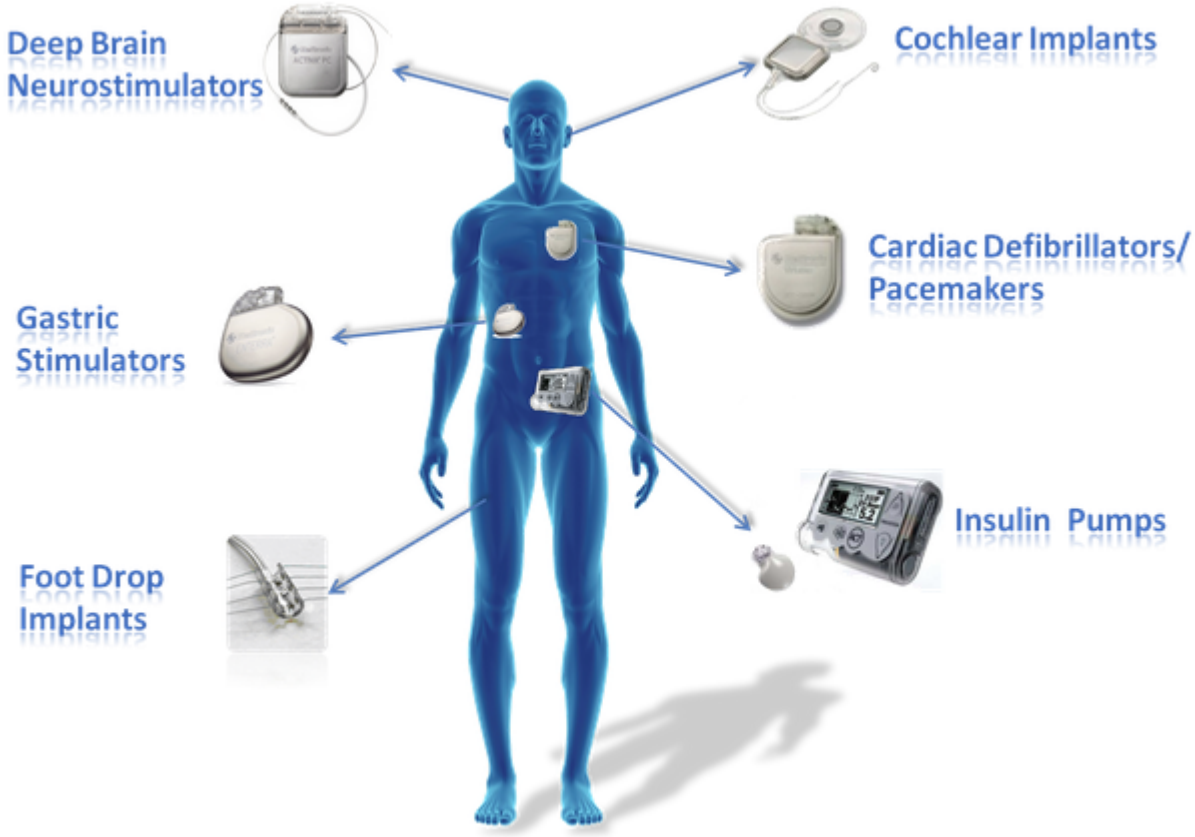
- "Safety-critical systems are those systems whose failure could result in loss of life, significant property damage, or damage to the environment." – John C. Knight

- Security in Safety-Critical Systems: maintaining safety in the presence of an active attacker

- Medical Systems
  - Implantable Medical Devices (IMD)

Implantable Medical Devices (IMD)

- Embedded computers
- 350K Pacemakers & 173K Cardiac Defibrillators in 2006



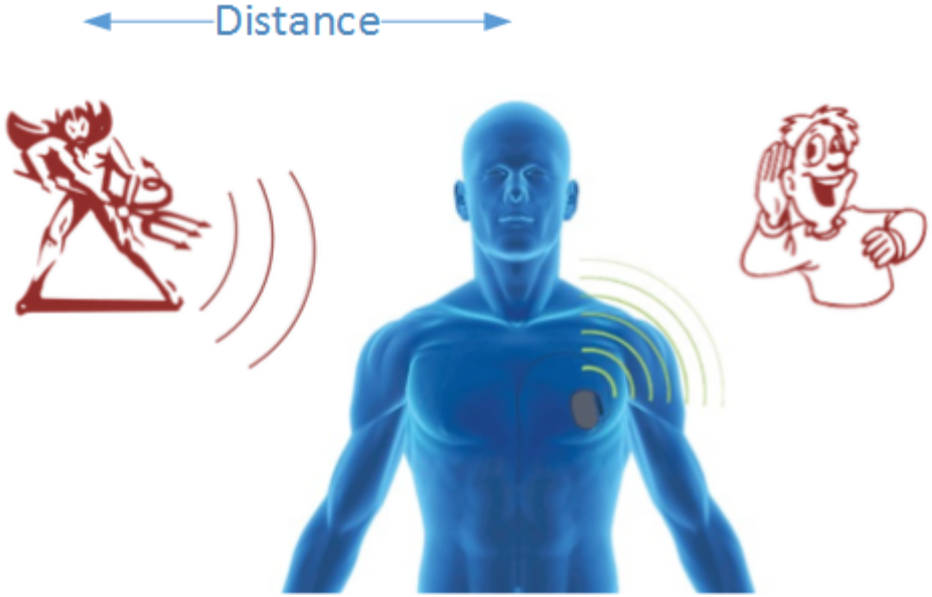
healthcareitsystems.com

Operational Requirements

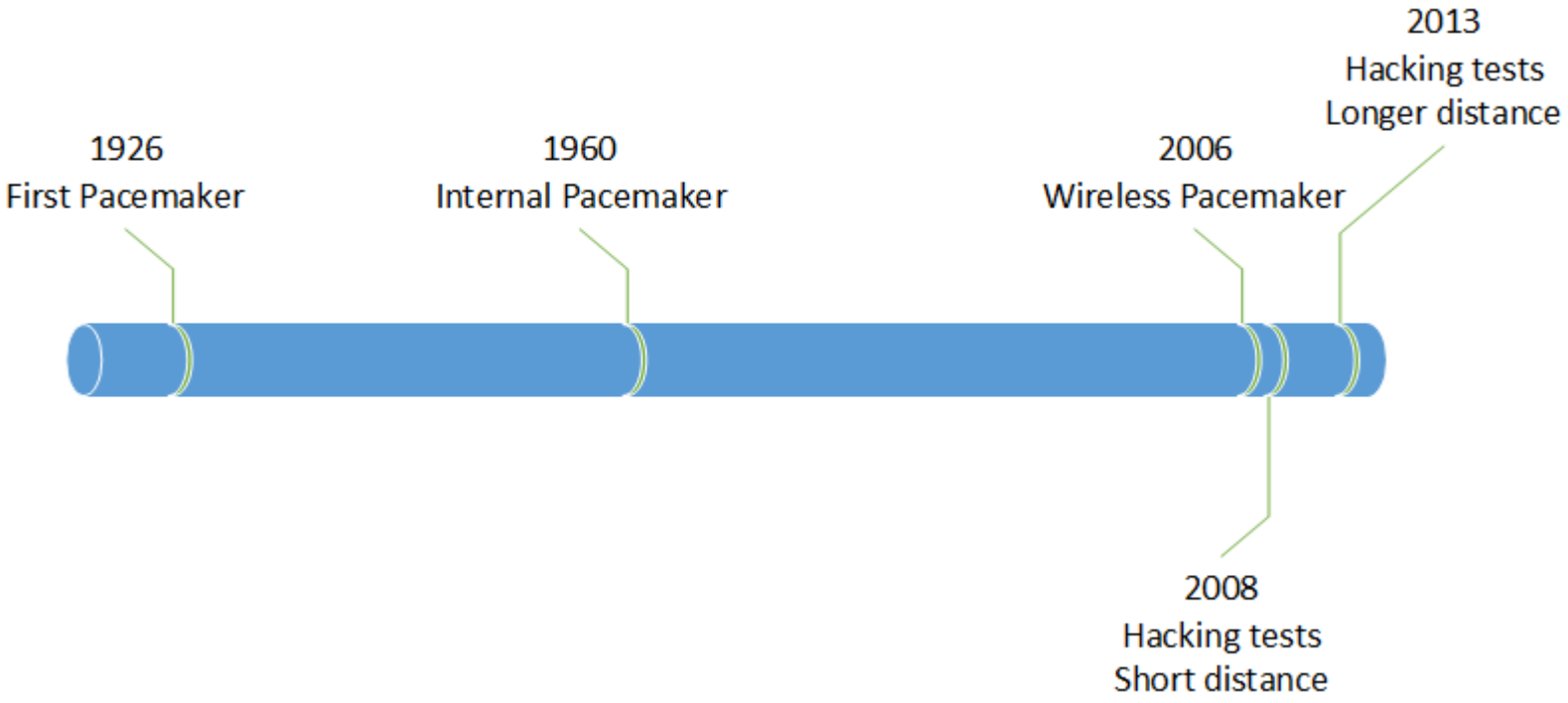
- Collect information (diagnostics)
- Disable IMD before conducting surgeries
- Reprograming
- Access in emergency situations (authentication)—rapid and reliable access --challenge
- Constraints
  - Limited capacity of battery (replacement -necessitates surgery). Implications: injuries and death
  - Microcontrollers

Risks in Medical Devices

- Vulnerabilities
  - Authentication
- Attack Vectors
  - Passive
  - Active
- Risks / threats
  - DoS
  - Changes in configuration
  - Replace medical records -- someone having a different operation
  - Injuries, death



Pacemakers



Networking changes the treat model

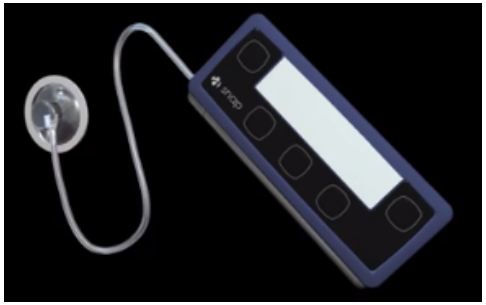
Hacking Tests (1)

- **2008:** wireless access to a combination heart defibrillator and pacemaker (within two inches of the test gear) –Kevin Fu
- Disclose personal patient data
- Reprogram IMD to shut down and to deliver jolts of electricity that would potentially be fatal
- Authors: “The risks to patients now are very low”

Hacking Tests (2)

2011-2012-2013

- Hacking Insulin Pumps



-- insulinpump.com

2013 – Black Hat /Defcon:

- "Implantable medical devices: hacking humans"
  - At 30 feet by compromising their pacemaker
  - Transmitter to scan for and interrogate individual medical implants
  - Security techniques for manufacturers

-- ioactive.com

Defense Approaches

- How do we achieve resistance to attacks?
- Fault-tree analysis --What can go wrong?
- How strong a security policy should be?
  - Security
  - Safety

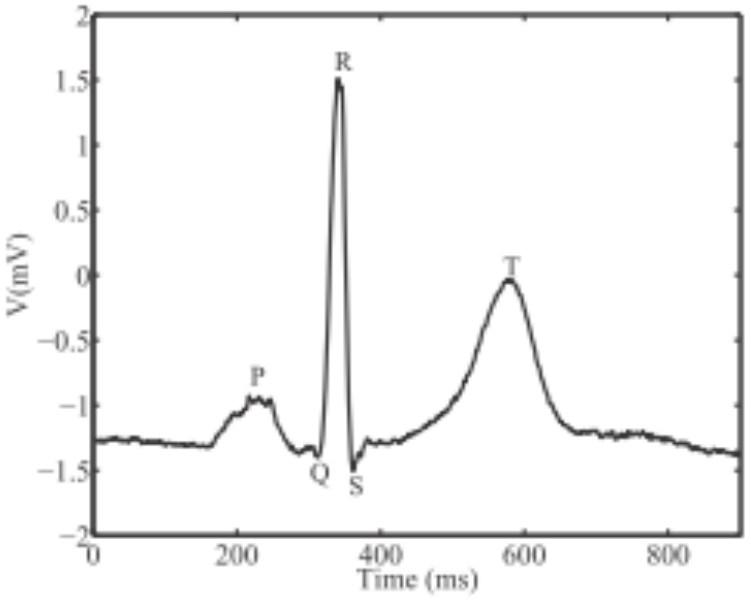
Access Control: Authentication Methods

- Passwords: how to make them available?
  - Tattooed passwords (visible, UV visible)
  - Bracelet
- Biometrics (face recognition)
- Smart Cards
- Touch-to-access policy
- Key-based systems
- Shields
  - Necklace
  - Computational wristband

-- Figures from Denning et al.

Authentication: Touch to Access Policy (1)

- Physiological value EGG as an authenticator
- IMD authentication based on Inter-pulse Interval (IPI)
- Extract uncorrelated random bits



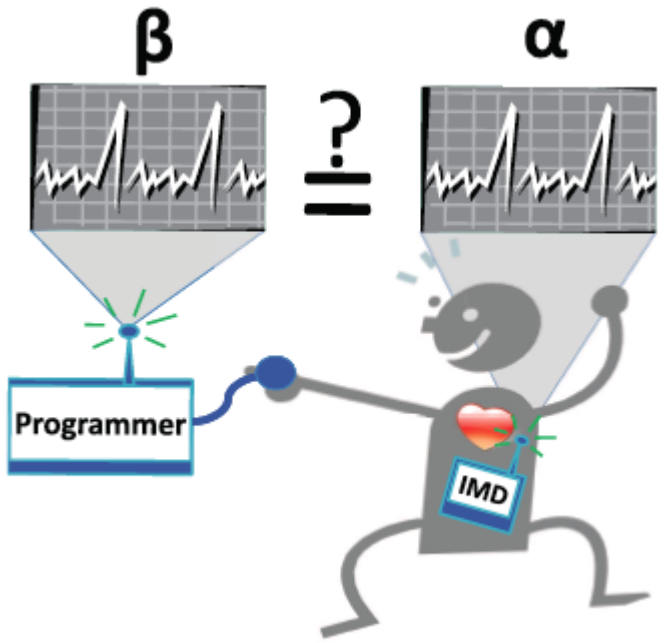
Electrocardiography (ECG) Wave form

- Rostami et al.

Authentication: Touch to Access Policy (2)

Independent synchronous readings --two steps:

- Establishing a secure channel (TLS)
  - Programmer - server
  - IMD – client (avoid burden of PKI)
- Mutual authentication
  - IMD reveals α (randomness of α)
  - Programmer reveals β
- Privacy
  - Medical data is not revealed –only α
- Detect attacks from deviations from (alpha)
- Promiscuous mode (IPI flat – Heart attacks)

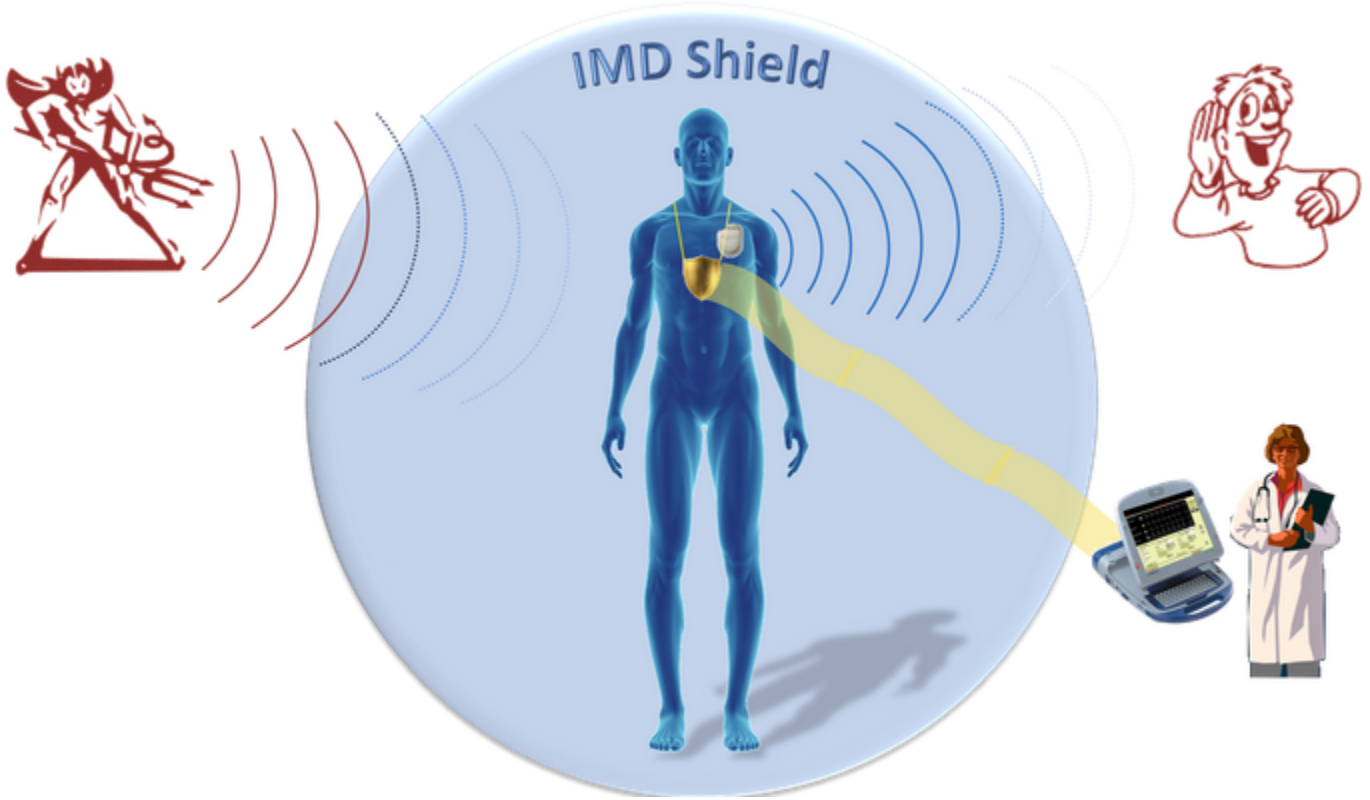


H2H operation

- Rostami et al.

IMD Shield

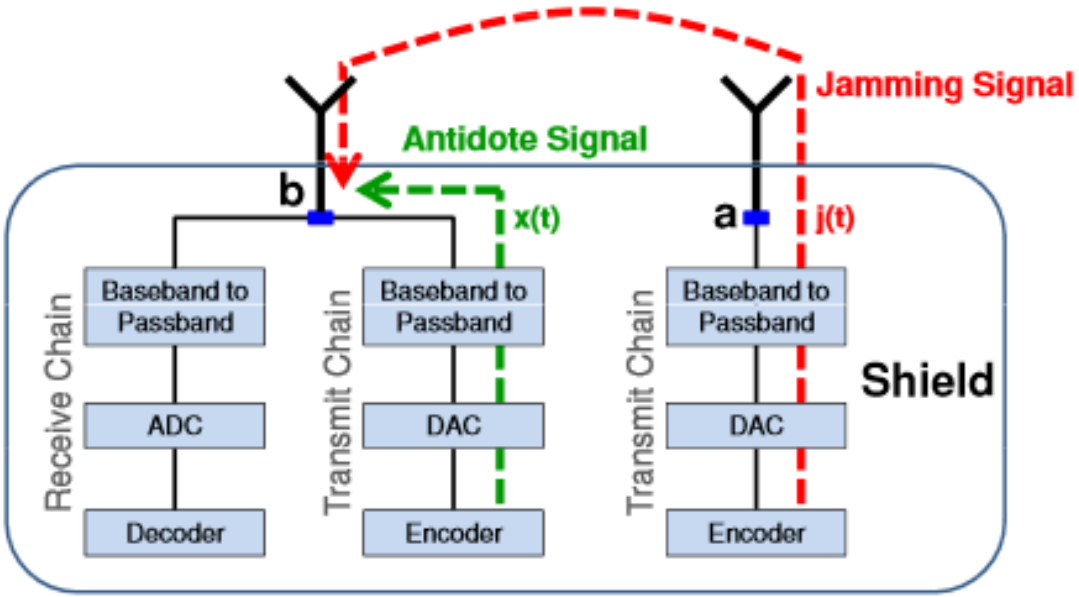
- Proxy (messages exchanges)
- Authentication + encryption (channel)



- IMDShield -mit.edu

IMD Shield - Implementation

- Jammer design (full duplex radio)



- S. Gollakota et al. MIT

Wristbands / Alert Bracelets

- Safety in emergencies
- Security & Privacy under adversarial conditions
- Battery life

Wristbands / Alert Bracelets

- Protection is granted while wearing the bracelet.
- Remove to gain access to the IMD
- Inform patients about malicious actions – But not preventive
- Authentication + symmetric encryption
- Disadvantages
  - Relies on the patient wearing the bracelet
  - Reactive
  - No desired scenarios (bracelet close but not found)
  - Cognitive effects on patients

--Denning et al.

Perceptions of Authentication Methods (1)

Concerns about safety and privacy

- Hospitals not having correct equipment to scan tattoos and UV-visible tattoos (emergencies)
- Visual indicator of patients condition (something is wrong). Personal dignity.
- Carrying one more device
- Aesthetics
  - Wristbands (especially). “Mockups are unaesthetic”
  - Tattoos
- Mental and physical inconvenience
- Cultural and historical associations (concentration camps, drunks)
  - Tattoos –negative associations
- Self-Image –consistence with desired image

Perceptions of Authentication Methods (2)

- Notification availability –strong negative reactions
- Medical information
- No concerned about someone getting access to their IMD change configurations
- Some do not have the perception of a real risk --“be my guess”

Evaluation Results

Password and Body Modification (n=11)			
Mockup System	Liked	Disliked	Would Choose
Medical Alert Bracelet	0%	27%	0%
Visible Tattoo	9%	55%	9%
UV-Visible Tattoo	18%	27%	18%

Data from T. Denning et al.

Group Activity

- Get into groups and discuss other possible attack vectors against any medical system. A frame to discuss about it may be:
  - Vulnerability
  - Attack (actor + motivation)
  - Consequences

Automobiles

- Modern automobile
  - Numerous interconnected microcontrollers
  - Some luxury models have more than 70 controllers
  - Many safety systems (e.g. airbag, brakes, seatbelt pre-tensioners, traction and stability control)

- Controller Area Networks (CAN) enable various controllers to communicate
  - All interface with the required OBD-II diagnostics port
- Since 2007, all automobiles have tire pressure monitoring systems (TPMS)

Automobiles: Attack Vectors

These numerous controllers and other systems are all potential security attack vectors

- Checkoway et al. examined external vectors
  - Indirect physical access
  - Short-range wireless
  - Long-range wireless

- Do vulnerabilities exist within these vectors?
- What can an attacker do upon gaining access?

Automobile: Indirect Physical Access

- OBD-II
  - Diagnostics port used by mechanics to check vehicle systems
  - Most auto shops use a wired or wireless “pass-thru” device to connect PC to OBD-II port
- Entertainment system
  - Fully integrated into CAN for the purpose of providing user feedback (e.g., chime, camera, proximity sensors)
- Checkoway et al.
  - Created an audio file which, when played through the entertainment system, exploits a vulnerability in the playback code to send arbitrary CAN packets to the bus
  - Demonstrated vulnerabilities in pass-thru device which could be used to attack every vehicle inspected with the device

Automobile: Short-range Wireless

- Bluetooth
- Remote Keyless Entry
- Tire Pressure Monitoring System (TPMS)

- Checkoway et al.
  - Exploited vulnerabilities in glue code between vehicle and popular embedded implementation of Bluetooth stack
  - Bluetooth device must be paired
    - Trojan on driver's device
    - Determined attacker with extended proximity

Automobile: Long-range Wireless

- Broadcast
  - FM RDS
  - Satellite radio
  - GPS
- Cellular

- Checkoway et al.
  - Reverse engineered common telematics data protocol
  - Call the car, bypass authentication, inject malicious code for command and control

Automobiles: The Future

- Dedicated Short-range Communications (DSRC)
  - Vehicle to Vehicle (V2V) for collision avoidance

US Department of Transportation

Other Safety-Critical Systems

- Infrastructure
  - Power grid
  - Water supply
- Transportation
  - Aviation
- Military devices

Other Safety-Critical Systems: Infrastructure

- Supervisory Control and Data Acquisition (SCADA)
- SCADA systems can be used in a wide variety of industrial contexts
  - Water purification
  - Power generation (including nuclear)
- Stuxnet
  - Known to target certain SCADA systems
  - Propagated via sneaker-net (i.e., USB key)

Other Safety-Critical Systems: Transportation

Aviation

- Like cars, airplanes use embedded systems
  - Avionics – electronic systems in the cockpit
  - Boeing 787 Dreamliner
    - wireless control systems
- Air Traffic Control
- Regulated by FAA

Vulnerabilities within Safety-Critical Systems

- Systems comprised of multiple components provided by multiple entities
- Components often suffer from common vulnerabilities (e.g., no buffer overflow protection, no guard against user-provided content)
- Manufacturer's do not have resources to conduct full security analysis of every component
- However, components are often treated as fully-trusted components of the system

Economics of Security in Safety-Critical Systems

- Gaynor et al. compared competition between hospitals to patient data protection practices
  - Found that greater competition within a given hospital market breeds looser data protection practices
  - Instead of security, budget is spent in ways that make the hospital more appealing to would-be patients
    - Consider Highmark and UPMC here in Pittsburgh
- Conclusion: in highly competitive markets, security will be sacrificed in favor of consumer visible features that affect the purchase decision
  - FDA: implementing cybersecurity requirements
  - NHTSA: Vehicle Electronics and Emerging Technologies Division

References

M. Rostami et al., Heart-to-Heart (H2H): Authentication for Implanted Medical Devices

T. Denning et al., Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices

T. Denning et al., New Directions for Implantable Medical Device Security

Gollakota et al. They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices

K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Commun. ACM*, vol. 56, no. 10, p. 35, Oct. 2013.

S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*, 2011.

S. S. Clark, B. Ransford, and K. Fu, "Potentia est Scientia: Security and Privacy Implications of Energy-Proportional Computing Shane," in *HotSec*, 2012.

M. S. Gaynor, M. Z. Hydari, and R. Telang, "Is Patient Data Better Protected in Competitive Healthcare Markets?," in *WEIS*, 2012, no. Weis.

<spectrum.ieee.org/podcast/biomedical/devices/hacking-pacemakers>

<groups.csail.mit.edu/netmit/IMDShield>

<blog.ioactive.com/2013/07/las-vegas-2013.html>

forbes.com <hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction>