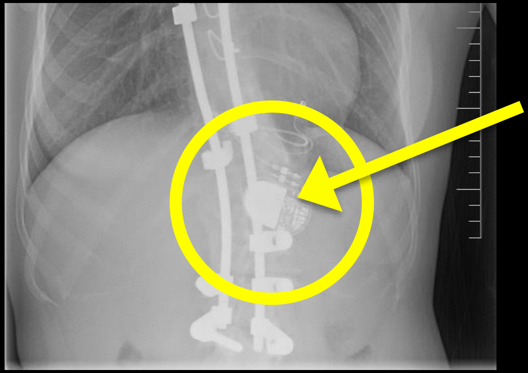
Some example UW security lab projects, related to emerging technologies

Tadayoshi Kohno

CSE 484, University of Washington

Wireless Implantable Medical Devices



- Computation and wireless capabilities lead to improved healthcare
- Question: Are there security and privacy risks with wireless medical devices? If so, how can we mitigate them?
- Approach: Experimentally analyze the security of a real artifact (implantable defibrillator introduced in 2003; short-range wireless)

D. Halperin, et al. “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.” IEEE Symposium on Security and Privacy, 2008. (University of Washington, University of Massachusetts Amherst, Beth Israel Deaconess Medical Center.)

Wireless Implantable Medical Devices

Findings

Ability to wirelessly (from close range, ~10cm):

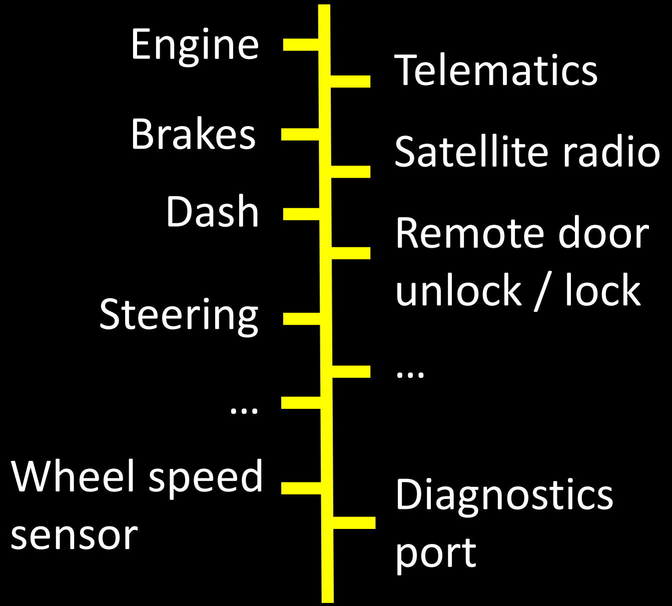
- Change patient name, diagnosis , implanting hospital, …
- Change / turn off therapies
- Cause an electrical shock

Big Picture

- Risk today to patients is small – no reason to be alarmed!
- These are life saving devices; the benefits far outweigh the risks
- Still important to improve security of future, more sophisticated and communicative devices

D. Halpe … m on
Security and Privacy, 2008. (University of Washington, University of Massachusetts Amherst, Beth Israel Deaconess Medical Center.)

Modern Cars



Engine

Brakes

Dash

Steering

…

Wheel speed sensor

Telematics

Satellite radio

Remote door unlock / lock

…

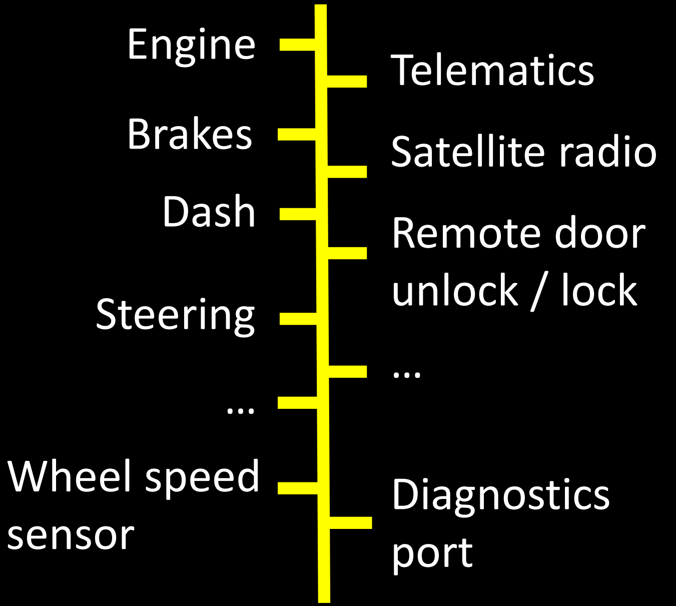
Diagnostics port

Example automotive computer network

K. Koscher, et al. "Experimental Security Analysis of a Modern Automobile." IEEE S&P, 2010. S. Checkoway, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." Usenix Security, 2011. (University of Washington, University of California San Diego.)

What About Security?

?



Engine

Brakes

Dash

Steering

…

Wheel speed sensor

Telematics

Satellite radio

Remote door unlock / lock

…

Diagnostics port

Example automotive computer network

K. Koscher, et al. “Experimental Security Analysis of a Modern Automobile.” IEEE S&P, 2010. S. Checkoway, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” Usenix Security, 2011. (University of Washington, University of California San Diego.)

Approach

Bought two, 2009-edition modern sedans

- UW team bought one, kept in Seattle
- UC San Diego team bought one, kept in San Diego

Work published in 2010 and 2011

(Recently new works published by others)

K. Koscher, et al. “Experimental Security Analysis of a Modern Automobile.” IEEE S&P, 2010. S. Checkoway, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” Usenix Security, 2011. (University of Washington, University of California San Diego.)

Findings

Adversary able to communicate on car’s internal computer network can affect many components within the car, e.g., dash, lighting, engine, transmission, brakes, HVAC, …

Adversary can gain ability to communicate on car’s internal computer network without every physically touching the car – through remote compromise

Road Test: Apply Brakes

K. Koscher, et al. “Experimental Security Analysis of a Modern Automobile.” IEEE S&P, 2010. S. Checkoway, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” Usenix Security, 2011. (University of Washington, University of California San Diego.)

Road Test: Disengaging Brakes

K. Koscher, et al. “Experimental Security Analysis of a Modern Automobile.” IEEE S&P, 2010. S. Checkoway, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” Usenix Security, 2011. (University of Washington, University of California San Diego.)

End-to-end Theft Example

Call car, exploit vulnerabilities to implant new software, car connects (over Internet) to UW server, then run theft program

End-to-end Surveillance Example

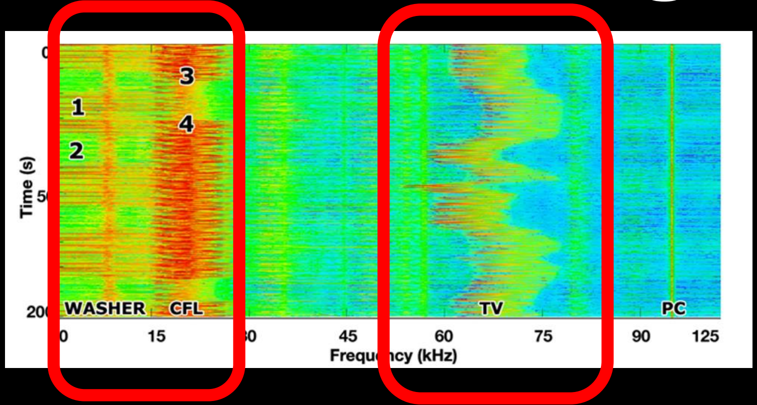
Call car, exploit vulnerabilities to implant new software, car connects (over Internet) to UW server, initiate surveillance

Automobile Sensors and Privacy

- Background:
  - Numerous sensors in modern cars
  - Sensor data may flow to various companies (car manufacturer, insurance company)
- Question: Can we identify drivers, even with access to the most “basic” sensors *already* installed in cars?
- Answer: Yes, with high degree of accuracy among a small set of drivers

M. Enev, et al. “Automobile Driver Fingerprinting.” Privacy Enhancing Technology Symposium, 2016. (University of Washington.)

Home Powerline Monitoring



- Background
  - Significant focus on powerline sensing for activity recognition
  - Prior works: Can determine when specific appliances are in use
- Privacy debate: does powerline sensing compromise privacy?
- Our work: Infer information about what TV show is being watched

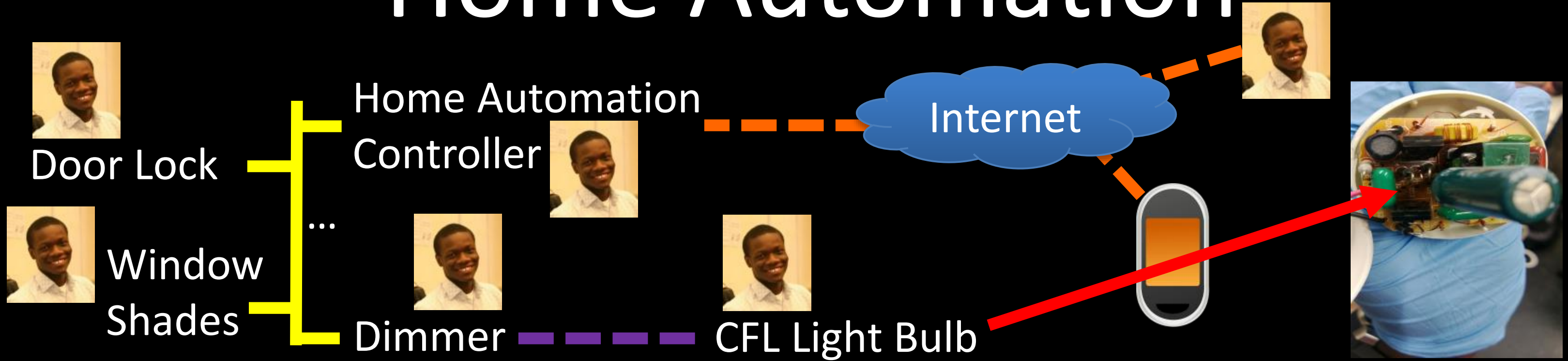
M. Enev, et al. "Televisions, Video Privacy, and Powerline Electromagnetic Interference." ACM Conference on Computer and Communications Security, 2011. (University of Washington.)

Children’s Toys

- Increasing computation in children’s toys too
- Question: What are their security weaknesses?
- Finding: “Easy” for unauthorized party to remotely access and control these toys
- Lesson: Security not forefront in consumer / developer minds

T. Denning, et al. “A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons.” International Conference on Ubiquitous Computing, 2009. (University of Washington.)

Home Automation



- Background: Home automation systems allow remote control and monitoring of home appliances
- Well known issue: Once compromise controller, can compromise any connected device (e.g., door lock, window shades)
- Less well known: Can use devices as stepping stones to devices without traditional network connections (e.g., pop CFL light bulbs)
- Lesson: Must consider security implications of exploits to *other* devices

T. Oluwafemi, et al. “Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security.” Learning from Authoritative Security Experiment Results (LASER), 2013. (University of Washington.)

Stepping Back

- Goal: Improve security of future technologies
- This talk: Example known risks with IoT type devices
- Opportunities:
  - Domain-specific defenses
  - Generic defenses
- Key directions / issues:
  - Threat modeling and risk evaluation
    - including privacy (and information leakage), safety, and stepping stones
    - Including thinking of actors involved and non-traditional interactions (e.g., light bulbs)
  - Software updates and the Zombie problem

Thanks!

Automotive computer security (UW, UC San Diego)

- Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage

Automotive driver fingerprinting (UW)

- Miro Enev, Alex Takakuwa, Karl Koscher

TV video fingerprinting (UW)

- Miro Enev, Sidhant Gupta, Shwetak Patel

Thanks!

Toy computer security (UW)

- Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith

Home automation security (UW)

- Temitope Oluwafemi, Sidhant Gupta, Shwetak Patel

Medical device computer security (UW, UMass Amherst (Michigan), BIDMC)

- Dan Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, William H. Maisel