Experimental Computer Security Research: Project Conception, Execution, and Communication

Tadayoshi Kohno
Computer Science & Engineering
University of Washington

Experimental Computer Security Research: Project Conception, Execution, and Communication

Tadayoshi Kohno
Computer Science & Engineering
University of Washington

Views of the Future

- Technology has the potential to greatly improve our lives

Education

Work

Healthcare

Environment

Accessibility

Social

Transportation

Views of the Future

- Technology has the potential to greatly improve our lives
- Technology also has the potential to create new security and privacy risks (and amplify old risks)

Views of the Future

- Technology has the potential to greatly improve our lives
- Technology also has the potential to create new security and privacy risks (and amplify old risks)
- My key interests in computer security research:
  - Anticipate risks with future technologies
  - Address those risks early
  - Inform policy, iterate with broader community
- Overall goal: the promises of new technologies, but without the associated security and privacy downsides

Types of Computer Security Research

System Design + Implementation

Humans and Security Systems

Measurements

Experimental Security Analyses (aka “Attacks”)

Types of Computer Security Research

System Design + Implementation

Humans and Security Systems

Measurements

Experimental Security Analyses (aka “Attacks”)

This Talk: Two Interleaved Parts

- Perspectives on Experimental Computer Security Analysis Research
- Computer Security and Privacy and the Internet of Things

Experimental Security Analyses

Experimental security analysis research can help:

- Define security for new technologies
  - who are the attackers
  - what are we protecting
  - what attack strategies might work
  - how significant are the risks
- Identify fundamental, domain-specific security challenges
- Provide a foundation for working with stakeholders to
  - refine challenges
  - refine solutions
  - implement defenses

Three Examples "Internet of Things" Technologies:

Medical Devices, Toy Robots, and Cars

First Step: Problem Selection

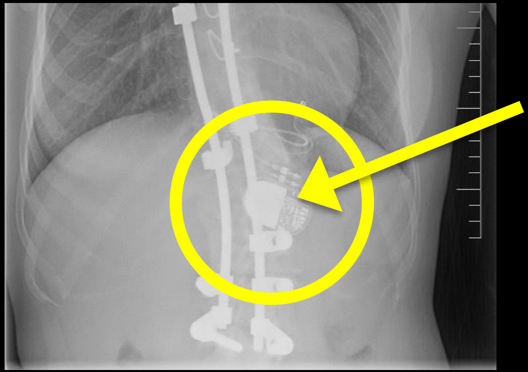
Good if the technology has these properties:

- High impact technology
- Lots of rapid, on-going innovation
- Unique interactions with users; unknown or unique constraints
- Something to learn from the analyses
- Security risks are potentially significant
- Security for these technologies not currently within focus of the security community nor the technology's "home" community: New problems/directions for both communities

Also desirable:

- Early in evolutionary lifecycle: Security considerations would be proactive, rather than reactive

Wireless Implantable Medical Devices



- Computation and wireless capabilities lead to improved healthcare

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.)

First Step: Problem Selection

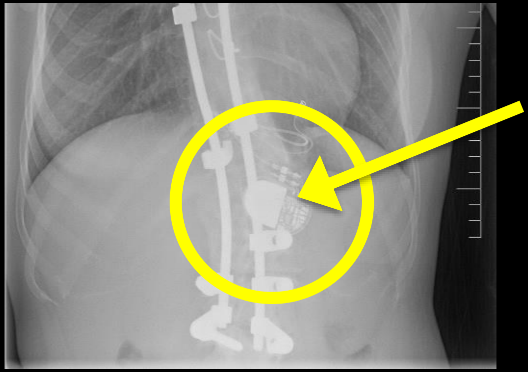
Good if the technology has these properties:

- High impact technology
- Lots of rapid, on-going innovation
- Unique interactions with users; unknown or unique constraints
- Something to learn from the analyses
- Security risks are potentially significant
- Security for these technologies not currently within focus of the security community nor the technology’s “home” community: New problems/directions for both communities

Also desirable:

- Early in evolutionary lifecycle: Security considerations would be proactive, rather than reactive

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?

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.)

Second Step: Identify Approach

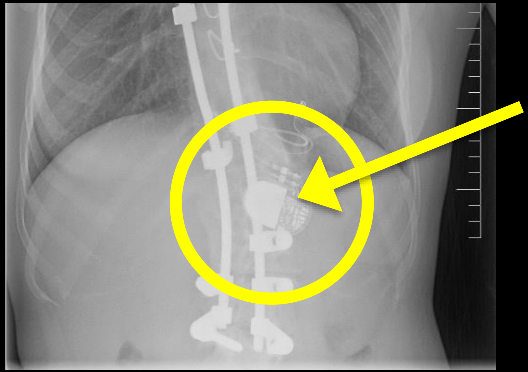
Approaches:

- Deep, thorough analysis of one representative artifact
- Broad analysis of a collection of representative artifacts

Practical constraints may affect choice:

- First approach is attractive when the technology is novel and/or the analysis is technically challenging and non-trivial
- The second approach is best if the principal contribution is a new attack method or synthesis over a set of technologies

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.)

Communication

- Process does not stop with the end of the "research"
- Communicating these types of results in an appropriate way is challenging and critical
  - Example undesirable case scenario: Media hypes these results, current and future patients become alarmed
  - Example undesirable scenario: Industry, FDA, and medical device community ignore results

Dealing with Media

- Three basic approaches:
  - Do nothing
  - Contact media, with a lot of hype
  - Contact media, shape, and undersell the story
- Other variants do exist

Media: Do Nothing

- Reasons for: Potential to avoid hype
- Reason against: Hard to control story
  - Possible for the story to take on a life of its own, become very sensational, and end up carrying a lot of misinformation
- Reason against: May not encourage action by industry and FDA

Media: Contact with Hype

- Reasons for: Gets story out, encourages action by industry and FDA
- Reasons against: Disproportionate hype for security issues can be bad for everyone (for patients, for the community, for those trying to address the problems)

Media: Contact Media, Undersell

- Reasons for: Preempt possible hype from uncontrolled media frenzy; story becomes more balanced
- Reason against: The story will receive some exposure

- We took this approach

Our Media Approach

We contacted respected media outlets prior to the paper being published

- Emphasized that these are life saving devices and that patients should not be concerned (risks today are low)
- Emphasized that we conducted our research to understand and address the potential risks with future version of the technologies, which will be more sophisticated

We also

- Prepared a FAQ so that anyone looking for further information on the Internet would see the above important points
- Given the medical context, we avoided "sensational" terms like "hacker", "attacker", "adversary", and "malicious"

Talking with Industry and FDA

Understanding and addressing risks requires concerted effort from all relevant stakeholders

- Security researchers
- Industry
- FDA
- Patients

Important to follow-through and talk with industry and government

Toy Robots

- Increasing computation in children's toys, and toy robots

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.)

Why Robots?

Future (Household) Robots

Future (Household) Robots

Future (Household) Robots

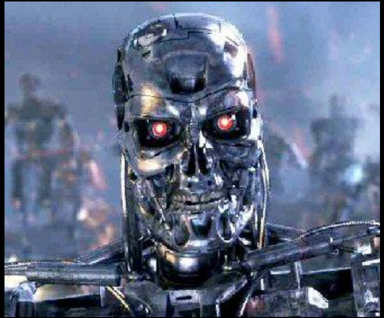
Future (Household) Robots

Future (Household) Robots

Risks with Robots

- Safety and protection against accidents (e.g., industrial settings)
- Robots become too smart: Popular topic of science fiction





- But what about malicious people controlling robots?
  - Not focus of research community
  - What about industry?
  - Are there unique challenges?

First Step: Problem Selection

Good if the technology has these properties:

- High impact technology
- Lots of rapid, on-going innovation
- Unique interactions with users; unknown or unique constraints
- Something to learn from the analyses
- Security risks are potentially significant
- Security for these technologies not currently within focus of the security community nor the technology's "home" community: New problems/directions for both communities

Also desirable:

- Early in evolutionary lifecycle: Security considerations would be proactive, rather than reactive

Second Step: Identify Approach

Approaches:

- Deep, thorough analysis of one representative artifact
- Broad analysis of a collection of representative artifacts

Practical constraints may affect choice:

- First approach is attractive when the technology is novel and/or the analysis is technically challenging and non-trivial
- The second approach is best if the principal contribution is a new attack method or synthesis over a set of technologies

Toy Robots

- Increasing computation in children's toys, and toy robots
- Question: What are their security weaknesses?
- Approach: Experimentally analyze three leading examples (at the time)

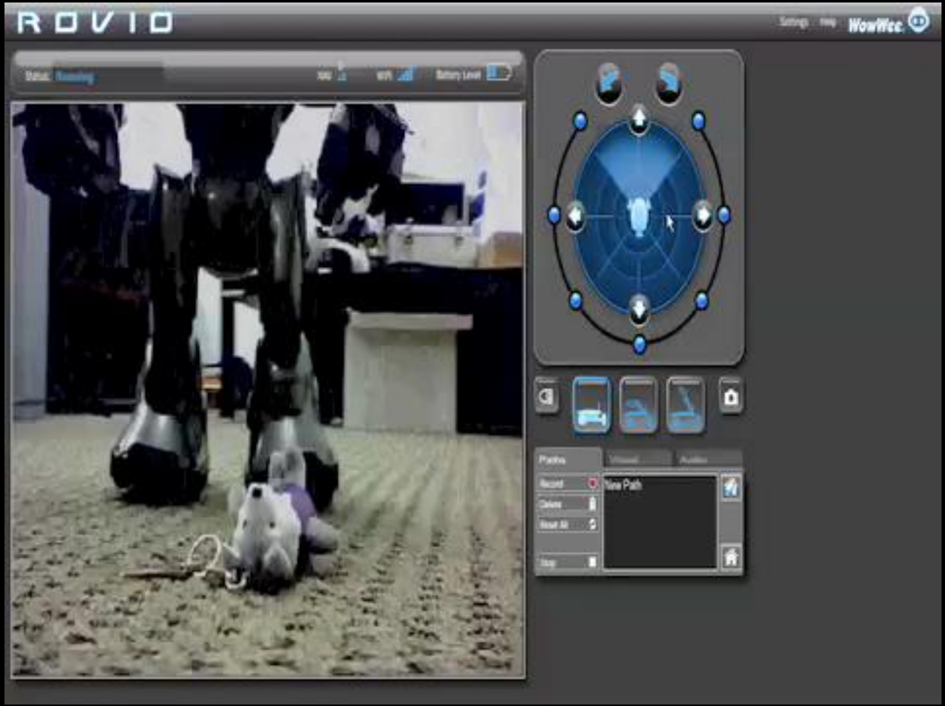
T. Denning, et al. "A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons." International Conference on Ubiquitous Computing, 2009. (University of Washington.)

Toy Robots

- Increasing computation in children's toys, and toy robots
- Question: What are their security weaknesses?
- Approach: Experimentally analyze three leading examples (at the time)
- Example findings: (1) "Easy" for unauthorized party to remotely access and control these toys; (2) seeing commonalities and differences is valuable; (3) novel multi-robot attacks

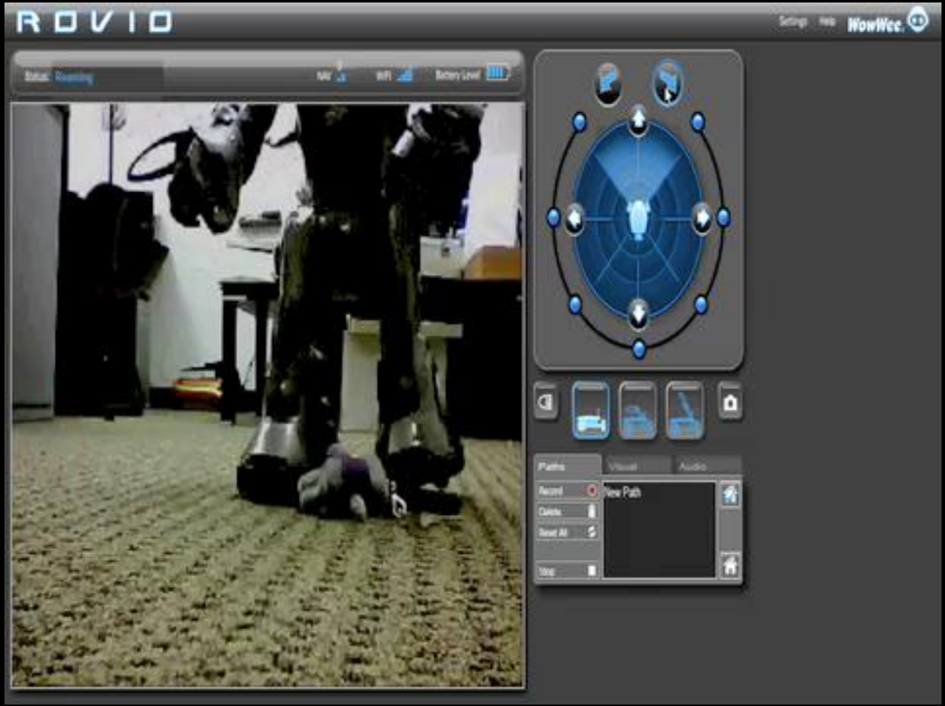
T. Denning, et al. "A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons." International Conference on Ubiquitous Computing, 2009. (University of Washington.)

Multi-robot Attack



What one robot can’t do, two can
RoboSapien v2: “high” dexterity grippers
Rovio/Spykee: video camera

Multi-robot Attack



Not easy today

But clear: In future need to consider interaction between multiple “hacked” devices

Reflections

Standard best practices can significantly improve security

Challenges remain for securing robots in the home:

- Tensions between goals, e.g., minimal interfaces and security
- Robots can move and/or effect environment
- Multi-device interactions
- No dedicated, trained admin; who is the “user?”
- Diverse collection of stakeholders (adults, children, elderly, pets, house guests)

Broader context:

- Policy
- Consumer education

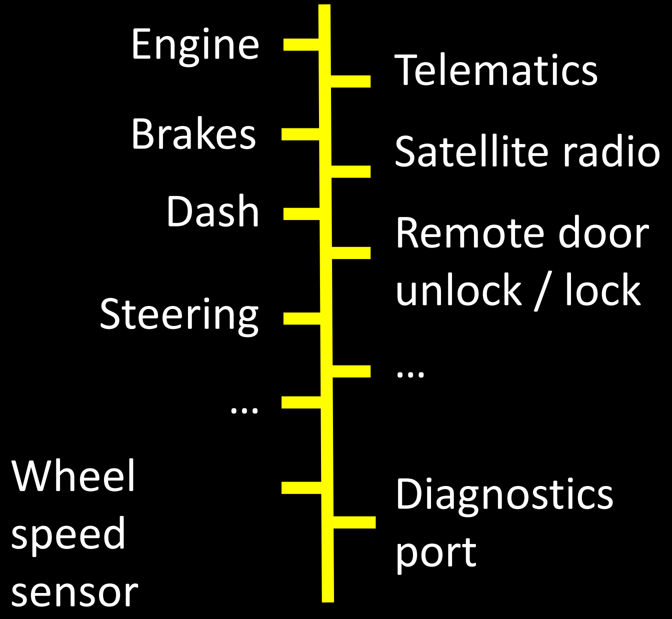
Communication

- Published at UbiComp
  - That community innovating rapidly in household, ubiquitous technologies
  - Minimize risk with next-generation consumer devices
- FAQ, with recommendations for owners

Communication

- Published at UbiComp
  - That community innovating rapidly in household, ubiquitous technologies
  - Minimize risk with next-generation consumer devices
- FAQ, with recommendations for owners
- BUT:
  - Maybe too early
  - Follow-through is important

Modern Cars



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

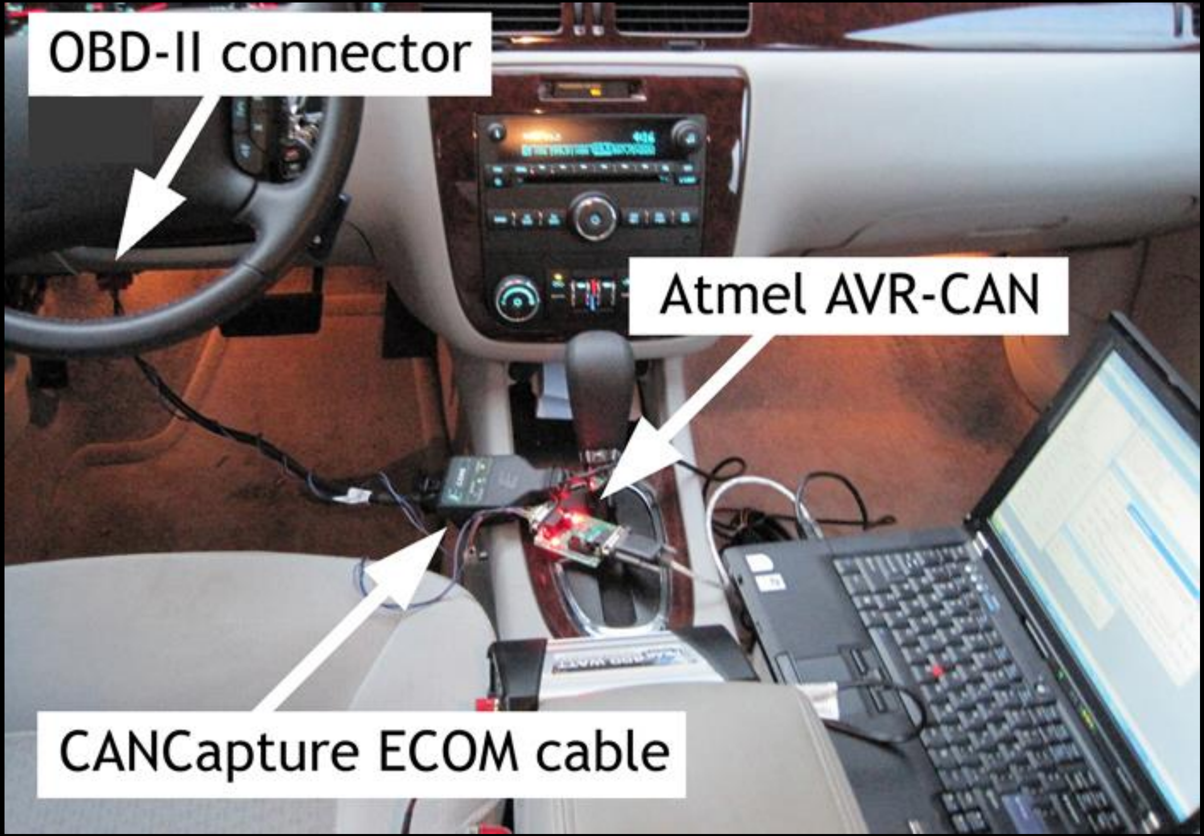
Example automotive computer network

Approach

Bought two, 2009-edition modern sedans

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

Experimental Setup



Findings

Arbitrary control over the dash: 140mph, while in park

Findings

Ability to affect:

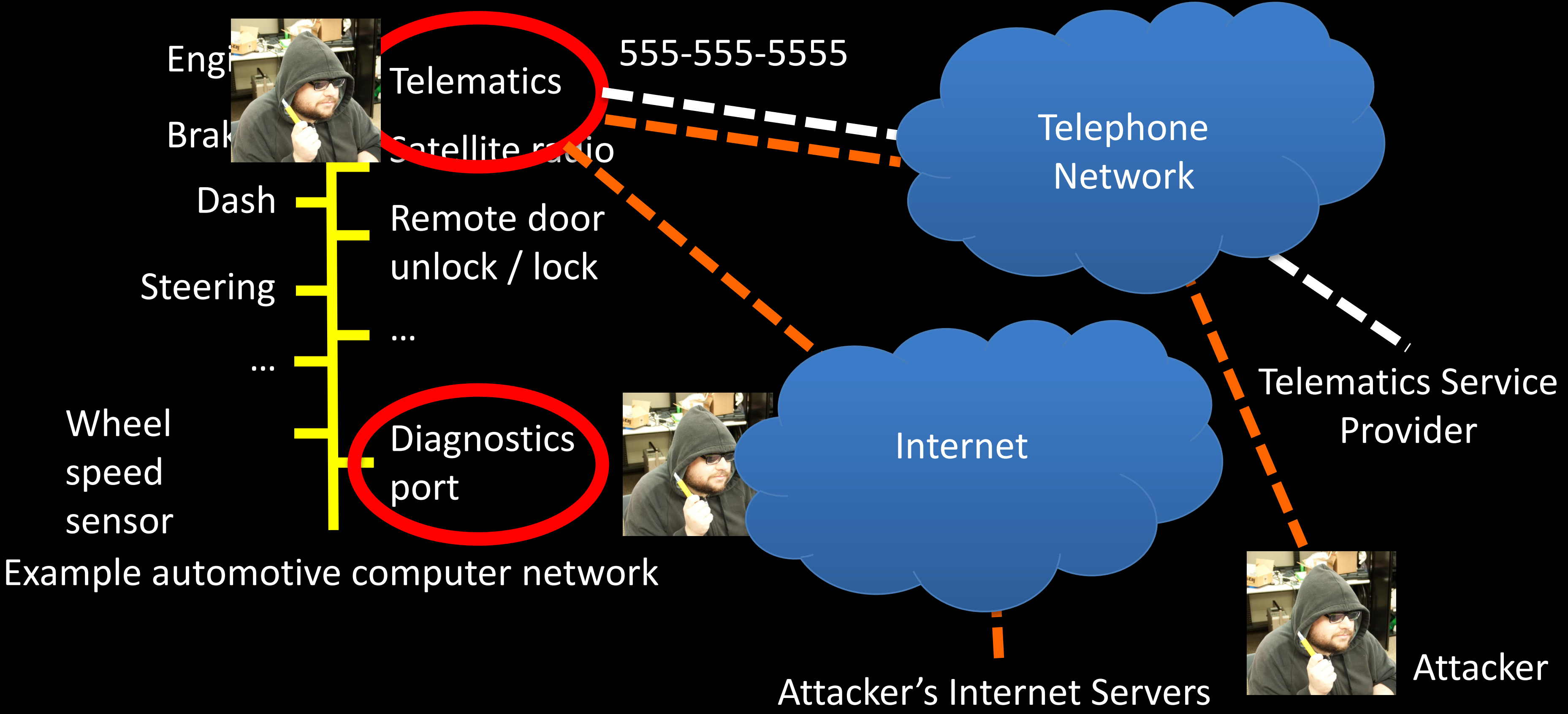
- Dash
- Lighting
- Engine
- Transmission
- Brakes
- HVAC
- …

Arbitrary control over the dash: 140mph, while in park

Road Test: Apply Brakes

Road Test: Disengaging Brakes

Non-contact Threats?



End-to-end Surveillance Example

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

Communication

- Early notification of results to the manufacturer and the government
- Significant follow-on interactions with key stakeholders
- Direct and indirect impact
  - SAE creates task force on automotive computer security
  - DARPA invests $60M to improve security for vehicles
  - NHTSA develops cyber security testing laboratory
  - Significant automotive industry hiring in computer security
  - Growing body of subsequent research efforts

Summary

- Overall goal: Improve security of future technologies
- Experimentally analyze real artifacts
  - Provides informed understanding of the risks
  - Provides understanding of technical challenges to defenses
  - Helps raise awareness among consumers, designers, researchers, and policy makers
- Building defenses, human studies, measurement studies are all critical too!
- Computers are pervasive in consumer devices—not just laptops, desktops, and the Web

Thanks!

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

Toy computer security (UW)

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

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