ECE 547/647: Security Engineering

Lesson 4: Case Study: Automotive Security

Rationale

- Automobiles are a familiar cyber-physical system
- This NSF-funded research work in a prestigious IEEE/ACM conference resulted in significant changes in the automobile industry to address security concerns not before addressed.
- This example illustrates how a complex system can be compromised using a wide variety of techniques and vulnerabilities.
- It shows how the 6 C's and the fallacies from earlier lectures apply to a real system.
- It raises questions about threat models, cost functions, and defense.

Objectives

- Learn enough about automobile systems to understand the cyber risks and tradeoffs
- Extend these ideas to other systems
- Understand the tensions that an industry must confront to manage security

Prior Learning

- Let’s Review from Lesson 3: Foundations of Security
  - Random bit generation
  - Secure hash functions
  - Blockciphers
  - Advanced Encryption Standard (AES)
  - Identification and authentication – Passwords and Protocols

Pre-Work

- Review the paper for references to crypto technologies and how they are used or mis-used.

Comprehensive Experimental Analyses of Automotive Attack Surfaces

*"To be clear, for every vulnerability we demonstrate, we are able to obtain **complete control** over the vehicle's systems."*

Checkoway, S., et. al. (2011, August)

- Why this paper?
  - Presents a wide range of vulnerabilities in a very familiar system
  - Shows convincing experiments

Automotive IT Svstems

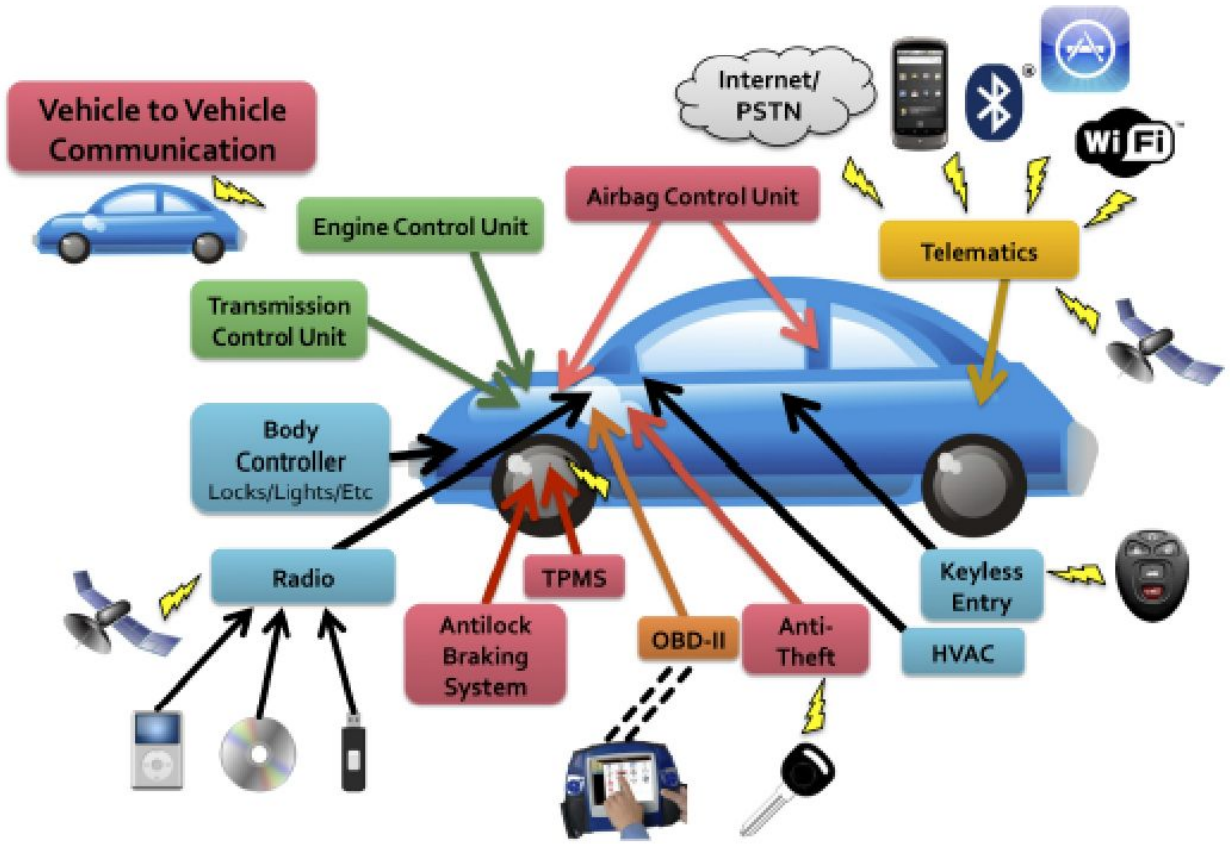

Figure 1: *Digital I/O channels appearing on a modern car.* Colors indicate rough grouping of ECUs by function.

Review paper. Display PDF.

Show how to read a technical paper.

- Survey
- Question
- Read
- Recite
- Review

Enemies of Security: “6 C’s” (cont’d)

- Convenience
  - Weak passwords
  - Unlocked doors, unencrypted data
  - Out-of-date software
- Complexity
  - Hard to validate. Backdoors left open.
- Connectivity
  - More attack vectors. Larger attack “surface”

Some examples for SSD paper…

- Convenience – Weak Passwords, Password Management,
- Complexity – Unnecessary features,
- Consolidation – Mis-use of standards, Credential Management,
- Connectivity – HW/SW, Firmware, Interfaces,
- Complexity – pin layouts

Enemies of Security: “6 C’s”

- Consolidation
  - All-in-one solutions (Swiss army knives)
- Cost
  - Cost-cutting often compromises security.
  - Naïve security design can increase cost and gain nothing
- Complacency
  - What, me worry?

Hitachi “Car Information System Solution”

Vulnerabilities in Cars Resulting in Full Control

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost	Section
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low	Prior work [14]
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium	Section 4.2
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High	Section 4.2
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low	Section 4.2
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low	Section 4.2
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium	Section 4.3
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium	Section 4.3
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High	Section 4.4
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High	Section 4.4

Results of Attack?

- Theft (old school)
- Sabotage (hit-man)
- Tracking (organized crime or big-brother?)
- On-line market of vulnerability information
  - mirrors the evolution of desktop computer compromises: from individual attacks, to mass exploitation via worms and viruses, to third-party markets selling compromised hosts as a service.

Why Were the Vehicles So Vulnerable?

- Unsecured external interfaces
- Interfaces in code
- Outsourced Software
- Weak code base
- Extraneous code

Activity:

Discuss automotive security metrics. Consider how much you should pay for a particular security product?

What other systems can we extend this to?
Smart-home, phone, airplane,… what is same what is different?

Conclusions from Part 1 of the Course

- Motivations and Examples for Secure Systems
- Foundations of Security
- Terminology
- Myths
- Measuring and Standards for Security
- Case Study: Automotive IT Security
- Case Study: SSD Encryption

Plan for next Meeting

- Before next class, read:
  - Password Similarity Models using Neural Networks
  - **True2F: Backdoor-resistant authentication tokens**
  - Optional Anderson textbook, Chapter 2 – Human Factors