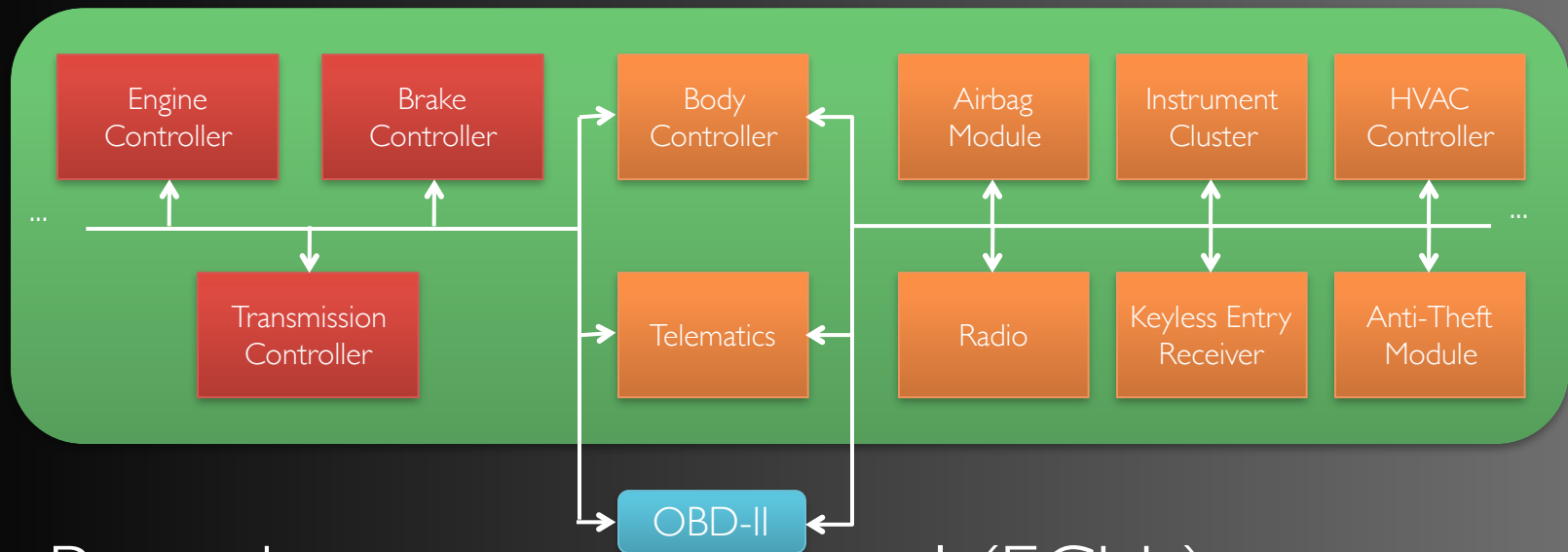


Stephen Checkoway, Damon McCoy, Brian Kantor,
Danny Anderson, Hovav Shacham, Stefan Savage (**UCSD**)
Karl Koscher, Alexei Czeskis, Franziska Roesner,
Tadayoshi Kohno (**UW**)



Cars: a review



- Pervasive computer control (ECUs)
- ECU interconnections driven by safety, efficiency, and capability requirements

Oakland 2010, we showed...

- Safety-critical systems can be compromised
 - Selectively enable/disable brakes
 - Stop engine
 - Control lights
- Owning one ECU = total compromise
- ECUs can be reprogrammed (while driving!)

- Key question: Do we need physical access?

[Oakland'10] Koscher et al. Experimental Security Analysis of a Modern Automobile.

Outline

- Intro
- Synthesize attack surface
- Experimental attack evaluations
- Post-compromise control
- End-to-end evaluations
- Reflections and next steps

Threat model

- Attacker capabilities
 - Indirect physical access
 - Short-range wireless signals
 - Long-range wireless signals
- Attack surfaces: what *might* be attacked

Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device

Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device



Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device



Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device



Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device



Indirect physical

- Definition:
 - Attacks over physical interfaces
 - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to that of the device



Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)

Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)



Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)



Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)



Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)



Short-range wireless

- Definition: Attacks via short-range wireless communications (meters range or less)



Long-range wireless

- Definition: Attacks via long-range wireless communications (miles, global-scale)

Long-range wireless

- Definition: Attacks via long-range wireless communications (miles, global-scale)



Long-range wireless

- Definition: Attacks via long-range wireless communications (miles, global-scale)



Outline

- Intro
- Synthesize attack surface
- Experimental attack evaluations
- Post-compromise control
- End-to-end evaluations
- Reflections and next steps

Attack surfaces explored in depth

- Components we compromised
 - Indirect physical: diagnostic tool
 - Indirect physical: media player
 - Short-range wireless: Bluetooth
 - Long-range wireless: cellular
- ***Every attack vector leads to complete car compromise***

Overall methodology

- Extract device's firmware
 - Read memory out over the CAN bus (CarShark)
 - Desolder flash memory chips in ECUs
- Reverse engineer firmware
 - IDA Pro
 - Custom tools
- Identify and test vulnerable code paths
- Weaponize exploits

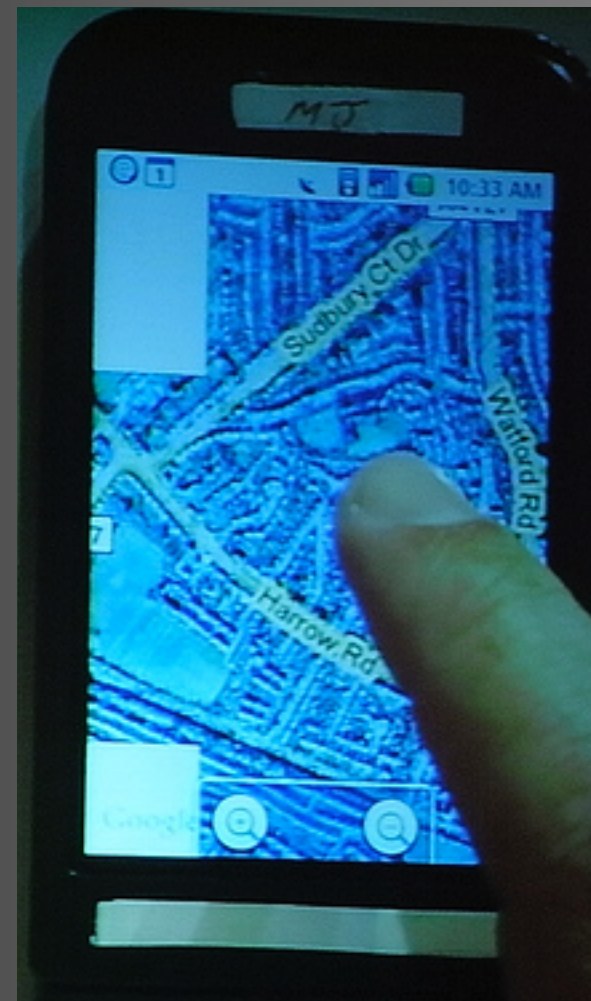


Indirect physical: Media player attack

- Code for ISO-9660 leads to
 - Attack 1: Vestigial radio reflash from CD code
 - Attack 2: WMA parsing bug; tricky overflow
- Karl writes an on-radio debugger in a night!
- Insert CD containing malicious WMA file
- Completely compromise car

Short-range wireless: Bluetooth attack

- Common embedded Bluetooth stack on telematics unit
 - strcpy() bug
- 1. Malicious, paired device can compromise telematics ECU
 - Android trojan
- 2. Can undetectably pair a device
 - USRP software radio
 - Brute force PIN

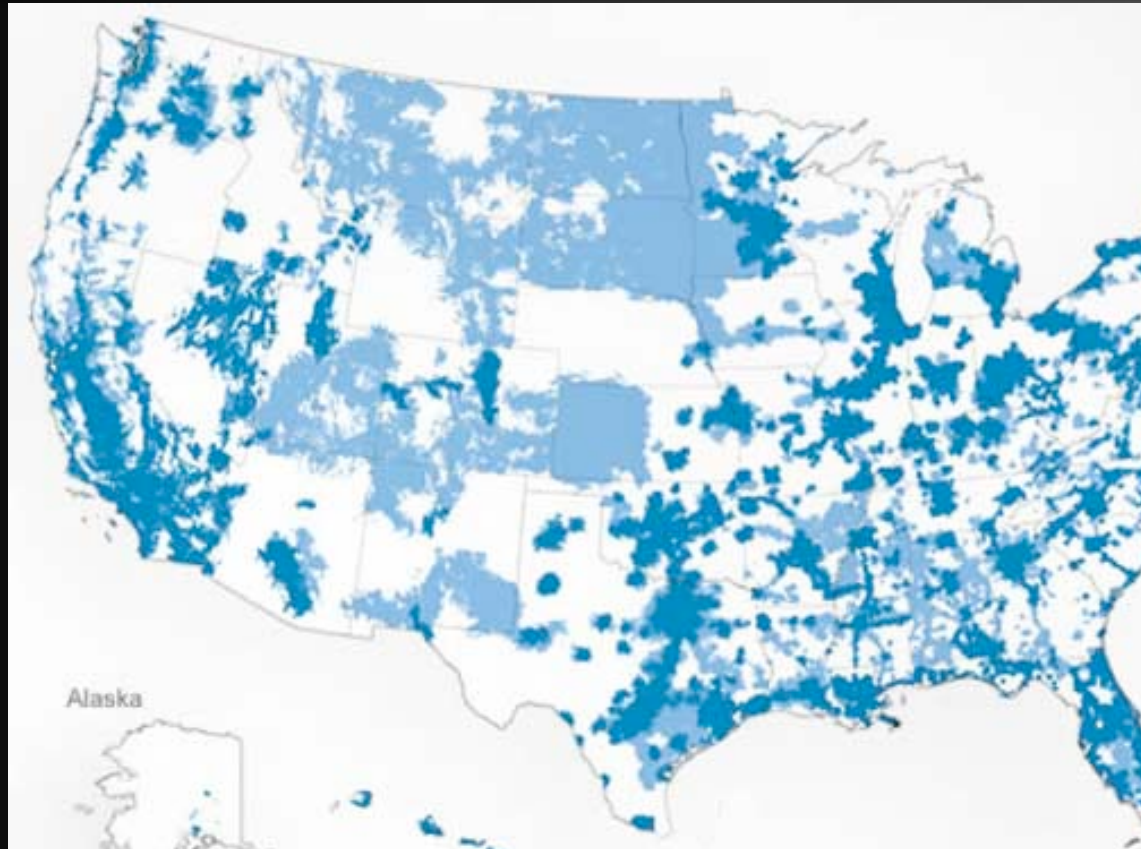


Long-range wireless: Cellular attack

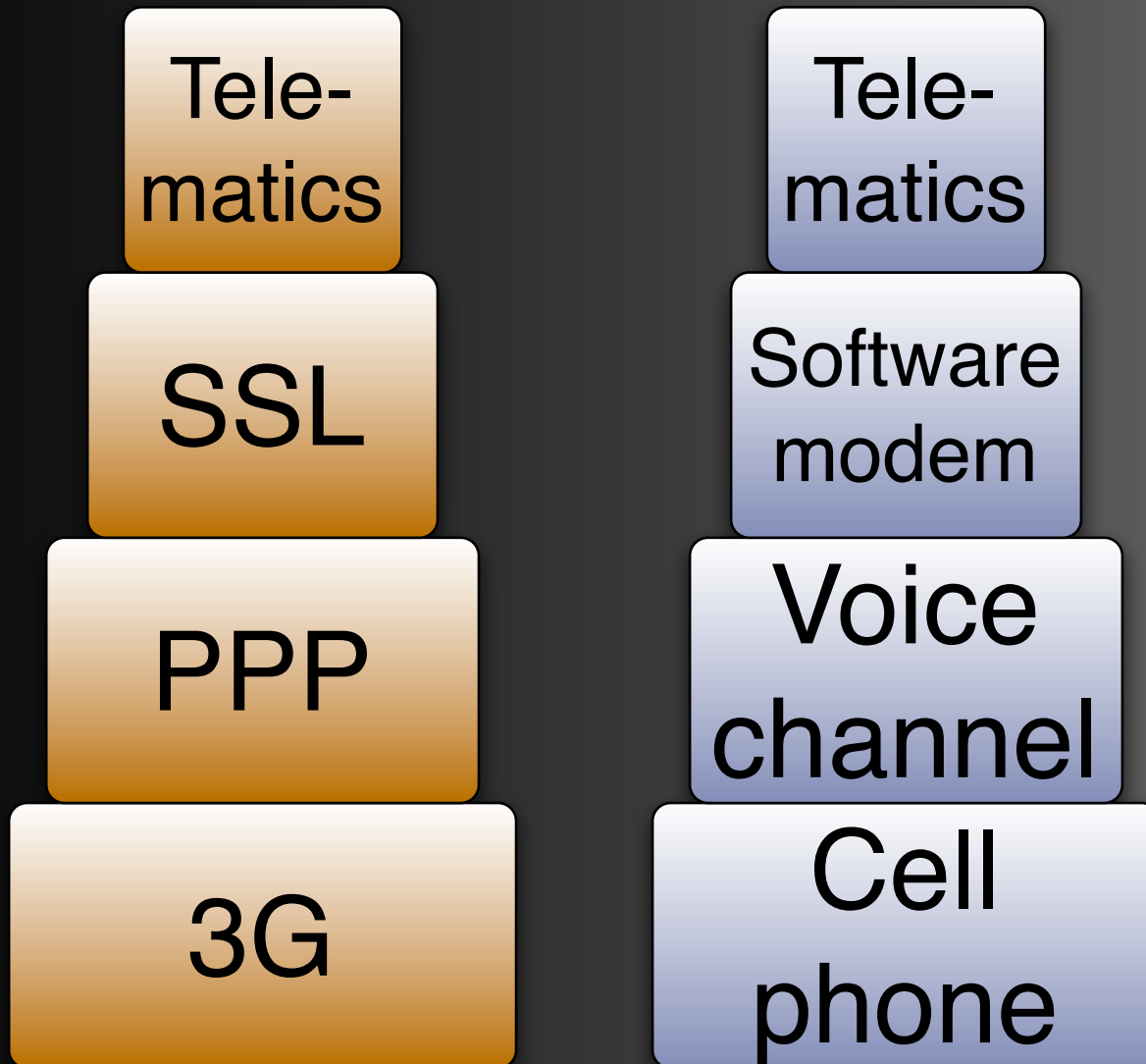
Long-range wireless: Cellular attack



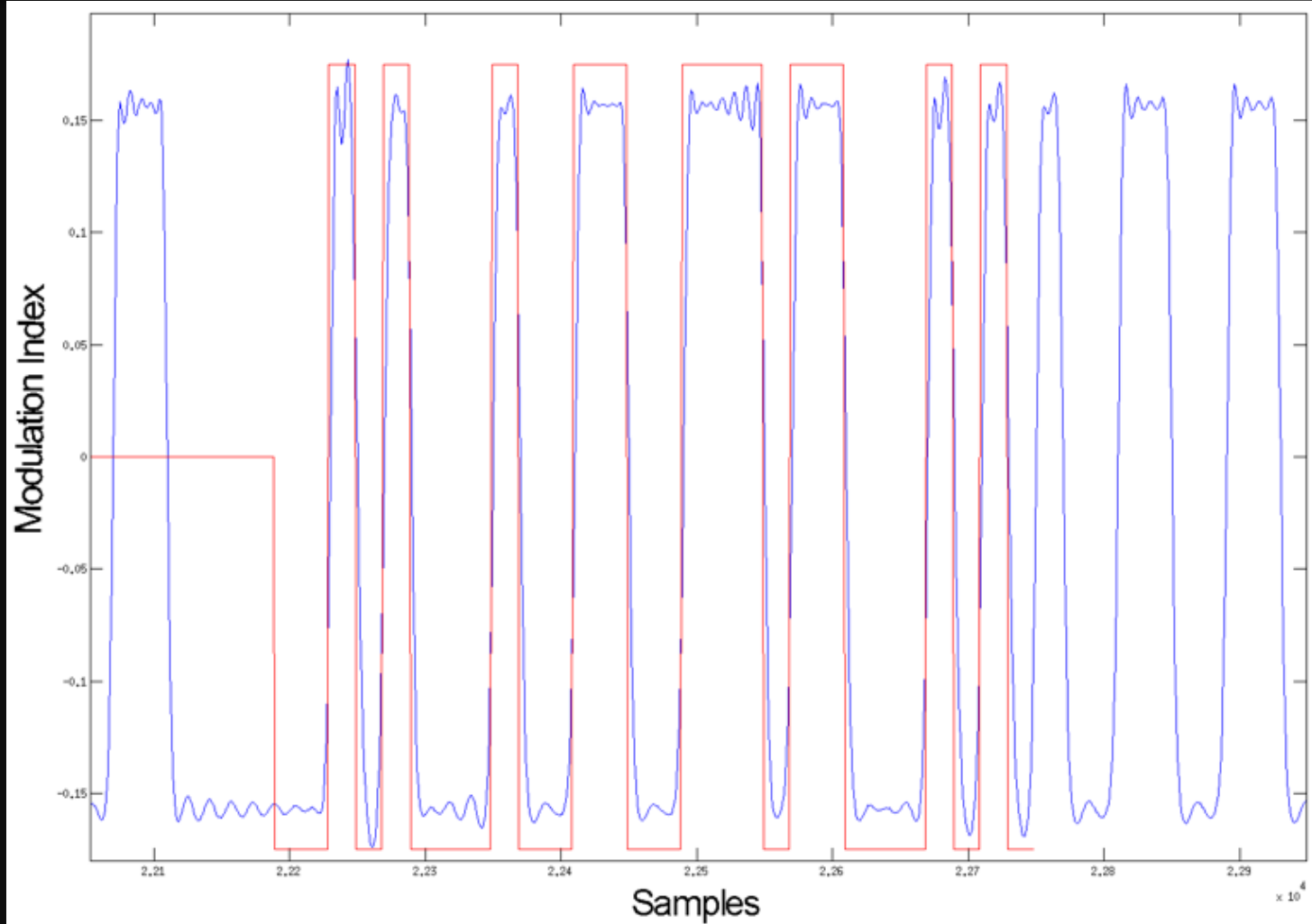
Long-range wireless: Cellular attack



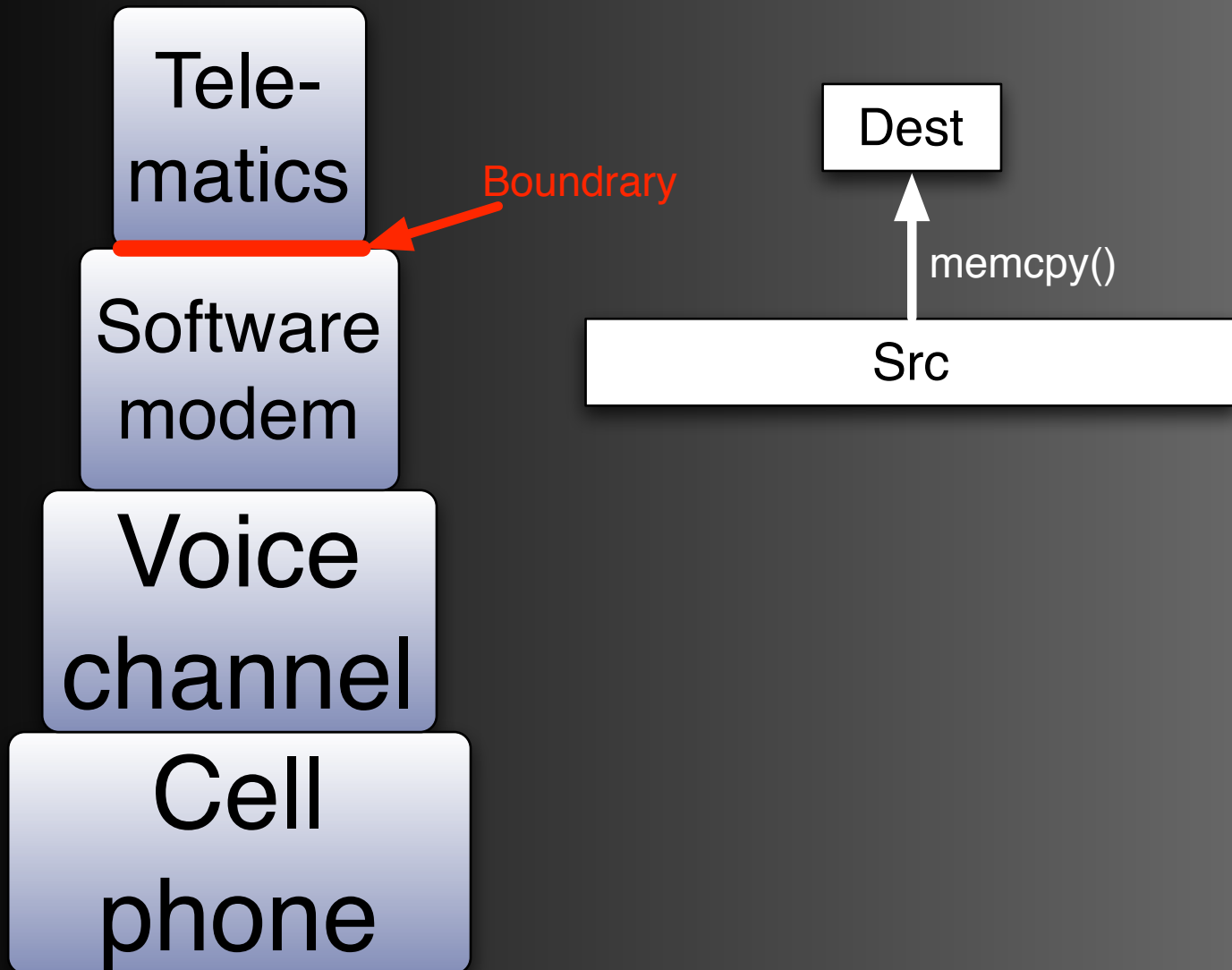
Long-range wireless: Cellular attack



Long-range wireless: Cellular attack



Long-range wireless: Cellular attack



Long-range wireless: Cellular attack

- Call telematics unit
- Transmit malicious payload
 - Instantiation 1. Implement modem protocol
 - Instantiation 2. Play MP3 into phone



Outline

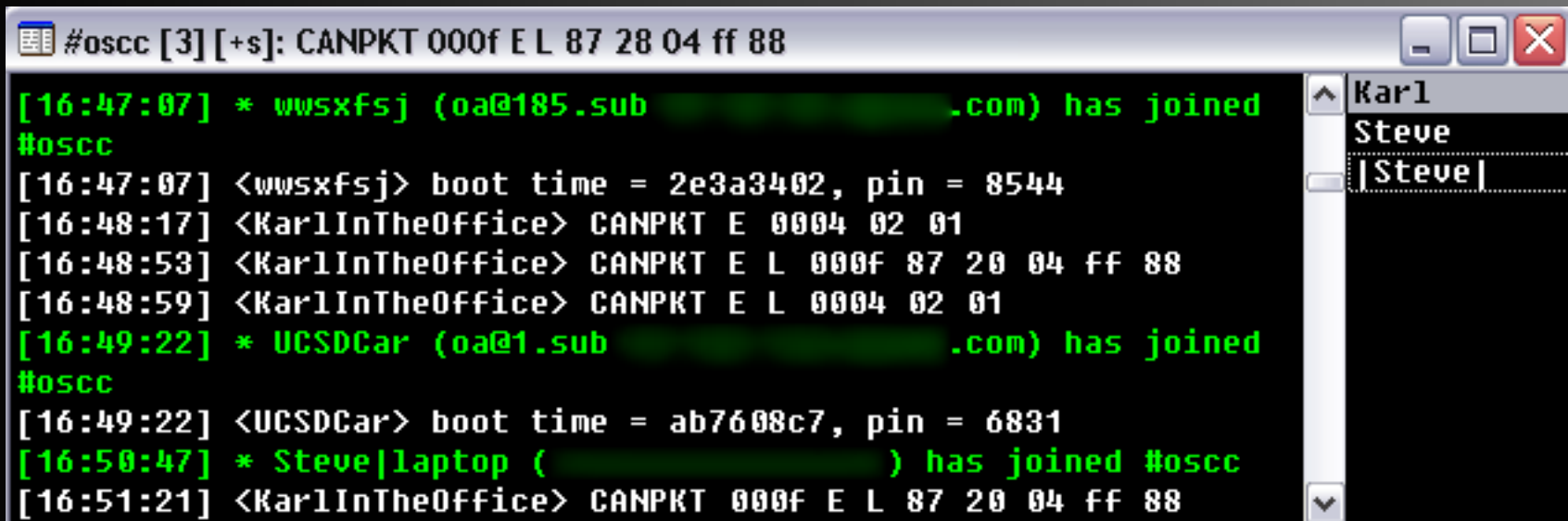
- Intro
- Synthesize attack surface
- Experimental attack evaluations
- **Post-compromise control**
- End-to-end evaluations
- Reflections and next steps

Post-compromise control

- Wireless channels are game-changers
- Remotely trigger code from prior compromise
 - TPMS: proximity trigger
 - FM RDS: broadcast trigger
 - Bluetooth: short-range targeted trigger
 - Cellular: global targeted trigger
- We implemented all of these

Example: IRC over cellular

- Install IRC client on telematics unit
- Targeted/broadcast commands
- Download additional functionality



The screenshot shows an IRC chat window titled "#oscc [3] [+s]: CANPKT 000f E L 87 28 04 ff 88". The chat log contains the following messages:

```
[16:47:07] * wwsxfsj (oa@185.sub [REDACTED].com) has joined #oscc
[16:47:07] <wwsxfsj> boot time = 2e3a3402, pin = 8544
[16:48:17] <KarlInTheOffice> CANPKT E 0004 02 01
[16:48:53] <KarlInTheOffice> CANPKT E L 000F 87 20 04 ff 88
[16:48:59] <KarlInTheOffice> CANPKT E L 0004 02 01
[16:49:22] * UCSDCar (oa@1.sub [REDACTED].com) has joined #oscc
[16:49:22] <UCSDCar> boot time = ab7608c7, pin = 6831
[16:50:47] * Steve|laptop ([REDACTED]) has joined #oscc
[16:51:21] <KarlInTheOffice> CANPKT 000F E L 87 20 04 ff 88
```

On the right side of the window, a user list is visible with the following entries:

- Karl
- Steve
- [Steve]

```
* wwsxfsj (oa@185.sub [REDACTED].com) has joined
<wwsxfsj> boot time = 2e3a3402, pin = 8544
<KarlInTheOffice> CANPKT E 0004 02 01
<KarlInTheOffice> CANPKT E L 000f 87 20 04 ff 88
<KarlInTheOffice> CANPKT E L 0004 02 01
* UCSDCar (oa@1.sub [REDACTED].com) has joined
<UCSDCar> boot time = ab7608c7, pin = 6831
* Steve|laptop ([REDACTED]) has joined #oscc
<KarlInTheOffice> CANPKT 000f E L 87 20 04 ff 88
```

Outline

- Intro
- Synthesize attack surface
- Experimental attack evaluations
- Post-compromise control
- End-to-end evaluations
- Reflections and next steps

Car theft

- Compromise car
- Locate car (via GPS)
- Unlock doors
- Start engine
- Bypass anti-theft





Surveillance

- Compromise car
- Continuously report GPS coordinates
 - Twitter-like service
- Stream audio recorded from the in-cabin mic
 - Detect voice (VAD)
 - Compress audio
 - Stream to remote computer





Outline

- Intro
- Synthesize attack surface
- Experimental attack evaluations
- Post-compromise control
- End-to-end evaluations
- Reflections and next steps

Stepping back: Why?

- Lack of adversarial pressure to date
 - Code rife with “old” vulnerabilities, e.g., strcpy()
- Heterogeneous, distributed, multi-vendor system
 - Internals of components frequently opaque
 - Incorrect assumptions between different suppliers
 - Almost all bugs found at component boundaries

Where to go from here?

- Stakeholders responding today:
SAE, USCAR, US DOT
- Short term: lessons from the PC world
 - Cheap software update
 - W^X (a.k.a. DEP)
 - ASLR
 - Stack cookies
 - Static analysis
 - Limit ECU communication
 - No inbound calls
 - Restrict internet connections
 - Remove unnecessary binaries
e.g., ftp/telnet/nc/vi

Where to go from here?

- Long term – more challenging
- Constraints
 - Low margins
 - Complex business model
 - Which are hard; which can be relaxed?
- Safety most important
 - Fail stop vs. fail safe

Summary

- Current autos have broad (and increasing) external attack surface
- We demonstrated real attacks that compromised safety-critical systems
- Industry and government are responding





Thank You
www.autosec.org
P R N D 3 2 1