Sandboxing Wireless/RF Vulnerability Research of Connected Systems

Michael Calabro
5 October 2016
33rd Annual International Test and Evaluation Symposium

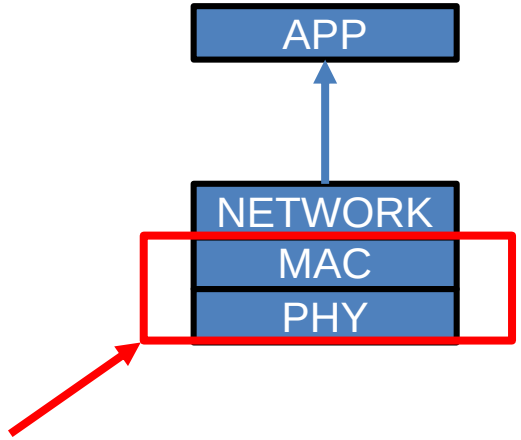
DARK LABS
Booz | Allen | Hamilton

Outline

- What is Wireless
- Motivating Wireless Security in a Connected World
- Automotive Overview & Cellular Deep Dive
- Conclusions

What is Wireless?

- Talking to a remote receiver
- Listening to a remote transmitter
- Wireless technologies are layer 1 and layer 2 technologies*

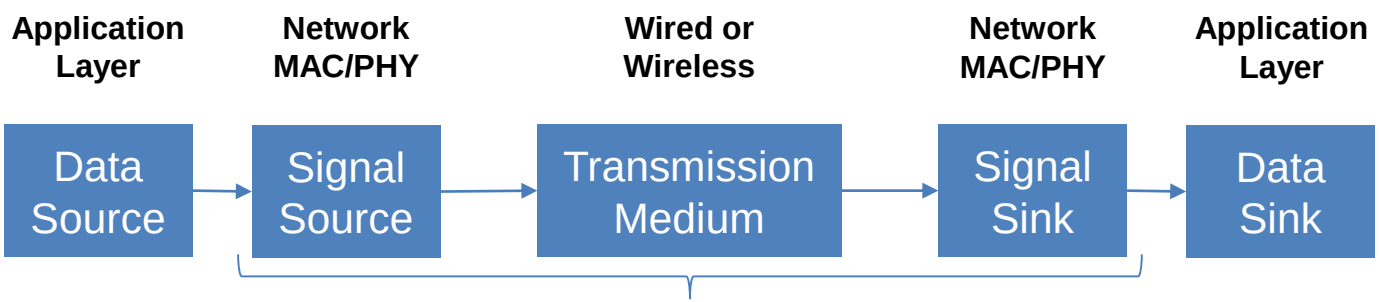


Wireless technologies enable communication over distance (modulation, coding, antennas) and solve fundamental interference challenges (near-far, resource scheduling)

***Some wireless signals are measured – e.g. GPS**

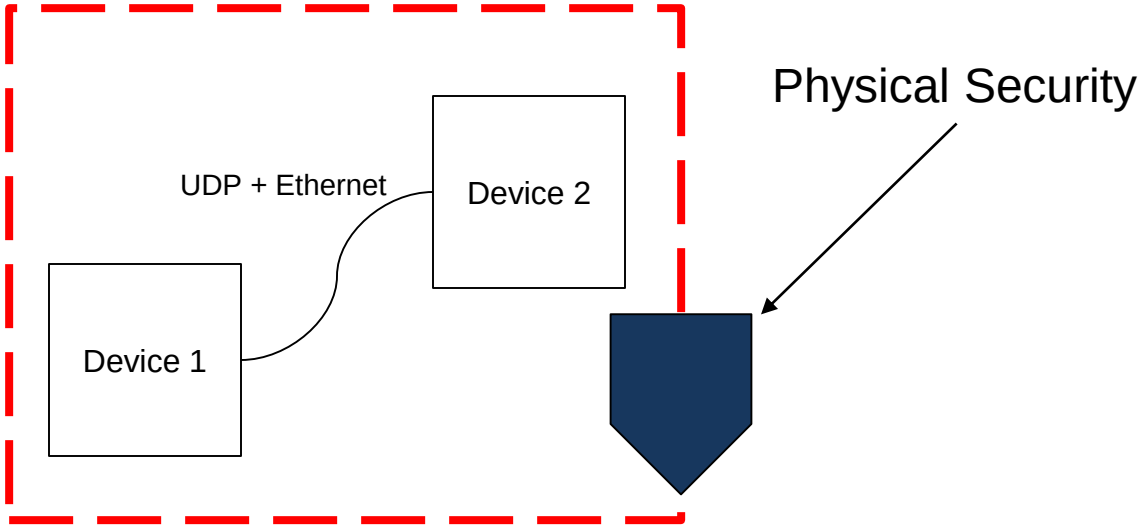
Motivating Wireless Attacks on Connected Platforms

- Wireless and wired interfaces are very similar
  - After the PHY/MAC layers, little or no difference in how data is processed
  - Same types of vulnerabilities are exploited (lack of authentication, weak encryption, plaintext PII)
  - Wireless attacks can be much harder to attribute and can have large payoffs
    - Standoff distance measured in 10s of ft to hundreds of miles
    - Specialized knowledge in RF engineering and Signal Processing can result in attack vectors far exceeding typical commercial wireless specifications (e.g. 1 mile Wi-Fi, city-wide PII collections, etc)



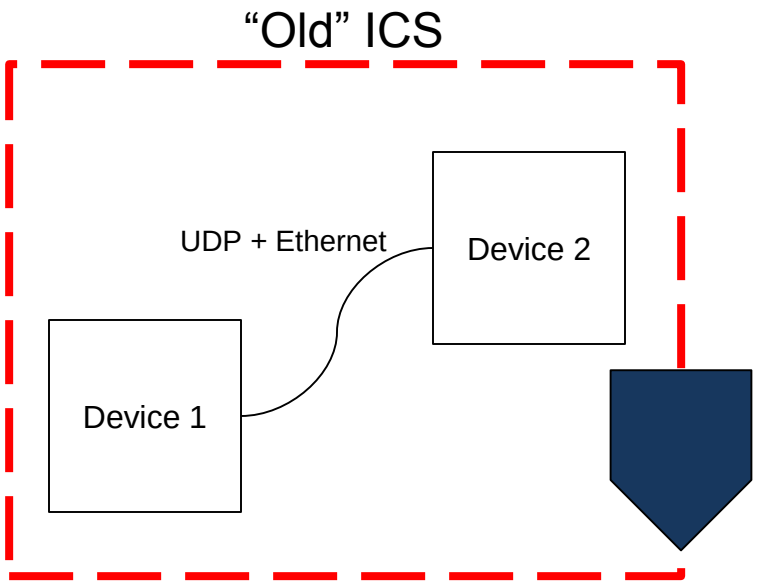
Applicability of Wireless Technologies

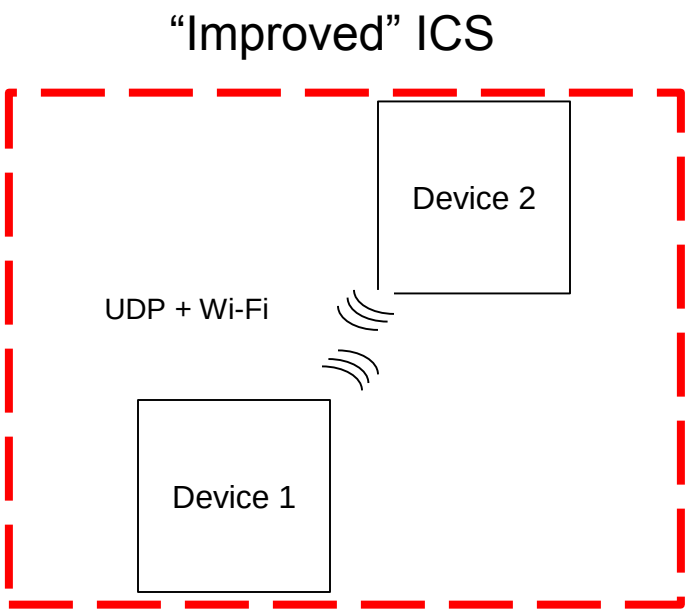
Two ICS Devices Exchange Data Packets via Ethernet…



10 years later…Ethernet is replaced with Wi-Fi

ICS protocol is still UDP-based





Spoofed Access Point; Effective Range Determined by **Link Equation**

RF-Cyber Range is Determined by the Link Equation

$$\frac{P_r}{N_0} = P_t + G_T + G_r - 20\log_{10}\frac{4\pi r}{c} - kT - X$$

$$\frac{E_b}{N_0} = \frac{P_r}{N_0} - R_b$$

+10 dBm/Hz — **May not be safe to exceed**

-10 dBm/Hz

Desired Signal Level

-85 dBm/Hz — **Below ADC Sensitivity**

-174.4 dBm/Hz — **Thermal Noise Floor**

	Parameter	How to Improve
P_t	Transmitted Power [dBW]	More amps
G_t	Transmit Antenna Gain [dB]	Improve Antenna
G_r	Receive Antenna Gain [dB]	
r	Distance from Tx to Rx	Move closer
k	Boltzmann's Constant [-228.6 dB J/K]	Physical Constants
c	Speed of Light (in RF medium)	
T	System Noise Temperature [K]	Add LNAs, Lower noise components
R_b	Bit Rate	Typically fixed
E_b	Energy Per Bit	
X	Atmospheric Noise; Atmospheric Loss; Non-Gaussian Noise Sources	

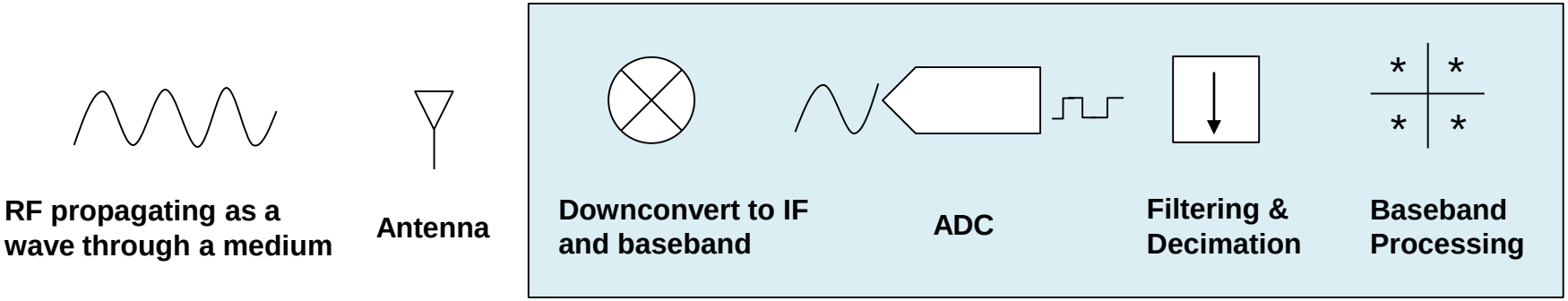
d ↔ Target

↔ Clever RF ↔ n*d ↔ Target

Wireless Attack Surfaces Are Common in the World…

How do we fuzz them?

Commercial Standards are Well-Supported by Current Open-Source SDR Frameworks



SDR has Made Fuzzing of Commercial Wireless Technologies Accessible

Cellular Technologies & Wi-Fi
Cyber-Goals: Remote data access / exploitation, passive characterization
Common Attacks: Infrastructure spoofing, data MITMs, protocol replays
Common Tools: OpenBTS, OpenEPC, mid-end SDRs (e.g. USRP)

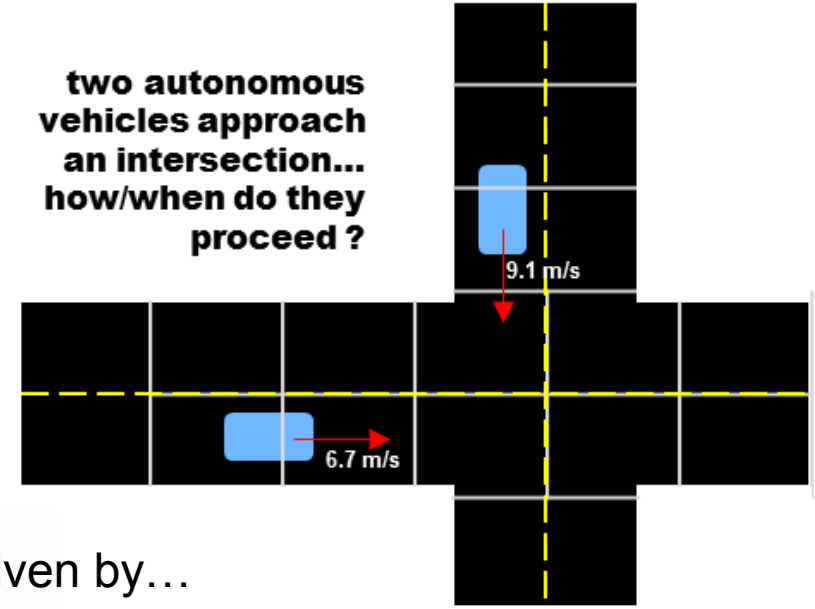
GPS L1
Cyber-Goals: Disruption or manipulation of system time or position
Common Attacks: Jamming L1; Record/Replay
Common Tools: GPS Simulators; OpenGNSS; mid-end SDRs (e.g. USRP)

RF Sensor Interfaces
Cyber-Goals: Remote vehicle access / exploitation, passive characterization
Common Attacks: Passive collection, Protocol Replay, Data Injection
Common Tools: low/mid-end SDRs (e.g. USRP), RF up or downconverters (to get to X-band) or other frequencies not common to commercial signals

The Automotive Industry is an Example of a Connected Industry with a Growing Wireless Attack Surface

The Automotive Industry is in a Period of Evolution

The automotive industry has been composed of disparate technologies, with significant technical differences between vehicle platforms and infrastructure



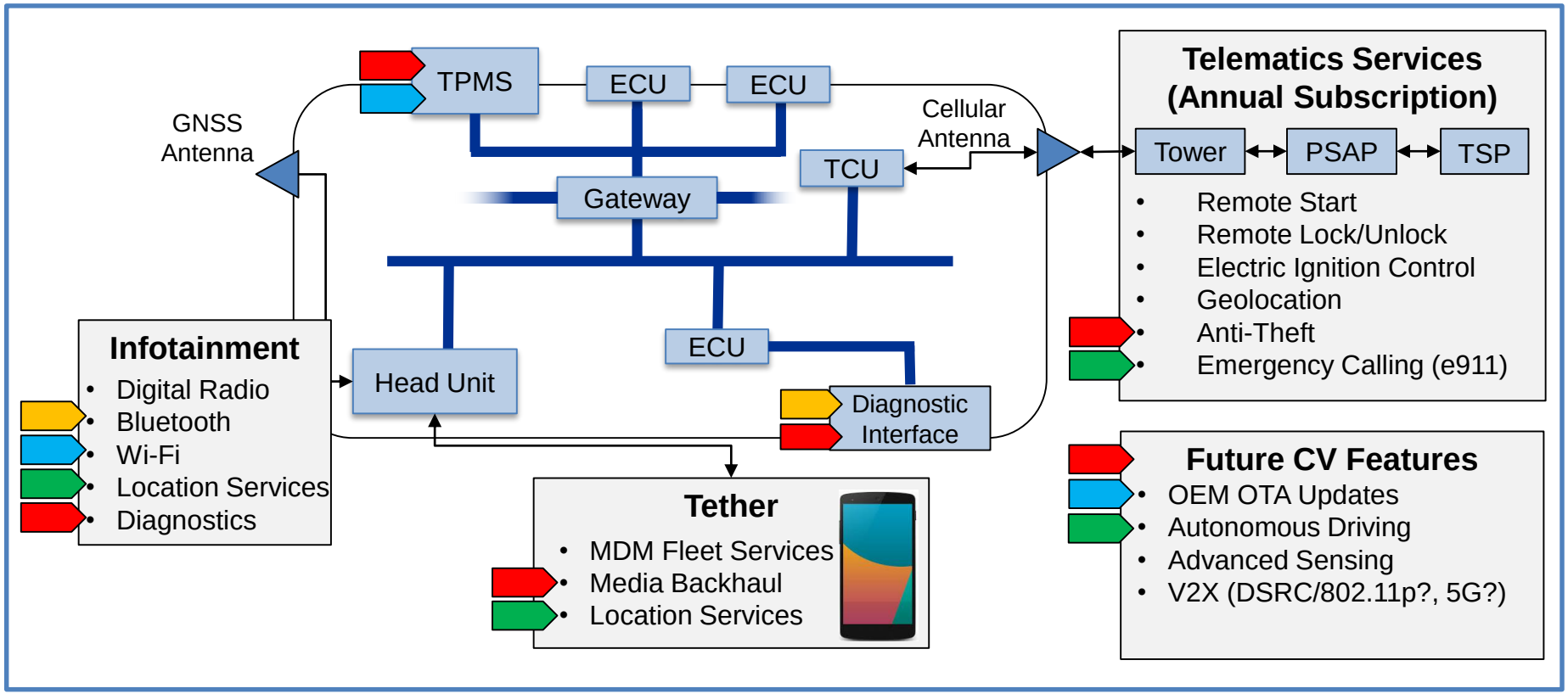
Automotive technology convergence is being driven by…

- V2X Communications
- Autonomous Technologies
- Automotive Cyber Security
- Infotainment Services

Wireless Technologies are Key Enablers

Wireless Attack Surface on Connected Vehicles is Growing

Notional Connected Vehicle Platform Architecture

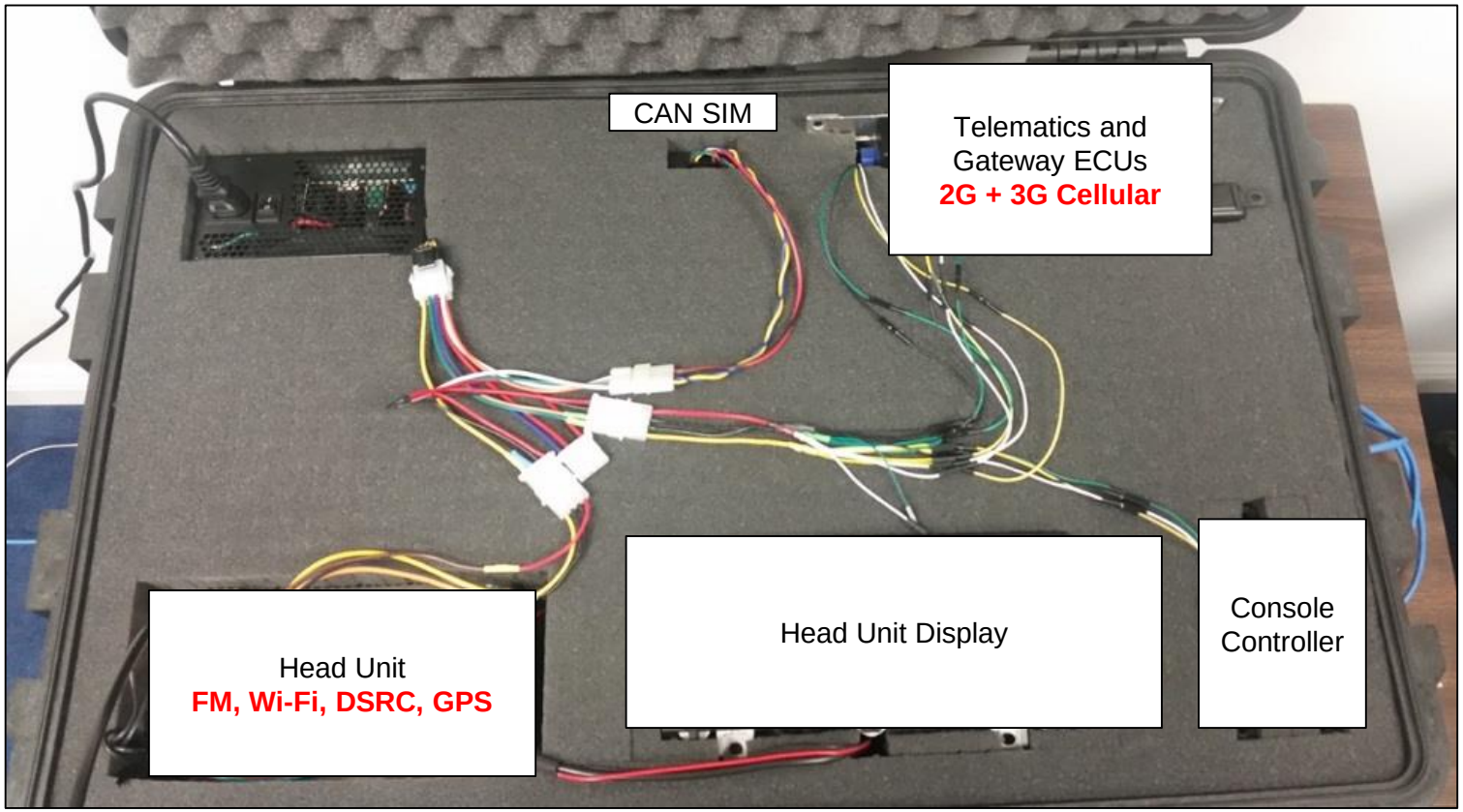


External Interface Classification

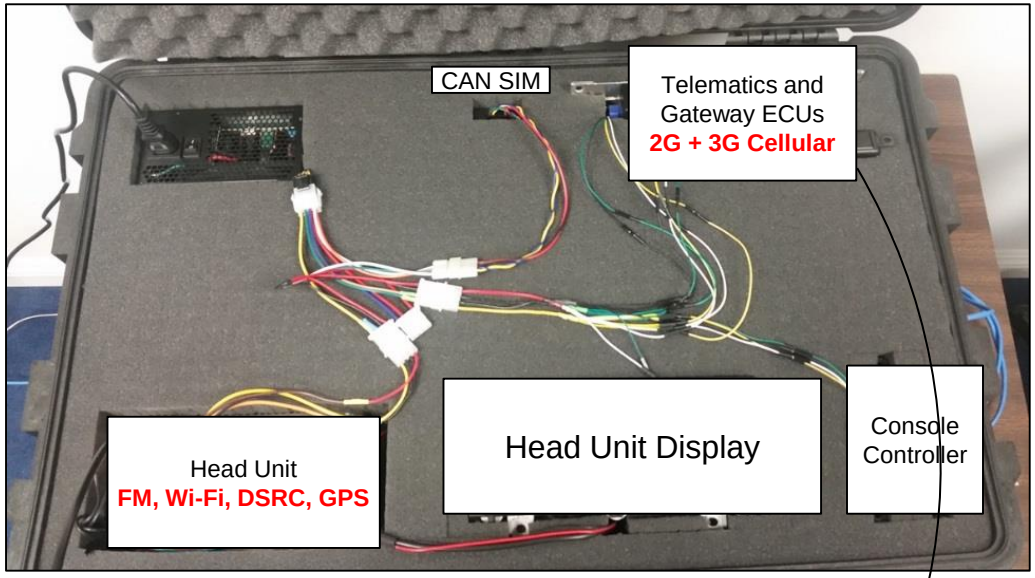
- Electromagnetic/RF
- Cyber-Physical
- Physical
- Network/IP-Based

Booz Allen Constructed an Automotive Security Testbed
"Car-in-a-Box"

2014 Top 10 Luxury Car
Cost of Vehicle: ~50k + Maintenance
Cost of Box: ~3k



Validated End-to-End Security Research on Testbed



1. Developed and Integrated Testbed

RF from Telematics ECU to SDR BTS

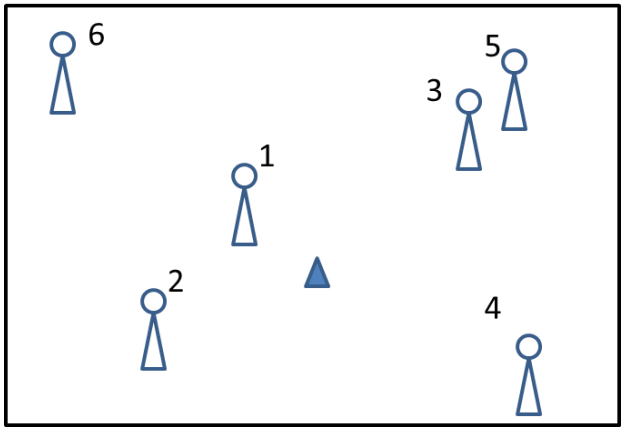
ETH to Fuzzing Machine

2. Spoofed BTS and Began Fuzzing

3. Validated Remote Access on Test Vehicle

GSM Cellular Reselection Deep Dive

Given following MS/BTS GSM network configuration…which cell tower will the MS camp or reselect to?



BTS = GSM Basestation
MS = GSM User Equipment (e.g. cell phone)

GSM cell selection by an MS is determined within MS based on an internally calculated metric. For each BTS, C1 and C2 are calculated and the MS chooses the BTS with the most favorable C2

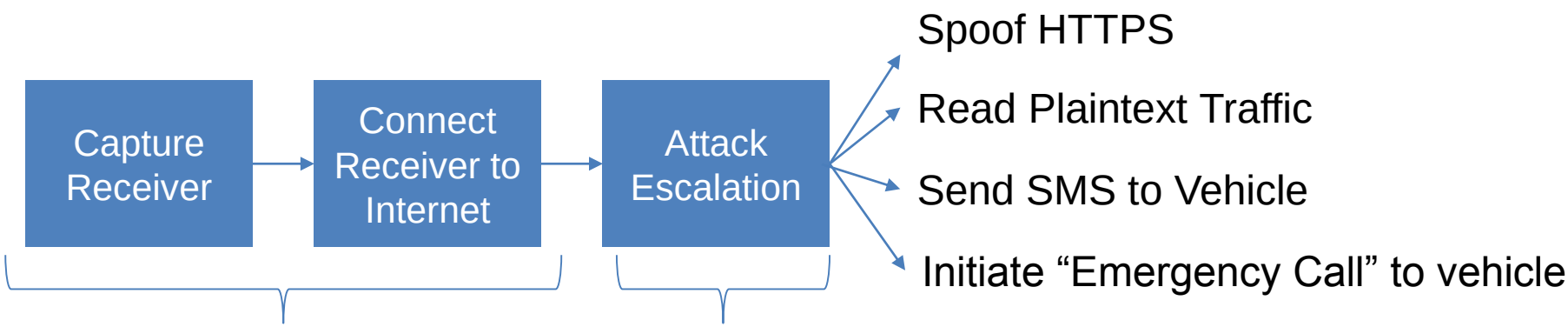
$$C1 = \left(A - MAX(B, 0)\right)$$

$$C2 = C1 + \boxed{CELL\_RESELECT\_OFFSET} - TEMPORARY\ OFFSET * H(PENALTY\_TIME - T)$$

CRO is a "magic" number set by each BTS

So what happens if I spoof a BTS and set CRO to its max value?

RF-Based Cellular Attack Workflow



Likely minimum level of access an attacker can obtain remotely. At this point, vehicle is likely experiencing denial of service of cellular dependent features

Attacker now has a large subsequent surface to escalate vehicle privilege on that covers multiple systems and protocols

Additional Automotive Wireless: TPMS, DSRC, GPS, FM Digital Sidebands, Wi-Fi, LTE Hot Spots…

Summary

- Commercial or Commercially-derived wireless technologies are commonly used to enable connectivity of systems across Transportation, Finance, Telecom, Power, and Space
- Security research of these wireless technologies has been commoditized by inexpensive software defined radios and open-source software development
- The barriers to entry to this type of RF-based security research have been significantly reduced