Southwest Research Institute® Overview

Robert W. Heller, Ph.D.

Program Director R&D – Intelligent Systems Department

Presentation Outline

- Cybersecurity
  - How prevalent
  - How it is accomplished
- Connected Vehicle
  - Where is it vulnerable
  - How is it hacked
  - What are the points of exposure in a deployment
- Next steps
  - What should you be concerned about

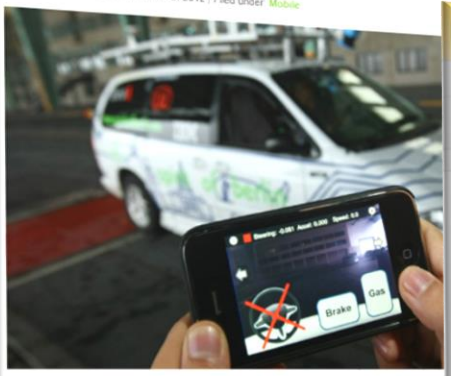
SET EDITION U.S. | INTERNATIONAL | MÉXICO | ARABIC
TV: CNN | CNNi | CNN en Español | HLN

CNN Tech

Home | TV & Video | CNN Trends | U.S. | World | Politics | Justice | Entertainment | Tech | Health

Could hackers seize control of your car?

By Barry Neild, CNN
updated 5:43 AM EST, Fri March 2, 2012 | Filed under: Mobile



(CNN) -- When car companies begin exhibiting at mobile
shows, it's a sign that the "connected" vehicle has truly ar
allowing us to take our digital lives with us as we hit the h

But while Ford's unveiling of its latest car at Mobile World
-- a major cell phone industry event -- this week may have
new automotive age, it also heightens fears that our techr
crammed cars could be hijacked by hackers.

Just like our PCs and smartphones, the computerized cor
that have infiltrated almost every aspect of modern vehicl
potentially be broken into, experts say. Only, with a car, th
have far more dangerous consequences.

COMPUTERWORLD

Topics | News | In Depth | Reviews | Blogs

Security | Application Security | Cybercrime and Hacking | Mobile Security | Privacy

Home > Security

Car-hacking: Remote access and other security issues

It's not time for full-on panic, but researchers have alre
applied brakes remotely, listened into conversations an

By Linda Melone
August 8, 2012 07:00 AM ET | 14 Comments

+1 | + Briefcase | More

Computerworld - A disgruntled former employee of Texas A
chose a creative way to get back at the Austin-based deale
into the company's computers and remotely activated the v
immobilization system, which triggered the horn and disabl
system in more than 100 of the vehicles. The dealership ha
system in their cars as a way to deal with customers who fe
payments.

Police arrested the man and charged him with breach of computer security.
His legal status was unclear as of our deadline for this story.

Out-of-control honking horns may be annoying, but other types of hacking, such as cutting the engine of unsuspecting drivers, could have deadly consequences. Although most experts agree there isn't an immediate risk, vehicle hacking is something that bears watching.

A 2011 report (PDF) by researchers at the University of California, San Diego and others site numerous "attack vectors," including mechanics' tools, CD players, Bluetooth and cellular radio as among the potential problems in today's computerized cars.

euronews

NEWS | EUROPEAN AFFAIRS | BUSINESS | SPECIAL REPORTS | SPORT | CULTURE

Africa | Americas | Asia | Europe | Middle East

Home | Sci-tech | Hackers steer a new route – to your car

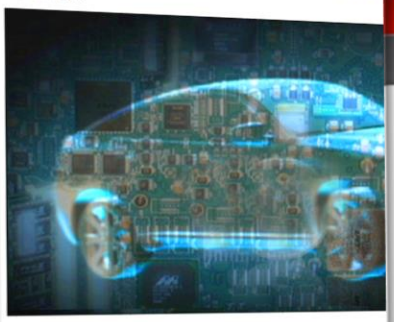
Search euronews.com

Breaking News: French President François Hollande says France will support military operation in Mali but st

SCI-TECH hi-tech

Hackers steer a new route – to your car

25/09/12 13:18 CET



AT&T Internet + Home Phone & Wireless or TV
you won't believe all you'll get
Details
less than $80/mo for 12 months
Tweet +1 4

c|net

Reviews | News | Download | CNET TV | How To

CNET | News | Security & Privacy | Predator drones hacked in Iraq operations

Exclusive: CEO says hackers tried to extort data, money

Karim Hijazi knew his nightmare was just beginning when he saw that a mysterious e-mail had arrived in his inbox at 3 a.m. on May 26 that included his e-mail password and the subject line "Let us talk."

That would mark the beginning of a weeklong saga of e-mail exchanges and Internet Relay Chat (IRC) discussions in which Hijazi says a group of hackers told him they wouldn't publicly divulge information they had gotten from snooping on his accounts if he revealed sensitive security information acquired by the botnet-tracking firm, Unveillance, that he launched last year. The hackers, who call themselves LulzSec, wanted to know the whereabouts of compromised computers on the Internet that when remotely controlled are used en masse to attack Web sites, he told CNET in an exclusive phone interview late last night.

When he refused, LulzSec went public with his data, Hijazi says, posting his personal contact information, e-mails, and chat logs for download online yesterday as part of a campaign to embarrass the FBI and its InfraGard partner. The group had hacked the Web site of InfraGard Atlanta and grabbed usernames and passwords for about 180 members, including Hijazi. Because Hijazi had used the same password on the InfraGard site that he used on his personal Gmail account and his corporate Google Apps account, the hackers were easily able to spy on his personal and business activities.

Hijazi contacted the FBI right after that first LulzSec e-mail and said he plans to prosecute if he can.

"They had me under the gun for a little over a week with threats and extortion," said Hijazi, chief executive of Unveillance. "The very nature of having to contend with someone who is holding something ransom is not pleasant."

Get an assessment. LEARN MORE RAPI

8/13/2015
02:15 PM

Ericka Chickowski
News

The Summer Of Car Hacks Continues

New research shows how SMS messages manipulating vulns in insurance dongles can kill brakes on cars.

The summer of car hacks continues this week as another set of researchers demonstrated how it's possible to affect the control of a car's braking system without even engaging with any electronics embedded in the car itself.

Related Content
Resources Twitter

Cyberthrea
This report
security res
provides a
organizatio

Big Data S

Cellular Security Topics in the News…

TECH 9/03/2014 @ 3:00AM | 13,849 views

Rogue Cell Towers Could Be Intercepting Your Call

A--REQUEST FOR INFORMATION (RFI) / SOURCES SOUGHT (SS) NOTICE INVESTIGATION FOR CELLULAR LONG TERM EVOLUTION (LTE) TECHNOLOGIES

Solicitation Number: W56KGU14RA012
Agency: Department of the Army
Office: Army Contracting Command
Location: ACC-APG - Aberdeen Division A

Markets | Fri Jan 30, 2015 10:15am EST

BMW fixes security flaw in its in-car software

FRANKFURT

Army examines feasibility of integrating 4G LTE with tactical network

September 25, 2012

By **Edric Thompson, RDECOM CERDEC Public Affairs**

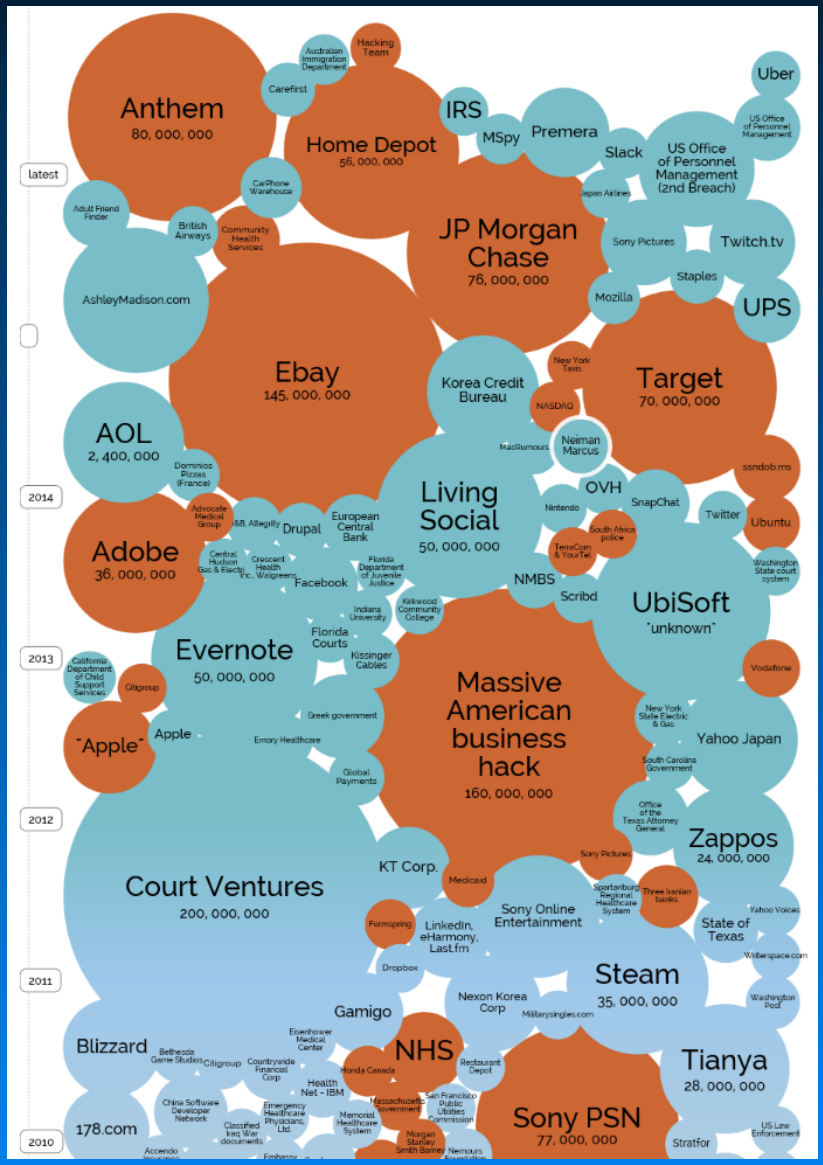
Stingray Tracking Devices: Who's Got Them?

Cybersecurity is not “one” Entry Point

Data Hacks

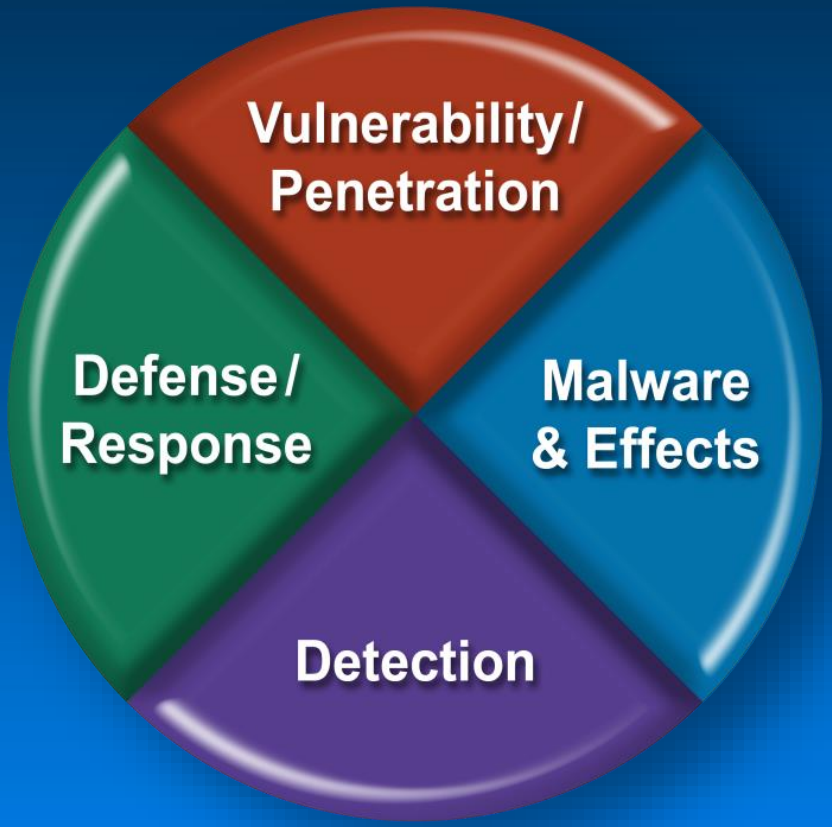
(source: http://www.informationisbeautiful.net)

- What is being hacked:
  - Social network data
  - Smartphone app data
  - Online/Offline shopping
  - Car navigation data
  - Biometrics
  - Healthcare data
  - IoT telemetry
  - Smart grid pricing & usage
  - Intellectual property
  - Industrial diagnostics
  - Demographic data
  - National security data
  - Etc.
- What is your story?



Four Major Aspects of Cybersecurity

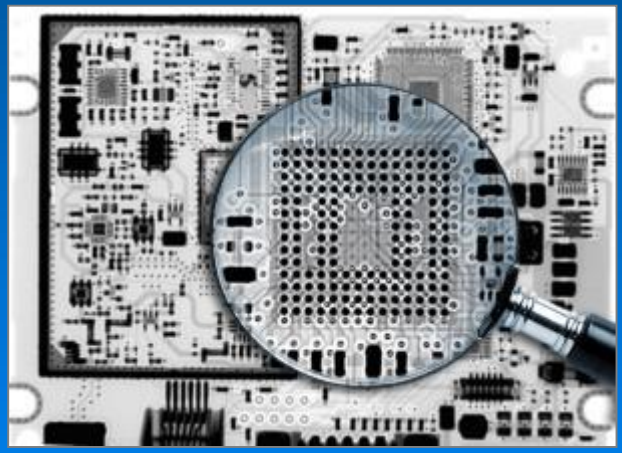
- How Can Someone Gain Unauthorized Access?
- What Could They do if They Gained Access?
- How Can We Detect Unauthorized Access?
- What Can be Done in Response to an Attack?



How Do Cyber Attacks Occur:

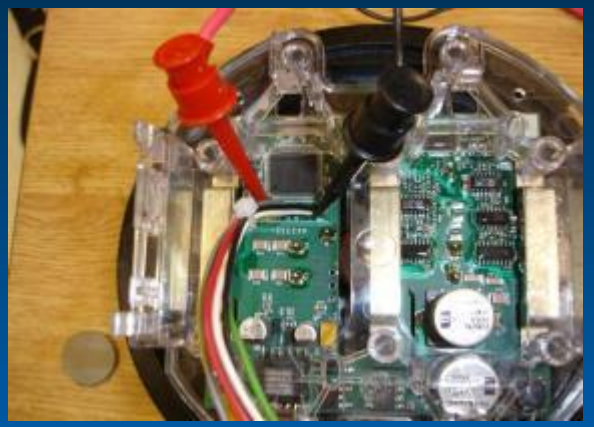
Penetration Testing

- Assesses the susceptibility of a system to a security intrusion
- Methodical approach ensures that most frequent and most damaging attacks are mitigated
- Helps create and maintain a secure system at an acceptable level of risk



How Do Cyber Attacks Occur:
Physical Attacks

- Assesses what attacks may be performed with physical access to a system.

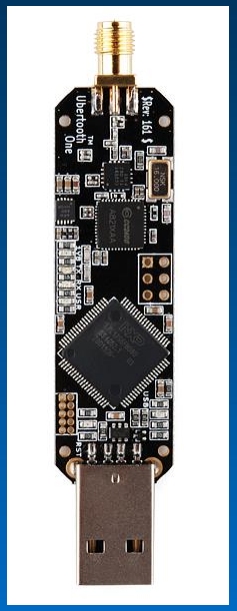


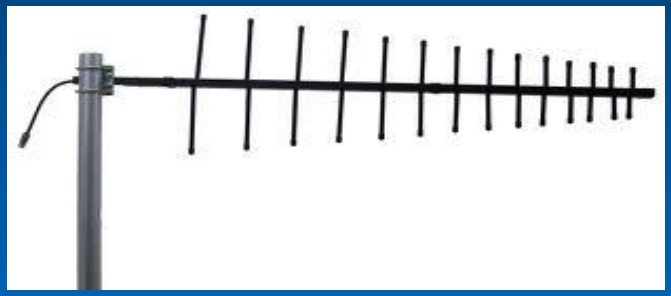
- Recovery of system secrets
  - Cryptographic Keys
  - Passwords
- Intercept communications
  - Network and IP Traffic
  - Internal Signals

- Modify and inject traffic
  - Serial
  - Cellular
  - CAN

How Do Cyber Attacks Occur:
Wireless Attacks

- Types
  - Cellular
  - CB Radio
  - Mesh Network
  - WiFi
  - Bluetooth®
- Approaches
  - Denial of service
  - Device Spoofing
  - Traffic Injection
- Tools
  - Software Defined Radio
  - Custom Hardware and Software

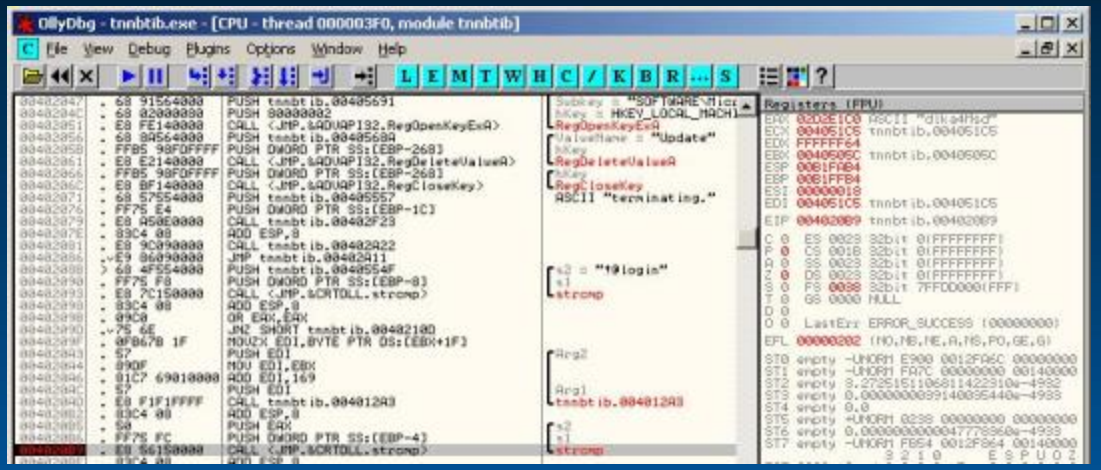




How Do Cyber Attacks Occur:

Software Attacks

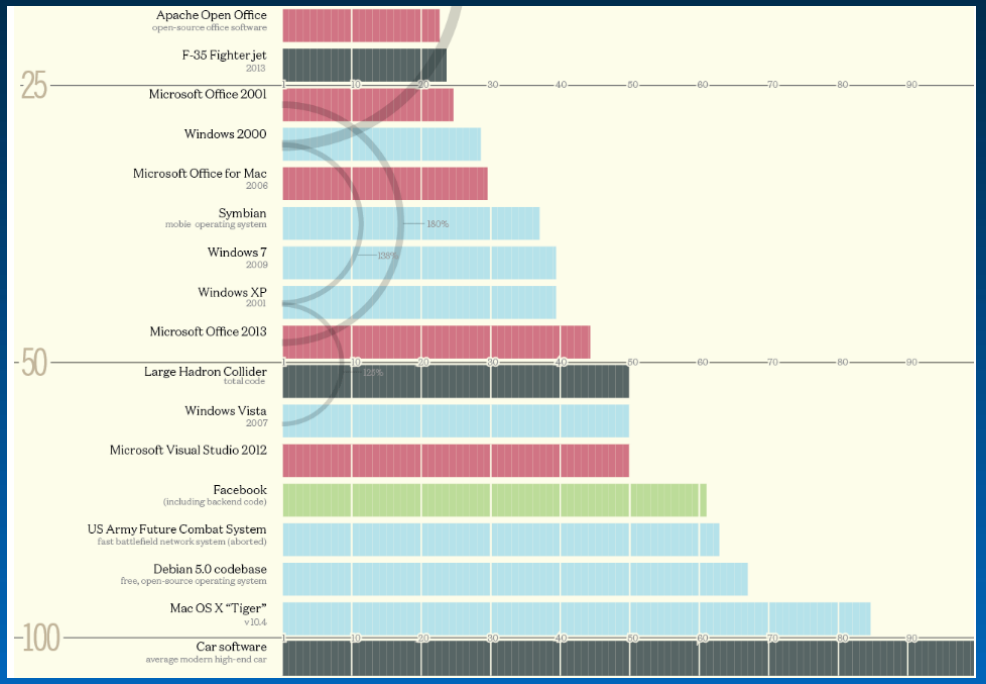
- Types
  - IP / Network
  - Embedded Firmware
  - Business Applications
  - Web Applications
- Approaches
  - Reverse Engineering
  - Fuzzing
  - Configuration Analysis
  - Design Review
- Tools
  - Backtrack / Kali Linux
  - Disassemblers / Debuggers
  - Custom Scripts



Connected Vehicle (CV) Cybersecurity

- From a DOT / County perspective “connected vehicle” is a system of systems – its NOT just one connection
- Where is the responsibility for cybersecurity:
  - Standards
  - Network
  - Vehicle
  - Etc.
- CV is not just “DSRC”
- There are MANY entry points into a CV infrastructure

Cars are becoming complex…
(and Connected Vehicle is only part of it)



http://www.informationisbeautiful.net

- 1965:
  - No computers
  - No software
- 2015:
  - Up to ~200 computers
    - Consider TPMS are 4 computers and wireless…
  - >100 million lines of code
  - LTE (or similar) enabled vehicles are becoming commonplace

Challenges with Connected Vehicles

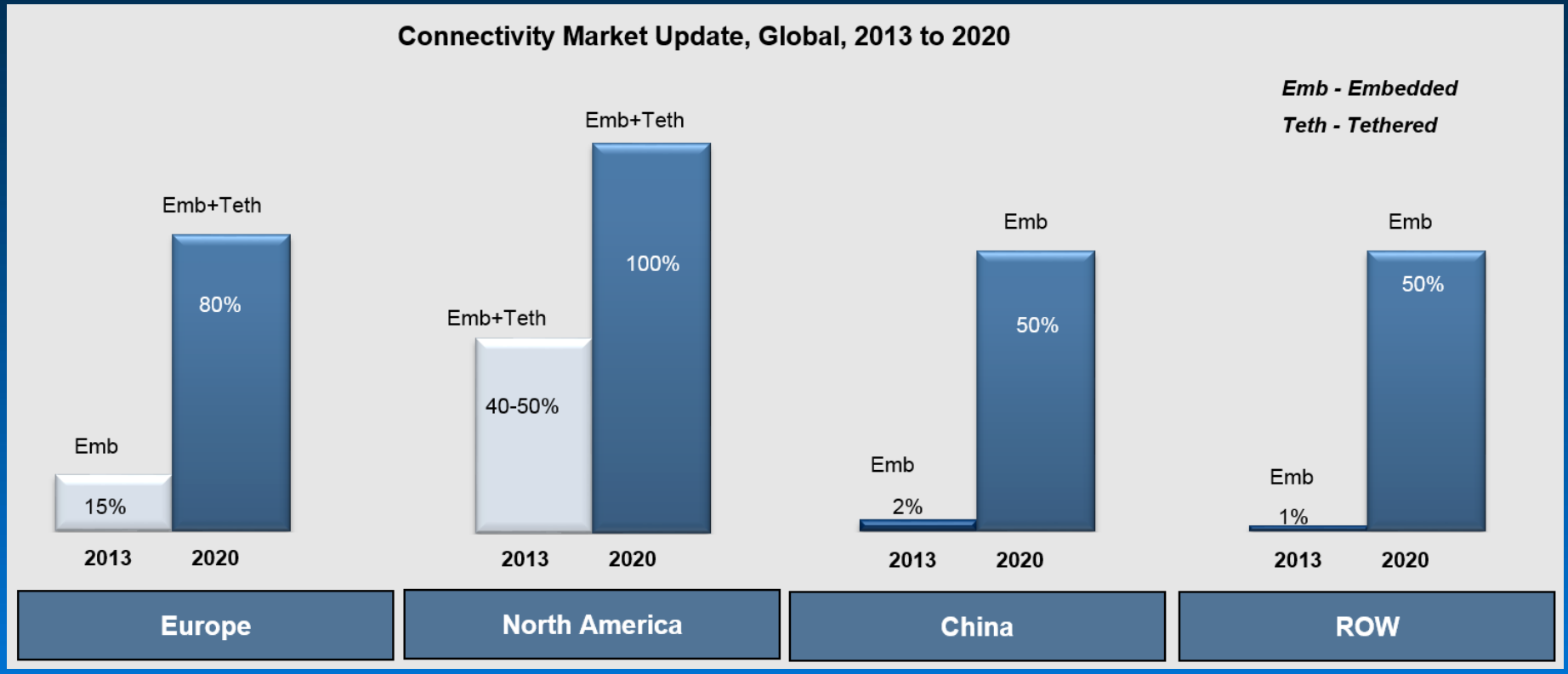
- **Recent attacks on Connected Vehicles:**
  - **Jeep Cherokee: *"Hackers Remotely Kill a Jeep on the Highway—With Me in It"***
  - **GM OnStar: *"This Gadget Hacks GM Cars to Locate, Unlock, and Start Them"***
  - **Tesla Model S: *"Researchers Hacked a Model S, But Tesla's Already Released a Patch"***


Image Source: Wired Magazine


Image Source:
Wired Magazine

- Impact of these attacks:
  - Erodes public trust
  - Raises awareness – improves security practices
  - Not a setback for DSRC

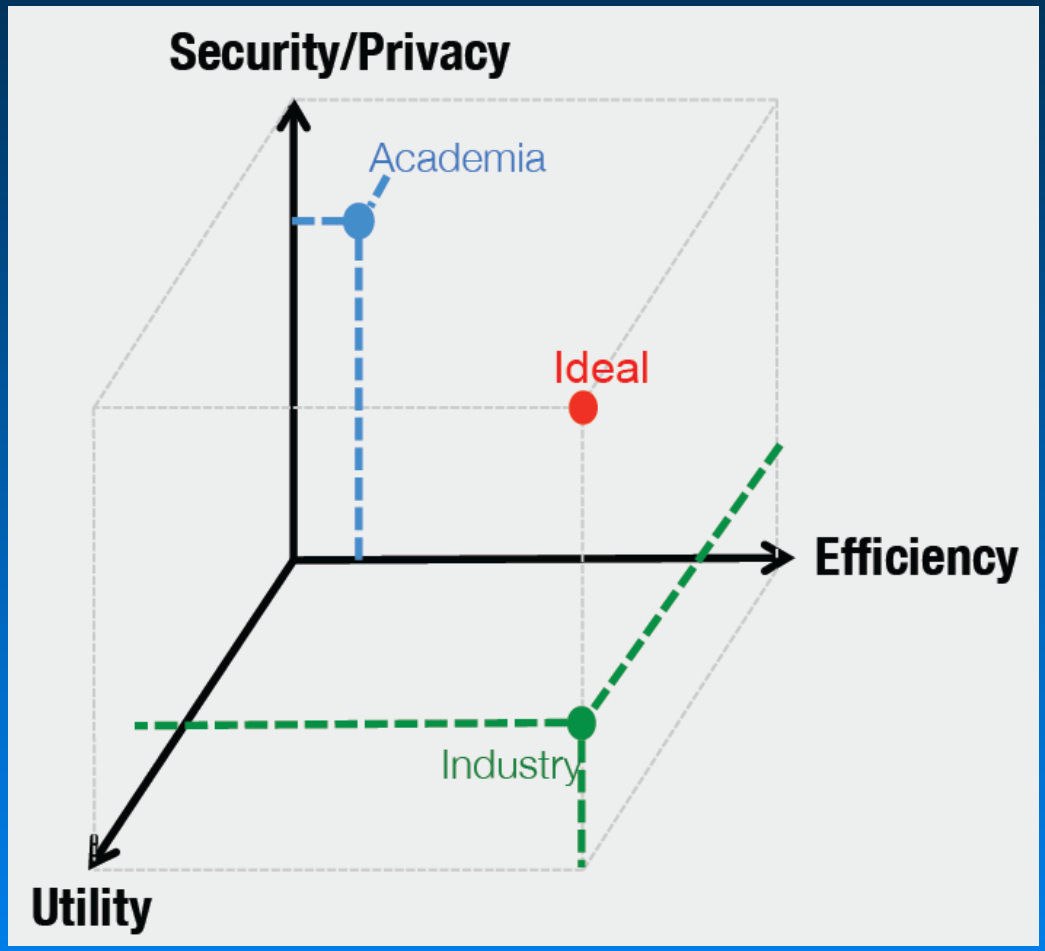
The Auto World is Quickly Becoming Connected – by 2020…



Source: Frost and Sullivan analysis

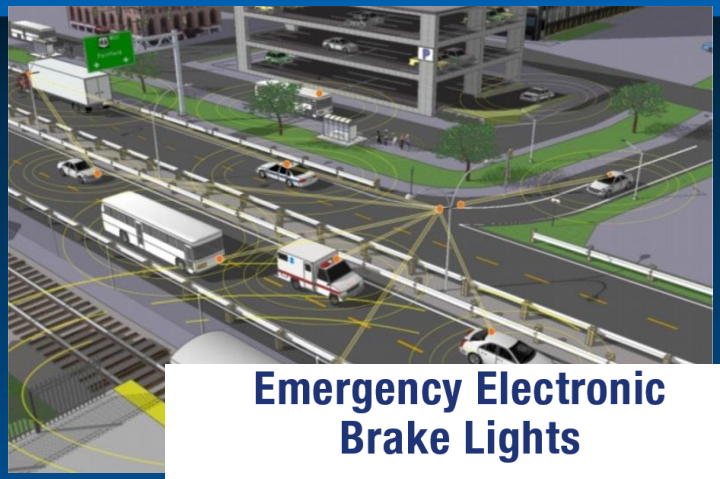
Security is a Balance…

- How much do you want to pay for security?
  - Usually not a lot until you are compromised ☺
- Like all technology solutions, a balance has to be reached based on funding, accessibility and reality
- Every organization has to decide the level of "acceptable risk"

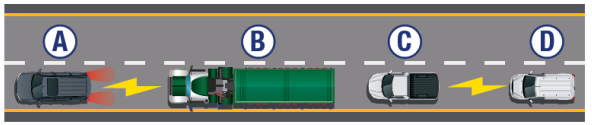


Connected Vehicle Overview

- Cooperative system where vehicles communicate:
  - With each other (V2V)
  - With infrastructure (V2I)
  - With pedestrians, bicycles, etc… (V2X)
- Improves: Safety, Mobility, Environmental Impact
- Example Applications:
  - Emergency Electronic Brake Lights (V2V)
  - Overheight Vehicle Detection and Warning (V2I)
- Major question:
  - Who should you trust?

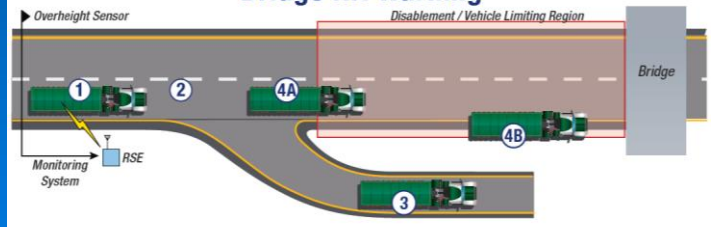


Emergency Electronic Brake Lights



A: Broadcasts hard-braking 'event' when decelerating over the defined threshold
B: Vehicle potentially obstructing the view of Driver C and D
C and D: Receives hard-braking event from A and displays a warning if the vehicle is in the forward path

Bridge Hit Warning

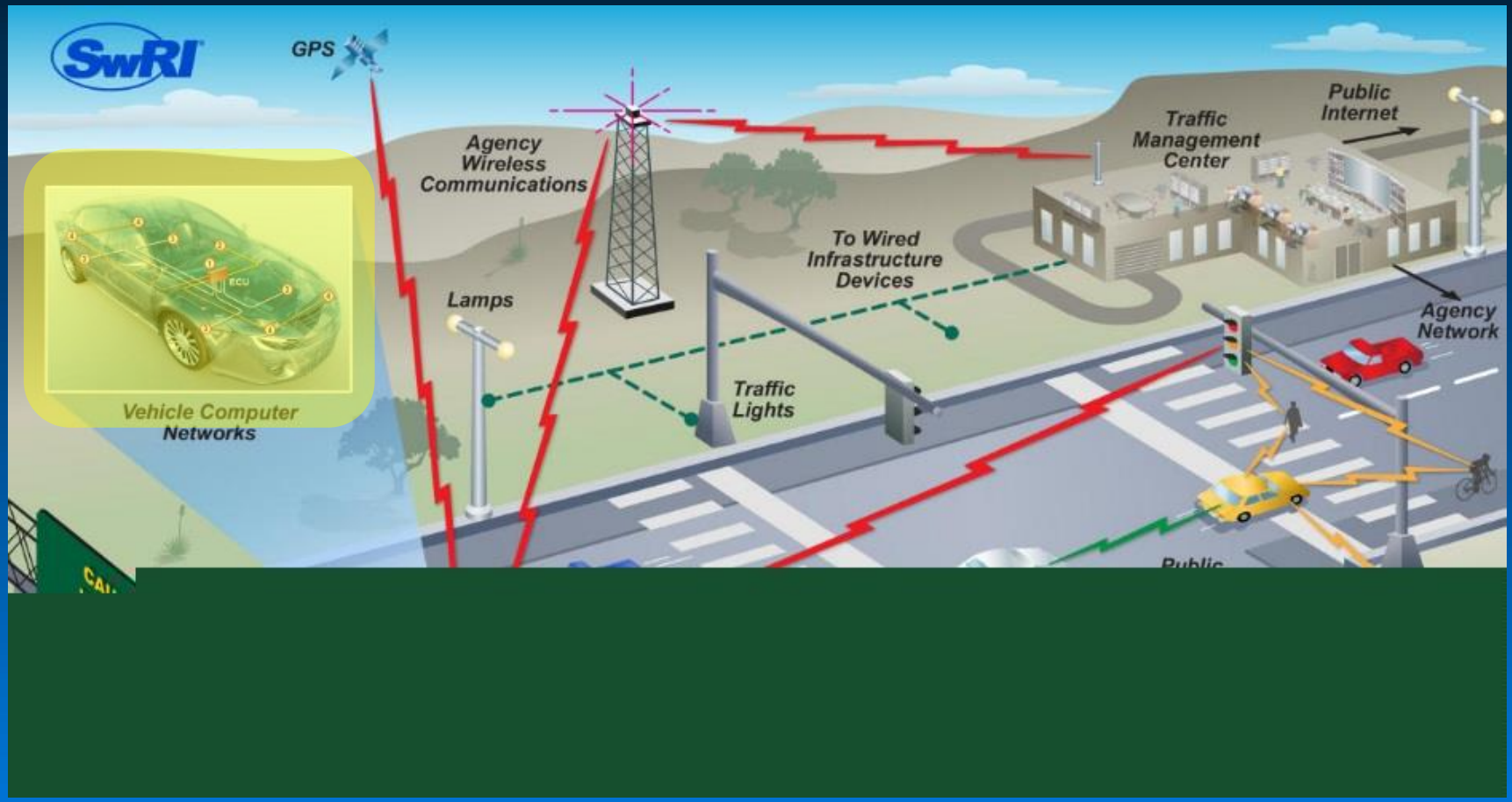


1: Infrastructure OH sensor detects OH vehicle
2: RSE identifies specific vehicle and warning is displayed to the driver
3: Vehicle exits and uses bypass –Warning is removed from driver display
4A: Vehicle does not exit – Additional warnings presented. Vehicle automatically slows if available.
4B: Vehicle is disabled or speed limited prior to hitting the bridge, if available. Emergency responders automatically notified.

Consider a CV Environment

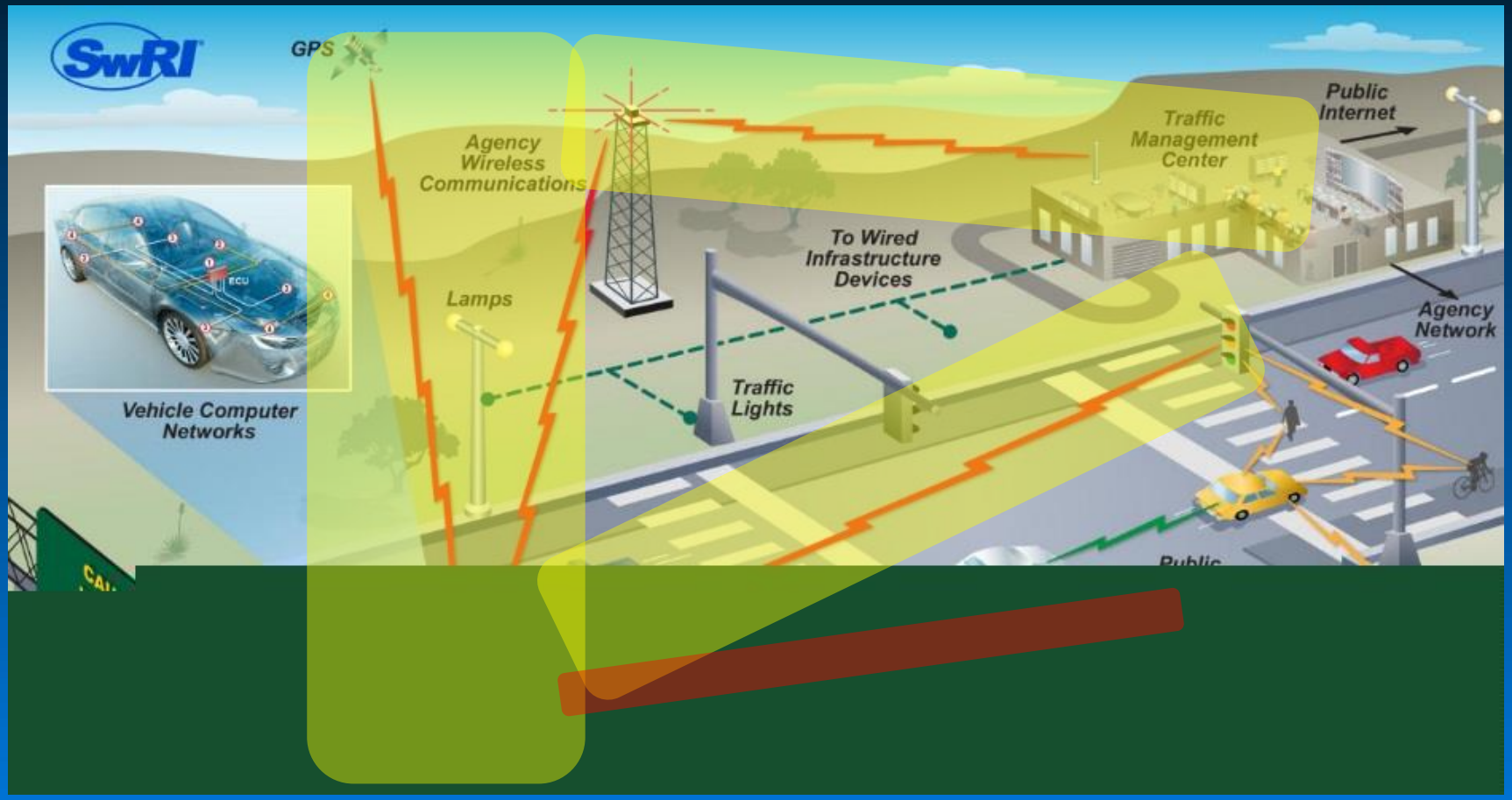
- For Connected Vehicle to be successful it must be integrated into the transportation infrastructure

Consider a CV Environment:
The Vehicle



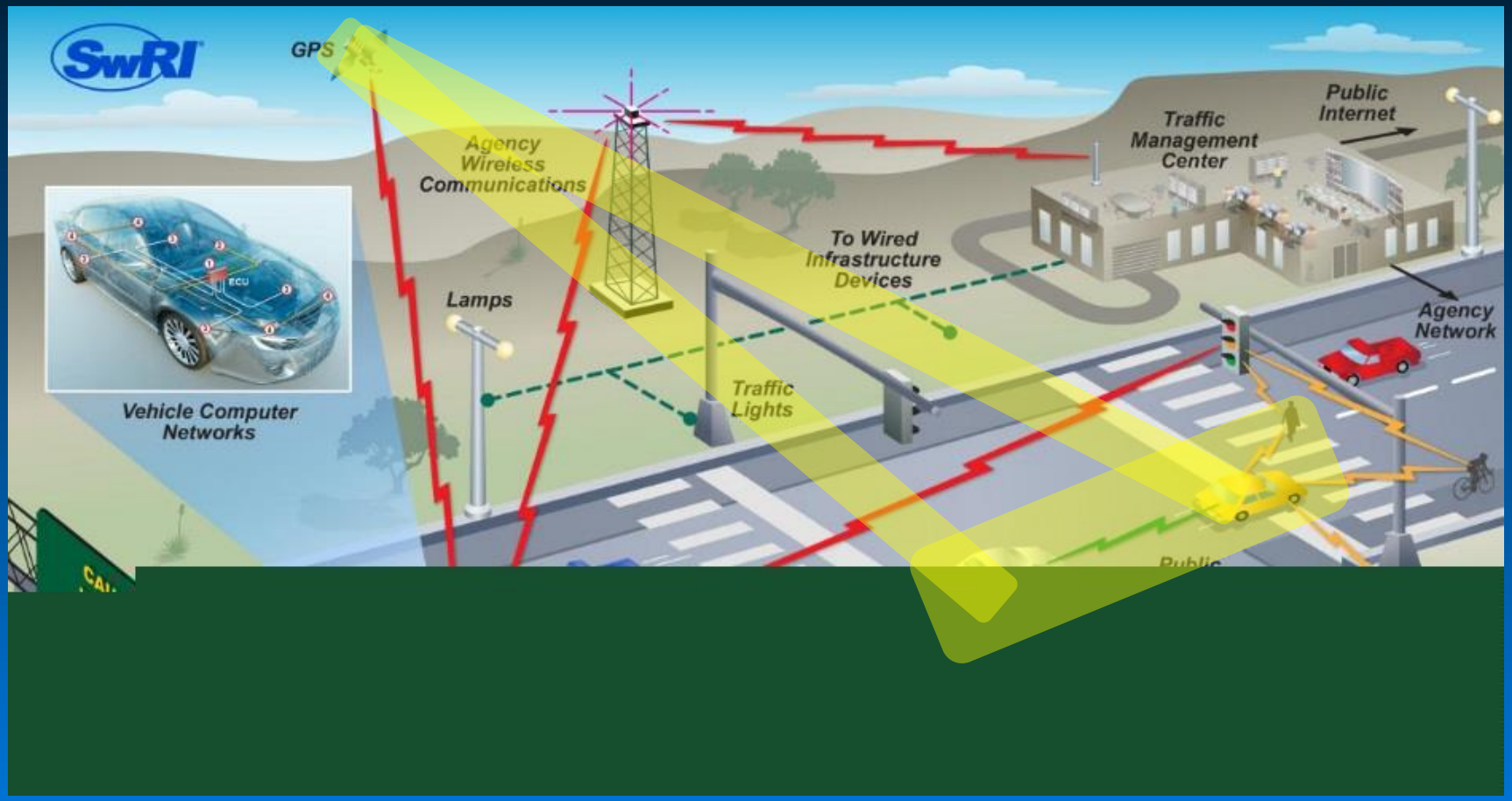
- Vehicle may have several hundred computers
- Multiple networks
- Each an entry point into the “infrastructure”

Consider a CV Environment:
Vehicle to Infrastructure (V2I)



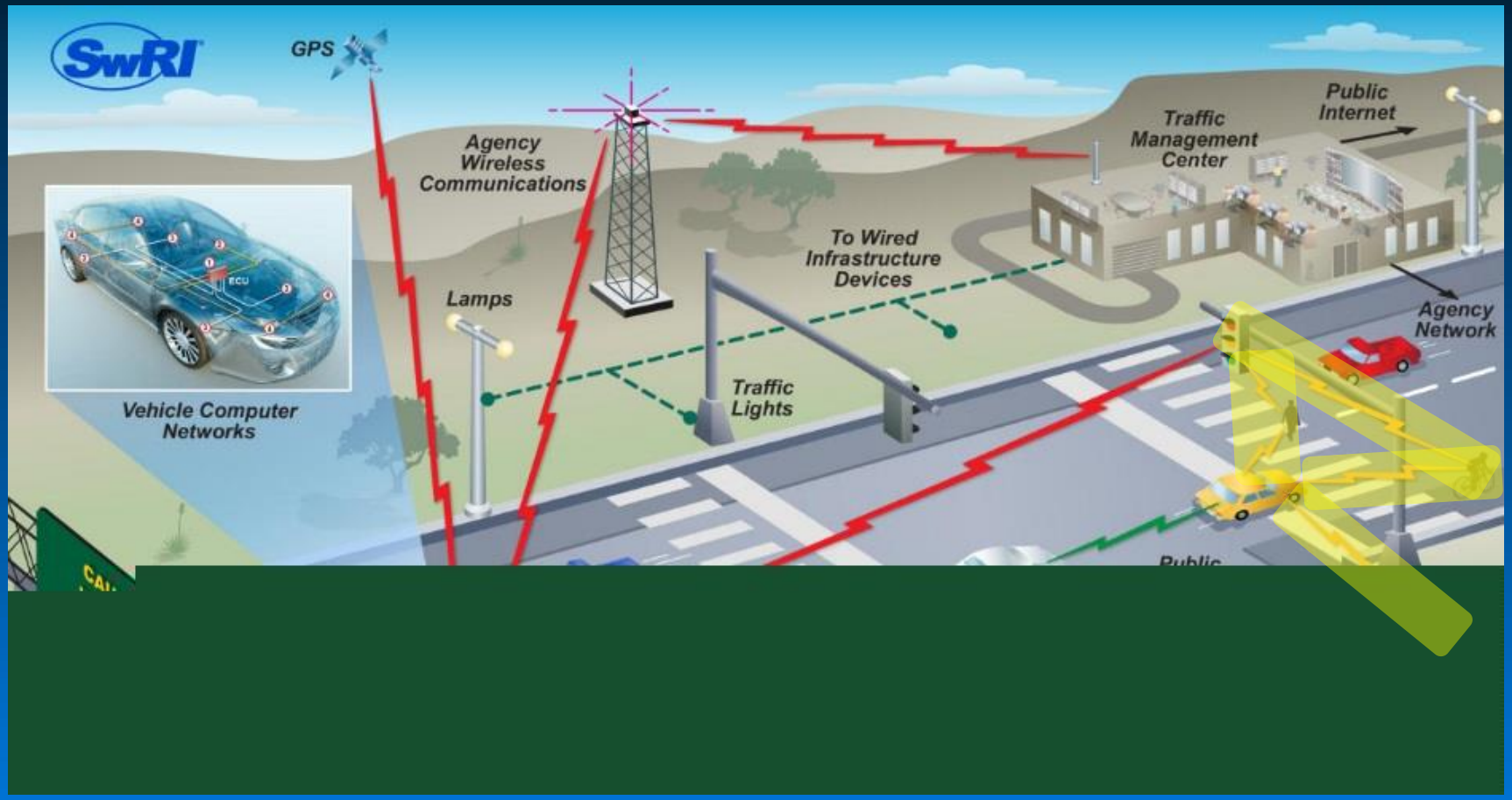
- Vehicle can communicate to agency networks (e.g. DSRC)
- Data may pass both directions
- Vehicle may communicate to NON-agency networks also

Consider a CV Environment:
Vehicle to Vehicle (V2V)



- Vehicles communicate directly with each other (trust issues)
- No public infrastructure required
- Focus of current NHTSA rulemaking

Consider a CV Environment:
Vehicle to Pedestrian (V2P)



- Improving the safety of vulnerable road users
- Communications link may be DSRC, cellular, etc.
- Low latency and highly reliable data very important

Connected Vehicle Security

- Connected Vehicles utilize a number of communication mechanisms and protocols:
  - Cellular
  - Bluetooth
  - Wi-Fi
  - Dedicated Short Range Communications

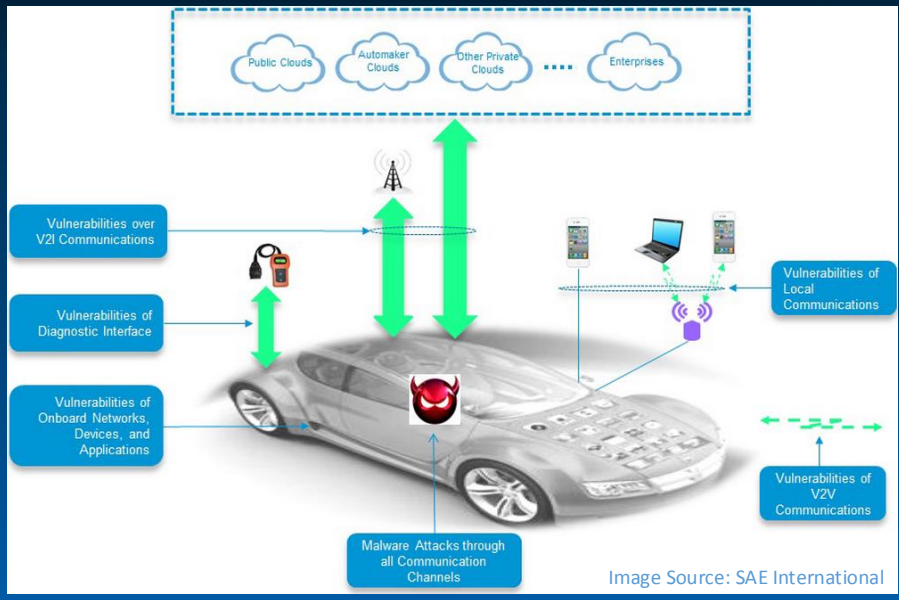


Image Source: SAE International

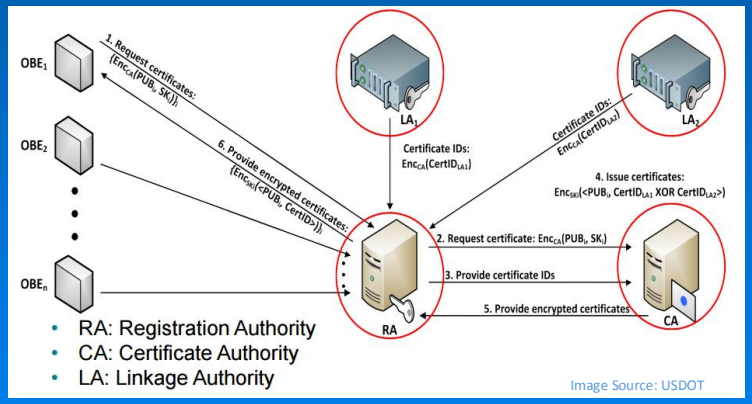
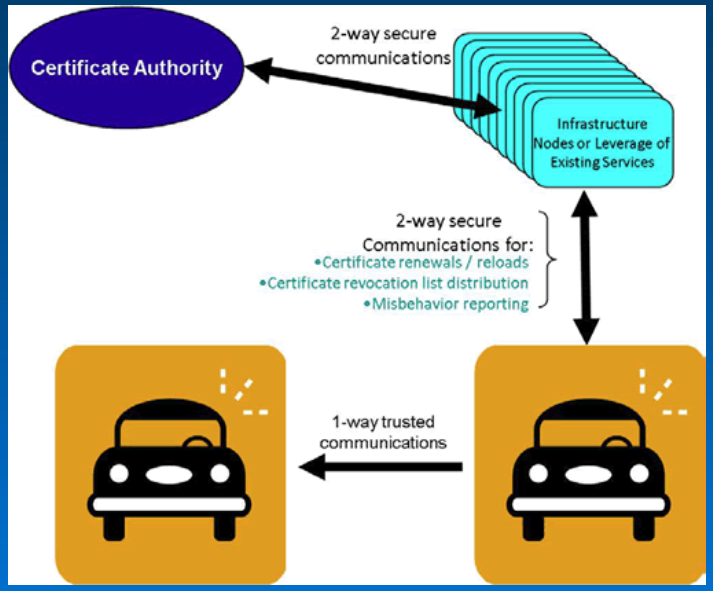


Image Source: USDOT

- DSRC standards have security designed in:
  - IEEE 1609.2 standard
  - Public Key Infrastructure (PKI)
  - Security Credential Management System

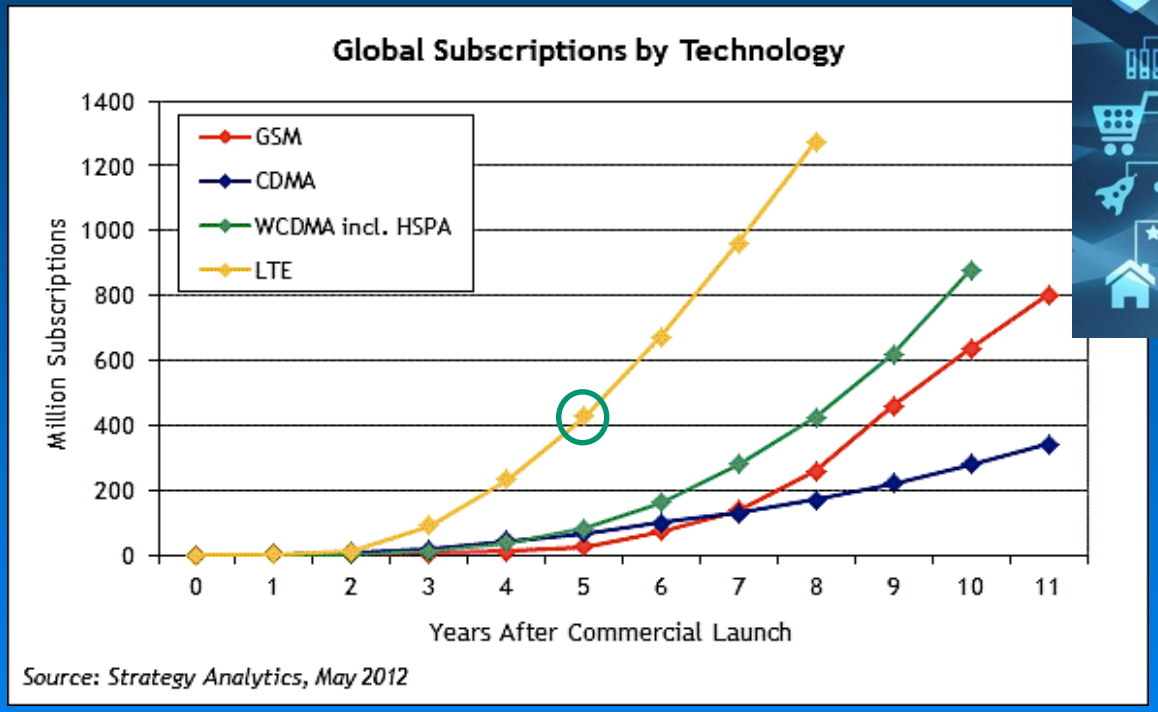
Connected Vehicle Privacy

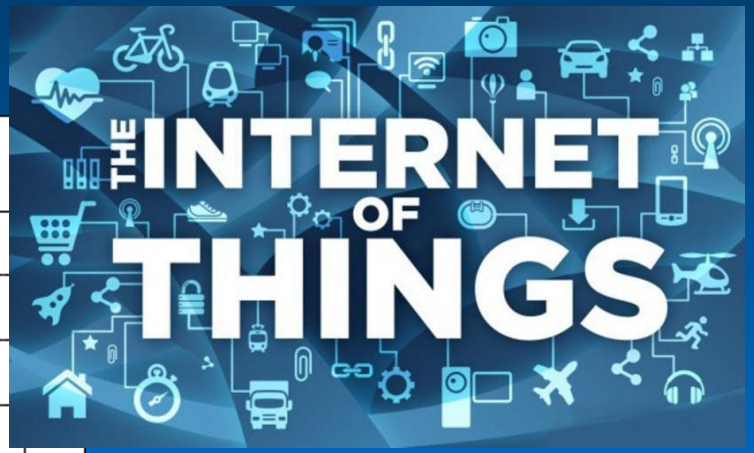
- NHTSA mandate will require that vehicles publish a Basic Safety Message over DSRC at 10 times per second
- This will generate a lot of rich data!
- Standards are designed such that all identifiers “tumble” frequently to make it extremely difficult to track someone
- Information cannot be connected to a particular individual
- Policies will need to be in place to handle this type of data



Projected Growth/Interest in LTE

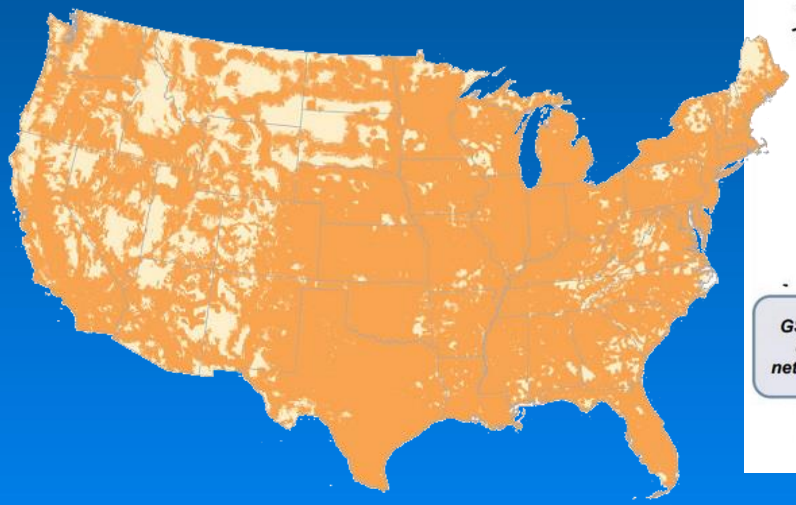
- Cyber Physical Systems & Internet of Things will drive future economy
  - Expected network revenue will exceed Cloud & Big Data
- LTE subscriptions will explode
  - 1 billion in 2016 (7 yrs after launch)

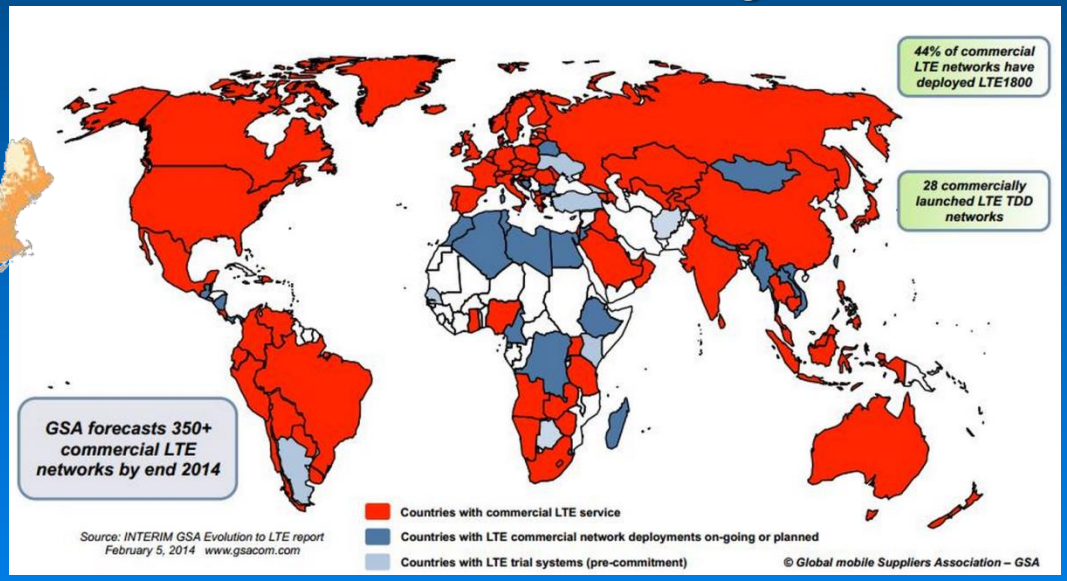




Fixed/Mobile Coverage (Convergence)

- **Mobile Coverage (Wi-Fi vs Cellular)**
  - WIFI coverage is limited, but cellular coverage already spans much of the country and world
- **Fixed/Mobile convergence**
  - Femtocells (10-20 m) extend cell coverage indoors and at edges of macrocell (esp. when spectrum is crowded (e.g. SxSW))
  - Users benefit: better coverage, data, battery life, and lower fees
  - Operators benefit: happy customers & more universal coverage

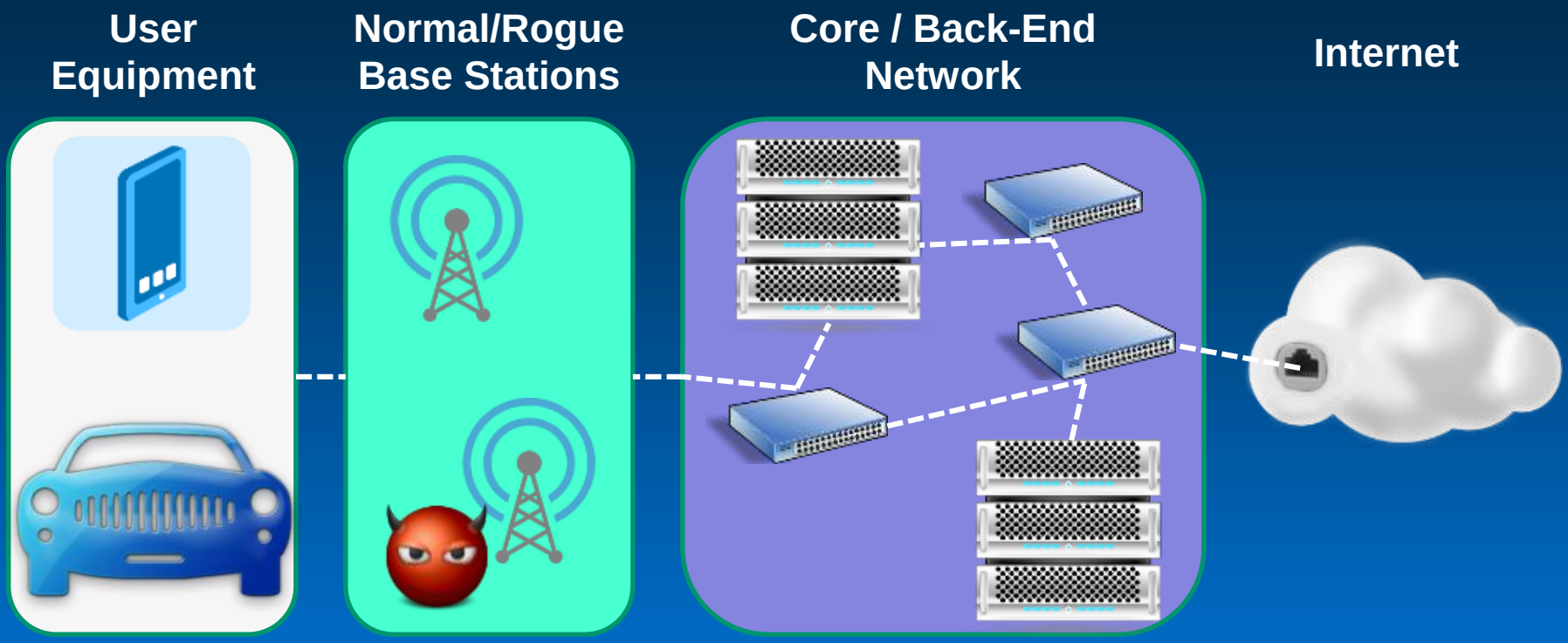




Wireless: What are the problems?

- Connected Car, Home, City
  - Many mobile platforms / sensors will likely connect via cellular (LTE has broad coverage, moderate cost / power)
- However, problems should be expected
  - 3G systems had numerous problems, including rogue femtocell attacks
  - LTE security better, but control segment still unencrypted & many problems probably remain hidden
  - Significant concern over a Man in the Middle attacks
    - Unknown vulnerabilities are always worse than what is known
  - Hints of DoD “cyber needs” related to cellular

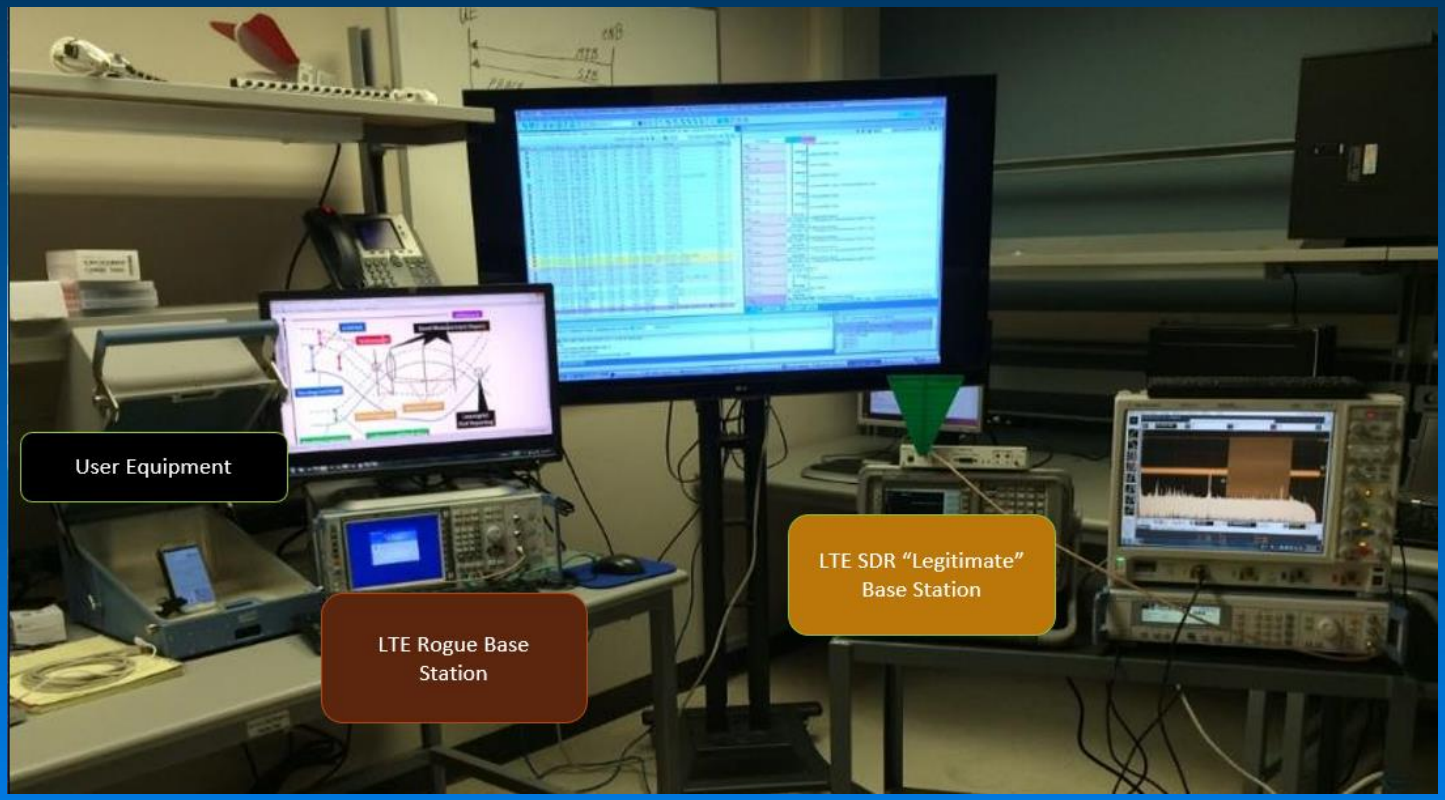
Rogue Base Station Attack Scenario



Rogue base stations could track users and intercept user data

How Hard is it to Hack a LTE Network?

- How real is the concept?



Cybersecurity “touch” Points:

Need to “worry” each of these…

- Field network
- Bluetooth
- Wireless networks
- Wired networks
- Vehicles
- Any device that is connected to one of the above

Connected Vehicle Environment

Potential Attacks

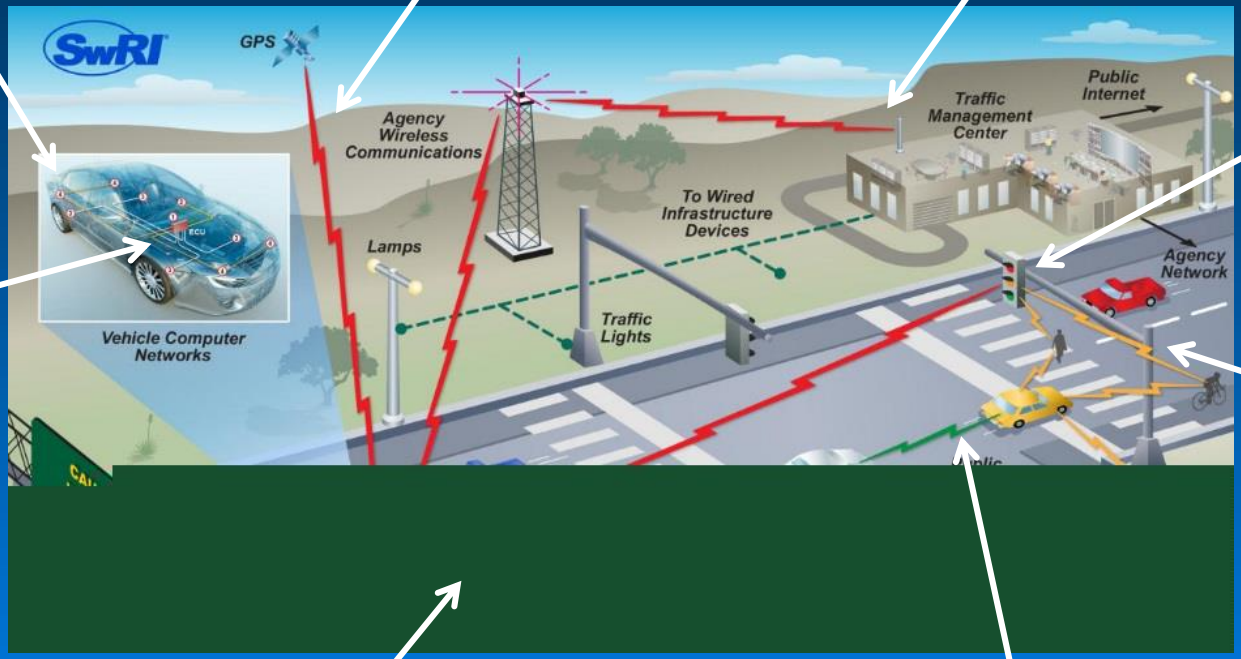
Injecting bad data that is then communicated over trusted comms

Spoofing, jamming, or subtle skew of GPS signal

Use roadway infrastructure to infiltrate TMC network

Hack RSE and alter SPAT/MAP messages

Using comms or physical means to hack vehicle and control it or obtain trusted security credentials



Broadcast incorrect messages to/from Vulnerable Road Users

Flood DSRC safety & control channels

Simulate vehicles that will trigger safety apps. Tough to detect if sensors are occluded

Summary

- Key takeaways:
  - Connected Vehicles are already here and the number of connected vehicles will increase in years to come
  - DSRC will add another “attack surface” for vehicles and infrastructure
  - Almost everything is “hackable” or “trackable”
  - DSRC standards are designed to make it much more difficult to hack or track than other communication mechanisms in the CV environment
- What can Florida do to prepare for DSRC deployment?
  - Extend security and data privacy systems, practices and policies to handle connected vehicle data and infrastructure
  - Small pilot deployments to analyze security and privacy impacts – this can inform a larger deployment in the future

Questions ?

Robert W. Heller, Ph.D.
Program Director R&D
Intelligent Systems Department
210.522.3824
rheller@swri.org