SRI International

# DHS Programs: Cybersecurity for Government Vehicles

Moderator: David Balenson
Infrastructure Security Research Group
Computer Science Laboratory
SRI International

Presented at ACSAC 2015
December 10, 2015

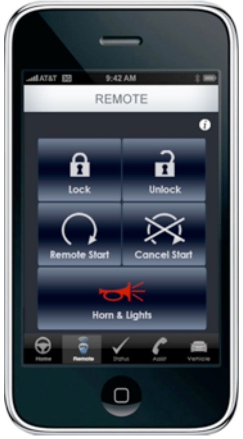
## Why We Are Here Today

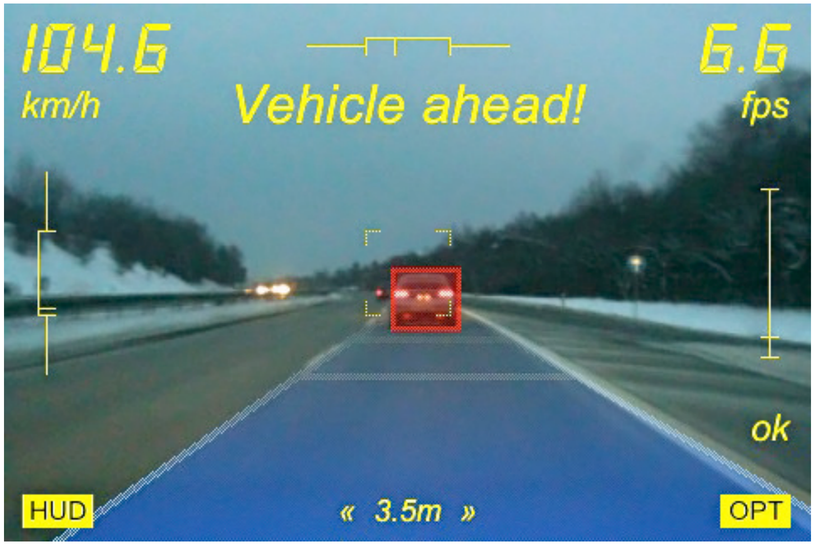
- “A modern car is a computer system with wheels”
- And we all know how perfectly secure most computer systems are…

# Features Galore

## What About Security?

– Telematics
  - Remote control (locks, start)
  - Remote diagnostics
  - Remote repair (updates)





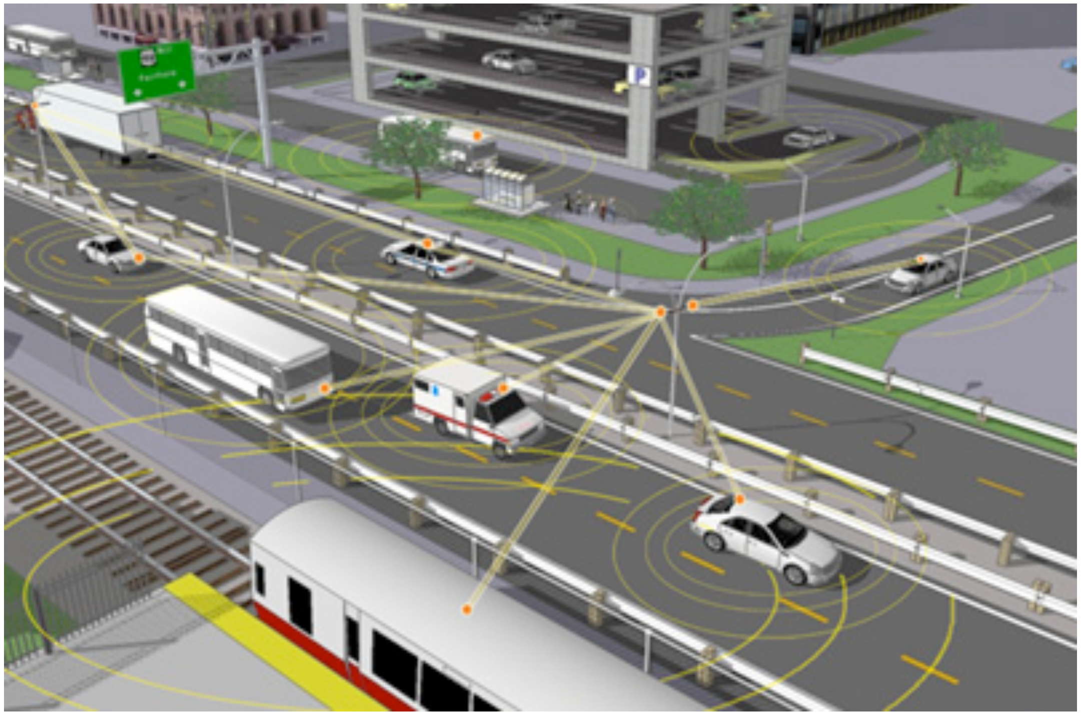
– Driver support
  - Navigation
  - Collision warning/avoidance
  - Augmented vision

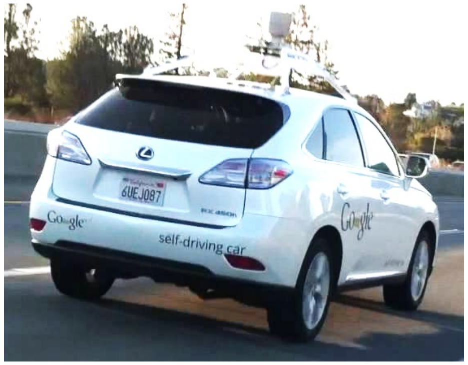
– System automation
  - Dynamic EV charging
  - Computer control of engine, brakes, etc.

– Content and communication
  - Voice and data communication
  - Information and entertainment

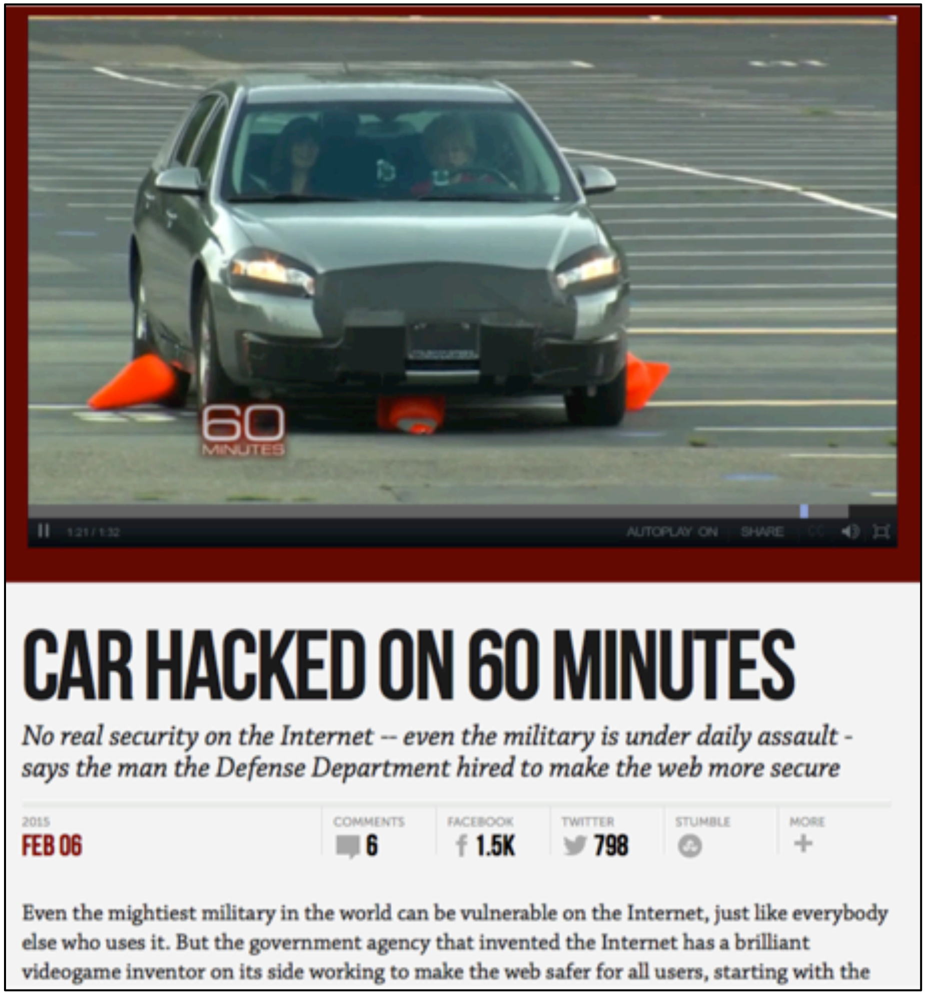
# Connected and Autonomous Vehicles Are Coming

- Vehicles are rapidly becoming more automated and connected
- Vehicles will communicate with fixed nodes and with other vehicles, all becoming part of a complex and highly dynamic system
- The next natural step is to relieve the driver of some driving duties





# Today's Cars are Vulnerable to Cyberattacks

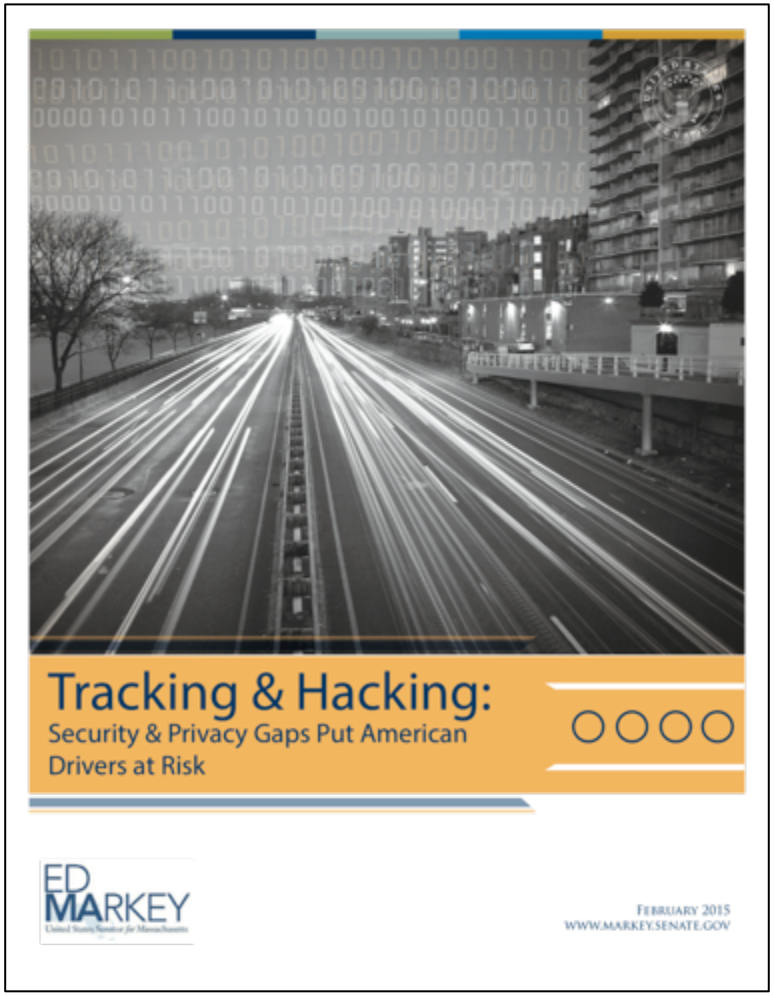


## CAR HACKED ON 60 MINUTES

*No real security on the Internet -- even the military is under daily assault - says the man the Defense Department hired to make the web more secure*

2015
FEB 06

Even the mightiest military in the world can be vulnerable on the Internet, just like everybody else who uses it. But the government agency that invented the Internet has a brilliant videogame inventor on its side working to make the web safer for all users, starting with the



## Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ED MARKEY
United States Senator for Massachusetts

FEBRUARY 2015
WWW.MARKEY.SENATE.GOV

# It Is Not Good Today, and Tomorrow Is Looking Worse

- Consumer vehicles are vulnerable today
- Government uses consumer vehicle models for law enforcement, emergency response, and other critical missions

➔ Government vehicles are vulnerable today

- Future vehicles will have more automation and connectivity
- Unless we do something different, future vehicles will be even more vulnerable

➔ Government vehicles will be even more vulnerable in the future

**NOW is the time to do something about this!**

This is the kind of scenario we need to prevent

# THE DAILY NEWS

Thursday, April 16, 2018 THE WORLD'S FAVORITE NEWSPAPER $1.25

# CHAOS AND TERROR

## Cyber-Sabotaged Fire Trucks Crash Into Bombing Scene

**Fire trucks responding to the bombing scene careened out of control after being sabotaged in apparent cyber attacks.**

At least 20 people are dead and hundreds are injured in what appears to be a coordinated terrorist attack. Fire trucks and police units rushing down city streets to the scene of a downtown car bombing had their brakes and steering remotely disabled by cyber attacks.

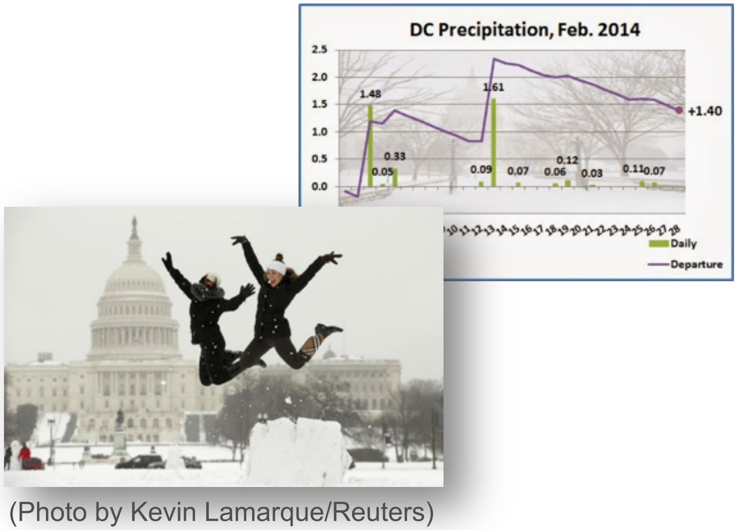
Hundreds of bomb victims lay injured in the streets waiting for hours for help and many died because they did not get to a hospital in time.

According to police sources, officials have been aware for some time that emergency vehicles could be vulnerable to remote "car hacking" attacks but they did not consider it a likely terrorist threat.

# Joint Focus on Vehicle Cybersecurity

- Joint effort among DHS S&T, DOT Volpe Center, and SRI International
- Three primary focus areas:
  - Promote automotive cybersecurity best practices and guidelines in the private sector
  - Discuss key challenges and develop pre-competitive research consortium with industry
  - Address cyber security needs for government vehicles

# Cybersecurity for Government Vehicles – February 2014 Workshop



(Photo by Kevin Lamarque/Reuters)

- Focused on understanding the problem and possible solutions
- Summary of key points raised
  - Security by design and throughout the systems lifecycle; software assurance
  - Main types of solutions being developed: HSMs, firewalls, and IDS
  - Security is needed for wireless entry points, including OTA updates
  - DHS S&T is looking to start programs in the transportation sector
  - Government vehicles have some unique issues and requirements

# Cybersecurity for Government Vehicles – November 2014 Workshop

- Build on the results of the first workshop
- Focus on the development of concrete next steps to secure government vehicles
- Begin forming a community approach for developing and applying both stop-gap and longer-term risk mitigations to better secure government vehicles

- Working sessions
  - Government needs and coordination
  - Industry guidelines
  - Interim steps and testing
  - Key research needs

# November 2014 Workshop – Summary of Breakout Group Results

## Government Needs & Coordination

- Mission-critical use of vehicles
- Limited year/make/models (fleets)
- Ease of attack (vulnerability)
- Attractiveness of target
- Monetary or political gain

## Industry Guidelines

SAE J3061

- Best practices
- Use cases
- Automotive security controls
- Supply chain assurance requirements
- Automotive Information Sharing & Analysis Center (Auto ISAC)

## Interim Steps & Testing

- Best practices for new vehicles and after market components
- Systems / software engineering
- Defense in depth (firewalls & IDS)
- Regular security testing
- Government vehicle test method

## Key Research Needs

- Adaptive/context-aware safe mode
- Supply chain & counterfeit parts challenges
- Application of existing security technology (IDS, firewall, etc.)
- Secure reference models for vehicles

# Cybersecurity for Government Vehicles Steering Group Kickoff Meeting – October 2015

- OBJECTIVE:
  - Provide actionable information on cybersecurity for vehicles operated by federal, state, local, and tribal governments, who all depend on commercially available vehicles for their missions
- MEMBERS:
  - Government fleet managers, technical experts (who are not vendors), researchers, other key stakeholders
- OUTCOMES:
  - Clearing house for threat information, guides for how to actions, information sharing, transition between R&D and operations

# Cybersecurity for Government Vehicles Steering Group Kickoff Meeting – October 2015

- Can You Contribute To:
  - Gathering inputs and requirements for government vehicle cybersecurity?
  - Identifying near term solutions that can be deployed today?
  - Guiding longer-term government R&D?
  - Influencing work by industry and academia?
  - Sharing information on threats, mitigations, and outreach efforts?
- Immediate Next Steps:
  - Group charter, including refinements of objectives and outcomes
  - Review technical document on threats and mitigations
  - Planned presentation at GSA FedFleet 2016 on Jan 26-28

## Session Structure and Presenters

- **Introduction** (David Balenson, SRI International)

- **Summary of Recent Vehicle Cybersecurity Attacks/Vulnerability Research and State-of-the-Art Mitigations** (Kevin Harnett, Graham Watson, Brendan Harris, DOT/Volpe Center)

- **DHS S&T Automotive Cybersecurity R&D Program** (Dan Massey, DHS S&T)

# Thank You

*Headquarters: Silicon Valley*

**SRI International**
333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.2000

*Washington, D.C.*

**SRI International**
1100 Wilson Blvd., Suite 2800
Arlington, VA 22209-3915
703.524.2053

*Princeton, New Jersey*

**SRI International Sarnoff**
201 Washington Road
Princeton, NJ 08540
609.734.2553

*Additional U.S. and international locations*

**www.sri.com**