Security Research in Connected and Autonomous Vehicles

Dan Klinedinst

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Disclaimer

I work for the CERT Division at Carnegie Mellon University.

Most of this research was performed under contract to US-CERT and the US Dept. of Transportation.

I do not speak for the US government.

URLs:

The URLs for all resources in this talk are at:

https://pastebin.com/8e66av75

Background – Who is CERT/CC?

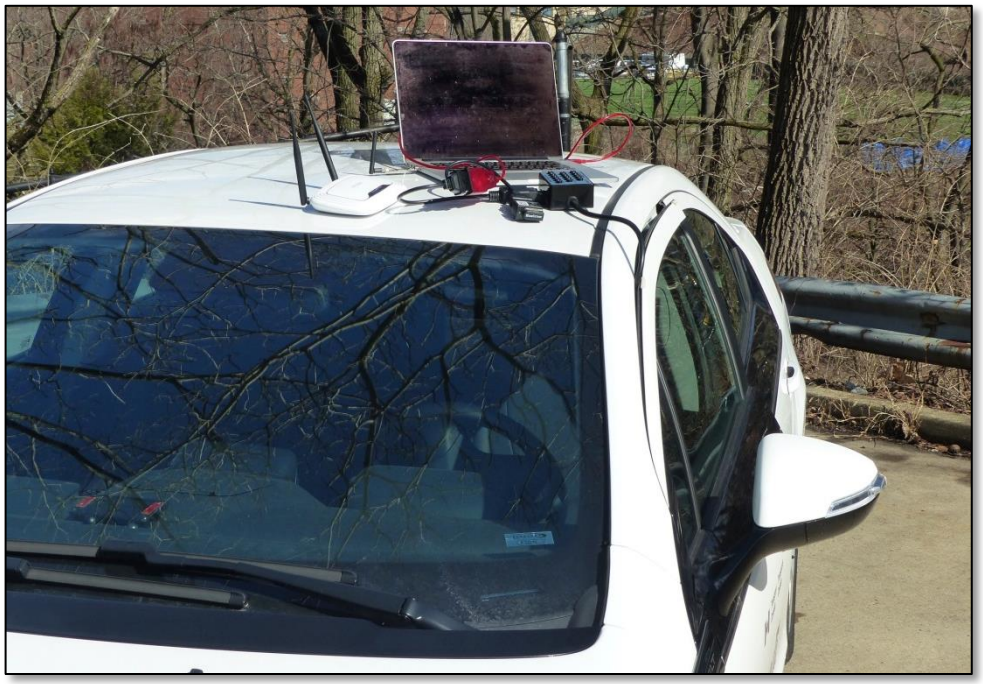
Carnegie Mellon University
- Software Engineering Institute (SEI)
- Federally Funded Research and Development Center (FFRDC)

• CERT/CC
- CERT Coordination Center

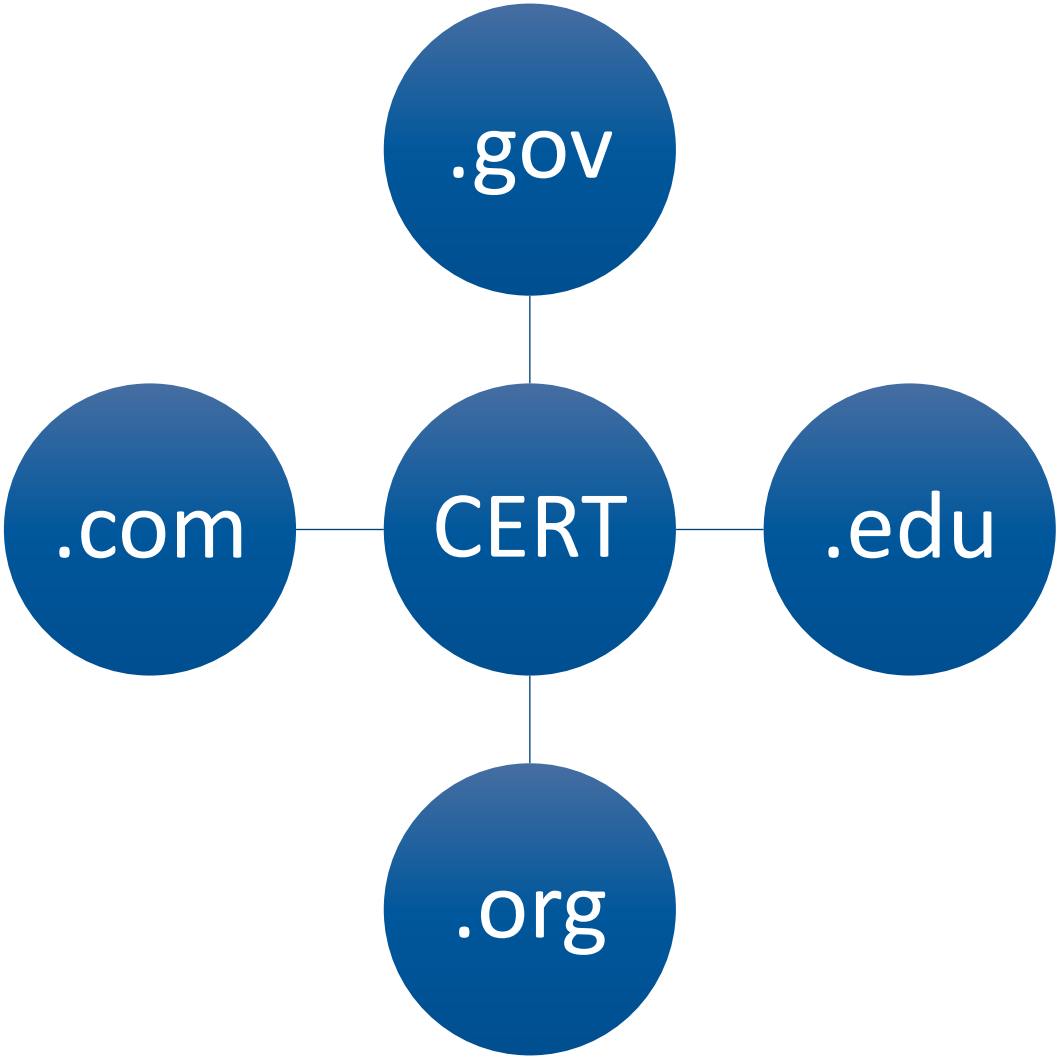
• Vulnerability Analysis
- Sponsorship from US-CERT, Department of Transportation, others

Who Is Dan?

- Vulnerability Researcher on Attack Modeling Team
- Focused on cars, robots, IoT, edge computing
- Previously helped build national penetration testing program
- Co-founder of BSides Pittsburgh



Our place in the industry



Example: CAN vulnerability

- CERT/CC analyzed and forwarded pre-publication information to OEMs and Auto-ISAC

A Stealth, Selective, Link-layer Denial-of-Service Attack Against Automotive Networks

https://www.politesi.polimi.it/handle/10589/126393

Collaborations

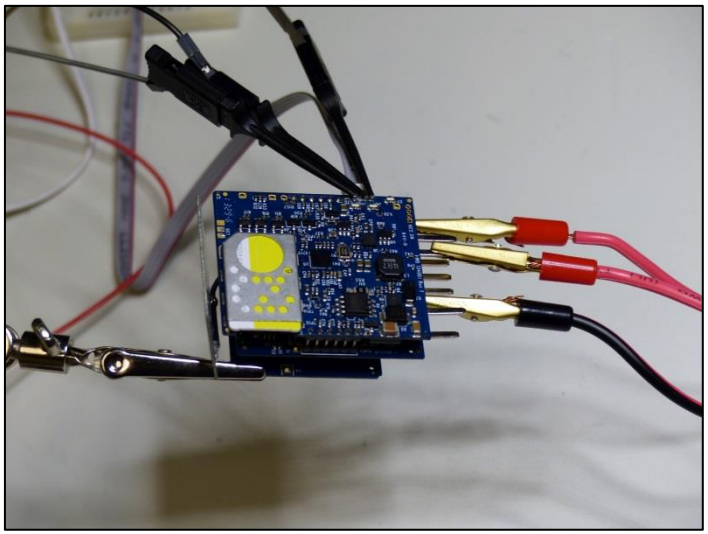
- US-CERT
- Dept. of Transportation
- Auto-ISAC
- SAE
- IEEE Center for Secure Design
- FASTR (Future of Automotive Security Technology Research)
- US Govt. Fleet Cybersecurity Steering Committee
- NMFTA (National Motor Freight Traffic Association)
- Carnegie Mellon Robotics Institute, Traffic 21, Mobility 21

Aftermarket Telematics

On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle

April 2016
By Dan J. Klinedinst, Christopher King

- Collaboration with DoT Volpe Center and US-CERT
- Examined sample of OBD-II devices
- Vulnerabilities in most of them



https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=453871

http://www.kb.cert.org/vuls/id/251927
http://www.kb.cert.org/vuls/id/615456

OEM / Third party / Aftermarket

Heavy Trucks / Buses / Construction

Vulnerabilities in fleet management systems*

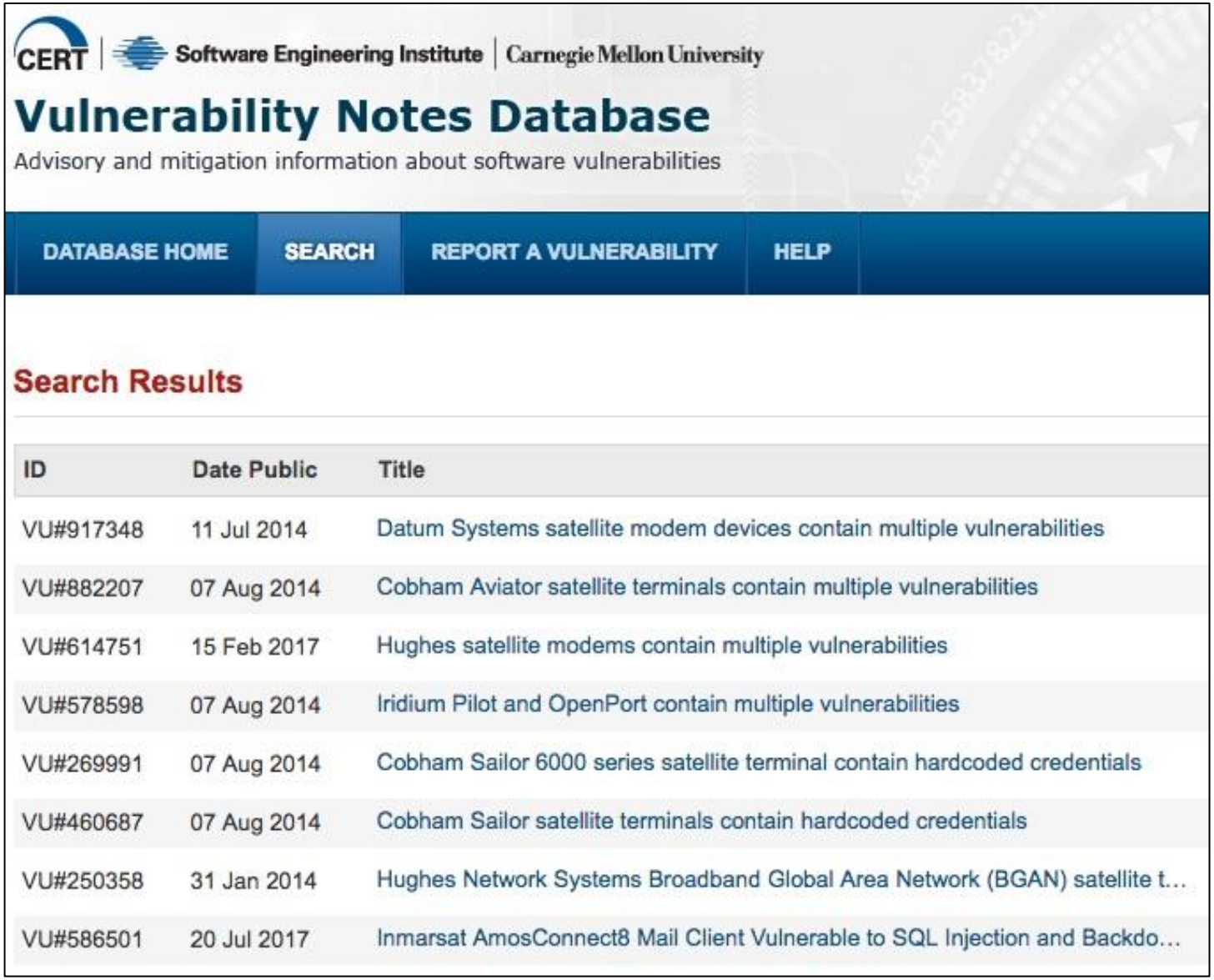
* https://www.youtube.com/watch?v=EWba-wAbQBw

Cellular Security

https://www.escar.info/downloads.html

"Cellular connections… are the front door from the Internet to the vehicle."

Satellite communications are vulnerable, too.



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Search Results

ID	Date Public	Title
VU#917348	11 Jul 2014	Datum Systems satellite modem devices contain multiple vulnerabilities
VU#882207	07 Aug 2014	Cobham Aviator satellite terminals contain multiple vulnerabilities
VU#614751	15 Feb 2017	Hughes satellite modems contain multiple vulnerabilities
VU#578598	07 Aug 2014	Iridium Pilot and OpenPort contain multiple vulnerabilities
VU#269991	07 Aug 2014	Cobham Sailor 6000 series satellite terminal contain hardcoded credentials
VU#460687	07 Aug 2014	Cobham Sailor satellite terminals contain hardcoded credentials
VU#250358	31 Jan 2014	Hughes Network Systems Broadband Global Area Network (BGAN) satellite t…
VU#586501	20 Jul 2017	Inmarsat AmosConnect8 Mail Client Vulnerable to SQL Injection and Backdo…

V2X – US-DOT Pilot Programs

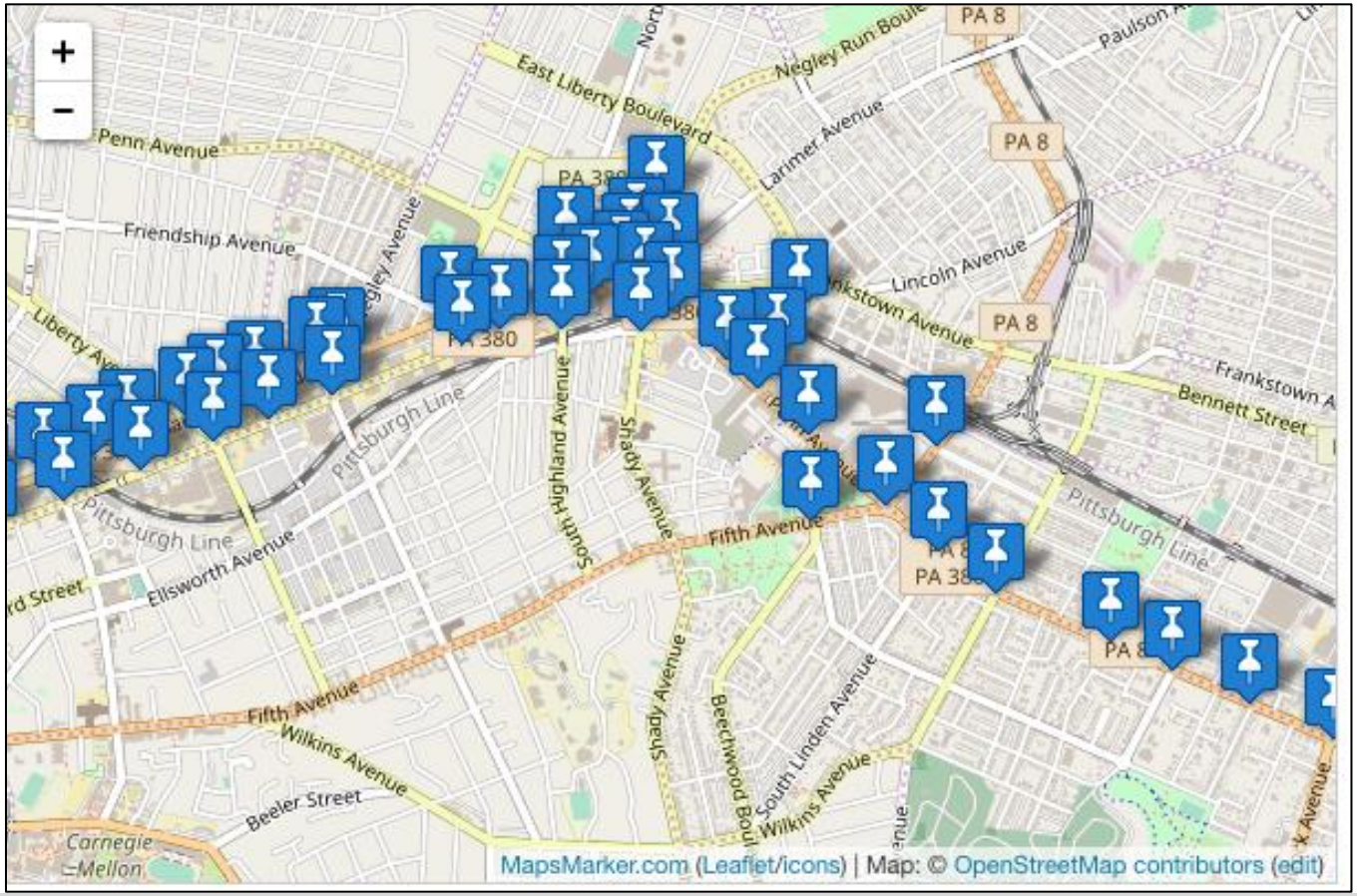
- New York City – Dense urban environment
- Wyoming – Busy freight corridor
- Tampa – Combined expressway / surface streets

V2V and V2I must be secure

- Secure Credential Management System
- Largest PKI deployment in the world
  - 250M cars with hundreds of certificates each
- Security is a big challenge
- Privacy is also a big challenge
  - Obscure location
  - Pseudonym certificates

Intelligent Traffic Signal Testbed

City of Pittsburgh /
Carnegie Mellon Robotics Institute

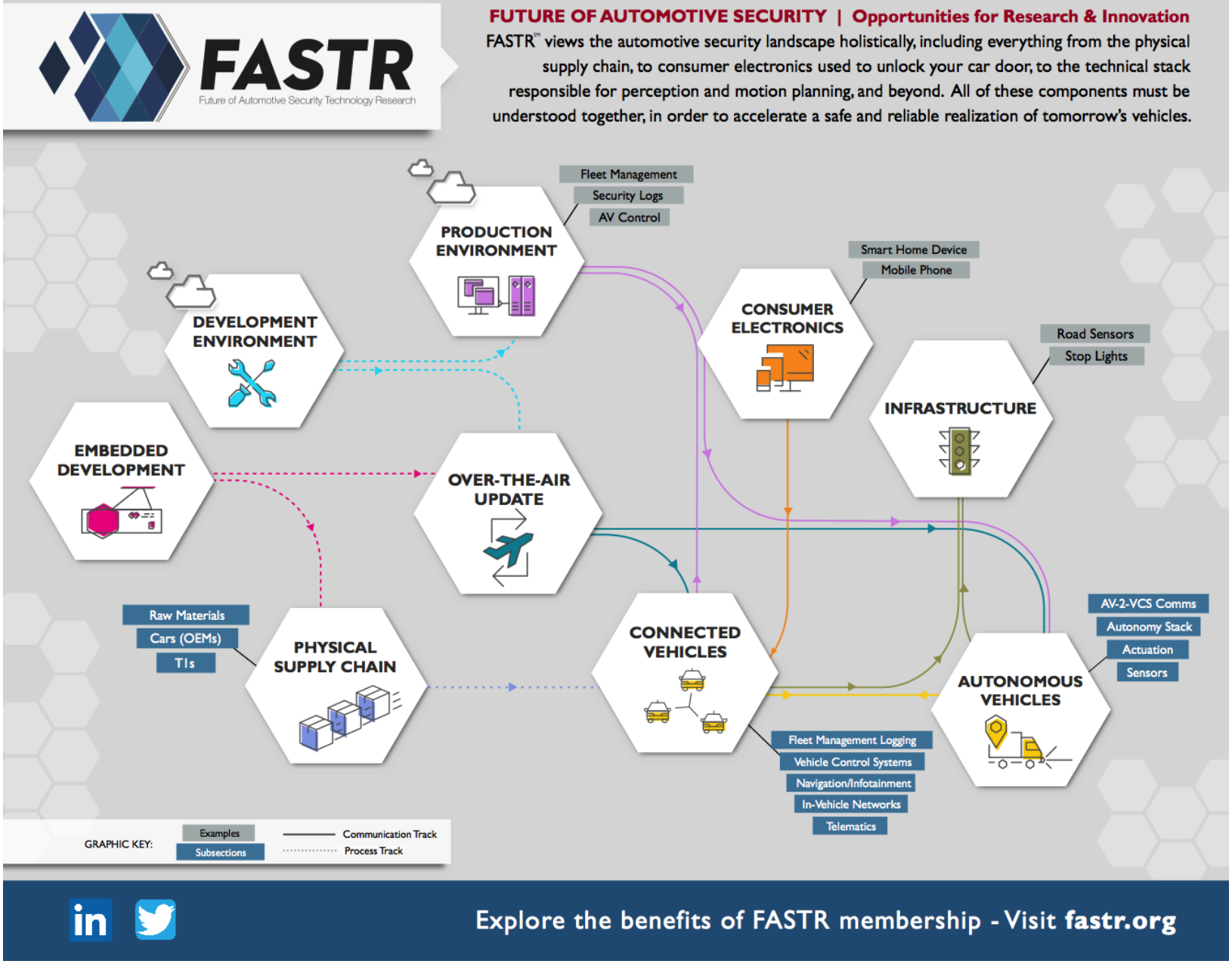


Uber Advanced Technology Center
Pittsburgh, PA, USA

Standards / Best Practices Work

- **NHTSA (US-DOT) Cybersecurity Best Practices**
- **National Telecommunications & Information Administration (NTIA)**
  - Series of guideline documents on IoT, vulnerabilities, etc.
- **Auto-ISAC Automotive Cybersecurity Best Practices**
- **IEEE Center for Secure Design**
  - "Design Flaws and Security Considerations for Telematics and Infotainment Systems"
- **FASTR Guidelines for Secure Over-The-Air (SOTA) Updates**
- **SAE J3061**

https://pastebin.com/8e66av75



Training from CERT Coordination Center

- Vulnerability Response Capability Development
- One day course, delivered at your site
- Basics of setting up a vulnerability response program
- Communications, tools, bug bounties, etc.
- 30 years of “lessons learned” from CERT/CC
- Software, hardware, cyber-physical products
- https://www.sei.cmu.edu/training/P123.cfm

Questions?

Contact Information:

Dan Klinedinst

djklinedinst@cert.org

Public Vulnerability Information:

www.kb.cert.org/vuls