Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Panel Discussion: Data Protection, Privacy and Security, and Smart Cities

Feb 1st, 2017

JOHN FEO, DIRECTOR, NORTHWEST INSTITUTE FOR ADVANCED COMPUTING

Pacific Northwest National Laboratory

GCTC Super Action Cluster Summit, Portland, OR

U.S. DEPARTMENT OF ENERGY

Panel Overview

- This panel will discuss transportation cybersecurity issues within a Smart Cities framework with an emphasis on privacy, trust, and identity, and EV charging, storage, and electrification. The panel will discuss the current technological state of practice, critical issues, and future/emerging capabilities.
- Participants:
  - Jeff Alan, Executive Director, Drive Oregon
  - Weisong Shi, Professor of Computer Science, IEEE Fellow
  - Isaac Potoczny-Jones, CEO, Tozny
  - Lorie Wigle, General Manager, IoT Security
  - Sean Docken, ICS-CERT, DHS

Thank you!

EVBatteryGuard: A Sustainable, Reliable and Safe Battery System for EVs

Weisong Shi

Wayne State University

weisong@wayne.edu

Motivation

- Role of battery is critical for EVs
  - Only energy source for a vehicle
  - Revolution from engine to sensors
  - Possible LSI integration
- Problem
  - How to design new battery system make the only energy system efficient, fault tolerant, and secure for EV
- Goals
  - Redesign battery system in EV toward sustainable, reliable, and safe
  - Protect the battery from hazardous and inefficient operating condition
  - All computation finished in real time

Background

- State of Charge(SOC)
  - Indicator of left capacity
  - Key factors: temperature, cell age, charge/discharge rates, etc.
  - Nonlinear battery dynamic modeling
  - Kalman Filter approach
- State of Health(SOH)
  - Measure of how well the battery can function compare to a fresh battery
  - Key factors: internal resistance, charge acceptance, self-discharge, etc.

Challenges

- Limited power capacity
- Lack of research/tools that enable users to extend battery life on demand
- Efficient power-management requires
  - Power requirements may change suddenly and dramatically
  - Calculation should be done in real time to avoid obsolescence
- Cell balancing architecture design
  - Lack of approaches to manage the discharging of the individual cell
  - Highly sensitive to operating parameters and battery chemistry

Our Solution: EVBatteryGuard

- *Key Idea*: *edge vehicular data analytics platform* for battery system
- Battery lifetime extension
- Battery cell failure predication and recovery
- Abnormal battery behavior detection
  - Anomaly detection on charging/discharging
  - Fingerprinting battery cells for tamper resistance

Why Edge Computing?

- Not new, a classical example is Web cache
- But …
- Push from Cloud providers
  - Reduce latency, e.g., 30ms
  - Improve efficiency
  - Save bandwidth
- Pull from Internet of Things
  - Real time context computing
  - Resc
  - Secu

amazon web services EC2

Azure

Aliyun
Alibaba Cloud Computing

Enabled by the rapid growth of computing and communication technologies

IEEE Computer, May 2016

The Promise of Edge Computing

Weisong Shi, Wayne State University

Schahram Dustdar, TU Wien

The Second ACM/IEEE Symposium on Edge Computing

San Jose, CA, October 12-14, 2017

- Program Chairs
  - Mung Chiang, Princeton University
  - Bruce Maggs, Akamai Technologies/Duke
- Steering Committee
  - Victor Bahl, Microsoft Research
  - Flavio Bonomi, IoXWorks
  - Rong N. Chang, IBM Research
  - Dejan Milojicic, HP Labs
  - Michael Rabinovich, Case Western Reserve University
  - Weisong Shi, Wayne State University (Chair)
  - Tao Zhang, Cisco

Due: April 2nd, 2017

Industry Partners

- **BASF Battery Materials**
  - Provide consultant to our team
  - Cell materials performance
- **DENSO International America (in progress)**
  - Vehicle related data
  - Driving behaviors
  - Battery statistics
- **NextEnergy**
  - Testing environment
  - Charging station access
- **GM Battery Engineering (in progress)**
  - Battery architecture
  - Collaborate on battery behaviors

Additional Information

http://mist.cs.wayne.edu

weisong@wayne.edu

Prior Work

- Power profiling tools
- Autonomous battery cluster system (ABC)
- Failure predication and recovery
  - disk for large scale data centers
- Abnormal behavior detection in computer systems

Privacy, Security, and Trust

Do More with Data by Doing Right with Data

Isaac Potoczny-Jones
ijones@tozny.com
http://tozny.com/

TOZNY

Overview: Trusted Identities Group Pilot

- Tozny has a pilot program with NIST's Trusted Identities Group
- Collaborating locally with moovel (transit) and IOTAS (IoT)
- Our focus is on privacy and security for normal people
- We build crypto, policy, and privacy tools for software developers

NIST & TOZNY

Connected Transportation Vulnerabilities

“Increased security threat from cyber and data privacy breaches is the *number one risk* on the minds of executives in the transportation industry,”

- Willis Towers Watson (Oct, 2016)

It outranked:

- Geopolitical Instability
- Regulatory Uncertainty
- Talent Management
- …

TOZNY

When does a “vulnerability” become a “threat”?

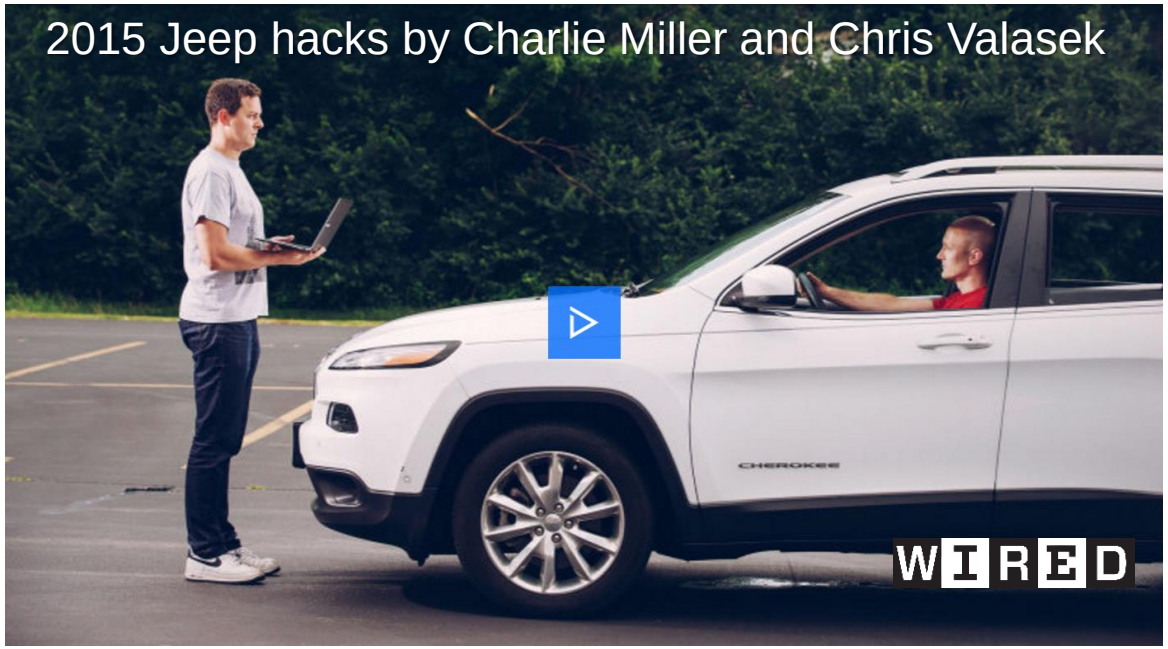
When

Value-to-Attacker > Cost-of-Attack

- Systems get easier to attack over time (CoA goes down)
  - In the old days, only sophisticated attackers could carry off hacks
  - Hacking software is like all other software. The user interface gets better
- Systematic weaknesses take a while to clean up
  - Systems we deploy today will be with us a long time
  - Cost to fix problems goes up
- Attackers’ motivations tied to financial and political needs
  - Value-to-attacker is outside the control of risk managers

TOZNY

Connected Vehicles are Vulnerable



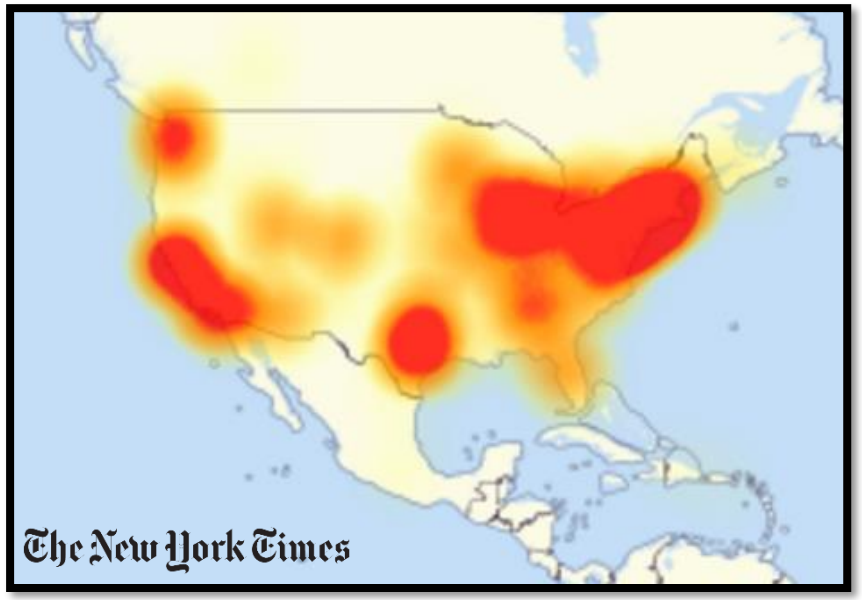
- Remotely disabled a vehicle on the highway
- Parts of the attack were very standard security misconfigurations
- Although the end-to-end attack was extremely complex

Lesson: Today, connected cars are hard to attack and there is little value in doing so. In the future, this may not hold true.

TOZNY

IoT Devices: Crashing the Internet

In October, a massive attack took out a big chunk of the Internet



- Accomplished by hacking computers in people's homes & businesses
- These systems were very easy to attack – used default passwords
- Large scale attack wasn't until there was strong motive

Lesson: Systems get attacked when the bad guys get value from attacking.

TOZNY

Doing the same thing over & over again…

- When email started with ***no*** security
  - Everyone knew everyone else and there was no value in hacking it
  - This persisted until SPAM made email almost unusable, 25 years later
  - We've been trying to bolt security on ever since

- The same security mistakes for each new technology
  - **Technical**: Bad encryption, bad login security, out of date software
  - **Policy**: Too much trust between systems, bolting-on security
  - **Privacy**: No visibility, no consent, collecting more than we should

IoT same story: Fast growth, terrible security

TOZNY

Connected Transportation Should Be:

1. **Authenticated and Secure:** It should be a part of the internet…
   - While maintaining appropriate segregation

2. **Interoperable and Compositional:** Protocols to work together
   - Applies to auth, crypto, and wireless

3. **Privacy-Preserving:** Take users into account
   - Avoid intentionally or unintentionally tracking users

4. **Risk-Based**: How to balance the limitations with the risk
   - Power, networking, crypto, and UI

TOZNY

Let's Face it: Security Gets in the Way

We could innovate faster…

…If Security was not a problem.

But Security matters…

…Think of it as a foundation, not a gate.

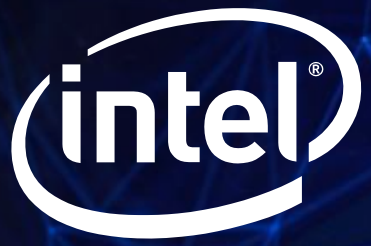
Do **more** with data by doing **right** with data.

TOZNY

Thank You!

Isaac Potoczny-Jones
ijones@tozny.com
http://tozny.com

TOZNY



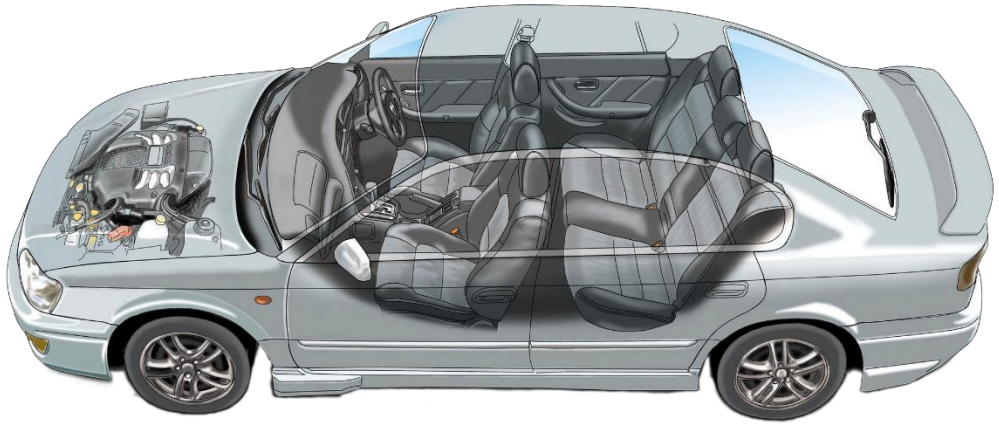
Next generation cars & cybersecurity

Lorie Wigle, General Manager, IoT Security

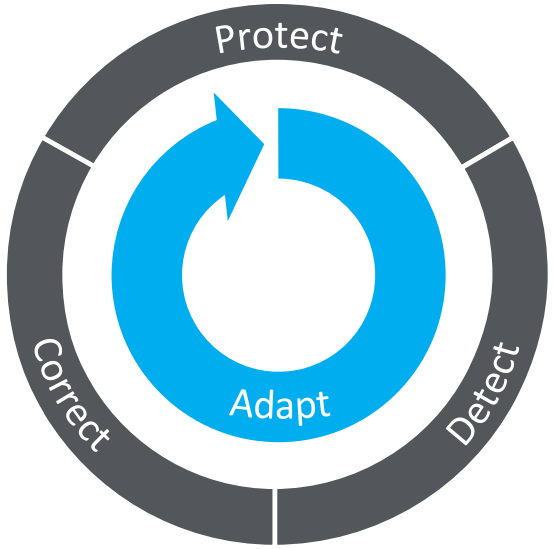
Cars are a special security challenge that is becoming even more complex

- System of Systems
- Safety and Security must be addressed
- Heterogeneous supply chain
- Protection required over long life – 8-15 years
- Connected cars have increased attack surface
- Clouds and infrastructure must also be secured

	Current State Low Complexity	Future State High Complexity
Vehicle Connectivity	Limited/Expanding (Telematics, Infotainment)	Fully Connected Environment (V2V, V2I, V2X)
Vehicle Automation	Developing/Immature (Partial/Semi-autonomous)	Pervasive/Highly Developed
Data Analytics	Focus on Vehicle Performance/Location	Focus on Consumer Experience/Personal Data



Addressing the threat defense lifecycle



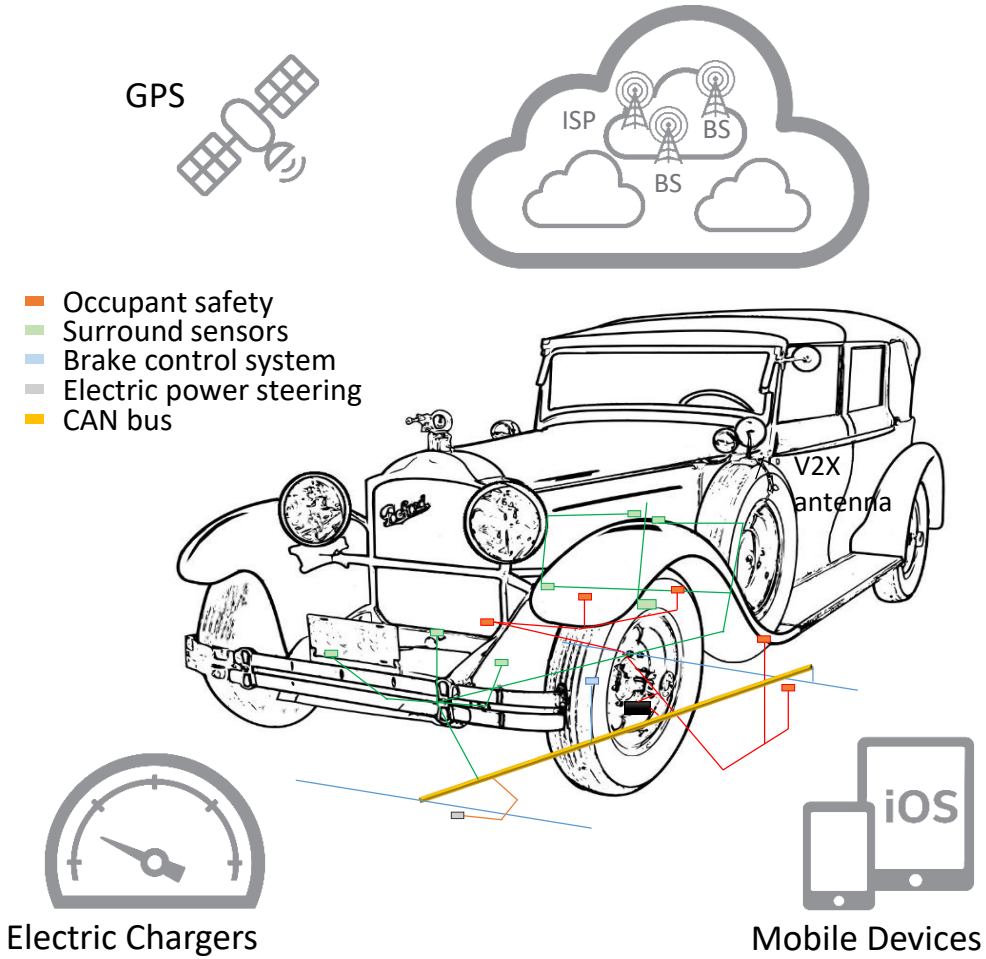
Protect – products and assets from tampering and misuse within the supply chain, while operating, and after deactivation

Detect – identity of hardware and software, the integrity of running software, the presence or absence of malware, the use of unauthorized services or applications, and verification of the safe deactivation of the device

Correct – loss of integrity, without regard to the genesis of the loss, through the execution of a predefined corrective action plan that preserves current operations and data

Adapt – Apply insights throughout an integrated security system.

Defense-in-Depth



Defense in Depth

Software and Services

1. Over-the-air updates
2. IDPS/anomaly detection
3. Network enforcement
4. Certificate management services
5. Anti-malware and remote monitoring
6. Biometrics

Hardware security services that can be used by applications

Fast cryptographic performance
Device identification
Isolated execution
(Message) authentication

Hardware security building blocks

Platform boot integrity and chain of trust
Secure storage (keys and data)
Secure communication
Secure debug
Tamper detection and protection from side channel attacks

Security features in the silicon, for example, memory scrambling, execution prevention, and more

Analog security monitoring under the CPU

Hardware Root of Trust