Trust & Privacy: Information Security and Identity Management for Autonomous Vehicles

March 31, 2016
Who We Are

• Exponent, Inc. is an engineering and scientific consulting firm providing services to a broad range of industries for almost 50 years.

• Consulting staff of more than 800 with 26 offices worldwide

• We provide independent, in-depth design reviews, analysis, testing and strategic consulting in more than 90 unique disciplines. We are well-known for our quality, independent investigations and well-recognized for our validation and testing methods. Exponent is certified to ISO-9001.
Exponent Offices

San Francisco Bay Area:
- Menlo Park
- Oakland

Southern California:
- Irvine
- Los Angeles

Chicago:
- Downtown Chicago
- Warrington

Detroit

Boston:
- Maynard
- Natick

New York

Philadelphia

Washington DC:
- District of Columbia
- Maryland
- Virginia

Atlanta

Miami

Shanghai

Hong Kong

Derby

Harrogate

Düsseldorf

Basel
Test and Engineering Center (TEC), Phoenix AZ

Test and Engineering Center, Phoenix, Arizona
Central Facilities on Our 147-Acre Site
Security and Identity team

Brad McGoran, P.E. CSCIP-G, GSLC
Program manager, identity management, credentials, smart cards, payments

Christopher Williams, Ph.D., OSWP
Data collection, communications, sensors, embedded security, and cryptography, policy and evaluation

Ellick Chan, Ph.D.
Deep learning (teaches at Northwestern U.), and security

John Fessler, Ph.D., P.E. CSCIP, GSLC
Risk and reliability analysis, identity management, mobile device ecosystem

Srinivasan Jagannathan, Ph.D., M.B.A., CISSP, GSLC
Source code and software forensics, intellectual property analysis

Adam Sorini, Ph.D., CCFP-US
Digital forensics of consumer electronics, firmware, software, intellectual property analysis
Connected and Autonomous Vehicles

*Newly established hardware networks present new threats*

- Impossible to firewall external communications from vehicle operation without full vehicle redesign
- Increasing number of attack vectors as vehicles become autonomous and new sensors are added
- Vehicle manufacturers entering a market of connected devices where there is little precedence
- New vendors entering market that do not have experience in vehicle manufacturing
- Creation of third-party hardware and software solutions for autonomy
Connected and Autonomous Vehicles

Newly established hardware networks present new threats

• Threats:
  – Person: Remote take-over of vehicles can endanger passengers
  – Infrastructure: Vehicle-to-vehicle communication malfunction can cause mass gridlock
  – Privacy: Each connected vehicle is an entry point for hackers to access network putting personal information of all drivers at risk
  – Zombies: Unsupported & obsolete hardware still in use represent a threat even after solutions and patches are issued for discovered exploits

• Mitigate these risks through system of robust authentication and identity management
Strong Identity Management and Secure Authentication are Key Steps to Mitigate Threats to Connected Vehicles and Systems

- A Strong Identity Management System Helps Safeguard:
  - Physical Access
  - Logical Access

- Secure Authentication Can Help Safeguard:
  - User to System Communications
  - System to System Communications
  - Component to Component Communications (IoT)
Case Study: Identity Management Protecting DoD Networks and Connected Systems

*Embedded security proved transformative for network security at the Department of Defense*

- Exponent has supported DoD with their Identity Management Program and Systems since 2000
- DoD’s introduction of smart cards with cryptography key pairs reduced network intrusions by **almost half overnight (46%)**.
- More recently, the U.S. Army cut classified leaks by 85 percent using a software program tied to their smart card-based Common Access Card (CAC).
- >30 million Common Access Cards (CAC) issued
- CACs deployed with chip employing Public Key Infrastructure (PKI) encryption and signing.
- 3.5-4 million CACs in active use
Recent DoD Progress in Securing Communications and Strong Identity Management Applied to Connected Vehicles

- Exponent is helping DoD secure wireless (NFC) communication of authentication credentials and personal identifying information (PII) to/from mobile devices.

- OPACITY protocol
  - Open standard to for secure communication
  - Leverages fast PKI through elliptic curve cryptography

NFC + Elliptic Curve Cryptography + ECDSA + AES = Strong Mobile Authentication
Two Key Steps to Enhance Security For Connected Vehicles and Information Transfer

- Use embedded secure technologies for Person-to-Vehicle and Vehicle-to-Passenger mutual authentication and privacy through PKI based communications.

- Use the vehicle itself as the token to authenticate passengers to outside world (secure site access, payments, tolls, vehicle-to-vehicle, etc.)
Threat mitigation through embedded secure technology

- **Threats:**
  - **Person:** Remote take-over of vehicles can endanger passengers
  - **Infrastructure:** Vehicle-to-vehicle communication malfunction can cause mass gridlock
  - **Privacy:** Each connected vehicle is an entry point for hackers to access network putting personal information of all drivers at risk
  - **Zombies:** Unsupported & obsolete hardware still in use represent a threat even after solutions and patches are issued for discovered exploits

**Person-to-vehicle**
authentication for vehicle control (e.g. 2-factor when web browsing)

**Vehicle-to-vehicle**
authentication and PKI

**PKI for data communications**

**Policy and Regulation**
designed around autonomous vehicle use cases and lifespans