About me!

- I am a **CIVIL ENGINEER**! (The only one currently in the Hume Center)

- Started research cybersecurity when investigating *operations* of automated vehicles

- The biggest obstacles to completely driverless cars (Level 5) is *cybersecurity liability*.

- The operations of future vehicles are dependent on the mitigation of cyber threats.
Hume Center Transportation Program Summary

**Electronic Systems Lab**
- Assured Communications
- Radar and Spectrum
- Electronic and Cyber Warfare
- Counter A2AD

**Information Systems Lab**
- Embedded System Security
- Secure and Resilient Infrastructure
- Applied Deep Learning
- Security and Privacy for IoT

**Government Needs**
- Assured Communications
- Embedded System Security
- Secure and Resilient Infrastructure
- Security and Privacy for IoT

**Industry Needs**
- Assured Communications
- Embedded System Security
- Security and Privacy for IoT
Focus Area: Cyber-Physical System Security

Research Areas

- Embedded
  - RTOS Access Control
  - Physically Unclonable Functions
  - Embedded RNG
  - AES Sidechannel Attacks
  - Whitelist firewall for SCADA transactions

- Wireless
  - LTE Jamming
  - LTE/EPC Security
  - Android Security
  - Software Radio Exploitation
  - Mobile Key Management

- Transportation
  - Key FOB Security
  - Vulnerability Assessments
  - V2X Security
  - ADS-B Encryption
  - UAV C2 Attacks
  - Navy Airworthiness Center

CIKR Security
Safety-Critical Systems
IOT Privacy

8/21/2017
Intelligent Transportation Infrastructure

• Traditional Intelligent Transportation Systems have been shown to be vulnerable.
  • Traffic Signals
  • Variable Message Signs
  • Electronic Toll Collection
  • GPS Navigation
  • Vehicle to Infrastructure Communication
  • Road Weather Information Systems
  • Weigh-In-Motion Systems
  • Traffic Operating Center Communications

• DOTs need assistance to secure venerable systems
Communications Domains in Surface Transportation

- Each domain requires security to ensure safety and efficiency of the transportation system
- Integrated infrastructure and vehicle security is needed

**Infrastructure Domain**
- Trusted 3rd Parties
- Services Providers
- Trust Authorities

**V2X Domain**
- RSU
- OBU

**In-Vehicle Domain**
- AUs
- ECU
- Sensor
- GNSS
- TPM
Potential Traditional Vehicle Vulnerabilities

- Vulnerabilities Include:
  - On-Board Diagnostic Security
  - Tire Pressure Monitor Security
  - Key Fob Security
  - Infotainment Security
Advanced Vehicle Communication and Sensing

- Communication systems and sensing systems add attack vectors that have not been seen in previous iterations of vehicles.
- These technologies enable efficiencies and create vulnerabilities.
Attacks possible on next generation vehicles

Communication security system
Provides and verifies V2V security certificates to ensure trust between vehicles

GPS, DSRC antennae

In-vehicle components

Dedicated Short Range Communications (DSRC) radio
Receives and transmits data through antennae

GPS receiver
- Provides vehicle position and time to DSRC radio
- Provides timekeeping signal for applications

Driver-vehicle interface
Generates warning issued to driver

Vehicle’s internal communications network
Existing network that interconnects components

Memory
Stores security certificates, application data, and other information

Safety application electronic control unit
Runs safety applications

This in-vehicle equipment can consist of either a single, integrated unit or a discrete set of components

Sources: Crash Avoidance Metrics Partnership and GAO.
Threats to ITS and Vehicle Systems

Additional solutions include:

**ITS Threats**

<table>
<thead>
<tr>
<th>Availability</th>
<th>Identification and Authenticity</th>
<th>Confidentiality and Privacy</th>
<th>Integrity and data trust</th>
<th>Non-Repudiation and Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of service</td>
<td>Man in the middle attack</td>
<td>Eavesdropping</td>
<td>Message tampering</td>
<td>Loss of event traceability</td>
</tr>
<tr>
<td>Jamming</td>
<td>Sybil</td>
<td>Traffic analysis</td>
<td>Message tampering</td>
<td>Wormhole</td>
</tr>
<tr>
<td>Broadcast tampering</td>
<td>Replay</td>
<td>Information gathering</td>
<td>Message suppression and alteration</td>
<td>etc.</td>
</tr>
<tr>
<td>Greedy behavior</td>
<td>GPS spoofing and position faking</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
<tr>
<td>Black hole</td>
<td>Masquerading</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
<tr>
<td>Malware</td>
<td>Tunneling</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
<tr>
<td>Spamming</td>
<td>Key/Certification replication</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
<tr>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>

**ITS Attacks**

- Bit commitment and signature
- Frequency hopping technique
- Authentication and non-repudiation
- Digital signature of software
- and sensors
- etc.

**ITS Security Solution**

- Digital certification and zero knowledge
- Trusted hardware
- Central Validation Authority
- Time stamping mechanisms
- Bit commitment and signature with positioning system
- Digital signature of software and sensors
- etc.

- Encryption of data and the corresponding positioning vehicle identification.
- Variable MAC and IP address.
- etc.

- Group key management system
- Zero knowledge technique.
- etc.

- Trusted hardware (modification only by the authorized). 
- etc.
Conclusions

• Next generation vehicles hold great opportunities to increase safety and improve operations.

• These benefits may be mitigated as cyber threats may limit the capabilities of these vehicles.

• ALL engineers and operators should be knowledgeable in cybersecurity.