Vehicular Cyber-security Challenges

Zeinab El-Rewini, Karthikeyan Sadatsharan, Dr. Prakash Ranganathan
Data, Energy, Cyber and Systems (DECS) Laboratory,
School of Electrical Engineering and Computer Science (SEECS), University of North Dakota

DECS — DATA, ENERGY, CYBER AND SYSTEMS

UND School of Electrical Engineering & Computer Science
UNIVERSITY OF NORTH DAKOTA

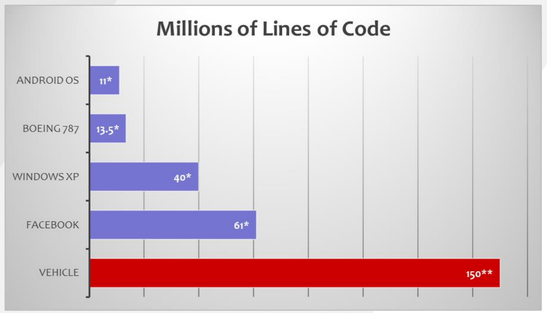
Motivation

Cybersecurity is a growing concern among vehicular manufacturers, transportation policy makers, drivers, and other third-party software service providers. Hackers, terrorist organizations, hostile intruders are possible attack vectors in exploiting communications causing sensor manipulation, disastrous collisions and traffic disruptions in vehicles. Today's modern vehicles are well-advanced that each vehicle contains atleast 80 or more processors, several in-vehicle networks, cables, I/O ports, and millions of lines of code. This combination of firmware increases the threat landscape. For example, according to Ford motors, F-150 Pickup truck has 150 Millions of Lines of Code in the overall architecture, which is higher than a modern Operating System or a Boeing 787. The following are challenges that hinders cyber security solutions:

- Limited external connectivity of the vehicle (Due to mobility)
- Limited Computational Performance (Due to high endurance and long life-cycle)
- Unpredictable attack scenarios and threats
- Hazard to drivers and passenger lives

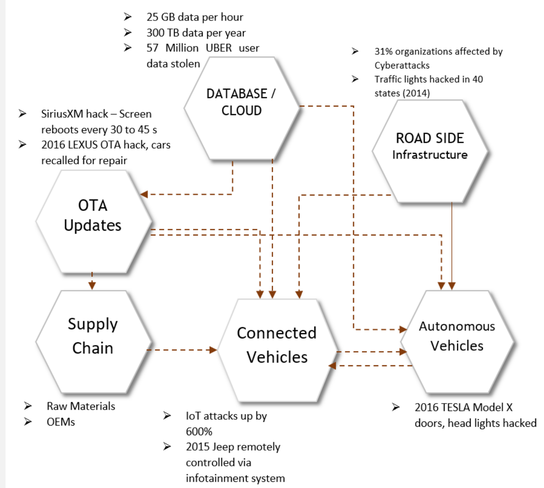
This poster classifies the attack types and security properties in vehicular networks in three hierarchical layers: sensing, communication, and control layers.

Overall Lines of Code (LoC)



*https://informationisbeautiful.net/visualizations/millions-of-lines-of-code/
** Source: Ford F- 150 release notes

Cyber Attacks - Statistics

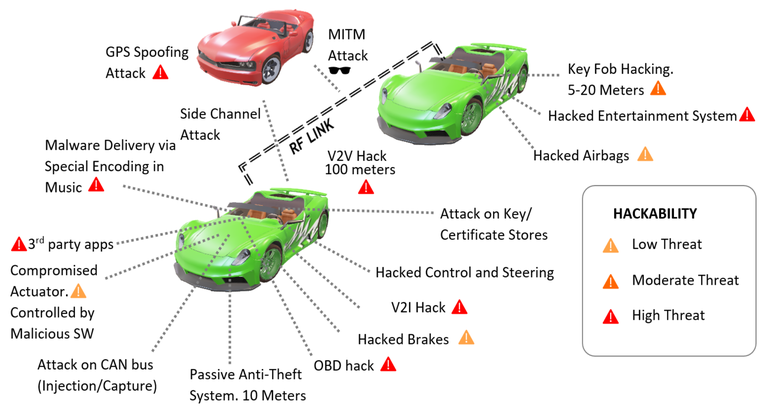


Multi-Layered Approach

According to NHTSA (National Highway Traffic Safety Administration), a comprehensive, multi-layered and methodical approach is required to address the cyber security challenges. The following are some examples:

- A risk-based identification and protection process for safety-critical control systems is necessary.
- Timely detection and proper response to security threats on roads;
- Architectures, methods, and measures that improve resiliency of the system and facilitate rapid recovery when any incidents occur; and
- Methods of effective intelligence and data communications across the industry to enable quick adoption of industry-wide lessons learnt. NHTSA encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.

Attacks in a Vehicular Ecosystem



Future Scope

With vehicle platooning being one of the upcoming technologies, a number of security vulnerabilities may soon surface, especially in instances where two platoons communicate with each other. Platoon connectivity sharing (MIMO) and On-the-Fly platooning are two scenarios where the possibility of security attack is high considering the number of different electronic systems that are involved. Further in-depth analysis of these test scenarios could be an area of future research.

Vehicular Cyber Threat Model

Attack	Property	Ease of Attack	Detection probability
Eavesdropping	Confidentiality Privacy	High	Low
Blinding Attack	Integrity Real-Time constraint	Moderate	High
Magnetic Attack	Privacy,Integrity, Availability Real-time Constraint	High	Low - Human, High - System
Illusion Attack	Authentication, Integrity	Low	Low - Driver and System
GPS Spoofing	Authentication, Privacy	High	Low
Black Hole Attack	Availability, Confidentiality, Integrity	Moderate	Moderate
Identity and Location Tracking	Privacy	High	Low at high traffic density
Bogus Information Attack	Integrity, Authentication	Moderate	Low - Driver, Moderate - System
Denial of Service	Authentication, Availability	High	High
Sybil Attack	Authentication, Availability	High	Moderate
Impersonation Attack	Integrity, Authentication	Low	High
Alteration/ Replay Attack	Integrity, Authentication	High	Low
Timing Attack	Availability, Real-time Constraint	High	High
MITM	Confidentiality, Integrity, Authentication	Moderate	Moderate
Injection Attack	Integrity	Moderate	Moderate-Driver, High-System