CyberSecurity
On Vehicles

Prof. Antonio Mauro, PhD
email: info@antoniomauro.it
Mobile: +39 335 6305073
About me...


- **Professor at University of Northwest** – U.S.A. - Department of Engineering – Computer Science and Member of the Academic Board;

- **Professor at University of Modena e Reggio Emilia** and **CRIS**: Interdepartmental Research Center in Security and Risk;

- **Professor at University of Milan, University of L’Aquila and University of Tor Vergata** – computer forensics and digital investigations


- **United Nations Office Drugs and Crime** (UNODC), **Euopen Police College** (CEPOL)

- Books and articles, Speaker at National and International events

- Permanent member at “The Osservatorio per la Sicurezza Nazionale”, by “The Ce.Mi.S.S. - Centro Militare di Studi Strategici” – **Ministry of Defense** – Italy and **New York/New Jersey Electronic Crimes Task Force** (NYECTF) - U.S. **Secret Service.**

- judge consultant of the Court of Justice in Rome (Digital Forensics and Investigations)
Car Story
Car Story
Do you remember...

Link 1:
Link 2:

Knight Rider
Car Story
Future Car

Connected Car
Future Car

Autonomous Car

Prof. Antonio Mauro, PhD
info@antoniomauro.it
What is a Car?

Cars are complex, highly-connected networks!
Facebook – 50M LoC
Connected Car – 100M LoC
Autonomous Car – 300M LoC

Source: http://www.informationisbeautiful.net/visualizations/million-lines-of-code/
CAN: Controller Area Network

- Low-level network protocol
- Part of OBD-II standard
- ECU: Electronic Control Unit
  - In modern cars there are hundreds of ECU and the CAN Bus is designed to allow data exchange between ECU and devices within a vehicle without a host computer
CAN Bus security design flaw:
- ALL nodes receive ALL messages
- Optimized for speed and reliability, not security
- Most transmissions are not authenticated
What is connected to CAN Bus?

- OBD-II port
- Media player
- Bluetooth
- Telematics unit
- Lightning System
- And many more…
The more the car is connected, the more the car is exposed to attacks.
**CAN Bus attack: entry point**

**From outside the vehicle:**
- Bluetooth (short range)
- WiFi (medium range)
- Cellular (long range)
- Radio Data System (long range)

**From inside the vehicle:**
- Audio input options: CD, USB
- OBD-II diagnostic ports
- Dashboard keyboard
Why infecting or compromising a car?

I’m a hacker but I’m harmless! Just for fun!

I’m a hacker but I’m a terrorist! Not for fun!
Nowadays or future scenario?

Can a compromised vehicle infect other cars?
Just an example

- Can I use the car to send the messages around the world? (like «pizzino elettronico» – digital hint);

**Car Message:** put a bomb in time square
Some questions

- Is it possible to prevent this attack?

- Can we intercept this message/communication?

- Can we use the car system for a massive attack (like DDoS)?

- What about Forensics investigation on Vehicles?
Five Star Automotive Cyber Safety Framework

- Safety By Design
- Third Party Collaboration
- Evidence Capture
- Security Updates
- Segmentation & Isolation

Source: iamthecavalry
## Standards

In synthesis the standards used in SAE J3005 is:

<table>
<thead>
<tr>
<th>Electrical</th>
<th>Usage</th>
<th>Communication</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAE J1962</td>
<td>Requirements of an OBD connector as required by U.S. On-Board Diagnostic (OBD) regulations</td>
<td>SAE J1978</td>
<td>Requirements of an OBD scan tool</td>
</tr>
<tr>
<td>ISO 15765</td>
<td>Requirements for controller area networks (CAN)</td>
<td>ISO 1503-4</td>
<td>Spatial orientation and direction of movement</td>
</tr>
<tr>
<td>ISO 11898-2</td>
<td>Specifies the high-speed transmission rate</td>
<td>SAE J1699/2</td>
<td>Define test cases for the OBD-2 interface on external test equipment</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>Road vehicles –Functional safety</td>
<td>ISO 15765-4</td>
<td>Requirements for controller area networks</td>
</tr>
</tbody>
</table>
Other Standards

J3061 – Cybersecurity Guidebook for Cyber-Physical Automotive Systems: Provides an automotive security guidebook that will help drive a process to address all the Cybersecurity threats the automotive environment is experiencing.

- APPENDIX D: Security & privacy controls description and application
- APPENDIX E: Vulnerability databases and vulnerability classification schemes
- APPENDIX G: Current cybersecurity standards & guidelines that may be useful to automotive industry
- APPENDIX I: Security test tools of potential use to the Vehicle industry

J3101 - Requirements for Hardware-Protected Security for Ground Vehicle Applications:
Defines a common set of requirements for security to be implemented in hardware for ground vehicles to facilitate security enhanced applications, developing expectations for necessary functionality to achieve an ideal system for hardware protection for ground vehicle applications, including examples, but not explicitly detailing implementation requirements.
Assessment of the Information Sharing and Analysis Center Model

This report presented findings from an assessment of the ISAC (Information Sharing and Analysis Center) model, and how ISACs are effectively implemented in other sectors. The report also explains how a new sector ISAC could be formed by leveraging existing ISAC models. This report was sent directly to the Association of Global Automakers and Alliance of Automobile Manufacturers to aid with their automotive ISAC activities.

A Summary of Cybersecurity Best Practices

This report documented results from the analysis and review of best practices and observations across a variety of industries in the field of cybersecurity involving electronic control systems. It provides benchmarks for the agency and the industry.
Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach

This report described a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems are included, along with a matrix containing a condensed version of the various potential attacks.

National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles

This report reviewed the NIST guidelines and foundational publications from an automotive cybersecurity risk management standpoint. The NIST approach is often used as a baseline to develop a more targeted risk management approach for use in specific industries and sectors.
Minimun Requirements for CyberSecurity

Investigate Minimum Requirements for Cybersecurity

- Safety-critical electronic control systems (ECS) governing the vehicle motion (i.e. steering, braking, propulsion and motive power);
- Others (regulated functions, safety relevant functions, etc.)

Study vehicle architectures and threat vectors and risks

- Significant variations across OEMs, vehicle platforms, even model years;
- Performance-based approach agnostic to architecture and technology choice.

Test and evaluate vehicle cybersecurity environment

- Need performance metrics; Validate theories in applied settings;
- Objective test procedures (practical, repeatable, reproducible).
Hackers Remotely Kill a Jeep on the Highway
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Tesla Model S car hacked, shut off while driving

Hackers Cut a Corvette’s Brakes Via a Common Car Gadget
Questions?
Thanks for your attention!!!

Prof. Antonio Mauro, PhD
info@antoniomauro.it