CYBERSECURITY FOR THE AUTOMOBILE
IS THE CAR OF THE FUTURE STILL A CAR?

Alberto Sangiovanni-Vincentelli
The Edgar L. and Harold H. Buttner Chair of EECS
University of California at Berkeley
Co-Founder, CTA and Member of the Board
Cadence Design Systems

I&C Research Days, Lausanne, 21 June 2012
Outline

• The evolution of the IT World
• The Evolution of the Automotive World
• Challenges in Design
• Cybersecurity for Vehicles
• Conclusions
The Emerging IT Scene!

Infrastructural core

Sensory swarm

Mobile access

The Cloud!

Courtesy: J. Rabaey

© Alberto Sangiovanni-Vincentelli. All rights reserved.
Computers and mobiles to disappear!

Predictions: 7 trillions devices servicing 7 billion people!
1,000 devices per person by 2025

The Immersed Human

Real-life interaction between humans and cyberspace, enabled by enriched input and output devices on and in the body and in the surrounding environment

Courtesy: J. Rabaey
IBM Smarter Planet Initiative:
Something profound is happening… CYBER PHYSICAL SYSTEMS!

**INSTRUMENTED**
We now have the ability to measure, sense and see the exact condition of practically everything.

**INTERCONNECTED**
People, systems and objects can communicate and interact with each other in entirely new ways.

**INTELLIGENT**
We can respond to changes quickly and accurately, and get better results by predicting and optimizing for future events.
Intelligent systems that gather, synthesize and apply information will change the way entire industries operate.

**Smart water**
Apply monitoring and management technologies to help optimize the availability, delivery, use, and quality of water as well as related systems including energy and chemical treatment.

**Smart traffic**
Use real-time traffic prediction and dynamic tolling to reduce congestion and its byproducts while positively influencing related systems.

**Smart energy**
Analyze customer usage and provide customized products and services that help to boost efficiency from the source through the grid to the end user.
Vision 2025

- Every object will be smart
- The Ensemble is the Function!
  - Function determined by availability of sensing, actuation, connectivity, computation, storage and energy
  - Collaborating to present unifying experiences or to fulfill common goals

A humongous networked, distributed, adaptive, hierarchical, hybrid control problem
Outline

- The evolution of the IT World
- The Evolution of the Automotive World
- Challenges in Design
- Cybersecurity for Vehicles
- Conclusions
The Evolution of the Automotive DNA

**CURRENT DNA**

- Energized by Petroleum
- Powered Mechanically by Internal Combustion Engine
- Controlled Mechanically
- Stand-alone
- Totally Dependence on the Driver
- Vehicle Sized for Maximum Use - People and Cargo

**NEW DNA**

- Energized by Electricity and Hydrogen
- Powered Electrically by Electric Motors
- Controlled Electronically
- “Connected”
- Semi/Full Autonomous Driving
- Vehicle Tailored to Specific Use

Courtesy: A. Taub, GM
360° SENSING CAPABILITY

**TODAY**
- Short-Range Blind-Spot Sensors
- Long-Range Sensors
- Rear Vision System
  - Object detection
  - Far IR capability
- Enhanced Digital Map System
- Forward Vision System
  - Lane tracking
  - Object detection
  - Far IR capability
- Long-Range Scanning Sensor

**FUTURE**
- Side Blind-Zone Alert
- Long-Range Side/Rear Lane-Change Assist
- Forward Vision System
- Dedicated Short-Range Communication + GPS (V2V)
- Short-Range Radars
- Ultrasonic Sensors

Courtesy: A. Taub, GM
CMOS mmWave Circuits and SoC: 60GHz Today

- Multiple 60GHz standards complete
- WirelessHD products available
  - SiBeam (BWRC startup)
  - Wall-powered
  - Dissipate <2W
- A $10 Radar is a possibility!
VEHICLE IS PART OF A “CONNECTED” ECO-SYSTEM

Courtesy: A. Taub, GM
The Problem: Typical Car Electrical Architecture
Each time a new function is required, the OEM starts a request to suppliers for a new ECU (an integrated HW/SW device realizing the function) to be integrated on the existing networks.

The device is developed by the supplier with its own choice of HW, RTOS, device drivers and communication layers (with some standardization).

The result is:

- Proliferation of ECUs (reaching 100)
- Complex distributed architectures with the need of high bandwidth and therefore multiple networks and gateways
- Complex functional and not-functional (timing) dependencies across the network, which OEMs struggle to control
- Missing opportunities for common set of libraries and (sub)functions
- Limited standardization, flexibility and extensibility
- Limited control on the execution platform by OEMs
Active Safety

- Sensors are becoming critical
- Fusion and Optimization are differentiating factors
Cyber™ Tire System

Vehicle dynamics control system

User Applications

Processing unit

Receivers

Marco Tronchetti Provera
Chairman of Pirelli & C. S.p.A.

Major broadcast channel in Italy
From federated to integrated architectures

Tomorrow?: Integrated Architectures

The execution architecture is completely selected and planned by the OEM. OEMs are free to standardize HW, drivers, RTOS and communication layers, leveraging competition among suppliers.

Each time a new function is required, the OEM starts a request to suppliers for new functional content (SW) to be integrated on the existing platform.

The challenges are:
- Moving from specifications of ECUs with message interfaces to the specs of SW components
- Standardize interoperability among components
- Standardize access to the platform services
- Define models that allow to predict the result of the composition (functional and not-functional)
Outline

• The evolution of the IT World
• The Evolution of the Automotive World
• Challenges in Design
• Cybersecurity for Vehicles
• Conclusions
Trustworthy Computing: Safety
The ISO 26262 roadmap for MCUs

MCU

Systematic faults

Avoidance faults in the process
- Requirements tracking, Config. mgmt
- Control & verification of the design process
- Control & verification of usage, maintenance and changes

Avoidance bugs in SW
- Control & verification of tool suites (e.g. compiler, etc.)
- Control & verification of the SW test design
- Doc. & Verification of HW-SW interfaces

Analysis

Qualitative Analysis
- Dependent failures (CCF) analysis

Quantitative Analysis
- HW metrics analysis (SPFM, LFM, PMHF)
- HW metrics verification (fault injection)

Safety Mechanisms

HW random faults

HW diagnostic mechanisms (e.g. ECC, DCLS, etc.)

SW diagnostic mechanisms (e.g. SW tests)

Measures for CCF avoidance
A fundamental concept of AUTOSAR is the separation between:
- (functional) application and
- infrastructure
Supporting Theory

- Provide a semantic foundations for integrating different models of computation
  - Independent of the design language
- Maximize flexibility for using different levels of abstraction
  - For different parts of the design
  - At different stages of the design process
  - For different kinds of analysis
- Support many forms of abstraction
  - Model of computation (model of time, synchronization, etc.)
  - Scoping
  - Structure (hierarchy)
Outline

- The evolution of the IT World
- The Evolution of the Automotive World
- Challenges in Design
- Cybersecurity for Vehicles
- Conclusions
Trustworthy Computing: Vehicle Cybersecurity

- Modern vehicles are complex, networked Information Technology (IT) systems that comprise an increasingly sophisticated array of sensors and control processors connected by internal communication networks.

- Vehicles are networked entities that exist in cyberspace much like any other computational node, PC, tablet, or smartphone.

- As more and more technology is introduced into automobiles, the threat of malicious software and hardware manipulation increases.
  - Increasing connectivity and complexity is greatly expanding the attack surface of our systems.

- Recent work has demonstrated potential security weaknesses in vehicles.

Surface of attack

Vehicle to Vehicle Communication

Engine Control Unit

Airbag Control Unit

Transmission Control Unit

Body Controller
Locks/Lights/Etc

Radio

TPMS

Antilock Braking System

OBD-II

Anti-Theft

Telematics

Internet/PSTN

Keyless Entry

HVAC
Basic Findings

• Demonstrated the ability to control a wide range of automotive functions and **completely ignore driver input**, including disabling the brakes, selectively braking individual wheels on demand, and stopping the engine.

• Possible to bypass rudimentary network security protections within the car, such as maliciously bridging between two internal subnets of a car.

• Possible to embed malicious code in a car’s telematics unit that will **completely erase any evidence** of its presence after a crash.
## Attack Surface Capabilities

<table>
<thead>
<tr>
<th>Vulnerability Class</th>
<th>Channel</th>
<th>Implemented Capability</th>
<th>Visible to User</th>
<th>Scale</th>
<th>Full Control</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct physical</td>
<td>OBD-II port</td>
<td>Plug attack hardware directly into car OBD-II port</td>
<td>Yes</td>
<td>Small</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect physical</td>
<td>CD</td>
<td>CD-based firmware update</td>
<td>Yes*</td>
<td>Small</td>
<td>Yes</td>
<td>Medium-High</td>
</tr>
<tr>
<td></td>
<td>CD</td>
<td>Special song (WMA)</td>
<td>Yes*</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium-High</td>
</tr>
<tr>
<td></td>
<td>PassThru</td>
<td>WiFi or wired control connection to advertised PassThru devices</td>
<td>No</td>
<td>Small</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>PassThru</td>
<td>WiFi or wired shell injection</td>
<td>No</td>
<td>Viral</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td>Short-range wireless</td>
<td>Bluetooth</td>
<td>Buffer overflow with paired Android phone and Trojan app</td>
<td>No</td>
<td>Large</td>
<td>Yes</td>
<td>Low-Medium</td>
</tr>
<tr>
<td></td>
<td>Bluetooth</td>
<td>Sniff MAC address, brute force PIN, buffer overflow</td>
<td>No</td>
<td>Small</td>
<td>Yes</td>
<td>Low-Medium</td>
</tr>
<tr>
<td>Long-range wireless</td>
<td>Cellular</td>
<td>Call car, authentication exploit, buffer overflow (using laptop)</td>
<td>No</td>
<td>Large</td>
<td>Yes</td>
<td>Medium-High</td>
</tr>
<tr>
<td></td>
<td>Cellular</td>
<td>Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)</td>
<td>No</td>
<td>Large</td>
<td>Yes</td>
<td>Medium-High</td>
</tr>
</tbody>
</table>
Scenario

- What if a malicious node can get access to the network and send a message with rogue data?
  - A node becomes malicious because of physical tempering and/or cyber-tempering
The Dilemma

Raffaello Sanzio, The Athens School
Types of Attacks and Desired Properties

- **Types of attacks**
  - *Interception (eavesdropping):* unauthorized nodes read data
  - *Modification:* authorized nodes change data
  - *Fabrication:* unauthorized nodes generate additional data
  - *Interruption:* data becomes unavailable

- **Desired properties**
  - *Confidentiality:* data is not read by unauthorized nodes
  - *Data integrity:* data is not changed by unauthorized nodes
  - *Authentication:* a receiver or a sender is who it claims to be
  - *Non-repudiation (not discussed here):* a sender ensures that a receiver has received the message, and a receiver is sure about the identity of a sender.

- **Data integrity and authentication are the most relevant properties for an automotive communication system**
Our Work (UCB+GM): Provide a Security Solution for CAN

• First part: security mechanism
  – Define the attacker model (the attack scenarios that we want to address with our mechanism)
  – Point out the difficulties of using existing authentication approaches on CAN
  – Propose a security mechanism which is applicable to CAN and help prevent masquerade and replay attacks

• Second part: optimization framework
  – Support for optimization and trade-off exploration
    • e.g., maximizing degree of security vs. additional bus load penalty
  – Generalize to additional configurations
    • e.g., different secret key distributions and counter implementations
  – Easy to use, maintain, and support
Attacker Model

- **Masquerade attack**
  - An attacker sends a message in which it claims to be a node other than itself

- **Replay attack**
  - An attacker sends (replays) a copy of a message it has received from the CAN network
    - The message is not modified or altered
Existing Approach [Szilagyi & Koopman, CMU]

• **Achieve data integrity by authentication**
  – Each pair of nodes has a shared secret key
  – A sender computes Message Authentication Codes (MACs) and broadcasts the message with the MACs
  – A receiver computes a MAC and compares it with the sent MAC
Difficulties on CAN

- The communication overhead is too high
- There is no global time in CAN
Our Security Mechanism

• **Sender**
  1. Increases its sending counter
  2. Computes MACs *(for its receivers only)*
     • Using data, the counter, and the pair-wise keys
  3. Broadcasts a message w/ data, the counter, and MACs (plus the other CAN fields)

• **Receiver**
  1. Checks its ID table
     • Decides which key and counter to use based upon the sender ID
  2. Checks if the received counter > its local counter
     • Sees if the message is fresh
  3. Computes MAC’ and compares MAC and MAC’
     • Uses (received) data, (received) counter, and its pair-wise key
  4. Updates its local counter

---

prevent replay attacks

prevent masquerade attacks
Final Words of Wisdom