



Automotive and Industrial Data Security

André Weimerskirch

Cybersecurity for Cyber-Physical Systems Workshop

April 23-24, 2012

Overview



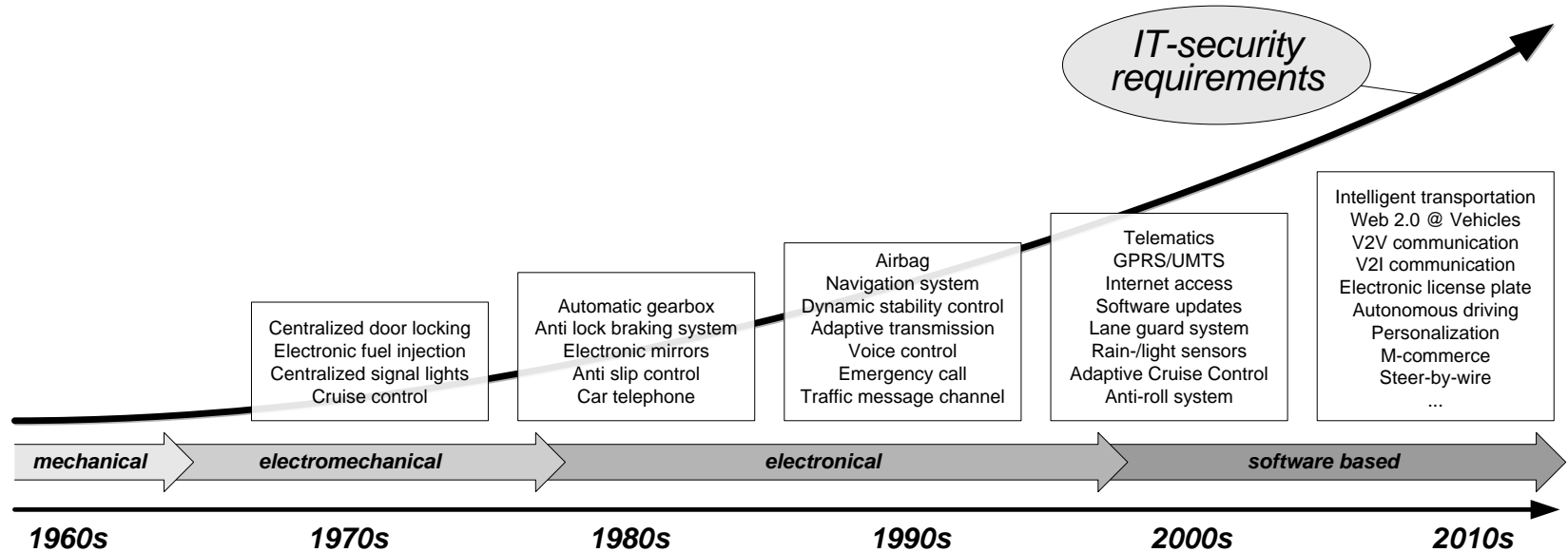
- **Introduction and Motivation**
- Risk analysis
- Current and future security solutions
- Conclusions

Communication and Cars

- “If vehicles had developed in the same manner as telecommunications, then an average car would reach top speeds of 10^9 km/h at 400 million horse power, and the car would be hacked four times per year.”
 - Prof. Christof Paar



Digital revolution in vehicles



- Vehicles changed from mechanical to software based systems
- Software and electronics accounts for up to 50% of total cost
- Software and electronics is a market distinction today
- Modern cars come with up to 80 CPUs, 2 miles of cable, several hundred MB of software, and 5 in-vehicle networks

Hacking

- Recent media reports suggest that data security in vehicle becomes an issue
 - Remote attack to vehicle by manipulated MP3 file via Bluetooth connected cell phone
 - Weakness in telematics module to gain remote access via cellular connection
 - Weakness in Bluetooth stack to gain access to CAN
 - Then remotely flash new firmware, e.g. for brake ECU: lock left rear brake once car reaches 70 mph. Attacker can be on another continent.

Trojan-Horse MP3s Could Let Hackers Break Into Your Car Remotely, Researchers Find

By Rebecca Boyle Posted 03.14.2011 at 4:57 pm 15 Comments



Dashboard Karl Frankowski via Flickr

Last year we told you how hackers could someday [infiltrate your car's control systems](#) and install malware to take things over, as long as they had some computer skills and a laptop. Now car-hacking researchers have [done it remotely](#), using innocent tech like Bluetooth devices and even a CD.

Researchers at the University of California, San Diego, and the University of Washington are researching vulnerabilities in electronic vehicle controls, trying to warn automakers about potential security holes. Many new cars have Bluetooth wireless technology and built-in connections for cell phones and other devices, and those connections [could be exploited](#). In one example, the researchers called the car's cellular connection and uploaded malicious code using an audio file. In another test, they found out how to pair the car to a Bluetooth-enabled device, which they used to execute code.

Source: <http://www.popsci.com/cars/article/2011-03/bluetooth-music-and-cell-phones-could-let-hackers-break-your-car-researchers-say>

Hacking

- Same researchers found local attack
 - Connect laptop to OBD-II port and flash manipulated firmware
 - Insert manipulated CD or USB flash drive to inject manipulated firmware
- Remotely mounted hacks via Internet to remote engine start and remote vehicle unlock have been demonstrated as well by other researchers.
- Knowledge is proprietary and no known attacks are known. However, it is a matter of time until the knowledge will leak.

Financial Damage

- Counterfeit black market is a gigantic problem
- Odometer rollback
 - 6 billion Euro damage per year in Germany
 - 10-30% of all sold used vehicles manipulated in USA



The screenshot shows the Havocscope Black Markets website. The header includes the logo and the text "AVOCSCOPE black markets online database of black market activities". A navigation bar contains links for HOME, PRODUCTS, MARKETS, COUNTRIES, and REGION. The main content area displays "Counterfeit Auto Parts Black Market Value" with a "Product Value" of "\$45 Billion".

Source: <http://www.havocscope.com/black-market/counterfeit-goods/counterfeit-auto-parts/>



The screenshot shows an eBay listing for a "Digimaster II Digimaster 2 Odometer Mileage Correction" device. The item is new, priced at \$1,100.00, and has a quantity of 1. The listing includes a "Buy It Now" button, an "Add to Watch list" button, and a "FREE shipping" badge. The seller offers a 7-day money back guarantee and free shipping. The listing also features the eBay Buyer Protection logo and a "Ducks" promotion.

Source: <http://www.ebay.com>

Financial Damage

- Warranty fraud
 - Owner performs chip tuning to increase engine power
 - Engine blasts and owner flashes original firmware

KWP2000 Plus OBD2 ECU Flasher Chip Tuning Kit KWP2000+



Item condition: New

Quantity: 9 available

Price: US \$29.99 [Buy It Now](#)

[Add to Watch list](#)

[Bucks](#) Join [eBay Bucks](#) and earn 2% back on this item. [See conditions](#)

Returns: 30 day exchange | [Read details](#)

Shipping: \$9.99
[See more services](#) | [See all details](#)
Estimated delivery within 13-22 business days.

 **eBay Buyer Protection**
eBay will cover your purchase price plus original shipping.
[Learn more](#)

Source: <http://www.ebay.com>

Privacy

- Event Data Recorder (EDR) record information during crashes and accidents.
- Navigation units include list of recent targets
- Theft protection devices track vehicles via GPS



Auto

NHTSA Working on Automotive Black Box Standards, May Release Guidelines Next Month

Tiffany Kaiser - May 25, 2011 6:20 AM

Print ShareThis 5

21 comment(s) - last by FITCamaro.. on May 25 at 5:24 PM

User privacy and costs regarding the integration of high-tech EDRs are the largest concerns

The National Highway Traffic Safety Administration may make event data recorders, or "black boxes," a requirement for all vehicles [starting next month](#) according to *Wired's Autopia*.

Event data recorders (EDR) are devices already installed in some automobiles, and record information during vehicle crashes or accidents. EDRs cannot be turned off, and once electronically triggered by problems in the engine or dramatic shifts in wheel speed, the EDR records this vehicle input and produces a snapshot of the final moments before the accident.



(Source: media.avvo.com)




Source:

<http://www.dailytech.com/NHTSA+Working+on+Automotive+Black+Box+Standards+May+Release+Guidelines+Next+Month/article21717.htm>

Area full of Pitfalls: Aftermarket

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.



Police with Austin's High Tech Crime Unit on

Source: <http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/>

Dutch Police Used TomTom's GPS Data To Target Speeders

Categories: Technology, Foreign News

by EYDER PERALTA



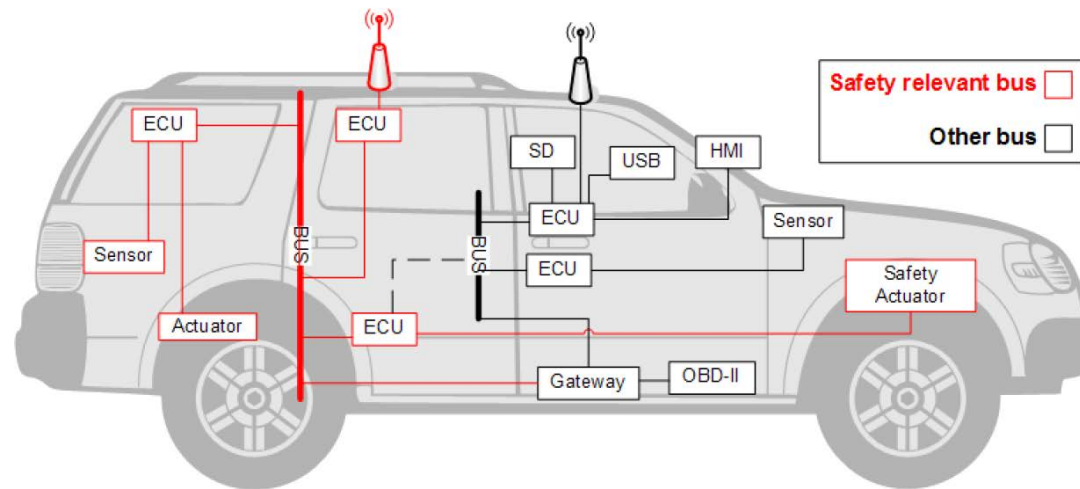
 [Enlarge](#)

Seth Perlman/AP

Source: <http://www.npr.org/blogs/thetwo-way/2011/04/28/135809709/dutch-police-used-tomtoms-gps-data-to-target-speeders?sc=17&f=1019>

- Be careful who “upgrades” your car!

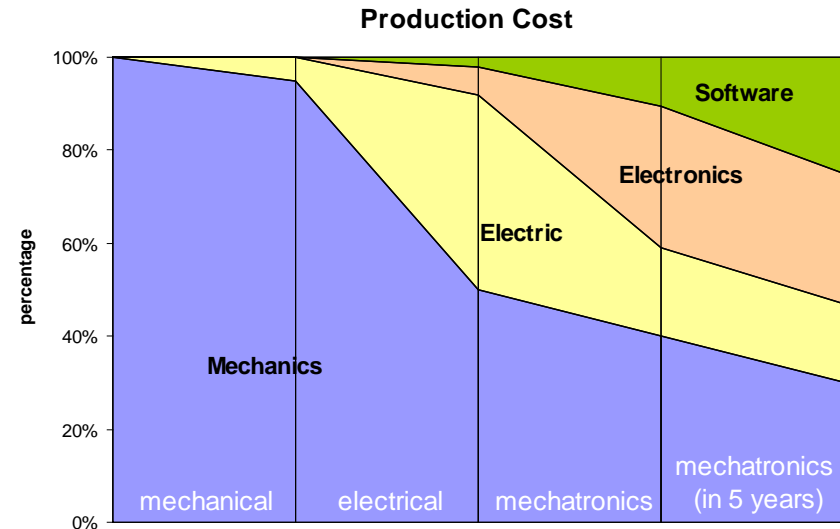
Underlying Problem: Vehicle Architecture



- There is a physical connection between safety relevant bus and non-safety bus
 - E.g. speed adjusted volume
 - Note the physical connection between cellular, USB, SD, HMI, and safety critical powertrain components
- The complexity of code increases, mainly due to infotainment
 - Almost impossible to avoid security flaws
- Access to bus via OBD-II, or remotely via infotainment system

Why is data security in vehicles special?

- Safety critical: a hacked vehicle might be different than a hacked PC
- Vehicles cannot regularly update software
- In many instances, attacker has physical access
- More infotainment will be introduced
- Modern cars include 100 million lines of code
 - Industry average is about one security flaw per 1,000 lines of code
 - Around 100,000 flaws?



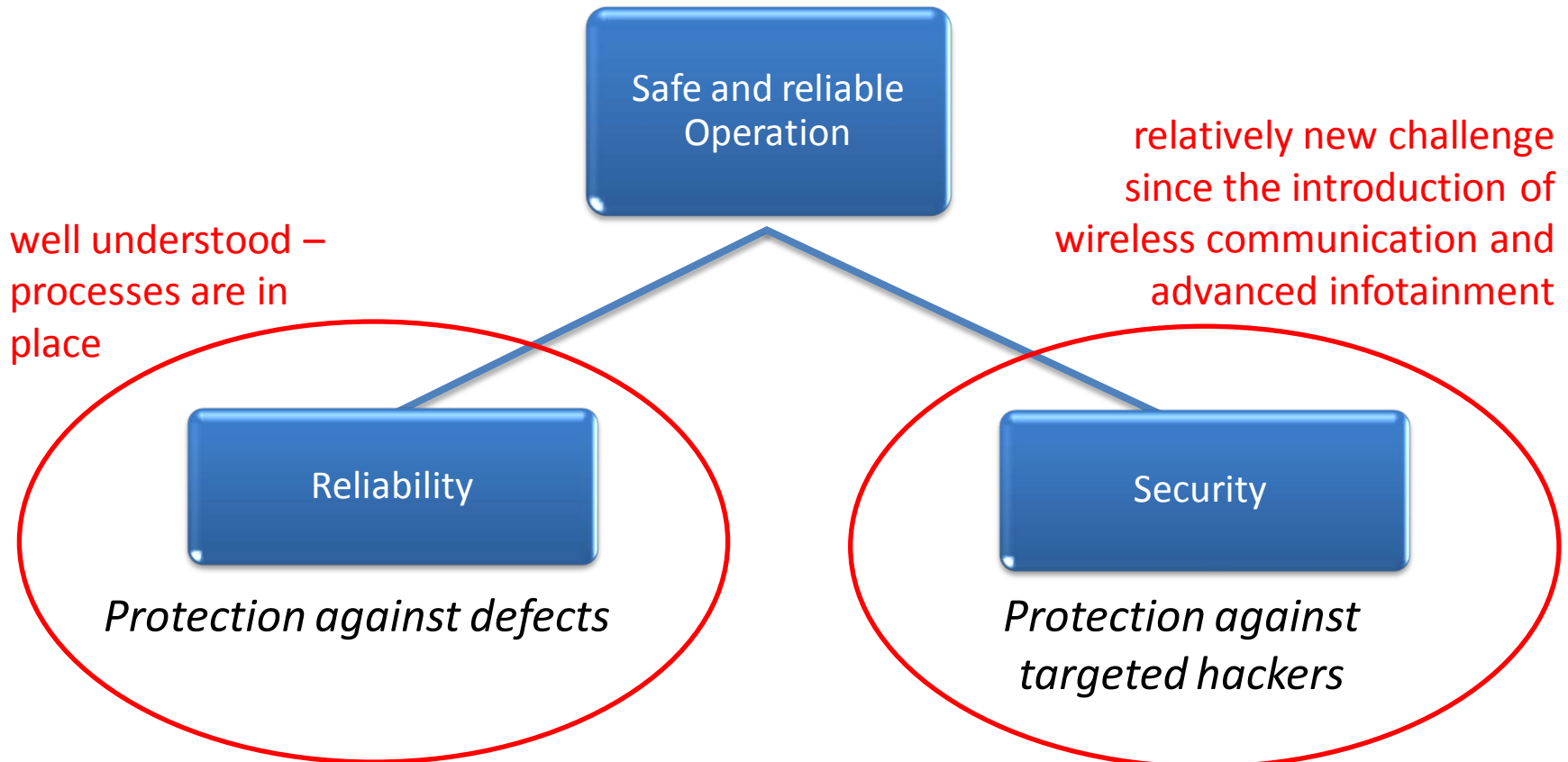
Source: Audi

Why is automotive security different to PC security (and hard)?



- Combination of safety and infotainment
 - Buyers demand modern connected infotainment systems
 - If a PC is hacked, data is lost. If a car is hacked, life is at stake.
- Automotive software cannot easily be updated
 - No monthly security update
- Attacker might have physical access to vehicle

Safety and Security



Overview



- Introduction and Motivation
- **Risk analysis**
- Current and future security solutions
- Conclusions

Who are the attackers?

- Today: different to iPhone hacker community (challenge, curiosity), similar to Pay-TV hackers; purely financial motivation
- Almost all attackers are active in black market
 - Illegal organizations
 - Mainly financial motivation
 - Significant financial damage
- Some individual “attackers” are motivated by curiosity
 - To turn off “annoying” seat belt warning
 - Turn off TV lock
 - Academic teams
 - Any damage?

Who are the attackers? (continued)

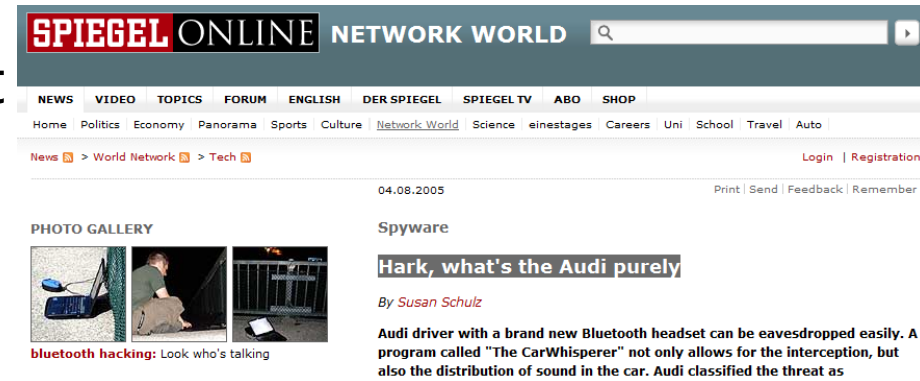
- The attacks are implemented and sold by black market organizations
- The *user* of the attack is in almost all cases the vehicle owner
 - Odometer rollback
 - Chip tuning
 - Buyer of cheap counterfeits (did you ever buy an original car key for \$250)?
- Question:
 - Will there be attackers to mount safety-critical attacks?
 - How will the attacks be offered/distributed?

Who is damaged?

- In many cases the buyers of used cars
 - Odometer rollback
 - Chip tuning (shortens engine life-span)
 - Counterfeits (shorter life-span)
 - Stolen vehicles (either direct damage, or damage due to increased insurance rates)
- Only a few cases where car makers are damaged directly
 - Counterfeits: lost sales
 - Potentially fines by EPA: if it becomes known that chip tuning is very easy, and that engine after chip tuning violates emission regulations
 - Warranty fraud: engine burns out after chip tuning during warranty period

Who is damaged? (continued)

- Indirect damage for car makers might be significant
 - Lost sales if insurance rates due to high theft are significantly higher than of competitors
 - Lost sales if there is negative press
- Some pressure on car makers to introduce security



Source:

<http://www.spiegel.de/netzwelt/tech/0,1518,368070,00.html>

Overview



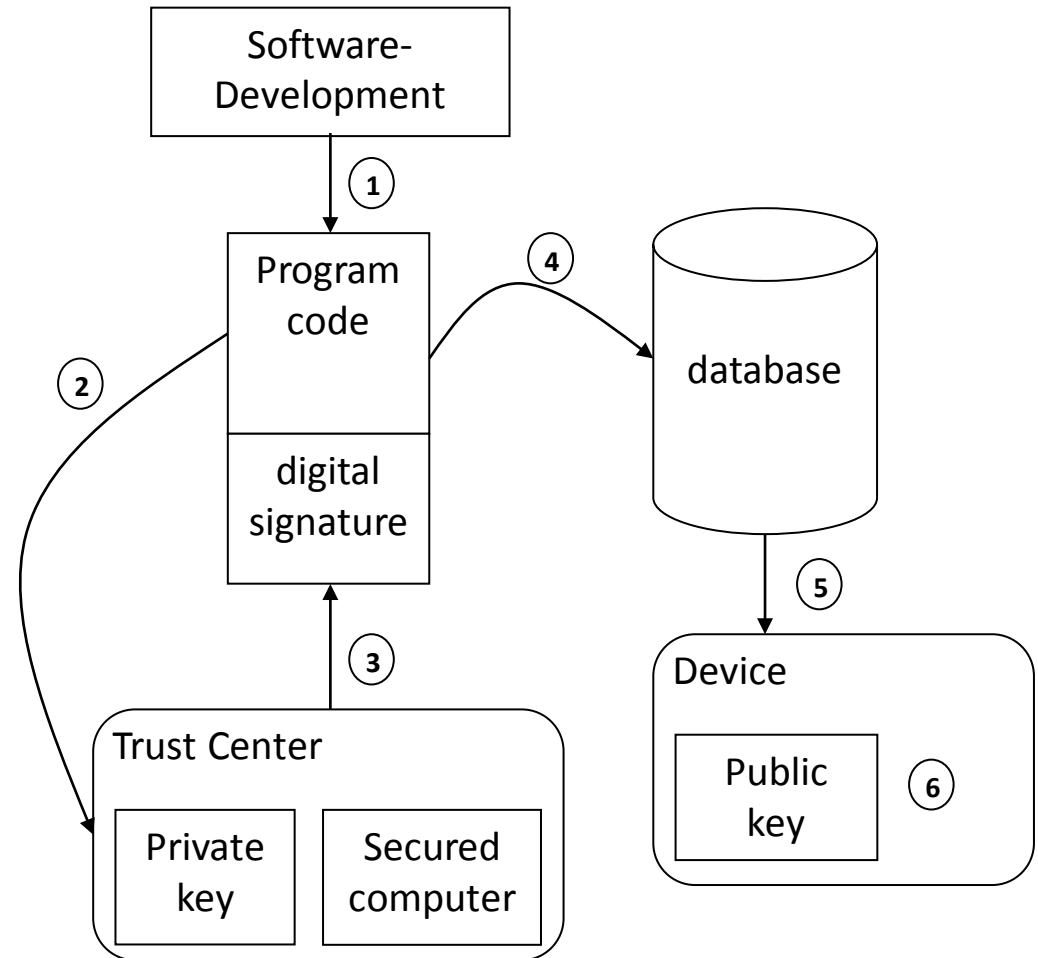
- Introduction and Motivation
- Risk analysis
- **Current and future security solutions**
- Conclusions

Examples of IT-Security Applications in Vehicles

- Theft protection
- Remote unlock
- Keyless entry
- Odometer manipulation
- Vehicle tracking
- Bluetooth and Wi-Fi
- eCall
- Tolling
- Business models
 - Feature activation
 - License agreements
 - Copyright protection
- Warranty: prove manipulation of firmware
- Counterfeiting of components and spare parts
- Vehicle-to-vehicle communication
- ...

Security Features: Today

- Secure flash programming
 - OEM signs firmware (usually RSA)
 - ECU verifies OEM's signature
 - Built-in public key in ECU that can be replaced with new boot-loader
 - Certificate based systems are going to be implemented



Security Features: Today

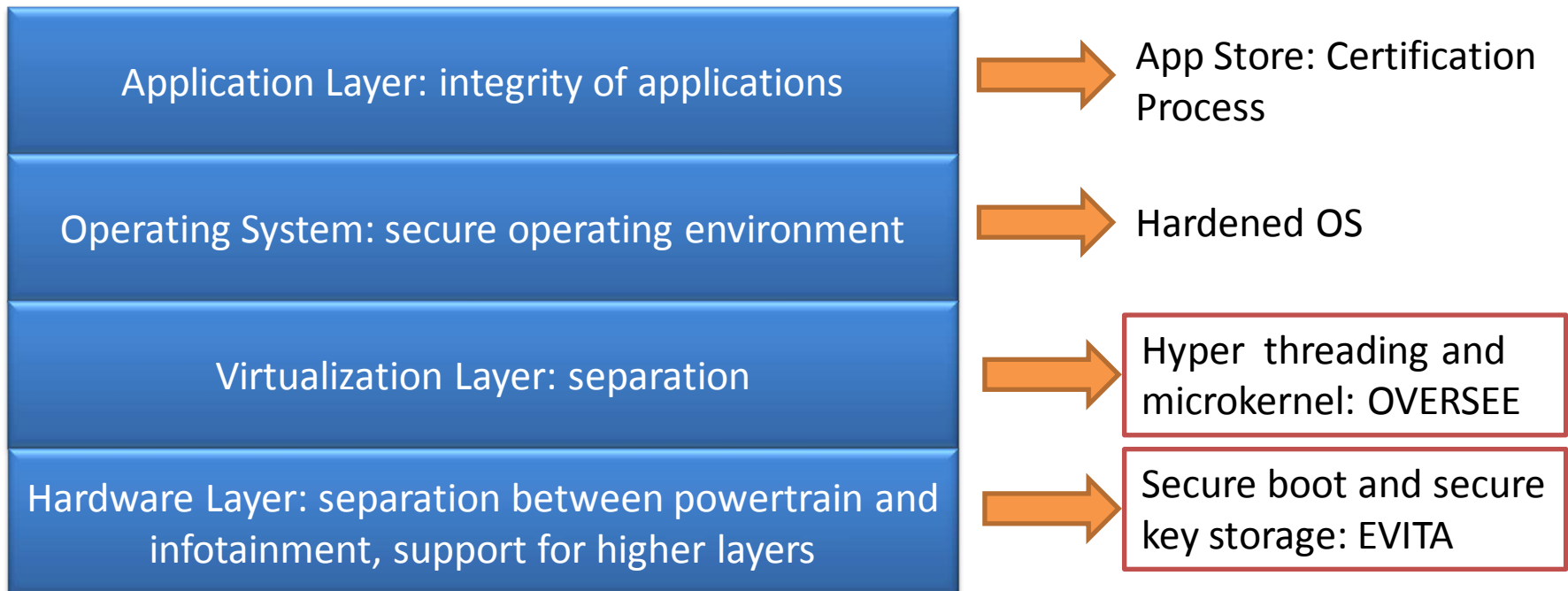
- Filter in gateway
 - Whitelists: designer explicitly define which packets are relayed between different bus systems
- Plausibility checks
 - Part of safety validation
 - Each ECU checks whether input is reasonable
 - If not, input is discarded and fail-safe mode is activated

Security Features: Today

- Standard security
 - E.g. Bluetooth security based on PIN entered pairing
 - Proprietary security
 - Theft protection
 - Feature activation
- Most OEMs focus on remote attacks

Future In-Vehicle Security Layers

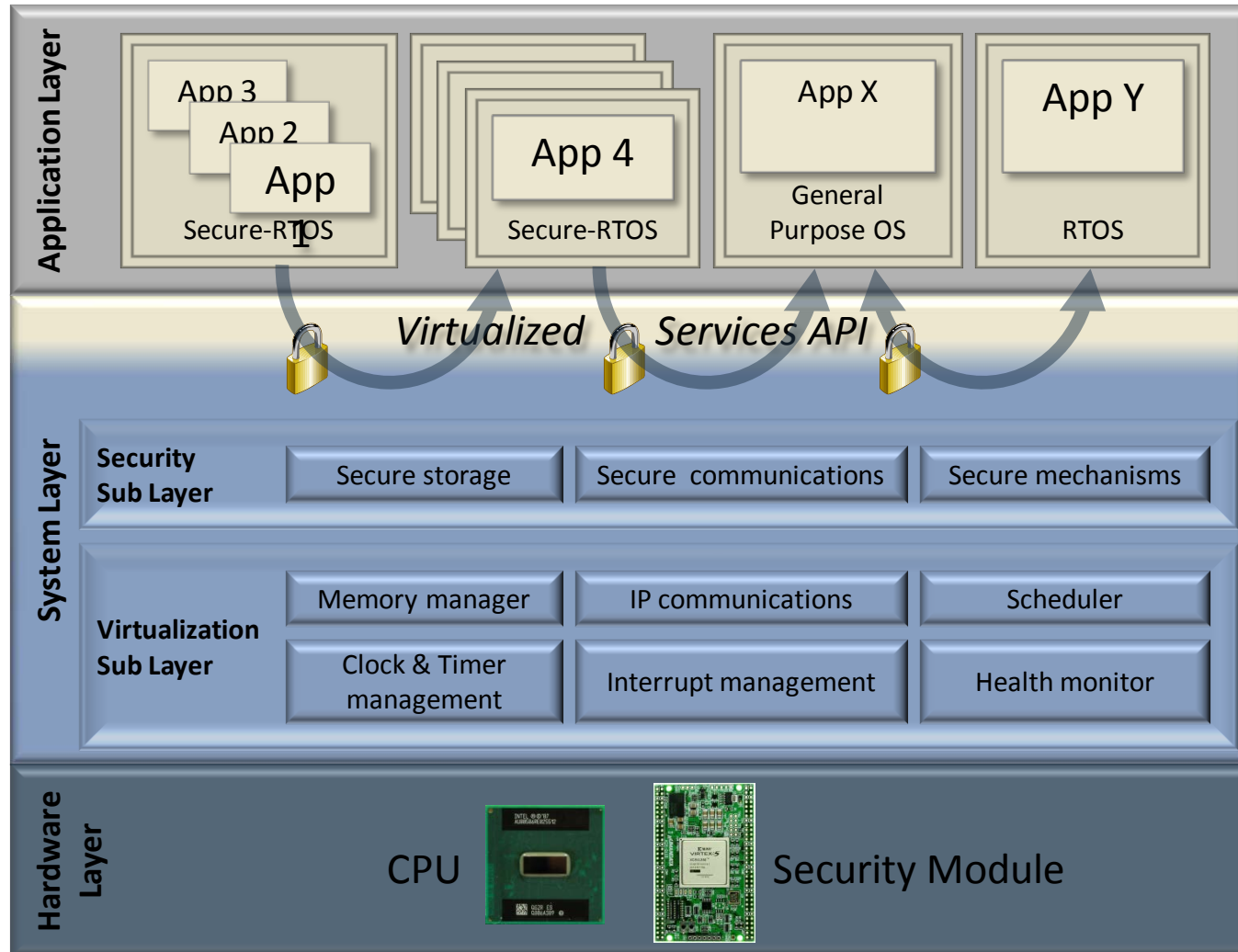
- Need for layered in-vehicle security:



Virtualization and Microkernel

- Rule of thumb: one security weakness per 1,000 lines of code
- Linux and Windows have many million lines of code
 - Thousands of security weaknesses
- Design microkernel
 - Remove drivers and non-essential modules from kernel
 - Between 10,000 and 100,000 lines of code
 - Hope: find all security weaknesses before deployment
 - Hope: formal verification of correctness

Hyper-Threading



Approach: OVERSEE

- OVERSEE: Open Vehicular Secure Platform
- Objective: Providing a standardized generic communication and application platform for vehicles, ensuring security, reliability and trust of external communication and simultaneous running applications.
- European Union funded project (3 million EURO)
- Runtime 2010 – 2012
- Members: Volkswagen, ESCRYPT, Fraunhofer, Trialog, Technical University Berlin, University of Valencia, Open Tech
- More information at www.oversee-project.com

Hardware Security

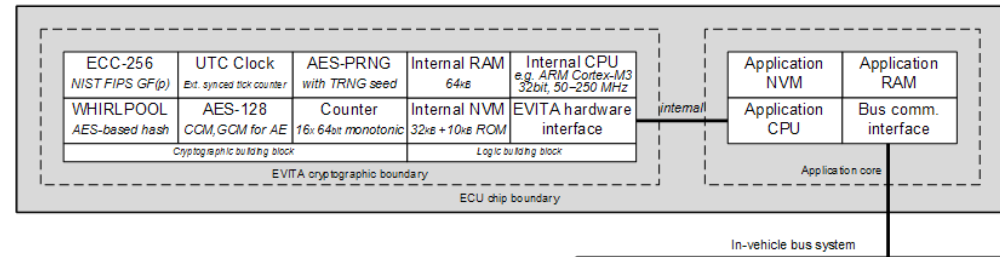
1. Hardware as ultimate separation between local and remote interfaces and powertrain
 - “Automotive Firewall”

2. Hardware as security anchor for higher layers
 - Protection of software manipulation
 - Secure boot
 - Secure key storage
 - Fast crypto performance

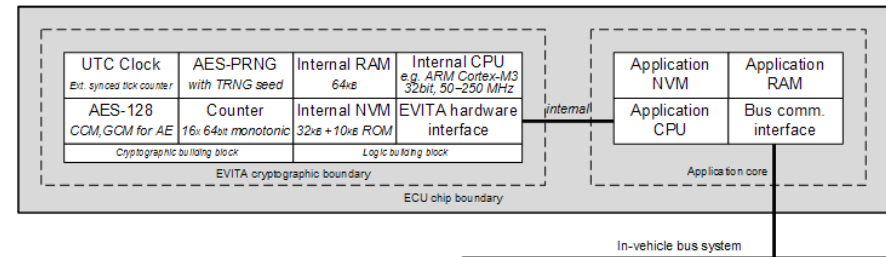
EVITA Security Levels

- **EVITA Full:** V2X (one per car)
- **EVITA Medium:** for advanced ECUs (gateway, headunit, engine control)
- **EVITA Light:** for sensors, actuators, ...

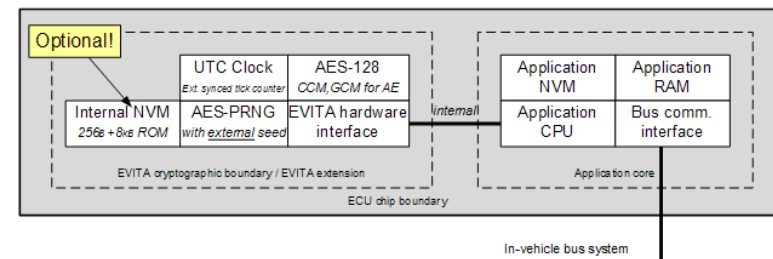
(a) Full version for V2X and large ECU level



(b) Medium version for standard ECU level



(c) Light version for sensor/actuator ECU level



EVITA in Cars

- EVITA provides hardware extensions
 - Just some more chip area
 - Cost very low
- EVITA does not provide security known from dedicated security controllers such as smart-cards
 - Only basic tamper resistance
- EVITA Light was standardized as Secure Hardware Extension (SHE)
 - Available by several semiconductors
 - Automotive grade
- A controller that implements EVITA Medium was recently introduced

Security of Future Vehicle Application: V2X

- Vehicles are equipped with Wi-Fi (but 5.9 GHz) and regularly broadcast location, speed, vehicle category, time, ...
- Receiver application creates map of environment (no line of sight necessary)
- Receiver safety application notifies driver
 - E.g. immanent crash warning
- Probably the “hottest” security application in vehicles today
 - 260 million nodes
 - Full of privacy pit holes
 - Security and safety intermix
- Security was recognized as major component and introduced from the beginning!



Overview



- Introduction and Motivation
- Risk analysis
- Current and future security solutions
- **Conclusions**

Conclusions 1/2

- Passenger vehicles are more and more connected
 - Users demand for infotainment known from mobile phones
- Main concern is introduced by connectivity
 - Infotainment, wireless connectivity, telematics, V2X
- Recent academic attacks suggest that modern vehicles are vulnerable to serious hacker attacks
 - No actual attacks known though
 - Knowledge very proprietary
- Also a problem (but not considered here): privacy
 - E.g. tracking based on RFID air pressure sensor

Conclusions 2/2

- Car manufacturers work on solutions
 - Plenty of data security mechanisms already implemented today
 - Powertrain needs to be efficiently separated from external communication channels
- Lots of momentum
 - Semiconductors introduce automotive security controllers
 - Secure Hardware Extension (SHE)
 - EVITA Medium (HSM)
 - US DOT discusses introduction of automotive Information Sharing and Analysis Center (ISAC)
 - SAE set up Vehicle Electrical System Security Committee

ES

Dr. André Weimerskirch
CEO
andre.weimerskirch@escrypt.com

Embedded Security