The 3rd International Workshop on
Safety and Security of Intelligent Vehicles (SSIV)
June 26, 2017

Embedded Automotive Systems Security: A language-based Intrusion Detection Approach

Mohamed Kaâniche

Ivan Studnia, Éric Alata, Youssef Laarouchi, Vincent Nicomette

Ivan Studnia, Intrusion Detection for Embedded Automotive Networks - A language-based Approach,
Phd, Université de Toulouse, France, 2015 (in French) - https://tel.archives-ouvertes.fr/tel-01261568

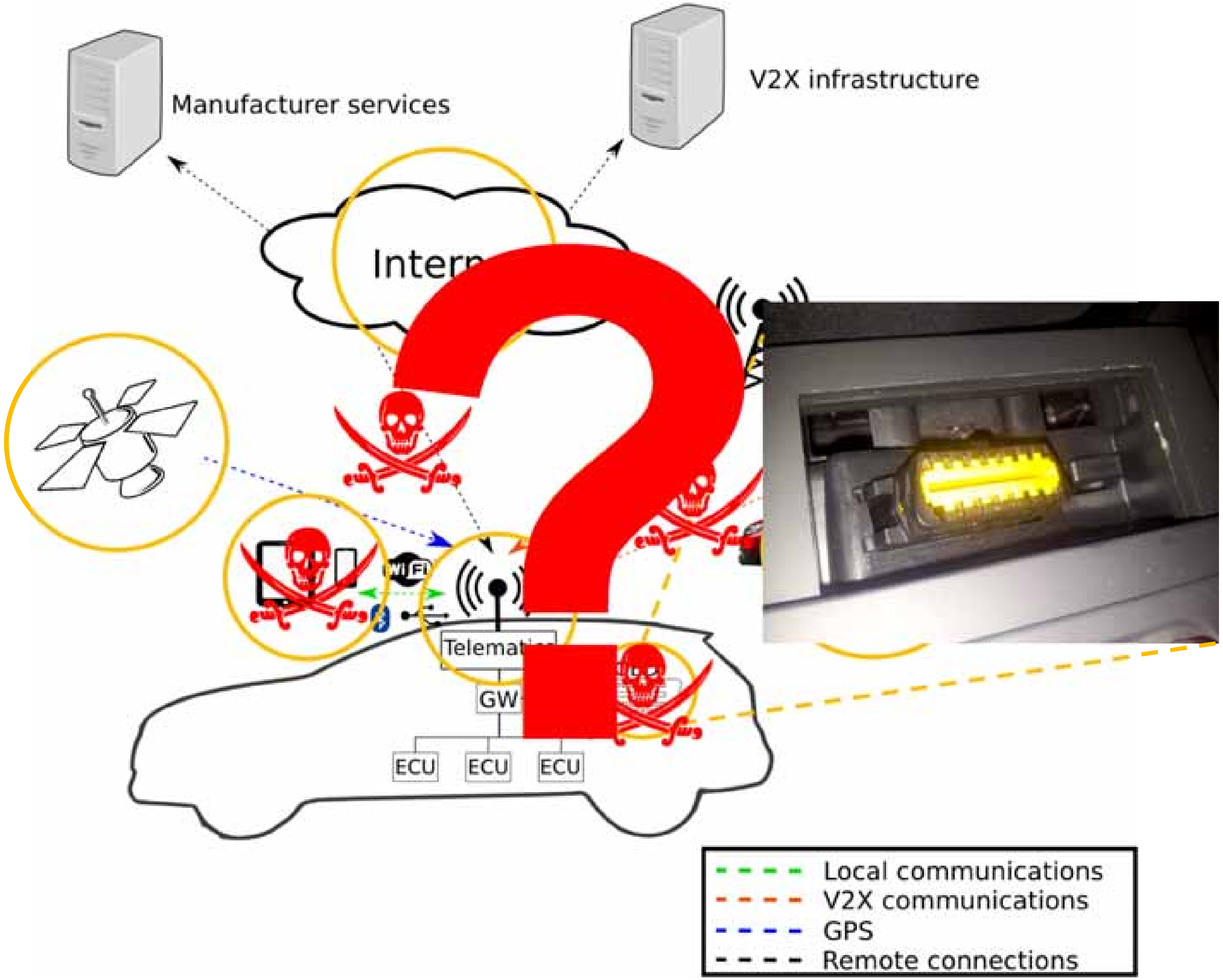
Evolution toward more intelligent vehicles

- Limited electronics
- No automation

- Partial electronic control
- More complex functionalities
- Driver Assistance Systems

- *X-by-wire* architectures
- Increasing number of sensors
- Higher connectivity
- Increasing levels of automation

Connected vehicles

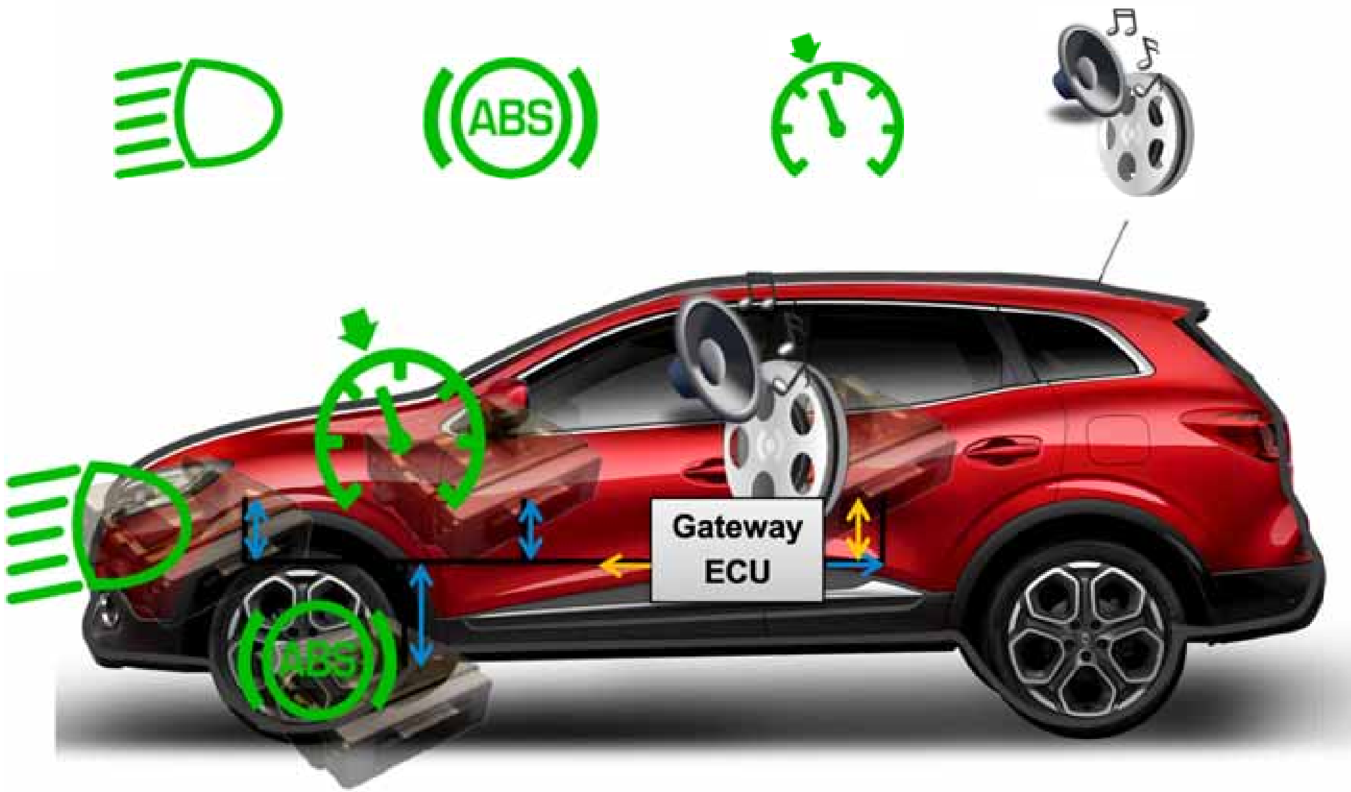


Outline

- **Review of security threats and some existing protection mechanisms**

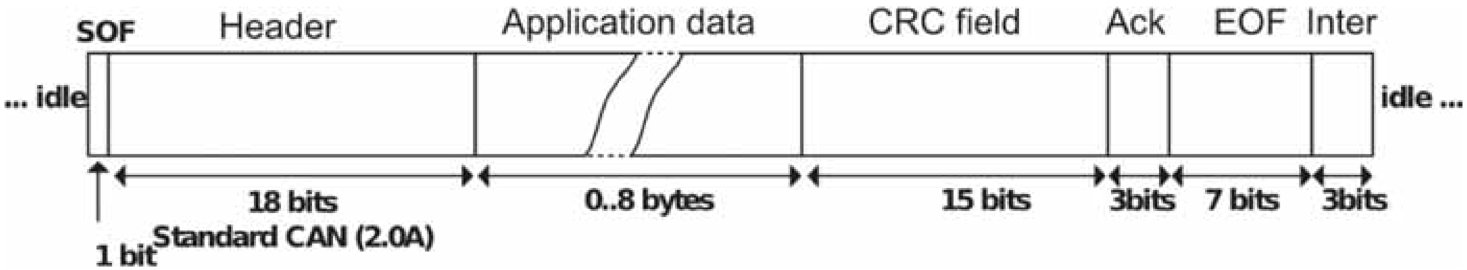
- **Design of an intrusion detection system for automotive embedded networks**

An embedded automotive network



- ***E**lectronic **C**ontrol **U**nit (ECU)*
- inter-ECU Communications
- CAN: ***C**ontroller **A**rea **N**etwork —de facto* standard
- Various network architectures

CAN & Security



Security Properties

- ~~Integrity?~~
- ~~Confidentiality?~~
- ~~Availability?~~
- ~~Authenticity/Non repudiation?~~

- CRC insuffisant for security
- Broadcast only
- Easy Denial of service
- No authentification/logging

Attack goals

Attack

Malicious action aimed at violating one or some security properties

- Challenge
- *E-tuning*
- Theft
- Sabotage
- Privacy breach

Source: [Koscher et al., 2010]

Attack consequences

Impacts on the Driver

- *Safety*
- Loss of the vehicle
- Theft of personal data

Impacts on the Manufacturer

- Economic impact
  - costly maintenance recalls
  - damage to campany reputation
  - IP theft

RISK ASSESSMENT / SECURITY & HACKTIVISM

Fiat Chrysler recalls 1.4 million cars over remote hack vulnerability

Uconnect bug can shut down engine and brakes, take over steering.

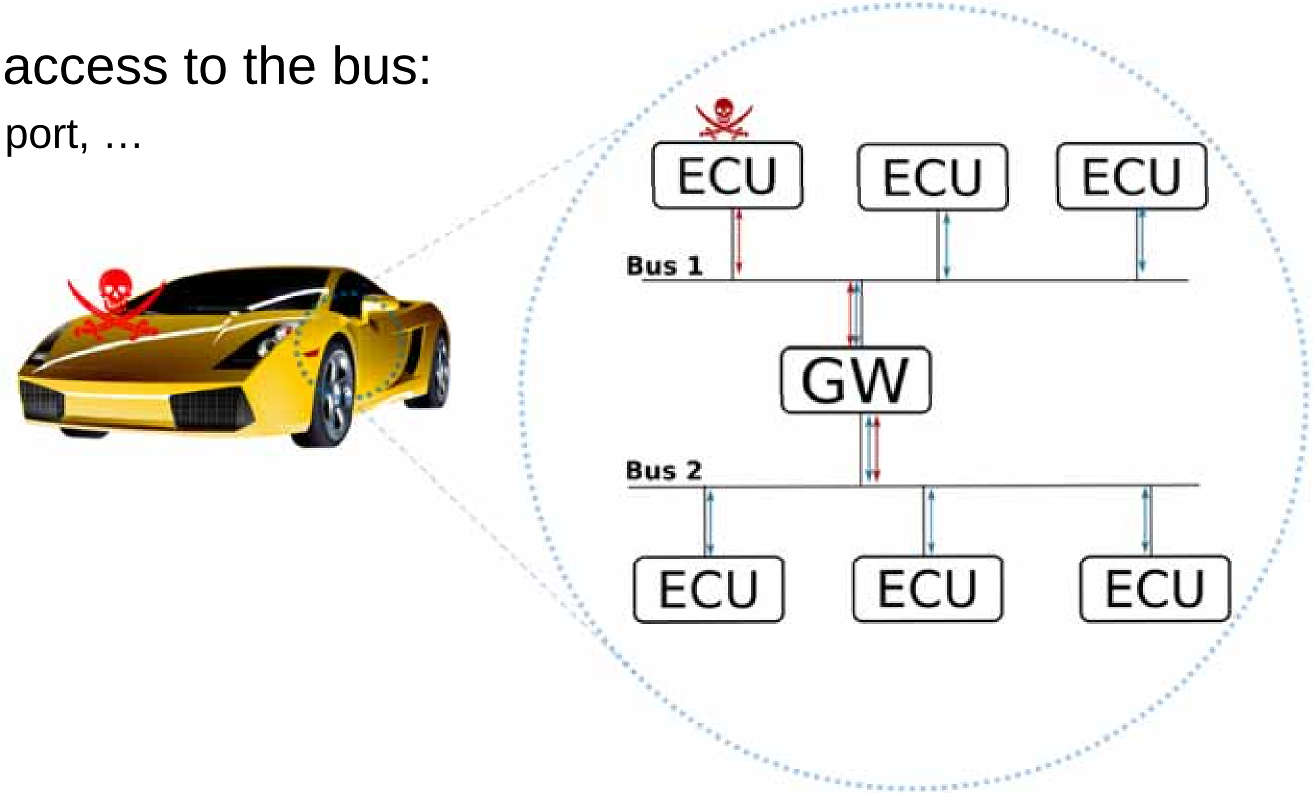
by Sean Gallagher - Jul 24, 2015 5:54pm CEST

Security researcher Charlie Miller attempts to extract a Jeep Cherokee from a ditch after its brakes were remotely disabled in a controlled test.

Local attacks

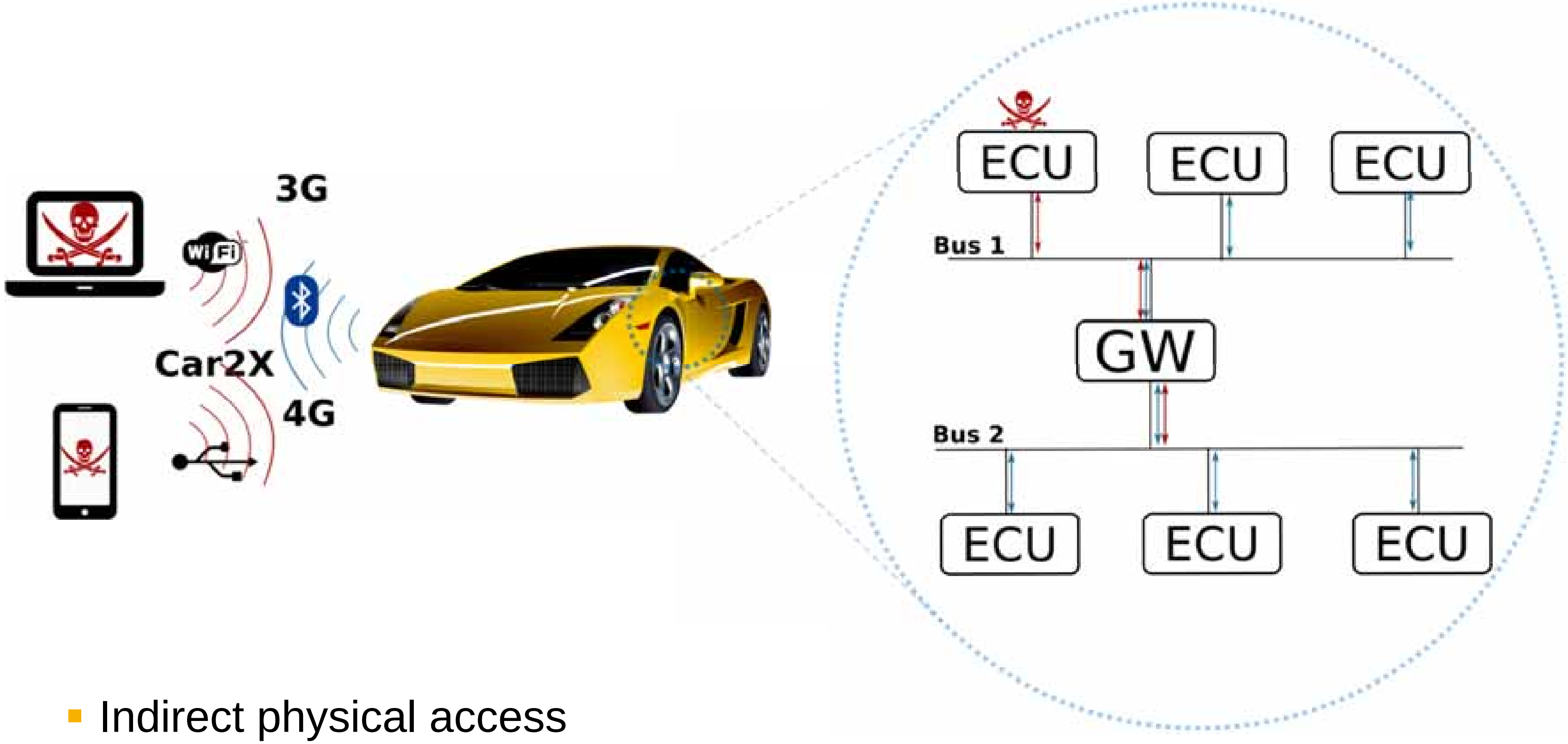
Attacker has direct access to the bus:

- Through the OBD port, …



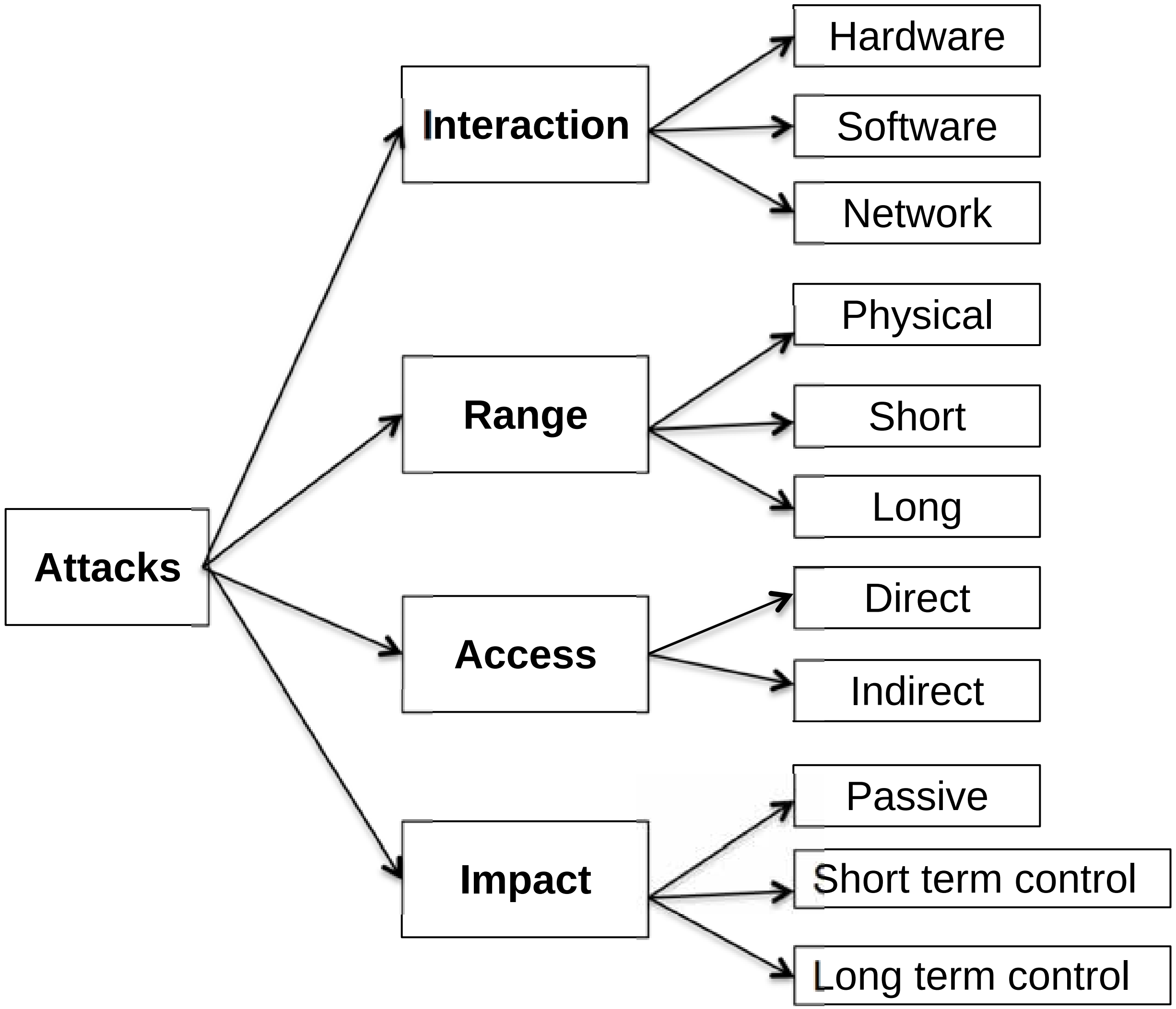
- **Possible Actions**
  - Read data
  - Send crafted frames
  - Interrupt traffic
- **Impact**
  - Knowledge Acquisition
  - Temporary Control
  - Permanent Control

Remote attacks



- Indirect physical access
  - multimedia player via usb, compromized diagnostic tools…
- Short range wireless access
  - a few meters: Bluetooth, remote keyless entry, RFID car keys, …
- Long range wireless access
  - mobile communication networks: GSM/3G, web, …

Classification of attacks



Classification of attacks

Incident (spans Attackers → Objectives)
Attack (spans Tool → Unauthorized Result)
Event (spans Action → Target)

Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Malicious code	Design (protocol, specification, application)	Read	Automobile	Increased access	Challenge, Status, Thrill
Spies	Attached devices	Implementation	Create/Spoof	Bus system	Disclosure of information	Political gain
Terrorists	Wireless equipment	Configuration	Copy	Control Unit	Corruption of information / programs	Financial gain
Corporate raiders	Manipulated media	Misbehavior of a user	Steal	Operating map	Blocking of resources (denial of service)	Damage
Professional criminals	Social engineering		Delete	Occupants/ Owner	Theft of resources	Security evaluation
Vandals			Modify/ Reconfigure	User data	Causing costs	Tuning
Voyeurs			Probe	Manufac-turer data	Violation of Confidentiality, Authenticity, Integrity, Availability, Non repudiation, Privacy	
Security scans			Scan	Road safety		
Tuners			Flood			
Thieves			Authenticate			
Competing manufacturers			Bypass			

Adaptation of CERT taxonomy to Automotive environment [Hoppe & Dittman 07]

Classification of Attacks

Vector	Description	Agents
#1	Attacks on global V2I/I2I communication infrastructure	X, L, E
#2	Attacks on local V2V communication infrastructure	X, L, E
#3	Attacks on in-vehicle communication infrastructure	L, P
#4	Attacks on vehicle computing nodes' software	L,P
#5	Attacks on road-side units'software	X, P, E
#6	Attacks on sensors and control-sensitive data	X, L, P, E
#7	Attacks on authentication mechanisms	X, L, P
#8	Physical-level attacks	P

X: External (computers on the Internet, compromised RSU)

L: Local (compromised computers inside car, connected media

P: Physical (compromised computers on maintenance sockets, …)

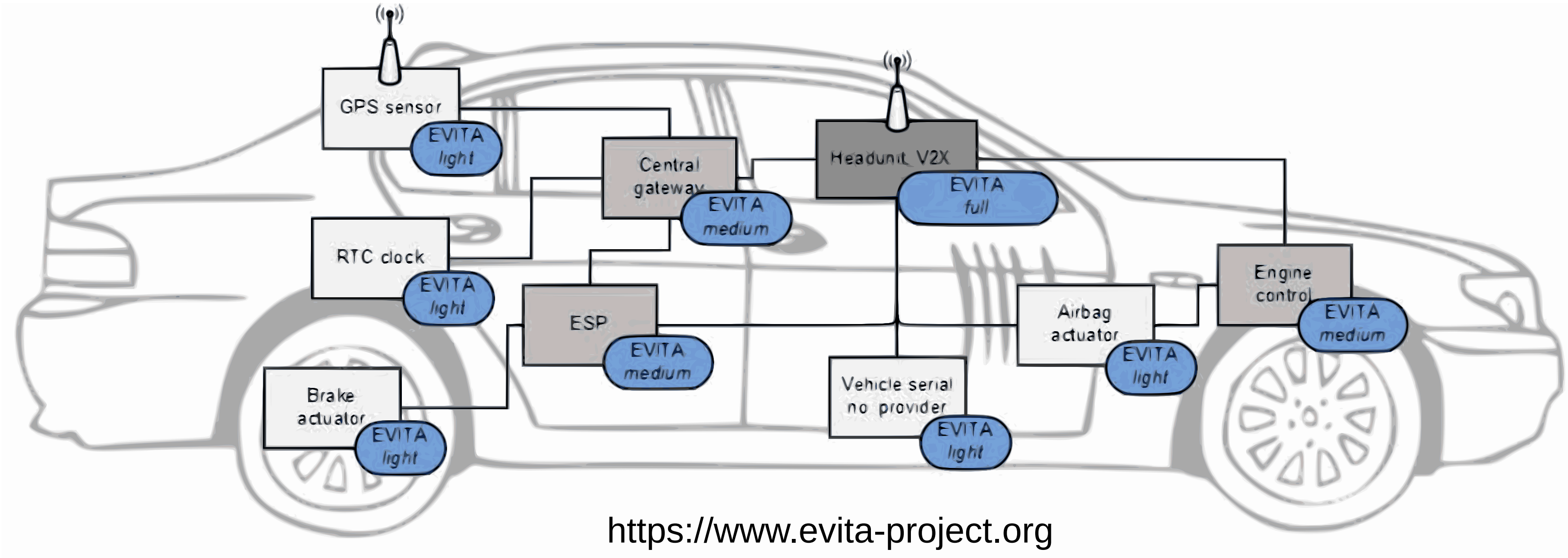
E: Environment (devices interfering with physical env. properties (jammers, fake RSU

Toward Safe and Autonomous Cooperative Vehicle Ecosystems [Lima et al. 2016]

Protection: a major concern …

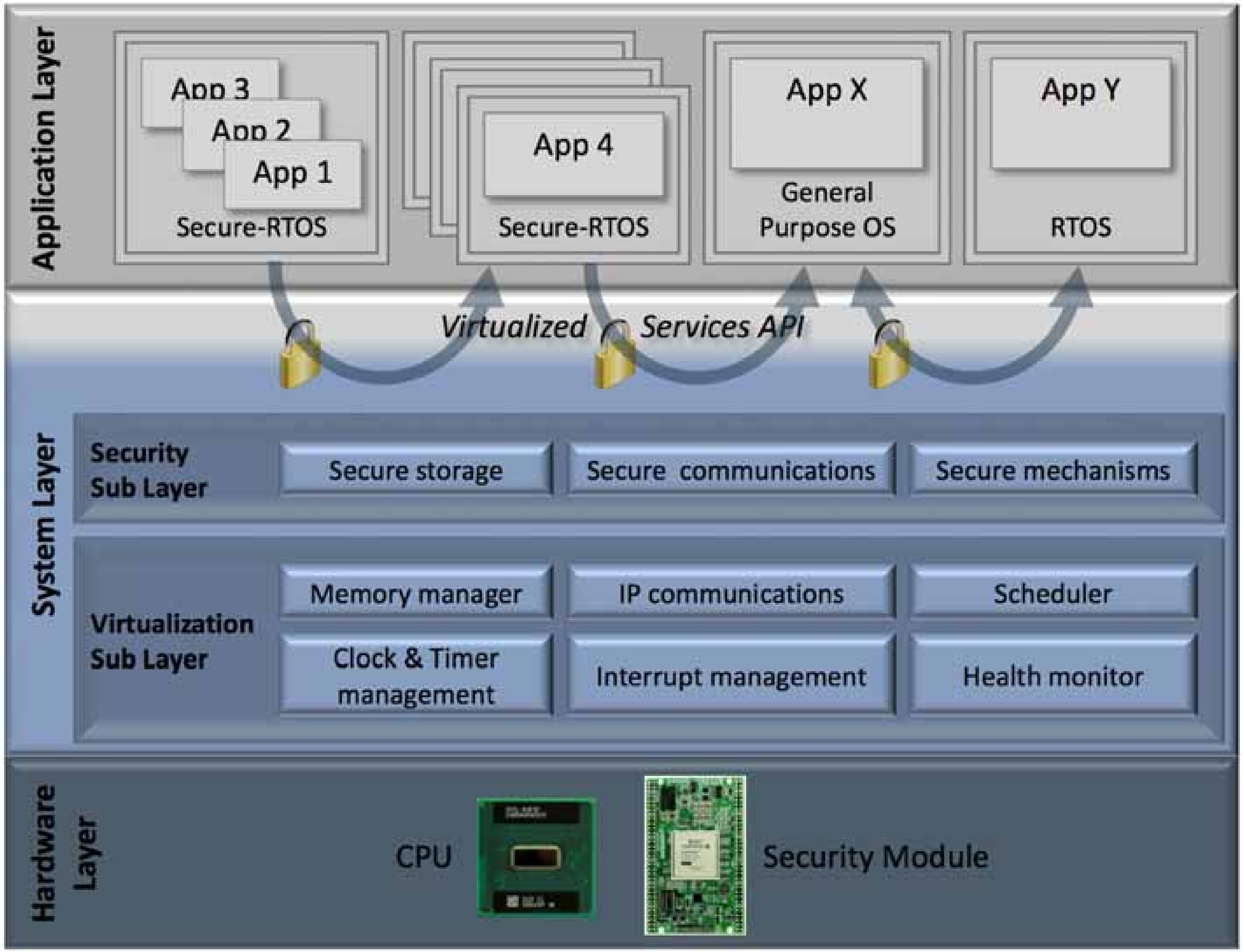
- **Defence in depth**
  - prevention, detection, containment
- **Various techniques**
  - Trust management and access control
  - In-car and car2X secure communications
    - cryptographic protocols, …
  - Trusted hardware modules deployed in ECUs
    - Key management
    - Secure boot
  - Embedded software protection
    - Code signing
    - Virtualisation and sandboxing
    - Hardened execution platforms
    - …

Hardware Security Modules: EVITA Project



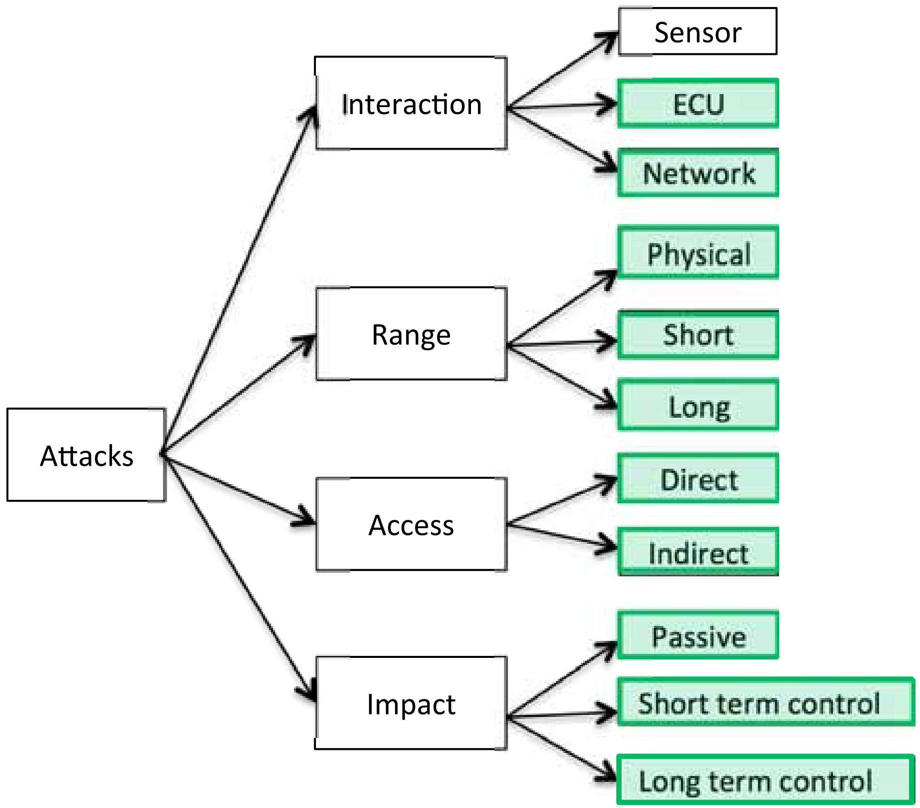
- **Three classes of HSM, different costs, different security protection**
  - **Full**: high performance asymmetric/symmetric crypto, powerful internal processor & memory : for V2X communication unit, central gateway
  - **Medium**: fast symmetric crypto HW, firmware asymmetric crypto: for in-vehicle security modules with strong cost & security requirements (engine control, front/rear module, …)
  - **Light**: cost optimzed symmetric crypto HW with small internal memory: for less, but critical security-critical ECUs that provide/process security critical information (critical sensors/ actuators,

Oversee: Open Vehicular Secure Platform



https://www.oversee-project.com

A major concern …



Preventive Solutions

What happens if an intrusion is successful?

Outline

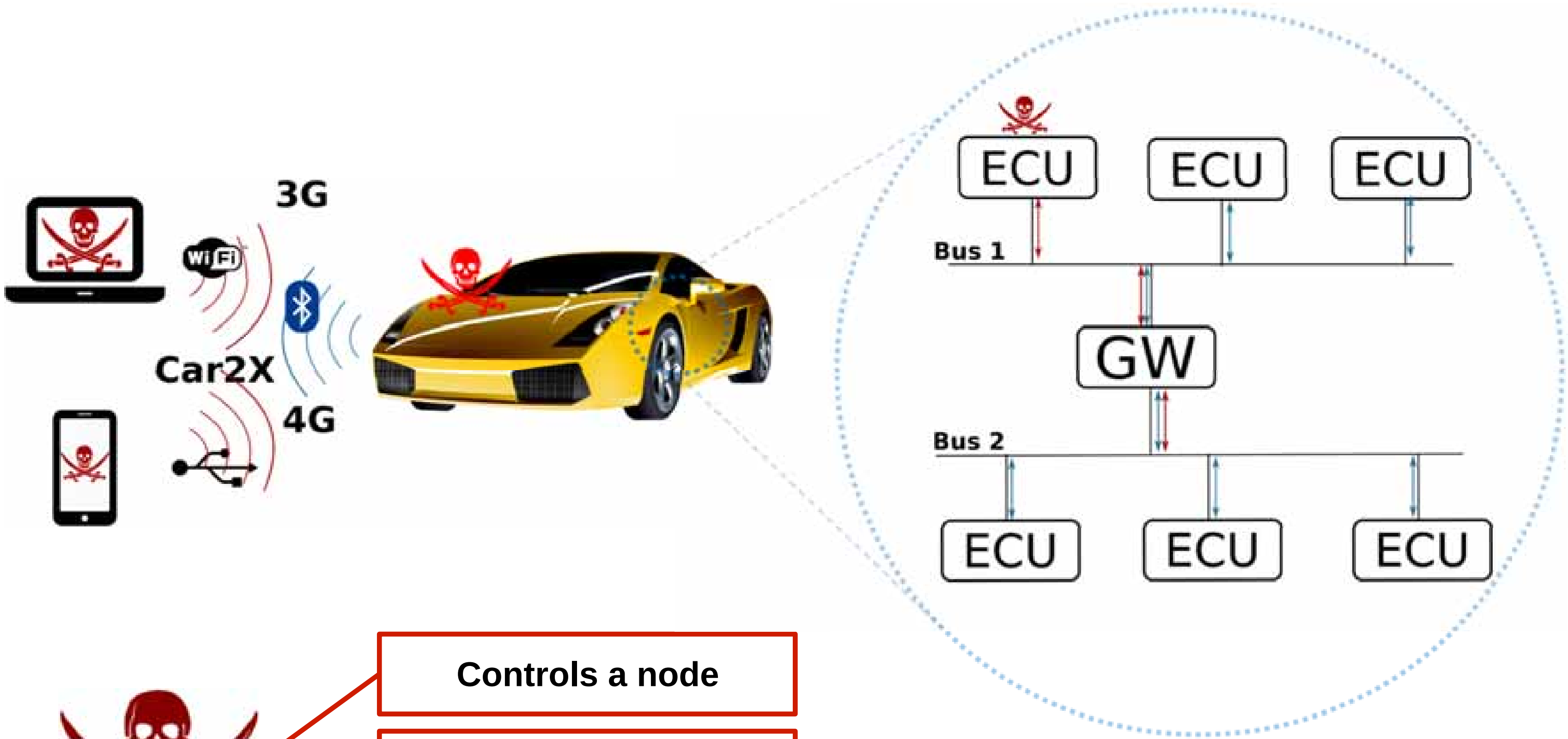
- Review of security threats and some existing protection mechanisms

- **Design of an intrusion detection system for automotive embedded networks**

Intrusion detection

- **Signature-based**
  - Known attacks
  - Need regular updates
- **Anomaly/behavioural based**
  - Detects unknown attacks
  - Requires a model of normal behaviour
    - Specification-based/machine learning

Attack scenario



- Controls a node
- Knows the system
- Emits frames onto the network

Constraints

Cost

- Carry over/COTS
- Limited resources

Diversity

- Many architectures
- Model specific attack scenarios

Lifecycle

- 20 years

Reactivity

- Fast detection required

Network-based monitoring

- No alteration of the ECUs
- No change in the network architecture

Behaviour-based approach

- System modeling
- Anomaly detection
- Requires few or no updates

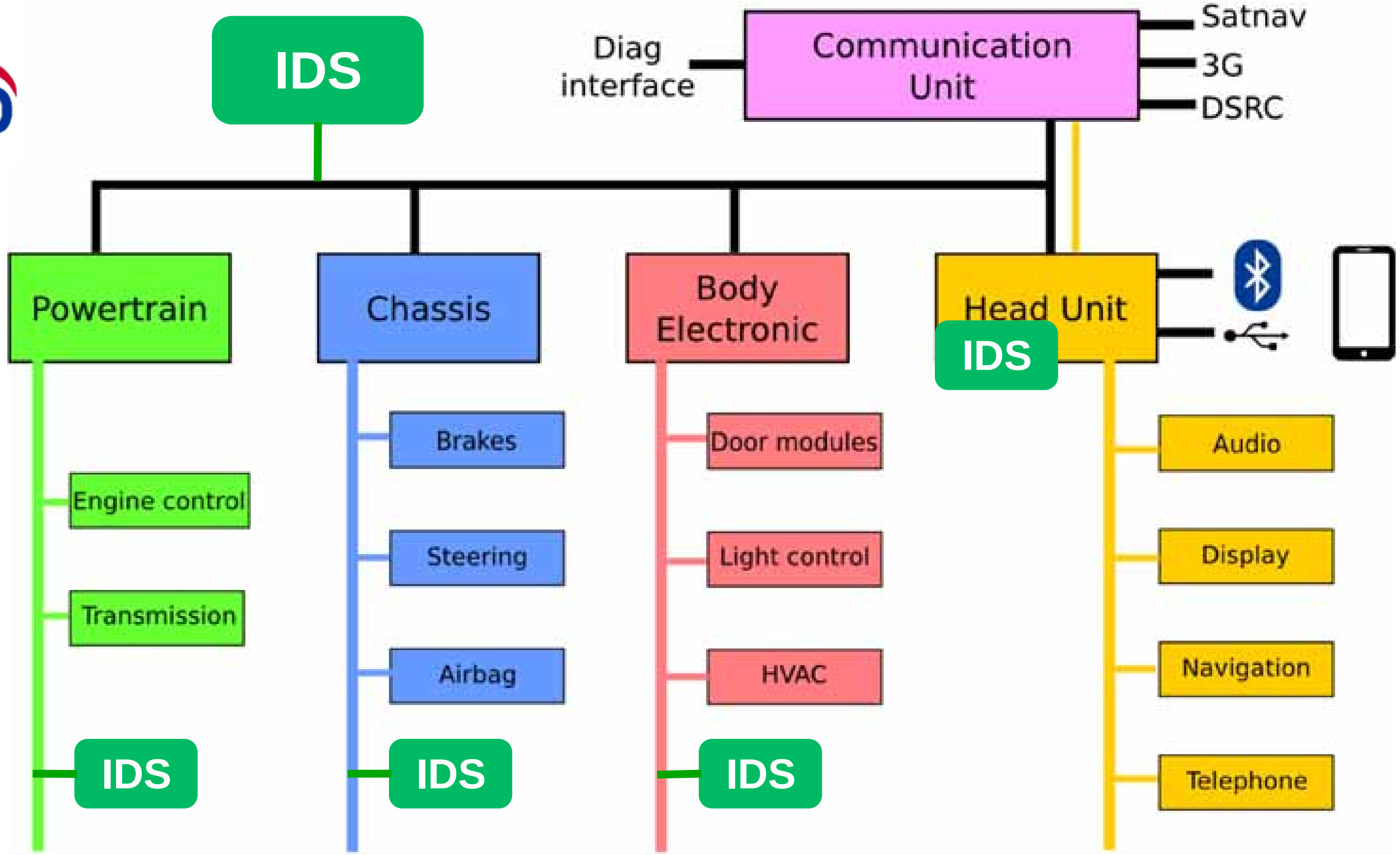
Passive system

- Detection only
- Open to evolutions

Optimisation

- Master complexity

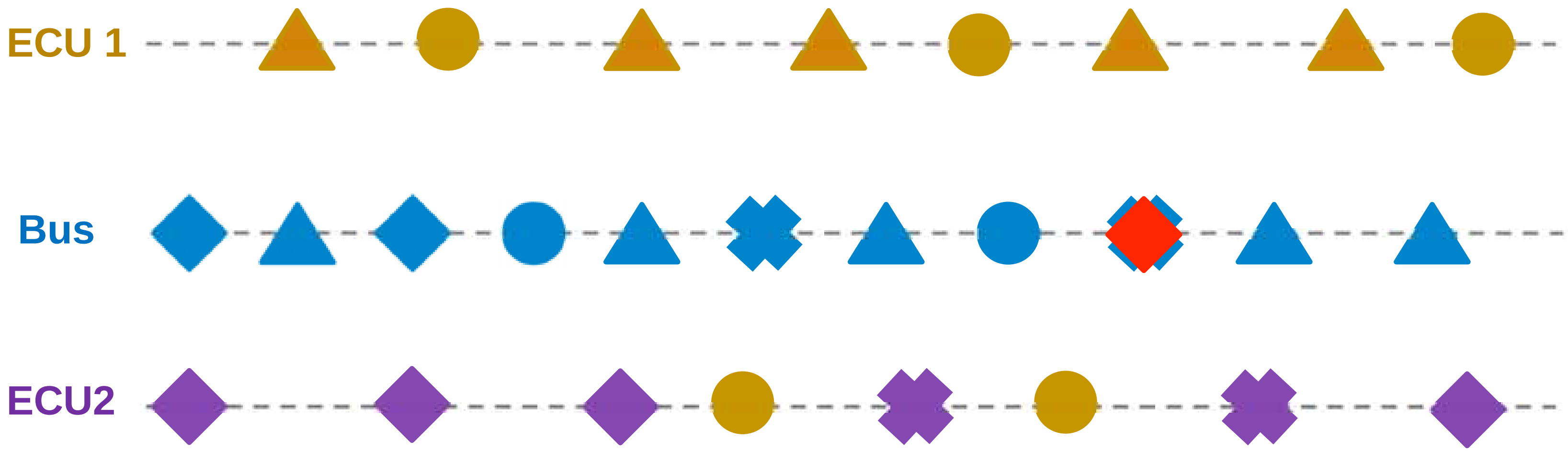
Location


IDS
Diag
interface
Communication
Unit
Satnav
3G
DSRC
Powertrain
Chassis
Body
Electronic
Head Unit
IDS
Brakes
Door modules
Audio
Engine control
Steering
Light control
Display
Transmission
Airbag
HVAC
Navigation
IDS
IDS
IDS
Telephone

One source of data: the network

Network traffic monitoring

Goal : Check the consistency of a message with the previously observed behaviour



Attack symptoms

Frames that do not conform to the protocol specifications

Set of formal checks

Periodic, forged frames added into the traffic

Monitoring of the frames frequency

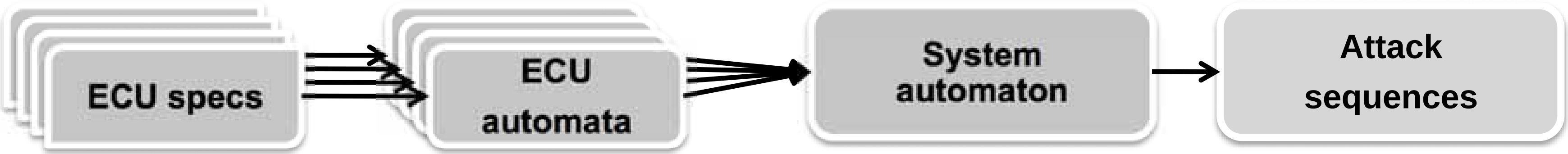
Periodic, forged frames replacing the legitimate traffic

Event-related forged frames

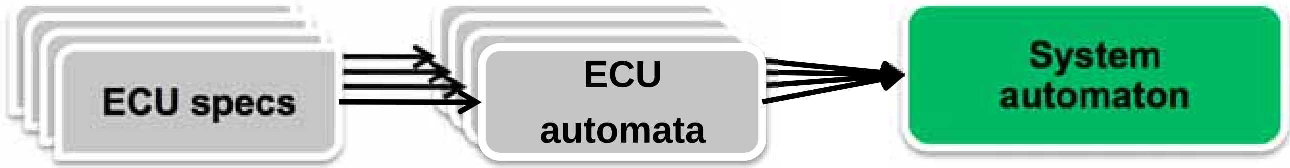
Correlation of contextual information

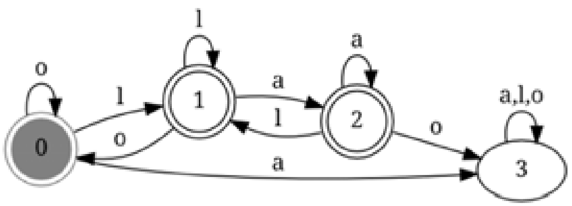
Context-sensitive anomaly detection approach

- **ECUs network behavior modeling with Finite State Automata (FSA)**
  - Based on specifications or on network traffic monitoring
- **Generate System Automaton from composition of ECUs FSA**
  - Represented by a langage L_{SYS}
- **Generate a langage of observable attack sequences**
  - $\overline{L_{SYS}}$ = complement of L_{SYS}

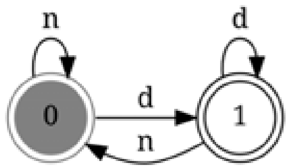


Context-sensitive anomaly detection

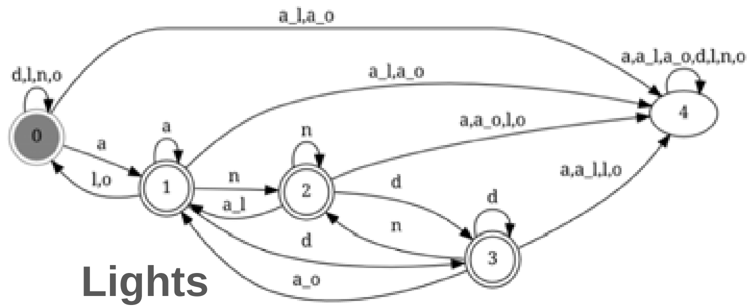




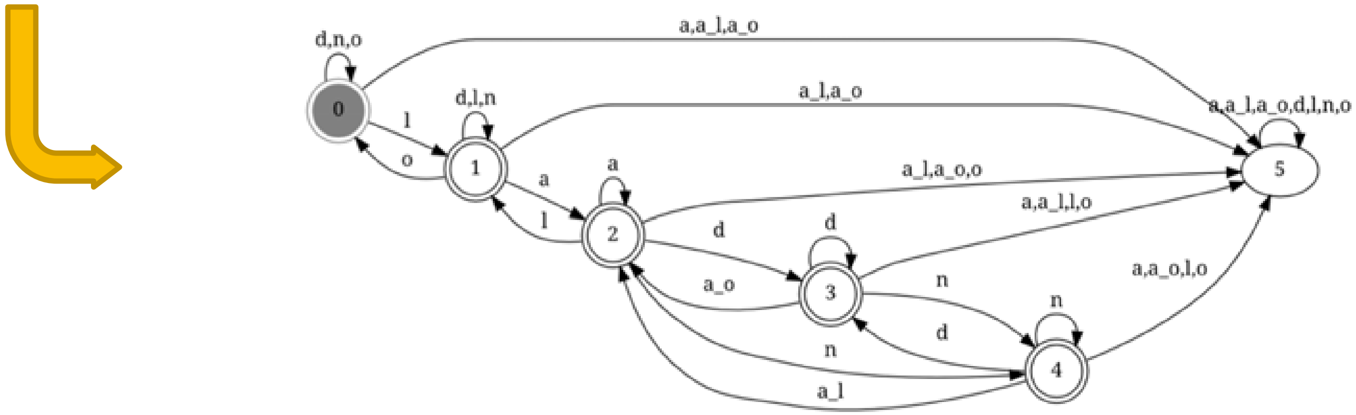
Command



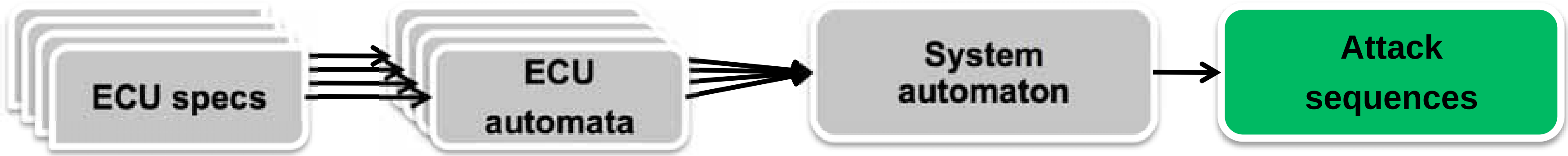
Sensor



Lights

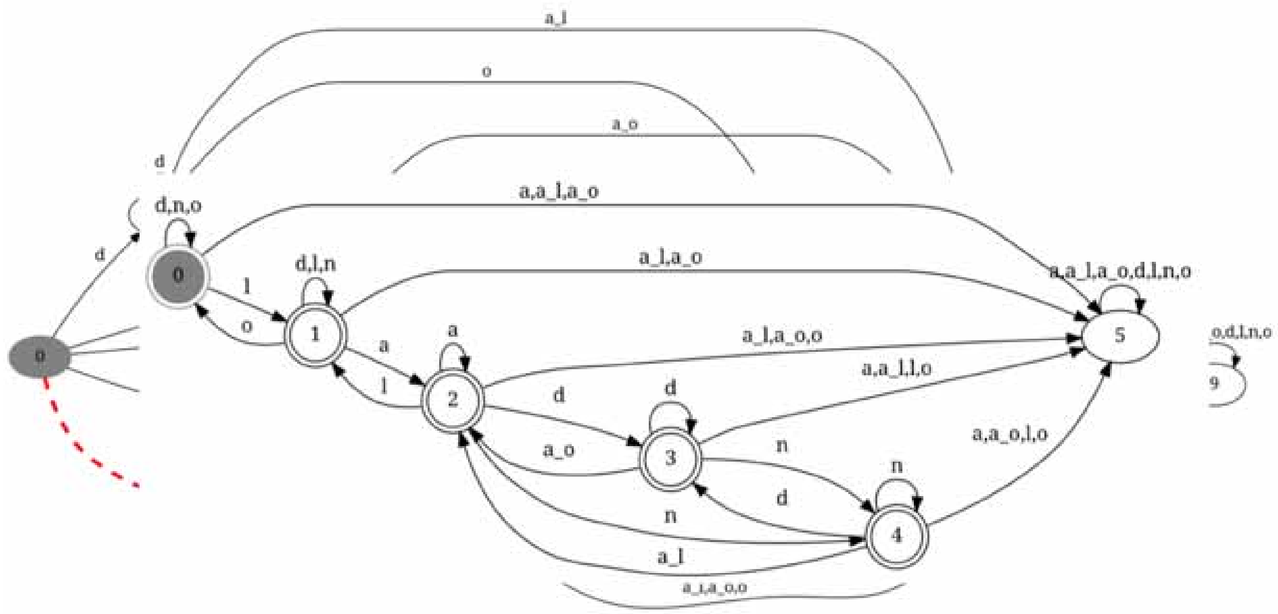


Context-sensitive anomaly detection



$$L_{attacks} = \underbrace{Suf\,(L_{sys}.\Sigma_{sys} \cap \overline{L_{sys}})}\cap\underbrace{\overline{Suf(L_{sys})}}$$

"The sequence ends with a forbidden transition **AND** is not a part of any legitimate sequence"



Complexity

1 automaton $\mathbf{A}_{attacks}$ accepting

$$\mathrm{L}_{\mathrm{attacks}} = \underbrace{\mathrm{Suf}(L_{sys}).\Sigma_{sys} \cap \overline{L_{sys}}}_{\mathrm{L}_{\mathrm{left}}}) \cap \underbrace{\overline{\mathrm{Suf}(\mathrm{L}_{\mathrm{sys}})}}_{\mathrm{L}_{\mathrm{right}}}$$

Time complexity $O(1)$

State complexity (worst case) $O(2^n)$

2 automata $\mathbf{A}_{left}$ and $\mathbf{A}_{right}$ accepting resp. $L_{sys}.\Sigma_{sys} \cap \overline{L_{sys}}$ AND L_{sys}

Handling the suffixes

2 *sets* S_{left} *and* S_{right} containing the possible states of $\mathbf{A}_{left}$ and $\mathbf{A}_{right}$ at a given time

Time complexity (worst case) $2n+1$

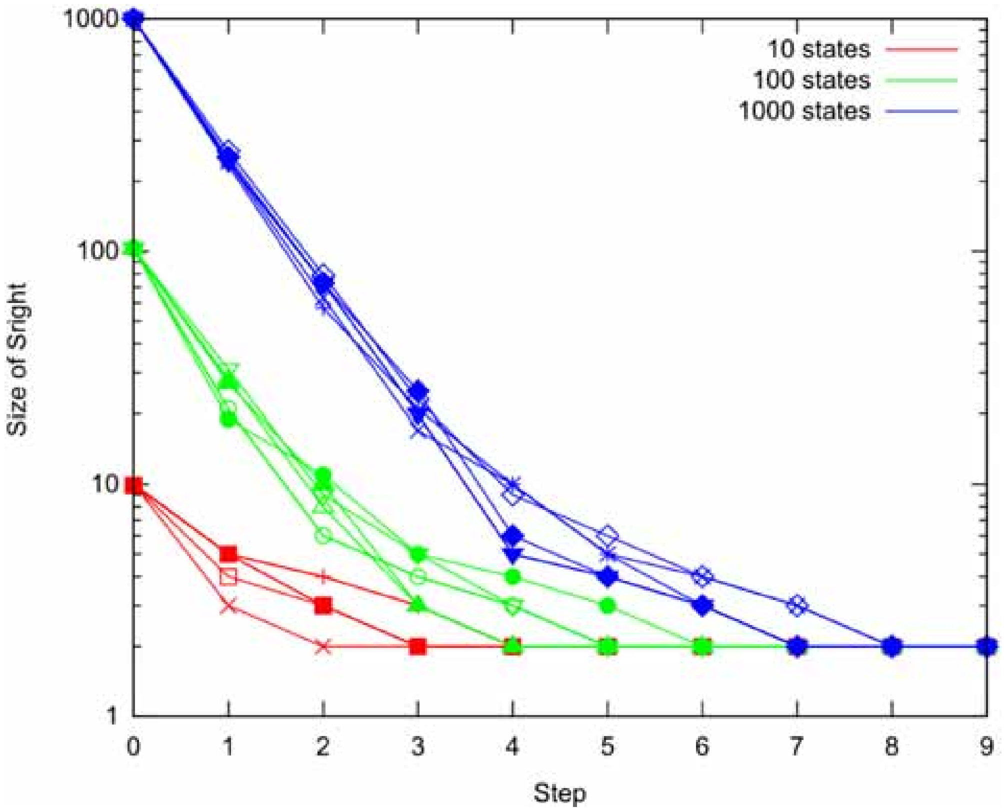
State complexity $(1+|\Sigma_{sys}|)(2n+1)$

1 automaton $\mathbf{A}_{right}$ and 1 set $\mathbf{S}_{right}$

Time. complexity (worst case) n

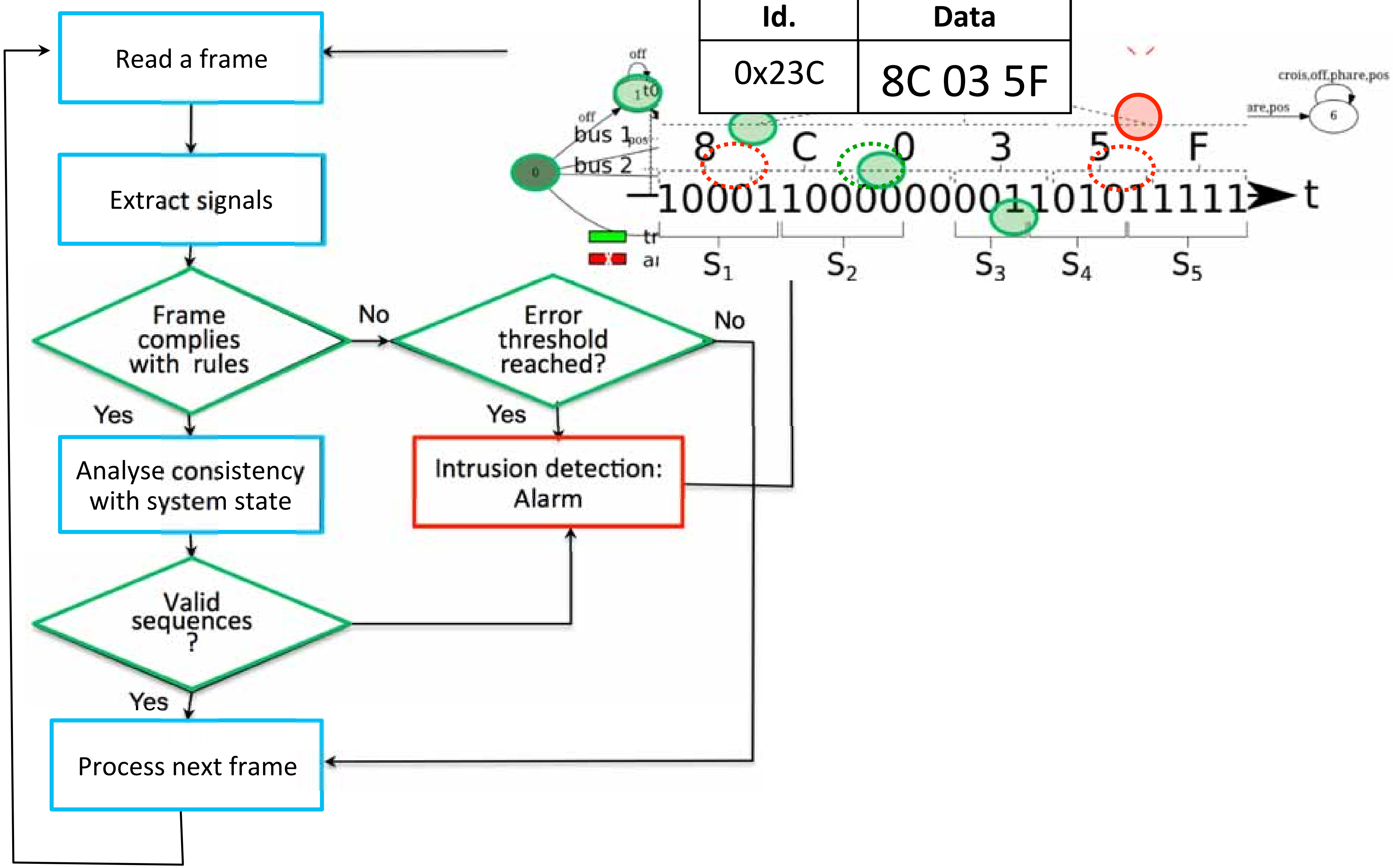
State complexity $n(1+|\Sigma_{sys}|)$

Complexity (2)

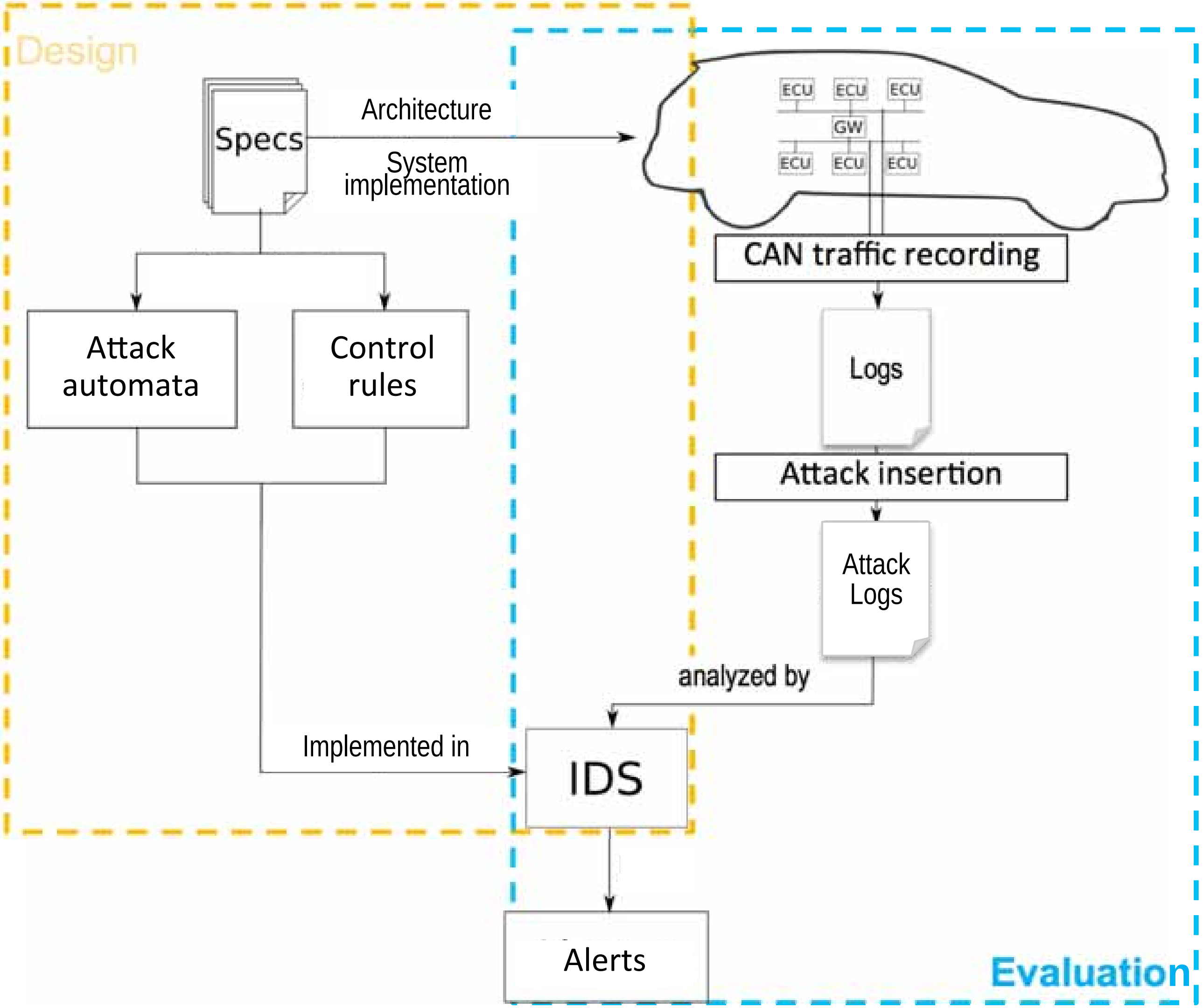


Overview

Id.	Data
0x23C	8C 03 5F



Experimental Protocol



Experimental Protocol

Data Set

102 log files / 49 min total
3000 – 400 000 frames per file / 2s – 3min

Studied Systems

Light control subsystem (LCS)
Speed control subsystem (SCS)
Composed system (LCS + SCS)

Objectives

Detection coverage
Detection time

Experimental results

Parameters
1 core – 1,2GHz 310 440 frames – 205 seconds ➔ 1514 frames/s – 660µs/frame Durations measured over 100 runs

- **Successful detection of all simulated attacks**

- **Frame checks**

Step	Average	Min	Max
Interpretation	32µs	8µs	517µs
Control rules	33µs	5µs	110µs

Large variation of the number of signals per frame (1 — 30)

Experimental results

- « Worst » case : composed system — 108 states
- State Complexity

	$A_{attacks}$	A_{right}
states	366	108

- Time Complexity
  - $A_{attacks}$

    Constant analysis time ≈ 12 μs

  - A_{right}

Avg. auto	Min auto	Max auto
49μs	20μs	779μs

Avg. frame	Min frame	Max frame
153μs	34μs	903μs

Conclusion

Automotive systems security: a major challenge

- Increasing complexity→ many potential vulnerabilities
- Connectivity → wider attack surface
- Documented attack examples

Design of a context-sensitive automotive IDS

- Language theory to characterize attacks
- Compatibility with existing architectures
- First implementation for CAN networks
- Can be adapted to other protocols and contexts

Extensions

Full scale evaluation
Distributed IDS

Other challenges

- **From detection to reaction**
  - Alert the driver
  - Trigger automatic recovery actions, consistent with safety rules
    - Safety – Security interactions
    - Extensions to compensate possible imperfect coverage of existing safety mechanisms
  - Intrusion tolerance
- **Protection against low level attacks**
  - Leverage advances from hardware architecture technologies
- **Privacy**
- **Holistic engineering approach to address inter-related safety-security-privacy requirements**
- **Standardisation : Extension of AUTOSAR ISO 26262**
- **Legal issues**

For further details …

- Ivan Studnia, Intrusion Detection for Embedded Automotive Networks: A language-based Approach, Phd, Université de Toulouse, France, 2015 (in French) – https://tel.archives-ouvertes.fr/tel-01261568

- I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, Y. Laarouchi, A language-based intrusion detection approach for automotive embedded networks, International Journal on Embedded Systems, Special Issue PRDC-2015, http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijes https://hal.archives-ouvertes.fr/hal-01419020/

- Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Youssef Laarouchi, Survey on security threats and protection mechanisms in embedded automotive networks. 2nd Workshop on Open Resilient human-aware Cyber-physical Systems (WORCS-2013), DSN-21013 Workshops, Budapest (Hungary), june 2013.

- Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al.: Comprehensive experimental analyses of automotive attack surfaces. 20th USENIX Security. San Francisco, CA (2011)

- Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H.: Experimental security analysis of a modern automobile. IEEE Symp. Security and Privacy. pp. 447–462. Oakland, CA (2010).

- H. Schweppe, Security and Privacy in Automotive On-Board Networks, Phd Telecom ParisTech, 2012