evs 27

The 27th INTERNATIONAL ELECTRIC VEHICLE SYMPOSIUM & EXHIBITION.

Barcelona, Spain
17th-20th November 2013

Impact of a Smart Grid to the Electric Vehicle Ecosystem From a Privacy and Security Perspective

Christophe Jouvray, Mourad Tiguercha (TRIALOG)

Gloria Pellischek (ERPC)

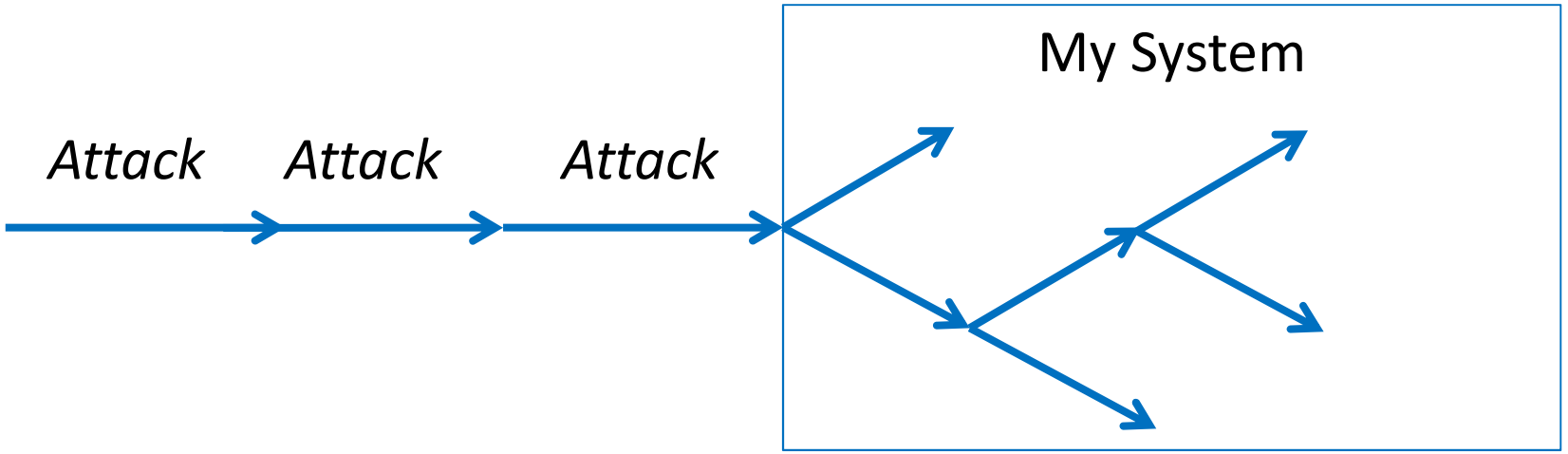
Organized by Fira Barcelona avele

Hosted by AVERE mea Ajuntament de Barcelona

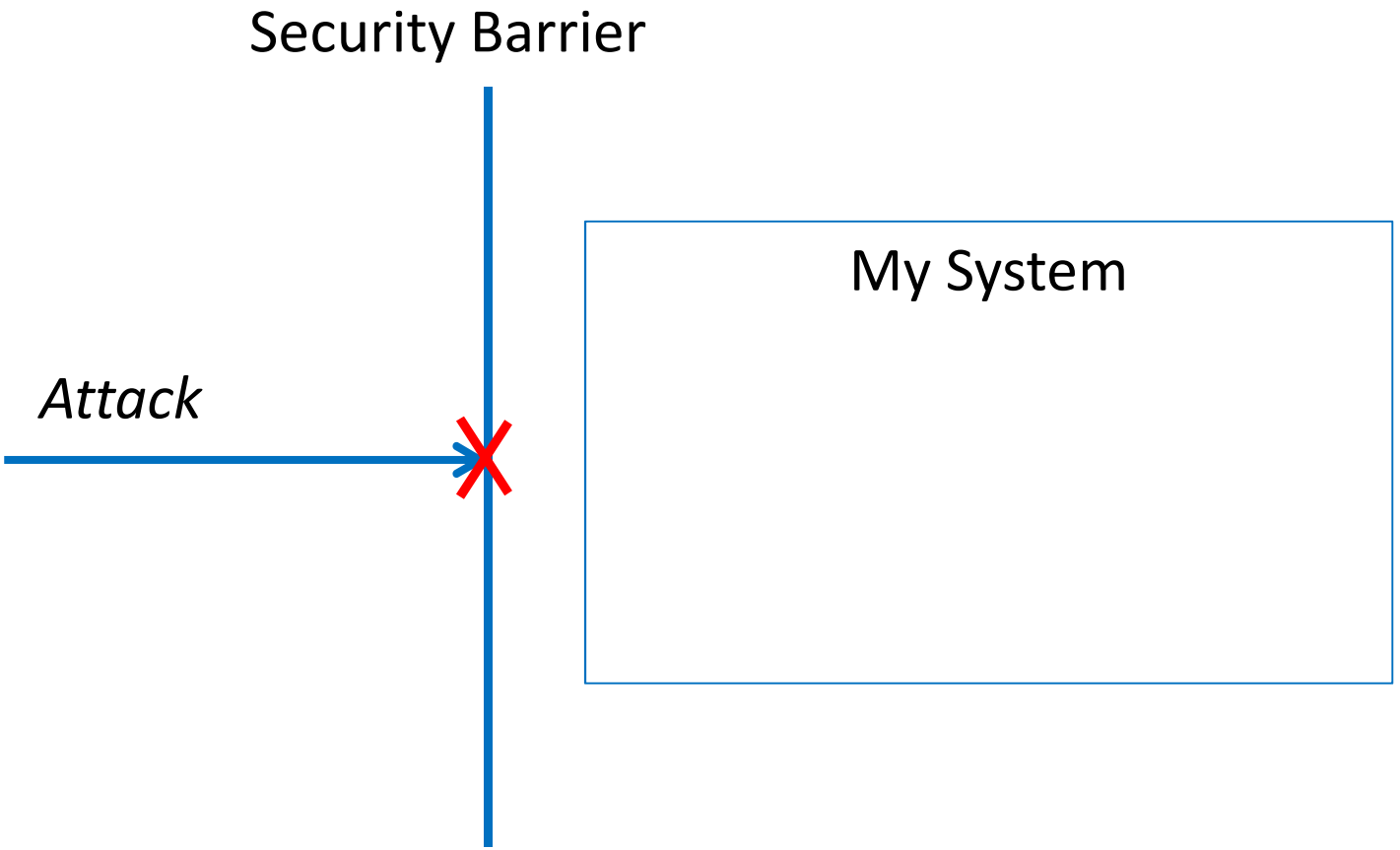
In collaboration with EVAAP EDTA

Supported by European Commission

Impact of Security Attacks



Holly Grail of Security



The reality

- To avoid all attacks is impossible

- What can we do?
  - Have a good knowledge of the system
    - The motivation of an attacker
    - The impact of a vulnerability (risk encountered by the system)
    - The possible countermeasure with their benefit
    - The cost of a countermeasure
  - Add security mechanisms for increasing the difficulty to launch an attack
    - Should be taken into account early in the V-Cycle

Privacy Issues

- Privacy leaks due to
  - Attacks
  - Breach of trust

Vehicle Identity

Personal information

Tracking and Tracing of user

Sequential past and present position/time data

Credit Card or ID Card details

mobile device data

EU Data Protection Legislation

EXISTING LEGISLATION

ITS Legal Framework

Standards and Specifications

Delegated acts

Art. 8 European Convention of Human Rights

Charter of Fundamental Rights of the European Union

Art. 16: Treaty on the Functioning of the European Union

Directive 95/46/EC on protection of personal data

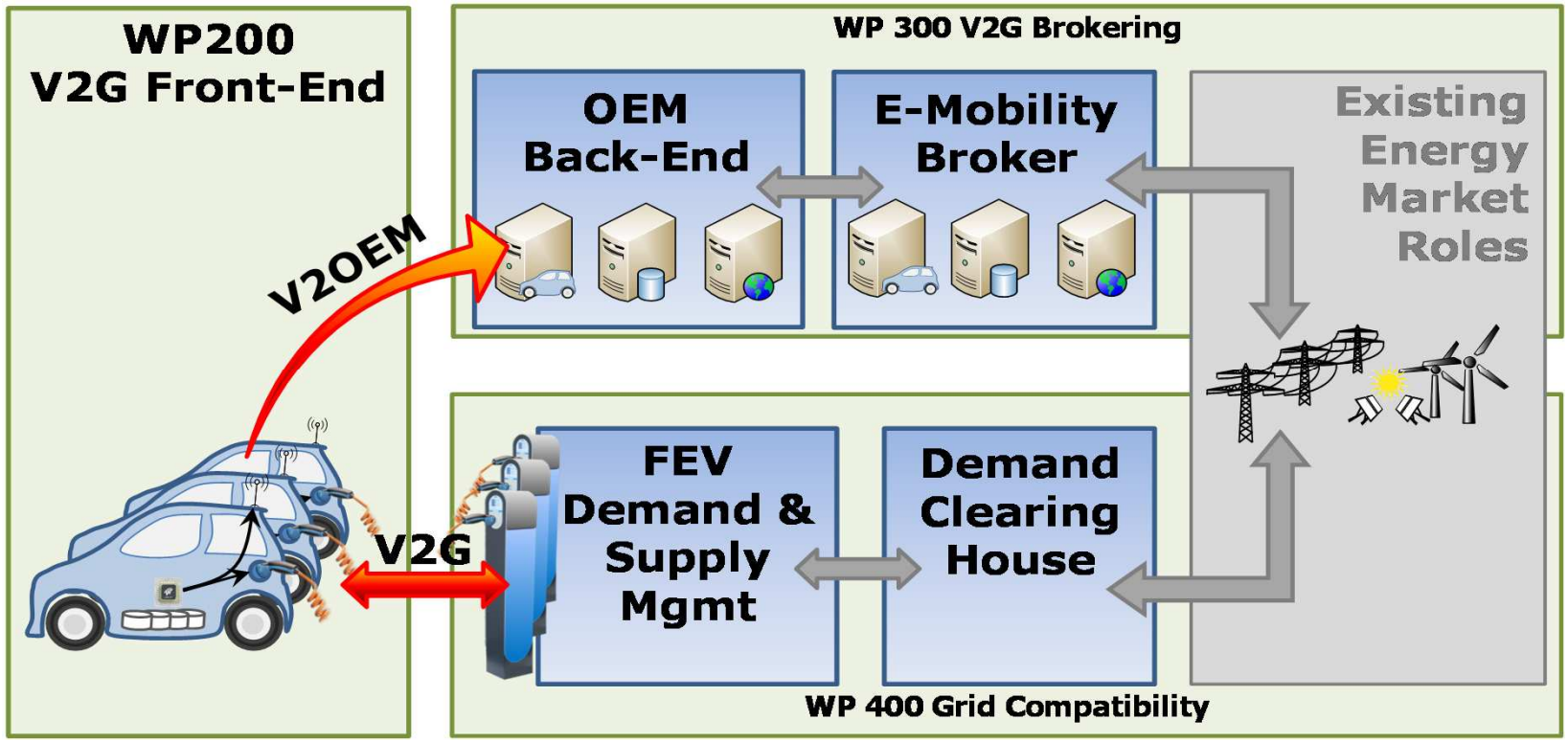
EMERGING LEGISLATION

- Guaranteeing easy access to one's own data and the freedom to transfer personal data from one service provider to another.
- Establishing the right to be forgotten to help people better manage data protection risks online. When individuals no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Ensuring that whenever the consent of the individual is required for the processing of their personal data, it is always given explicitly.
- Ensuring a single set of rules applicable across the EU
- Clear rules on when EU law applies to data controllers outside the EU

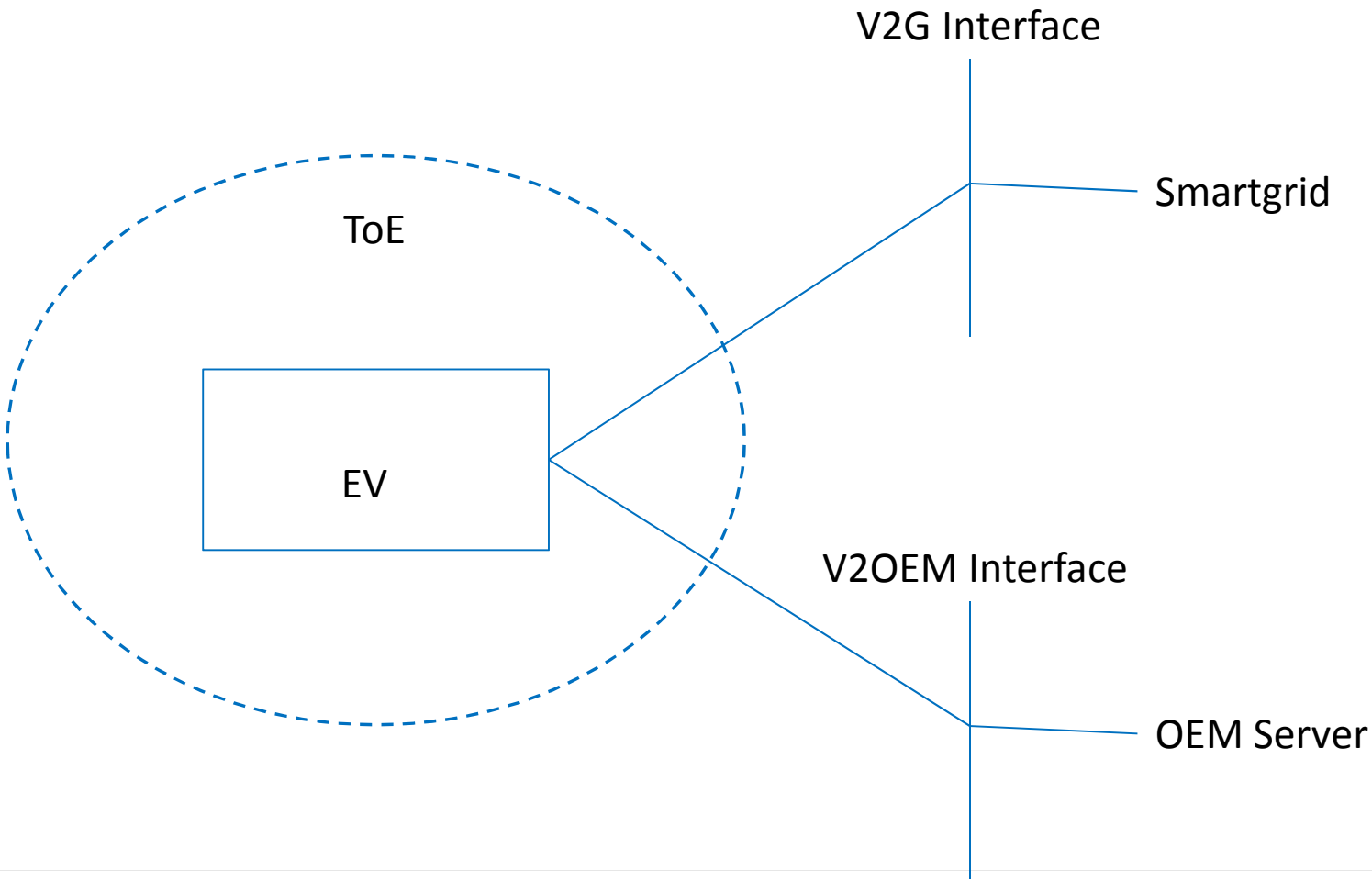
Approach used in the paper

- Proceed to a security analysis based on the ETSI TVRA approach
  - Risk-based analysis
  - Rely on 10 steps
  - But do not take into account the cost of a countermeasure

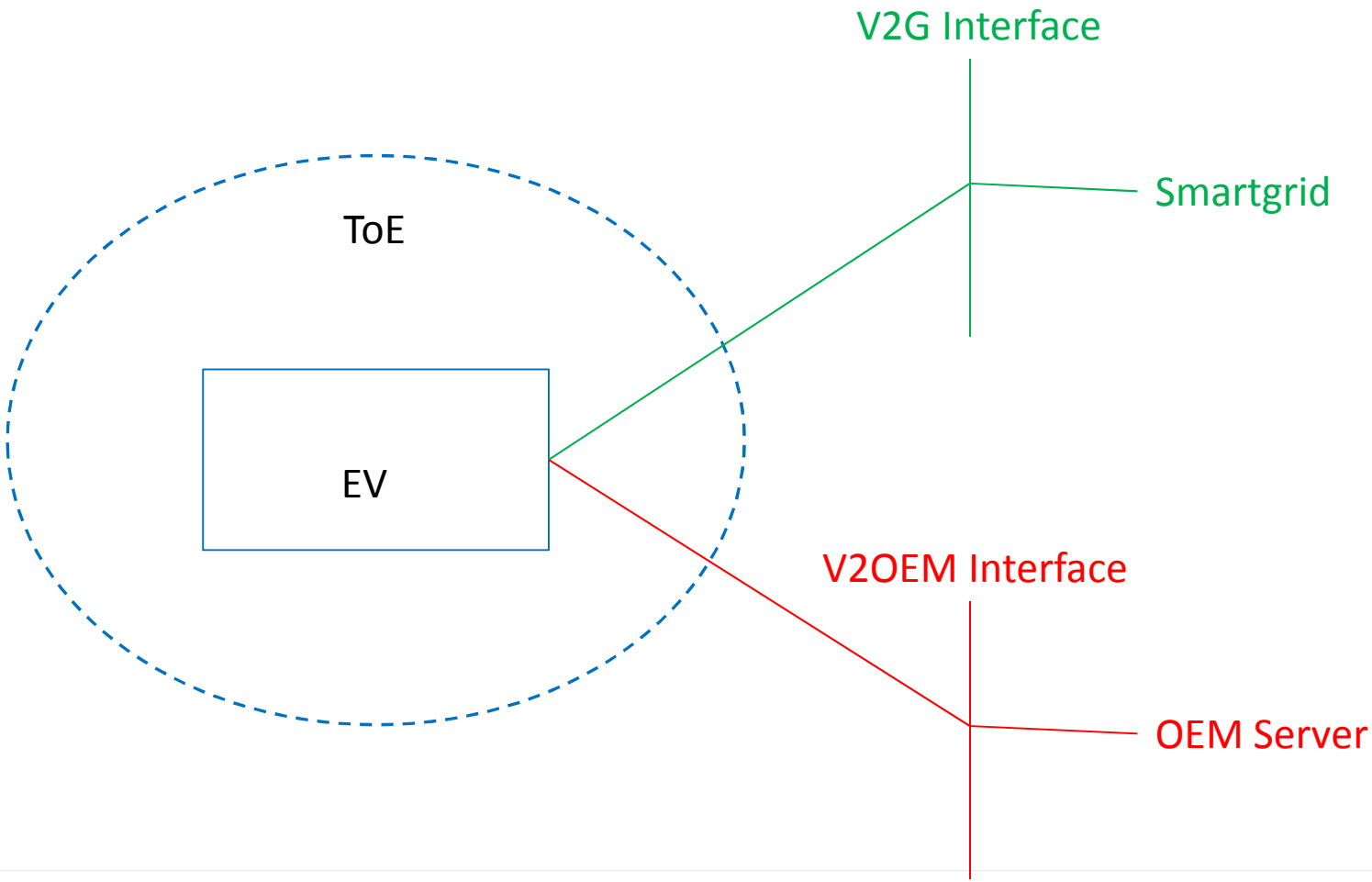
Context


WP200
V2G Front-End
V2OEM
V2G
WP 300 V2G Brokering
OEM
Back-End
E-Mobility
Broker
Existing
Energy
Market
Roles
FEV
Demand &
Supply
Mgmt
Demand
Clearing
House
WP 400 Grid Compatibility

Target of Evaluation (ToE)



Focus on V2G Interface



Security Objectives

Some ISO/IEC 15118 Services	Confidentiality	Integrity	Authenticity	Non-Repudiation	Availability
supportedAppProtocolReq	L	M	M	L	L
supportedAppProtocolRes	L	M	M	L	L
chargeParameterDiscoveryReq	L	M	M	L	L
chargeParameterDiscoveryRes	M	H	M	L	L
chargingStatusReq	L	H	H	H	L
chargingStatusRes	L	H	H	H	L
serviceDetailReq	L	M	M	L	L
serviceDetailRes	L	M	M	L	L

L = Low
M = Medium
H = High

Threat Identification

- 14 threats have been identified
  - Based on ISO/IEC 15118 specifications
  - Based on PLC Communications

- Most important threats identified in the system
  - Attacker provides a higher VAS than the CS (ISO/IEC 15118-2)
    - Trust in services without authenticity checking
  - Security weaknesses at some protocol layers (ISO/IEC 15118-3)
    - Unsecure key exchange at MAC layer
  - PLC weaknesses
    - Literature lists attacks based on denial of service, spoofing, tampering techniques

Impact of the Threats

- Usage of the Microsoft Classification (STRIDE)
  - Spoofing identity
  - Tampering with data
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of privilege

Risk-based Evaluation

Threat ID	Asset involved	Attack				Risk value	ranges of attack factors							value						
		Resistance to attack	Likelihood of the attack	Impact	Risk		time	expertise	knowledge	opportunity	equipment	asset impact	intensity	time	expertise	knowledge	opportunity	equipment	asset impact	intensity

Risk value = f(time, expertise, knowledge, opportunity, equipment, asset impact, intensity)

Countermeasures

- Most important ones
  - Use end-to-end security protocols
  - Check the identity

- All of them reduce the vulnerability of the system

Conclusion

- To avoid all attacks is impossible

- A good knowledge of our system is a key in security
  - Measure the risk encountered by the system
  - Take into account security at the beginning of the V-Cycle
  - Patch the system with countermeasures in operation is essential!

- Readiness of EU legal framework for ITS
  - In progress

evs 27

The 27th **INTERNATIONAL ELECTRIC VEHICLE SYMPOSIUM & EXHIBITION.**

Barcelona, Spain
17th-20th November 2013

Thank you for your attention.

Questions?

Organized by Fira Barcelona avele

Hosted by AVERE mea Ajuntament de Barcelona

In collaboration with EVAAP EDTA

Supported by European Commission