CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Cybersecurity Aspects of 5G Connectivity in Smart Cities Ecosystem via Connected and Autonomous Vehicles Use Cases

Athanasios Papadakis Dr. Antonios Lalas Dr. Konstantinos Votis Dr. Dimitrios Tzovaras

Information Technologies Institute
Centre for Research and Technology Hellas, CERTH
Thessaloniki, Greece

Contact: Dr. Antonios Lalas
CERTH/ ITI Postdoctoral Research Associate
Tel. : +30-2311-257779
E-mail : lalas@iti.gr

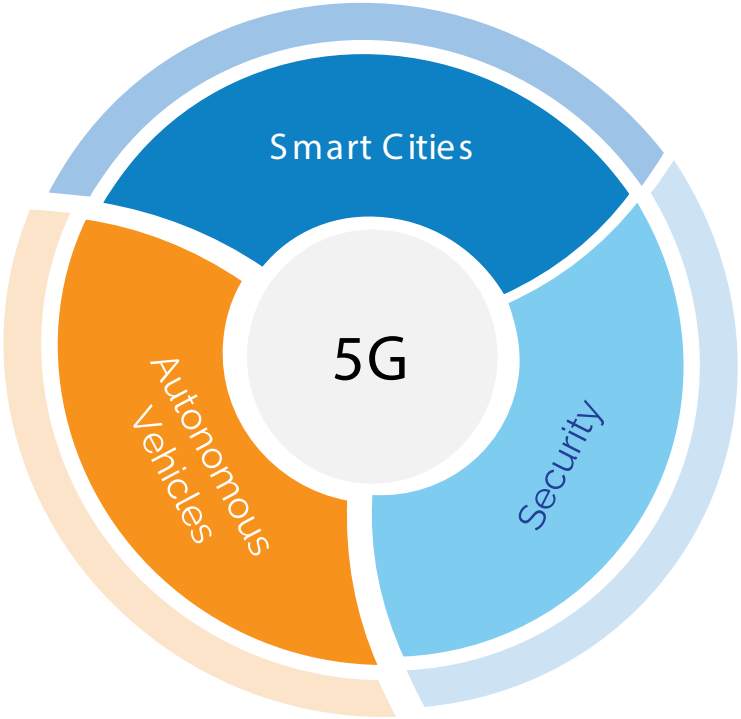
WIRELESS WORLD RESEARCH FORUM®

www.h2020-avenue.eu

AVENUE
Autonomous Vehicles to Evolve to a New Urban Experience

Presentation Outline

- Motivation
- Objectives
- Autonomous transport 5G smart cities
- Potential attacks
- Prevention techniques
- Conclusion & Future aspects



Motivation

- **Rapid expansion of cities** gathered more than half population of the world
- Preserve and **optimize resources** and organization

Infrastructure of Smart Cities

- **Ever-increasing needs** and requirements of a smart city
- The demand for service speed and reliability and the applications mandate **more bandwidth**.

5G Communications Network

An indicative application scenario is related to the **sensors of connected or autonomous vehicles in a smart city**, where a trusted connection between a large volume of low energy nodes is required.

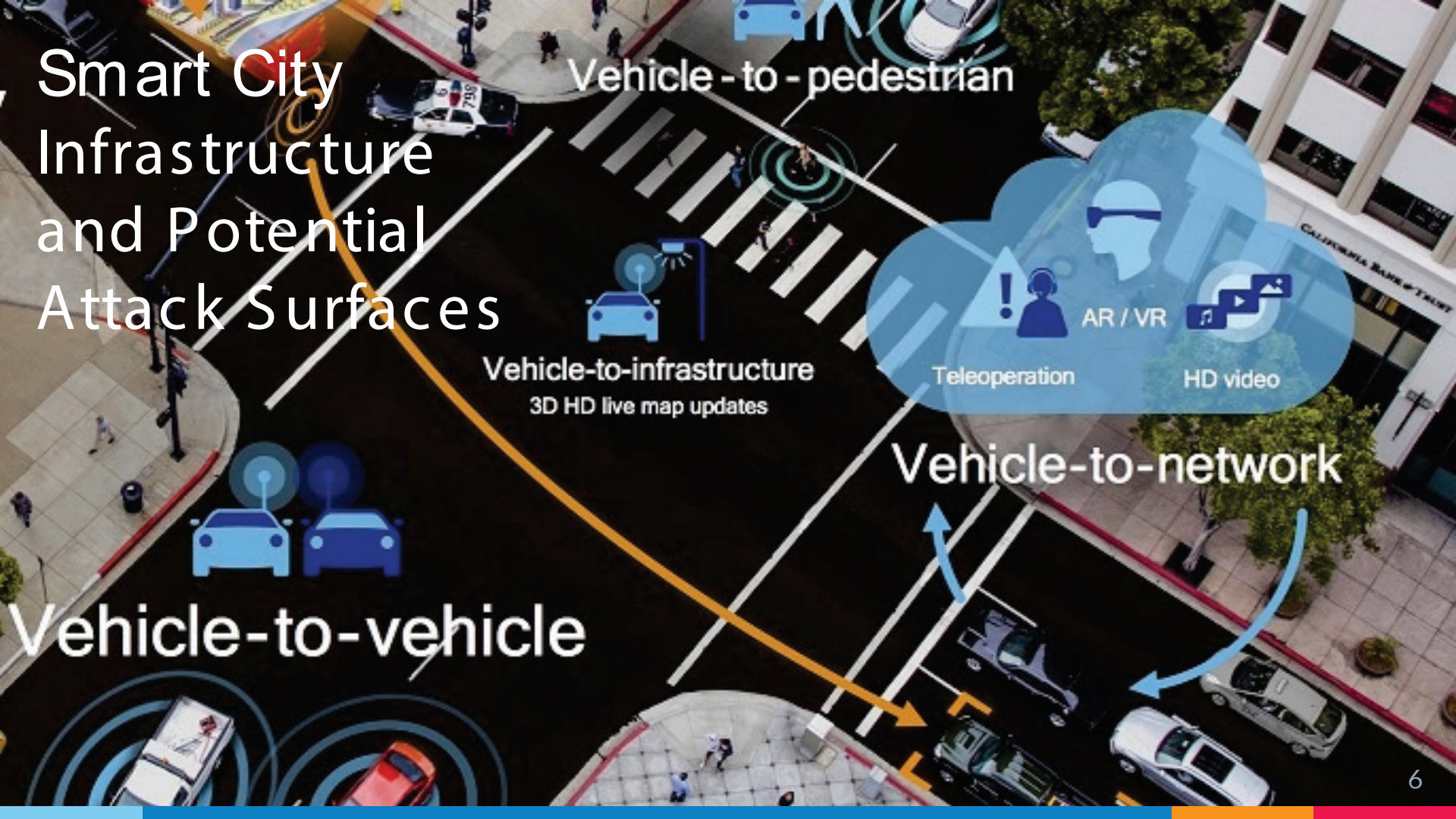
Motivation

- The popularity and growth of cellular technology has led the **5G networks** to be considered as the **emerging domain of future's communication architecture**.
- The **5G network** can successfully deliver the **connection of millions of devices** covering the limitations of their low-power consumption sensors.
- However, one concern arising with the new era of 5G is related to the **security aspects of connected or autonomous vehicles**, as more people are using them and soon they will replace the outdated public transportation system.
- Since security is the cornerstone of creating a safe and viable transportation system, **mitigation methods to tackle potential cybersecurity threats** are of paramount importance.

Objectives

- The connected and **autonomous vehicles** constitute an essential part of **smart cities infrastructure**, providing the answer for the city's mobility demands. With human safety being at stake, the **security assurance** is of the utmost importance.
- Denote the necessity of the implementation of **mitigation techniques to counter the cybersecurity issues and threats** that arise from 5G's embodiment in a smart city ecosystem.
- **Identify the main security challenges** in 5G networks applied in smart cities environment.
- Provide **suggestions related to mitigation and prevention** countermeasures within the scope of 5G connectivity, which can be implemented in this ecosystem.

Smart City Infrastructure and Potential Attack Surfaces



Definition of Smart Cities

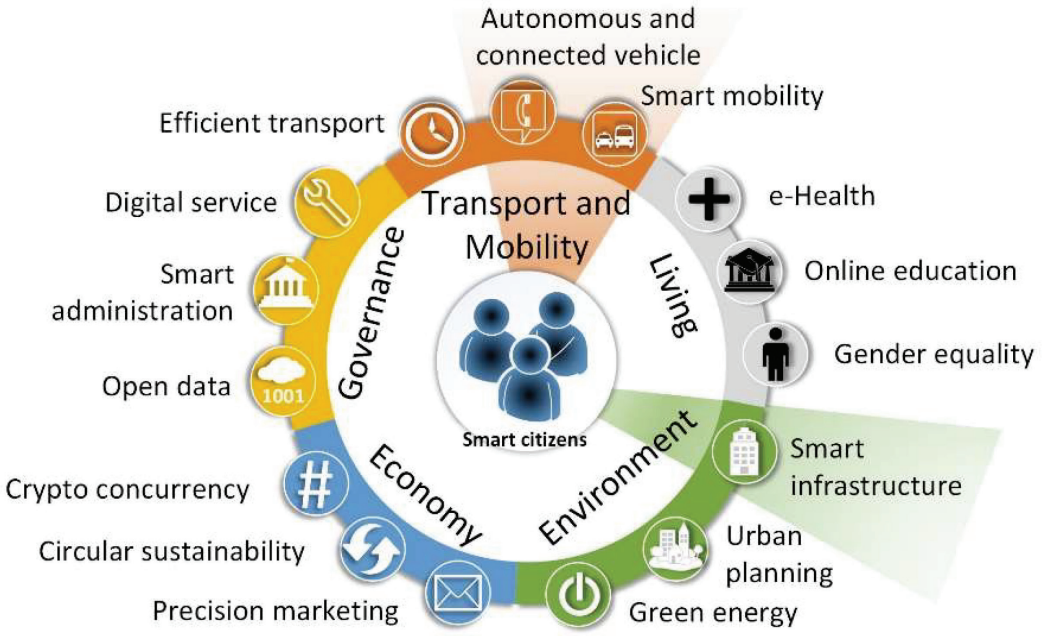
“

Smart Cities initiatives try to **improve urban performance** by using data, information and information technologies (IT) to **provide more efficient services to citizens**, to monitor and **optimize existing infrastructure**, to **increase collaboration** among different economic actors, and to **encourage innovative business models** in both the private and public sectors

Connected and autonomous transport in 5G-enabled smart cities

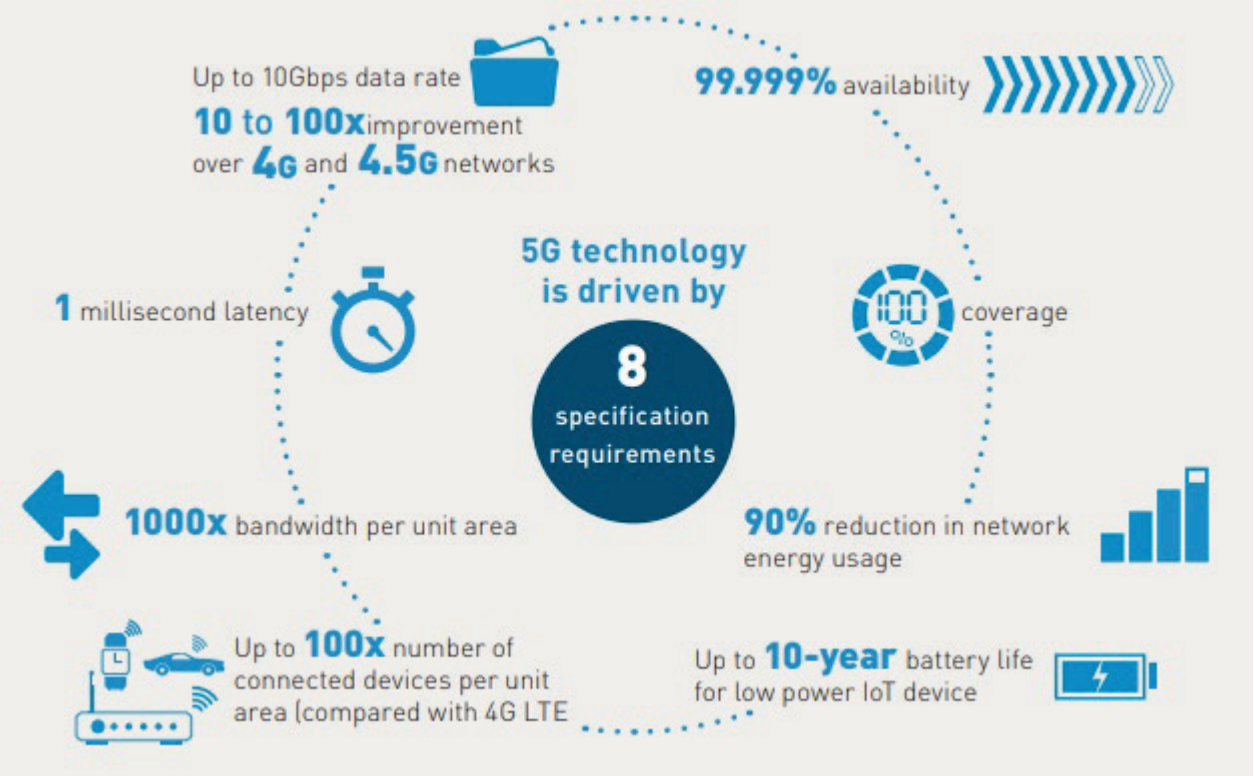
The pillars of Smart Cities:

- Economy
- Environment
- Living
- Governance
- Transport and Mobility



Characteristics of 5G

- Up to 10Gbps data rate
- 1-millisecond latency
- 1000x bandwidth per unit area
- Up to 100x number of connected devices per unit area (compared with 4G LTE)
- 99.999% availability
- 100% coverage
- 90% reduction energy usage
- Up to 10-year battery life for low power IoT device
- Millimeter-Wave communications



Potential Attack Surfaces

- Autonomous vehicles have a built in plethora of **cyber-connected components** and **multiple embedded sensors**
- As observed in all networked computing devices, involving connection mechanisms that support communication between the infrastructure and share data, the **risk of attacks has been exponentially increased** due to the **multiple attack surfaces and vectors** they employ
- **Software defined networking (SDN)** is considered an indispensable part of the 5G networks, since it is used to **control the switches in order to deliver network services** wherever they are needed, regardless of the specific connections between a server and devices

Software defined networking - SDN

“

Defined by the Open Networking Foundation:

The physical separation of the network control plane from the forwarding plane, where the control plane controls several devices

Potential Attacks on SDN 1/ 2

- Denial-of-Service (DoS)
- Distributed Denial-of-Service (DDoS)
- Versions of these attacks
  - TCP/ SYN flood
  - Teardrop
  - Smurf
  - Ping of death

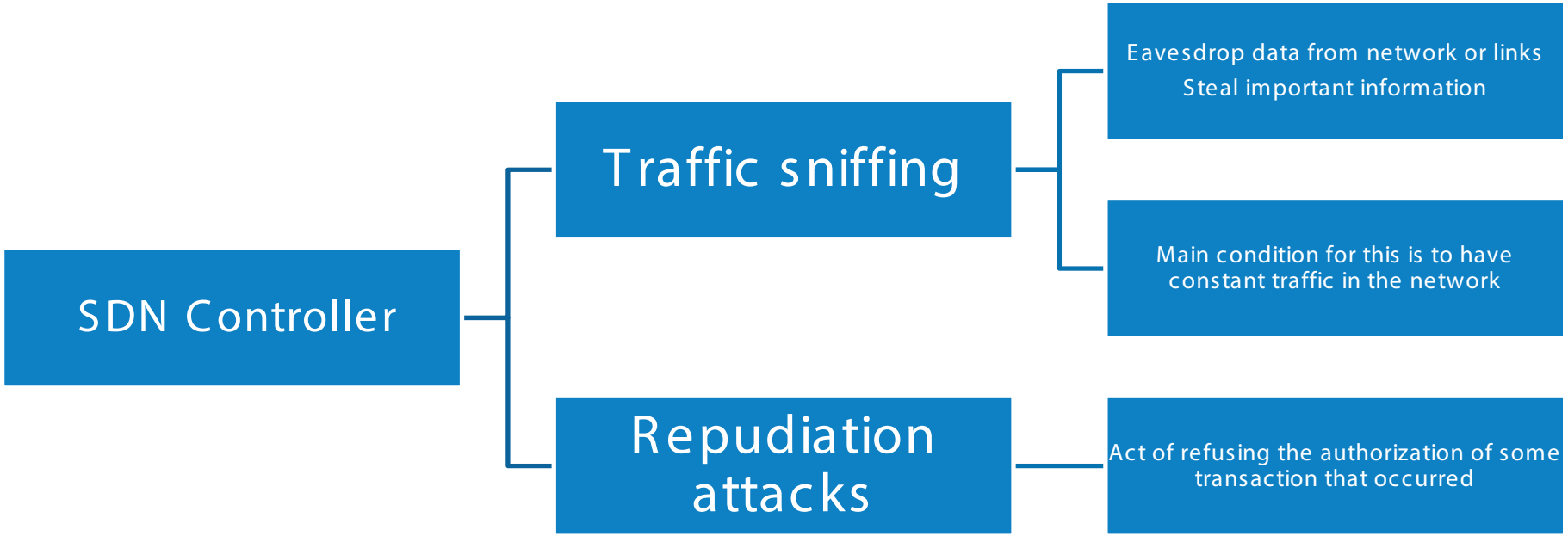
Lead the user to lose control of the system

Vulnerable element of SDN is the address resolution protocol (ARP)

- Targeted by Man in the Middle attacks
  - Hijacking
  - IP spoofing
  - Cache poisoning

Exploit the trust among a connection and gather information

Potential Attacks on SDN 2/2



Potential Attacks on API

- Some critical attacks, target either to **extract from the user information for their credentials** or to guess them with various techniques
  - Phishing
  - Spear phishing attacks

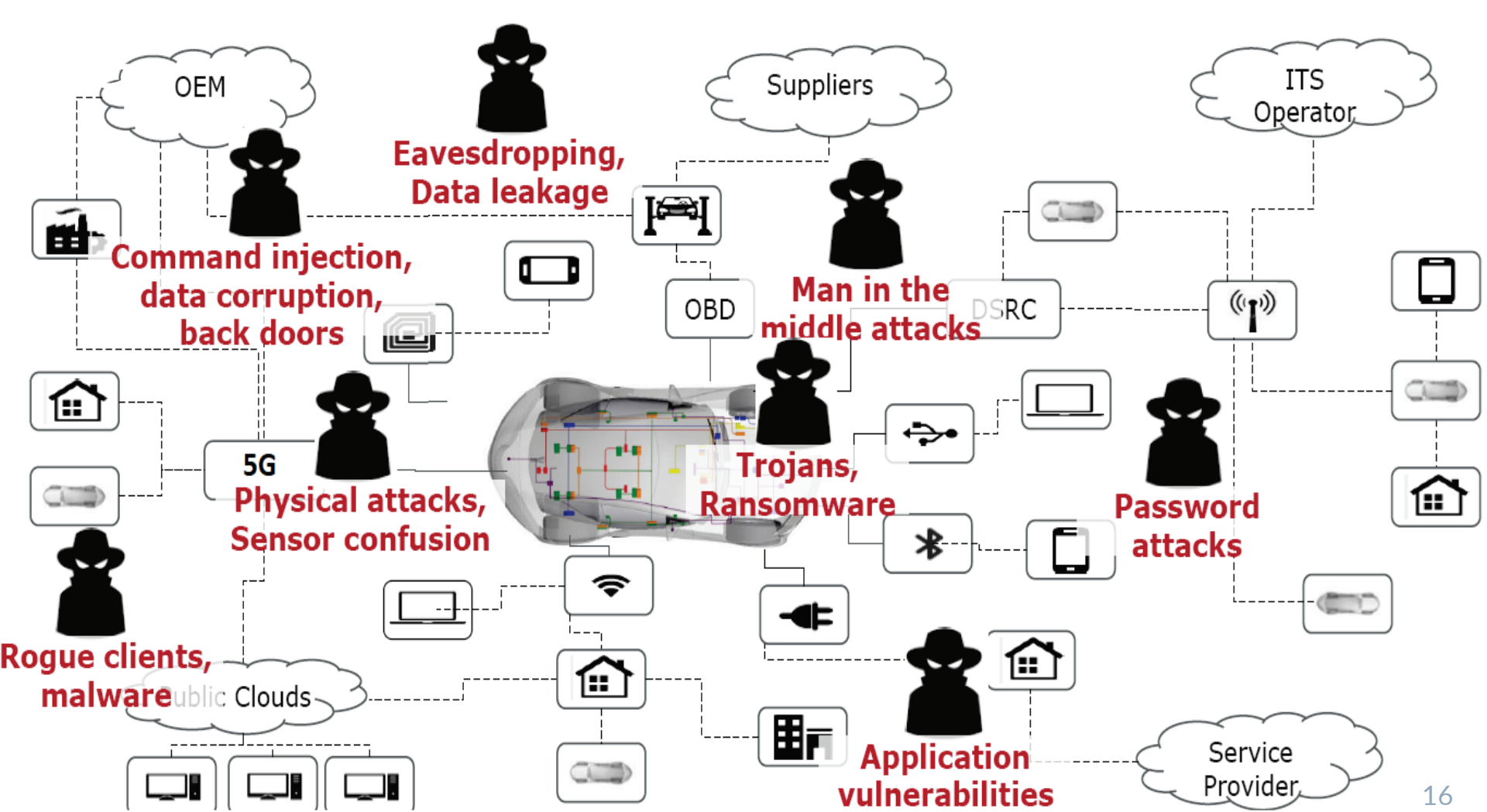
- **Login procedure, authorizations** are susceptible to password attacks
  - Brute force – Random combinations
  - Dictionary – Frequently used passwords, more personal

- **Potential problems**
  - Identity Theft
  - Personal Data leakage
  - Location privacy of subscribers

Potential Attacks on VNF

Another vulnerable component of 5G's architecture is the **virtual network functions (VNF)** Potential attacks involve:

- Eavesdropping, this method in the specific occasion is used to exploit kernel-based virtual machine (KVM) live block migration
- Special set of virtualization threats:
  - Side-channel attacks
  - Flooding attacks
  - Hypervisor hijacking
  - Malware injection
  - Cloud-specific attacks
- VNF are based on virtual machines, some attacks are able to steal resources:
  - Malicious malware
  - Monitoring evasion, by exploiting rollback process


OEM
Suppliers
ITS Operator
Eavesdropping, Data leakage
Command injection, data corruption, back doors
OBD
Man in the middle attacks
DSRC
5G
Physical attacks, Sensor confusion
Trojans, Ransomware
Password attacks
Rogue clients, malware
Public Clouds
Application vulnerabilities
Service Provider

Prevention Techniques 1/ 3

Network security of 5G's architecture, thus the smart city's ecosystem can be improved by implementing some **vital mitigation techniques**

- **Network firewall**
  - Inspects incoming and outgoing network traffic
  - Permits it or blocks it
  - Based on predefined rules
  - Can be multiple firewalls within network
  - Placed on nodal locations
- **Security Information and Event Management (SIEM)**
  - Aggregates
  - Analyses activity from infrastructure
  - Collects security data
  - Normalized
  - Fed to analytics processes

Prevention Techniques 2/ 3

- **Intrusion Detection System (IDS) / Intrusion Detection and Prevention System (IDPS)**
  - Analyses behavior based on previously seen data
    - Predefined deterministic set of rules

      OR
    - Creating a dynamic set of rules based on machine learning
  - Placed in similar fashion with firewall
- **Keep logs that**
  - Must include any anomalies found in the system
  - Attack attempts
  - Failed login attempts
  - Dropped messages
  - Must either be encrypted or stored in a secure location to prevent an attacker from reading the log or tampering with them
  - Send for inspection

Prevention Techniques 3/ 3

- **Authentication keys**
- **Encryption**
- **Anonymity techniques**
  - Group signatures
  - Short term certificates – Pseudonyms
- **Key management**
  - Include methods for adding new entities
  - Revoke existing that have been expired or compromised
- **Secure infrastructure**
  - Hardware trust modules
  - Secure boot

Conclusion and Future Aspects

- The cybersecurity requirements of **5G-enabled smart cities** have been introduced through the paradigm of smart mobility i.e. connected, autonomous or not, vehicles.
- More **stable and complete 5G architecture** will be available, thus enabling **smart transportation** to constitute the key piece of smart cities
- Vital attributes of 5G networks that have been modified in comparison to the previous 4G version, must be examined. The **main security challenges are analyzed** in terms of essential components that can threaten integrity in 5G implementations.
- **A set of prevention techniques is provided** to secure potential vulnerabilities for exploitation in the smart city ecosystem. The proposed approaches, whether considered during the design and deployment phases, are expected to **minimize the potential security breach.**
- **More detailed countermeasures** to be developed according the emerging needs of 5G networks and **autonomous mobility applications**.

Thanks for your Attention

Questions?

Dr. Antonios Lalas
CERTH/ITI Postdoctoral Research Associate
Tel. : +30-2311-257779
E-mail : lalas@iti.gr