Security threats and requirements analysis for IOV

Liang Wei

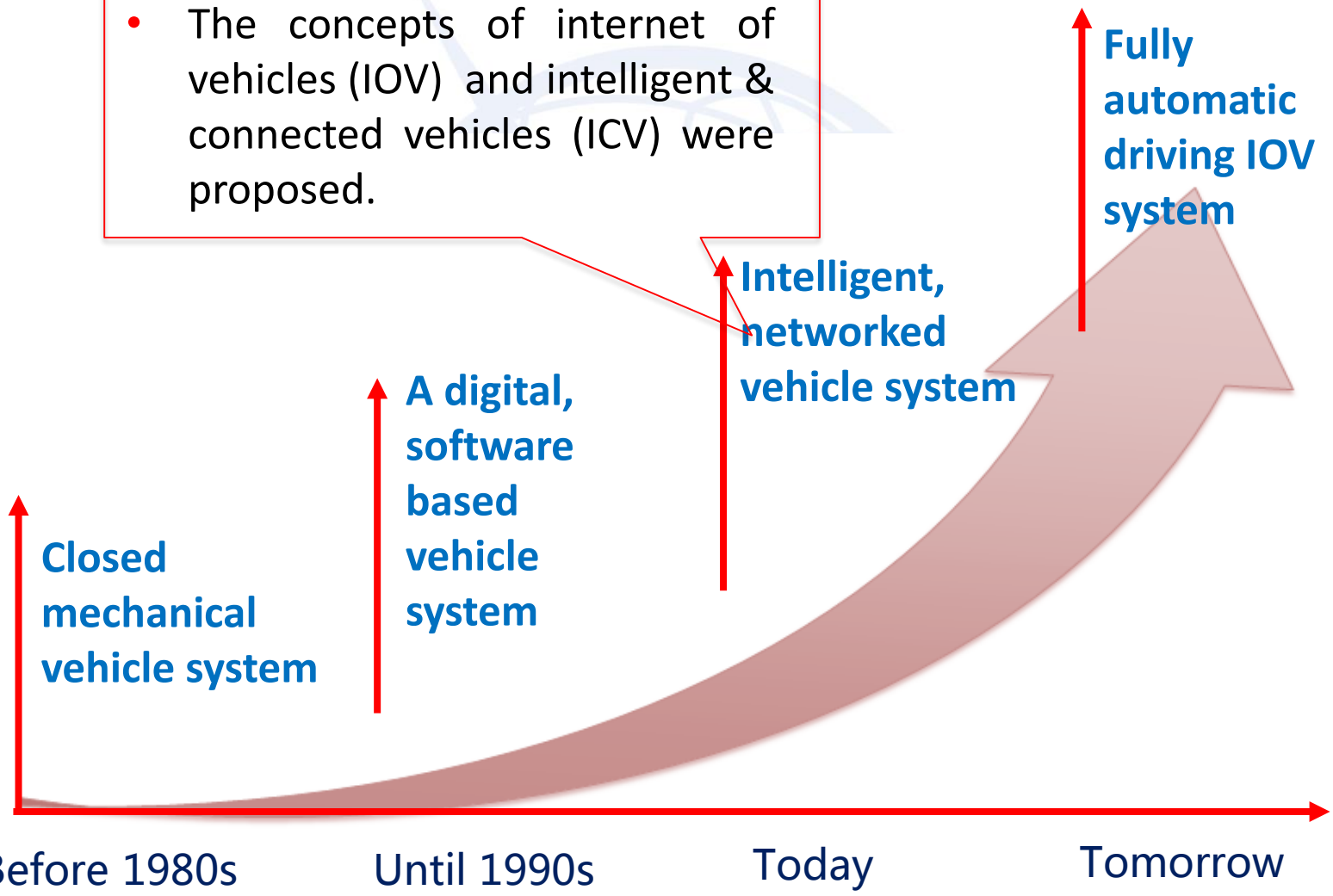
China Academy of Information and Communication Technology (CAICT)

Contents

- Introduction
- Security risks for IOV
- IOV security requirement analysis

Development process of vehicles

- The concepts of internet of vehicles (IOV) and intelligent & connected vehicles (ICV) were proposed.



Definitions of IOV and ICV

- A **highly integrated application** of the IOT and intelligent transportation
- **Not only the information and communication networks** of V2X, **but also an integrated service system**

- **A new type of vehicle**
- Combine modern information communication technologies
- The ultimate goal is to **achieve automatic driving**

The development of the ICV needs the strong support from IOV, the applications of IOV become more and more rich with the development of ICV.

Architecture of IOV

Data

Service Platform

CLOUD

- Public support platform
- Information service platform
- Big data platform

V2X Communication

CHANNEL

- Dedicated networks: DSRC, LTE-V2X
- Public networks: 2G/3G/4G, WIFI, SATCOM, wireless LAN comm.

Intelligent Devices

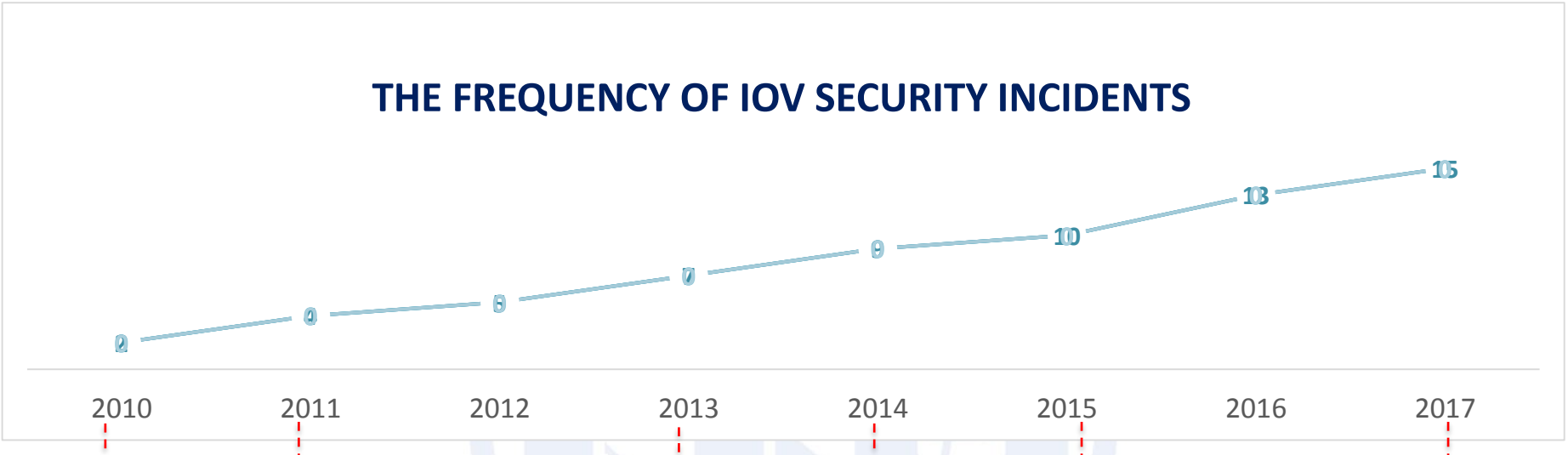
DEVICE

- Mobile terminal system
- APP

Connected Vehicles

- CAN Bus, ECUs, T-box, FOTA, IVI, OBD interface, FOTA, Sensors and Multi-function key

Security incidents of IOV



In Texas, more than 100 cars were attacked

Vehicle attack tests began to emerge

In DefCon, vehicles of TOYOTA and Ford were cracked

In GeekPwn, Tesla was invaded

Security vulnerabilities of many major car brands were exposed

American film <The Fate of the Furious>

The number of IOV security incidents has increased rapidly, and IOV security has attracted widespread attention.

International trends

- **Automotive security research and regulatory agencies are actively formulating IOV security Standards and Guidelines.**

UN/WP29

- To formulate the international regulations and standards
- ToR: network security, data protection and OTA security
- UN auto cybersecurity regulations or guidelines (2018)

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

- Focus on rules and guidelines
- Cybersecurity Best Practices for Modern Vehicles (2016)
- Guidelines and best practice on personal information protection, life cycle security management, etc.

- Pay attention to the implementation of security technologies, driven by government project plans
- PRESERVE, EVITA, SeVeCom, PRECIOSA

- The Key Principles of Cyber Security for Connected and Automated Vehicles(2017)

International trends

- **International standardizations are conducting standardized work.**

ISO/TC22

- To formulate the IOV security standards
  - SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)
  - ISO: International auto cybersecurity standard (2019)
  - ITU-SG17: established the ITS security working group
- To promote the international cooperation

- **Major auto OEMs begin to pay attention to IOV security, and increase IOV security investment.**

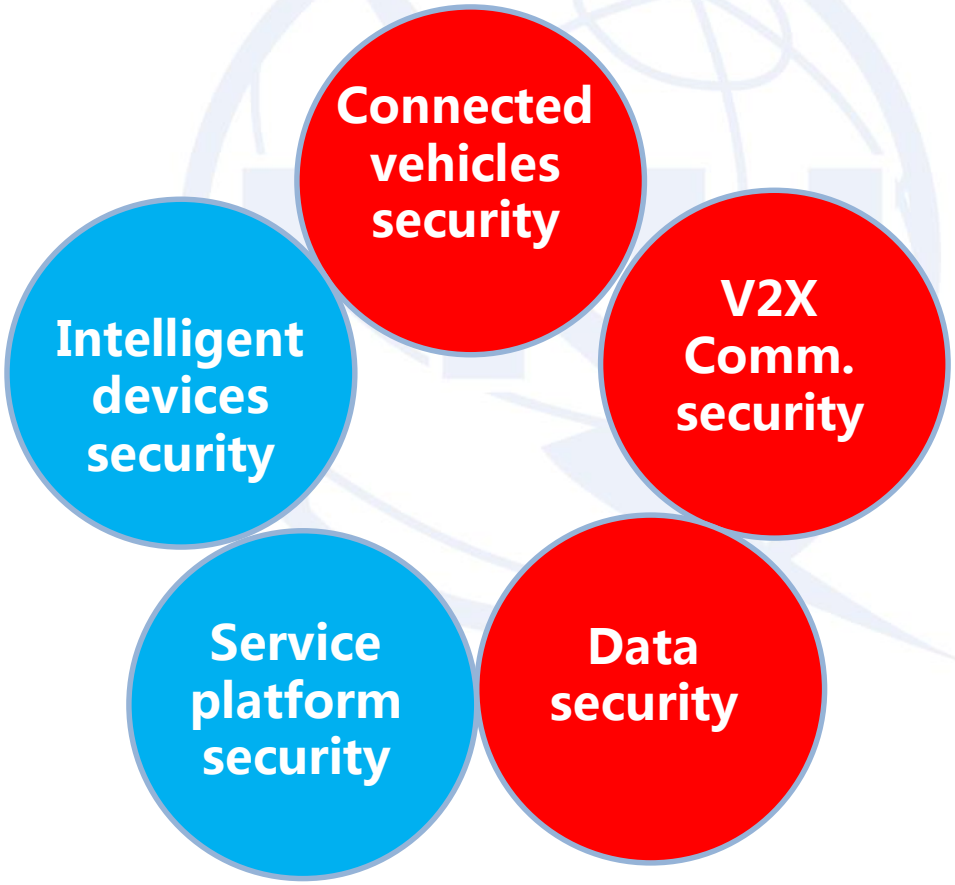
The above 7 enterprises issued joint statements: place the vehicle security in the first place, and carry out the security protection from hardware configuration and software development control, and conduct continuous security testing.

Contents

- Introduction
- Security risks for IOV
- IOV security requirement analysis

Security risks

The security risks of IOV are mainly on 5 aspects**: connected vehicles, intelligent devices, V2X communication, service platform and data.**



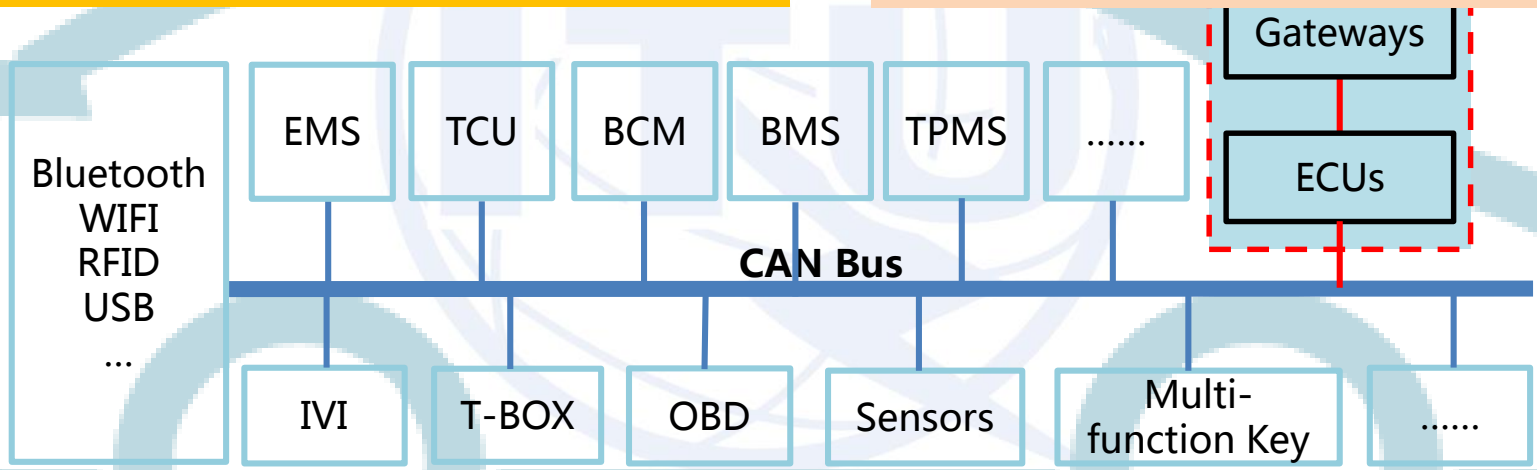
Security risks - Connected vehicle

① ECUs

- ECU chip security vulnerabilities
- ECU firmware application security vulnerabilities
- ECU update program bugs
- Hidden danger during the deployment of ECUs

② CAN bus

- Lack of encryption and access control mechanism
- Without authentication and message verification mechanism
- Defects of CAN bus protocol



③ T-BOX

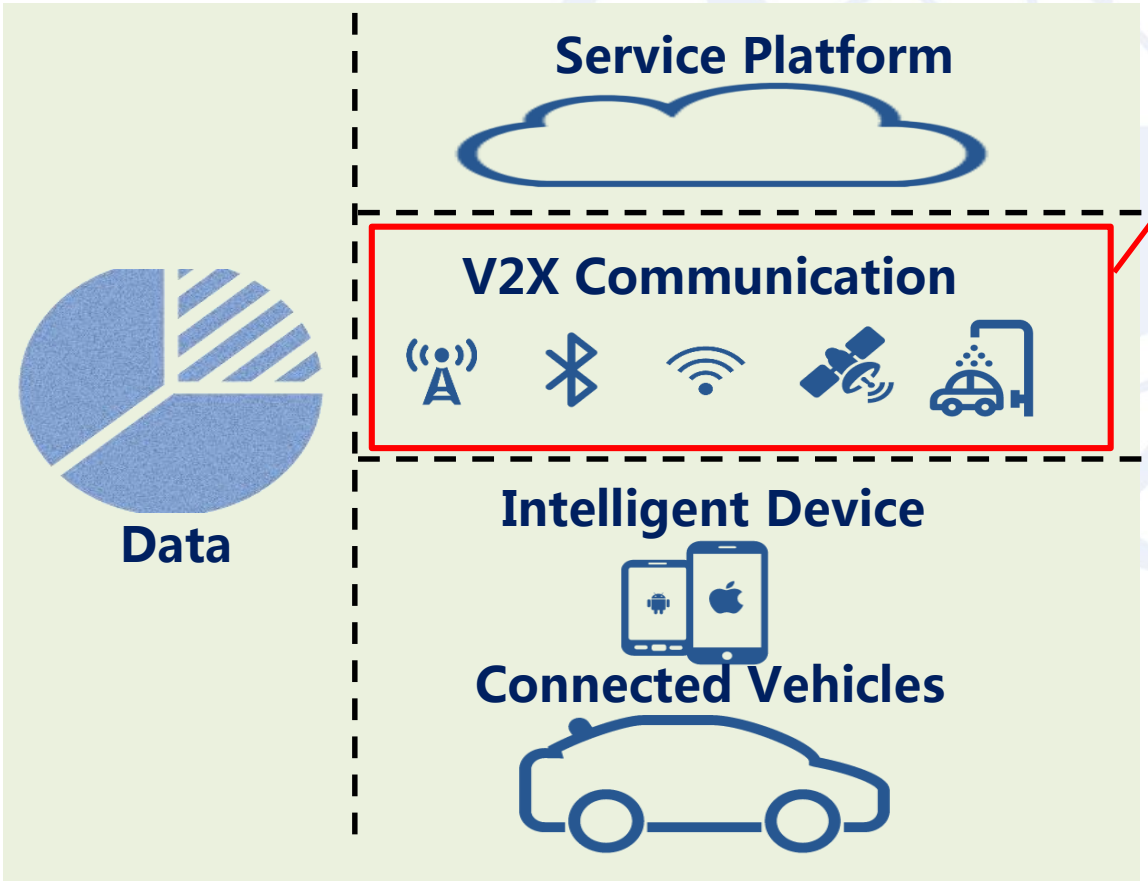
- Protocol crack (reverse analysis firmware)
- Illegal devices access
- Illegal data injection
- Man-in-the-middle attack

④ FOTA

- Malicious codes brush (firmware signature vulnerability)
- Information leakage

Security risks - V2X communication

KEY POINT: **Wireless, high-speed vehicle movement and flexible networking of vehicle nodes** bring the great security risks to V2X communication.



V2V + V2I

Dedicated networks:

- DSRC
- LTE-V

V2P + V2N + IVN

Public networks:

- 2G/3G/4G
- WIFI
- Satellite communication (GPS, BEIDOU)
- Bluetooth, Zig bee, etc.

Security risks – V2X communication

- **Security risks of LTE-V2X/DSRC**
  - **Dynamic changes of network topology** make it difficult to detect attacks
  - **Lack of security key update management mechanism** to manage the legality and timeliness of the vehicle identity
  - **The mechanism of isolation and punishment has not yet been established** to the vehicle nodes which are untrusted or out of control

- **Security risks of cellular mobile comm. (2G/3G/4G)**
  - Based on the cellular mobile communication systems, vehicular system can **provide remote WIFI hotspots, which brings potential an attack portal**
  - Through the cellular mobile communication system, the sound and data are transmitted between vehicle devices by means of microphones. Once an attacker breaks through the cellular mobile communication system**, it will cause the abnormality of automobile system**

Security risks – V2X communication

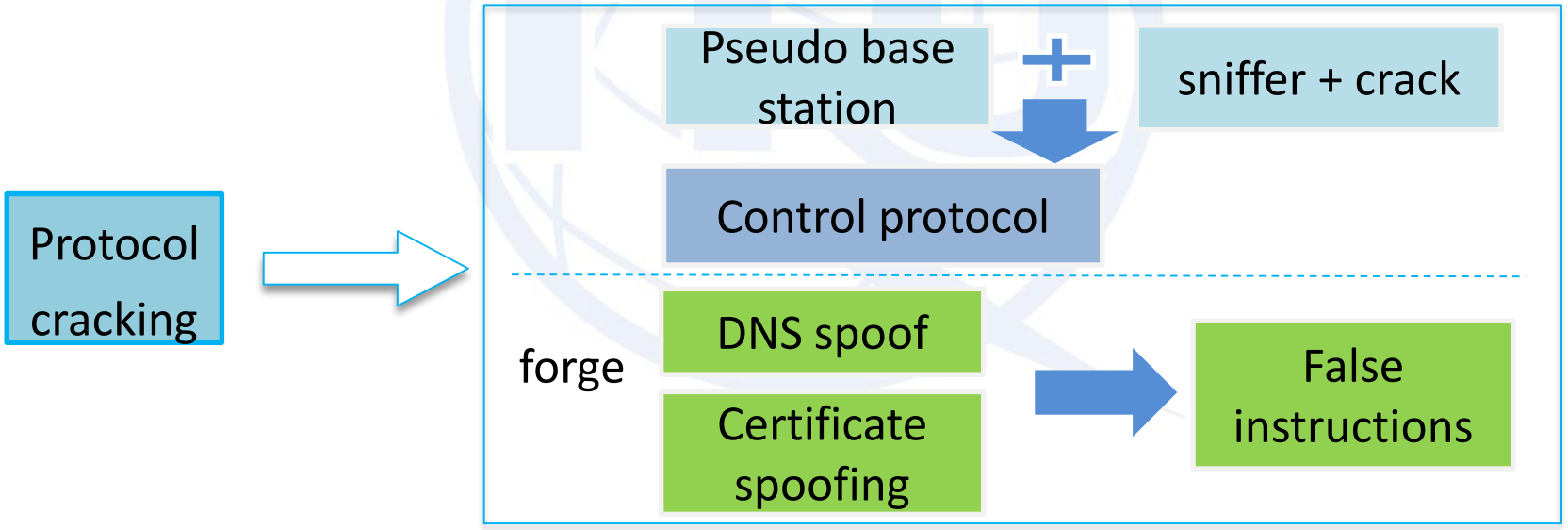
- **Security risks of WIFI**
  - It could **be a springboard for attackers to launch an attack on the vehicle**
  - Through WIFI, devices can access to the car's internal network, so attackers can get the internal data of vehicles
  - By setting up pseudo AP, attackers can access the vehicle communication data by cheating the users

- **Security risks of satellite comm. (GPS/BEIDOU, etc.)**
  - There are **security defects** in the satellite communication module equipped on on-board system
  - **Navigation location data spoofing, location data replay, etc.**

- **Security risks of wireless LAN communication (Bluetooth, Zigbee, etc.)**
  - **Attacks mainly concentrate in three aspects**: authentication process for security specifications, simple matching process, and data encryption and decryption

Security risks – V2X communication

- As the core of communication, **communication protocol** is the most vulnerable part of various communication networks, facing threats of protocol cracking.



Security risks - data

Why is data security the major issue of IOV?

I. **The importance of Data security**

- **The consequence of data security indecent is serious**. For example, once the traffic management data, or data related to automobile operating, such as brake data, speed, tire pressure, fuel consumption, etc. is falsified or tampered, it will threat the safety of vehicle or road management.

II. **The problem of data security is serious**

- From driver's license, vehicle identification number, and the user's trajectory, other business application data, almost can draw an individual profile. Once the data is disclosed, **individual privacy will be revealed without reservation.**

Security risks - data

Why is data security the major issue of IOV?

III. **As the data value is very high, the impact of data security issues is gradually expanding**

- Vehicle application data is widely used in other industries, such as vehicle insurance and vehicle loan, and the impact of security issues is gradually expanding.

IV. **Lack of mature and referenced solutions on data security**

- Comparison with connected vehicles security and V2X communication security, data security protection is lack of mature and referenced solutions, and **it is still in a gradually advancing stage**.

Security risks - data

Data security problems are mainly reflected in the following:

- What type of data can be collected?
- How to ensure the security of data in transmission, access, sharing and other processes?
- What data are trustworthy in the data sharing?
- How to protect the privacy in collection and sharing?
- What can the data be applied to?
- Can the data be shared with third parties?
- ……

Contents

- Introduction
- Security risks for IOV
- IOV security requirement analysis

Security requirements

Corresponding to the IOV security risks analysis, the IOV security requirements analysis are also mainly on 5 aspects: **connected vehicles, intelligent devices, V2X communication, service platform and data.**

- **Connected vehicle security**
- **V2X Communication security**
- **Data security**
- **Device security**
- **Service platform security**

The requirements are similar to the traditional security requirements.

Security requirements – connected vehicles

① ECUs

- Hardware security protection, such as secure communication, secure storage, information authentication etc.
- Software protection, such as secure code

② CAN bus

- Transport encryption on the CAN bus
- Detect the anomaly data transmitted between ECUs on CAN
- Integrity protection of ECU software

③ T-BOX

- Protect communication port security
- Prevent illegal terminal access
- Prevent illegal data injection
- Key management

④ FOTA

- Tamper-proof for date to be updated
- Secure transport during data update
- Data encryption
- Data rollback in case of update failure

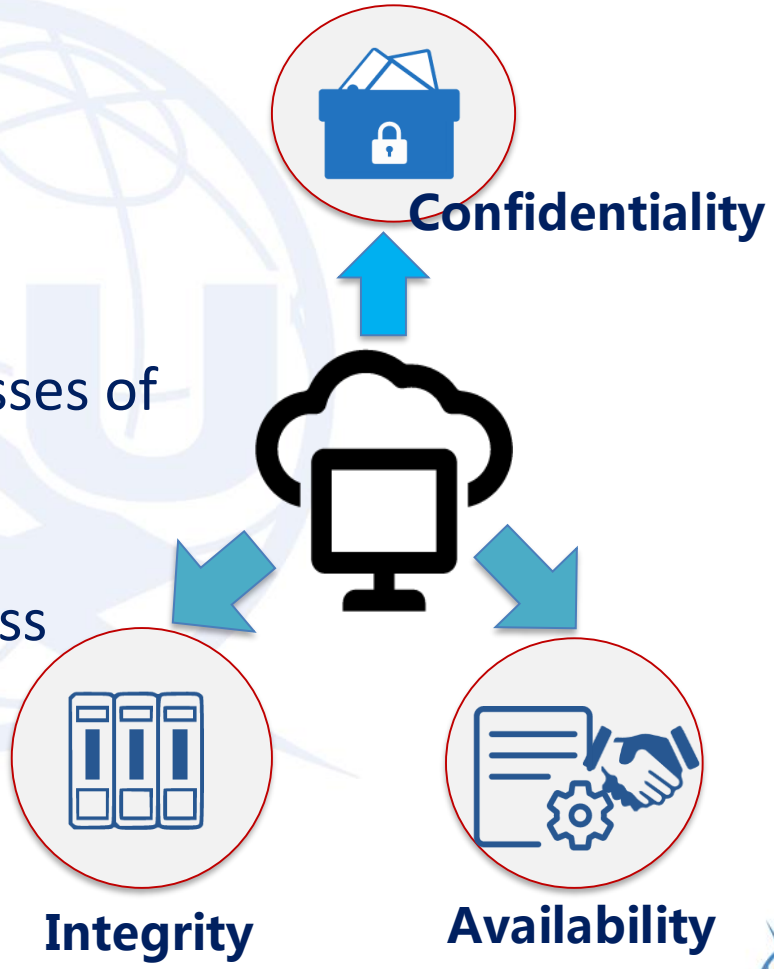
Security requirements -V2X Comm.

In all the comm. scenarios of V2X, i.e., V2V, V2I, V2P and V2N, the following security requirements need to be fulfilled.

- Basic security function, such as **encryption and decryption, generation and verification of signatures, access control**
- **Secure communication**:
  - Guarantee data such as sensors data, commands, and signals to vehicles can be transmitted securely without tampering
  - Verify the authentication, authorization and data-integrity checks for the communication outside the vehicles
- **Secure communication data:**
  - Ensure the security of data storage and exchanging of vehicles and infrastructure
  - Protect privacy security for drivers and the related personnel
  - Protect the consistency and rationality of communication data
- **Secure management for certificates related to secure communication**

Security requirements - data

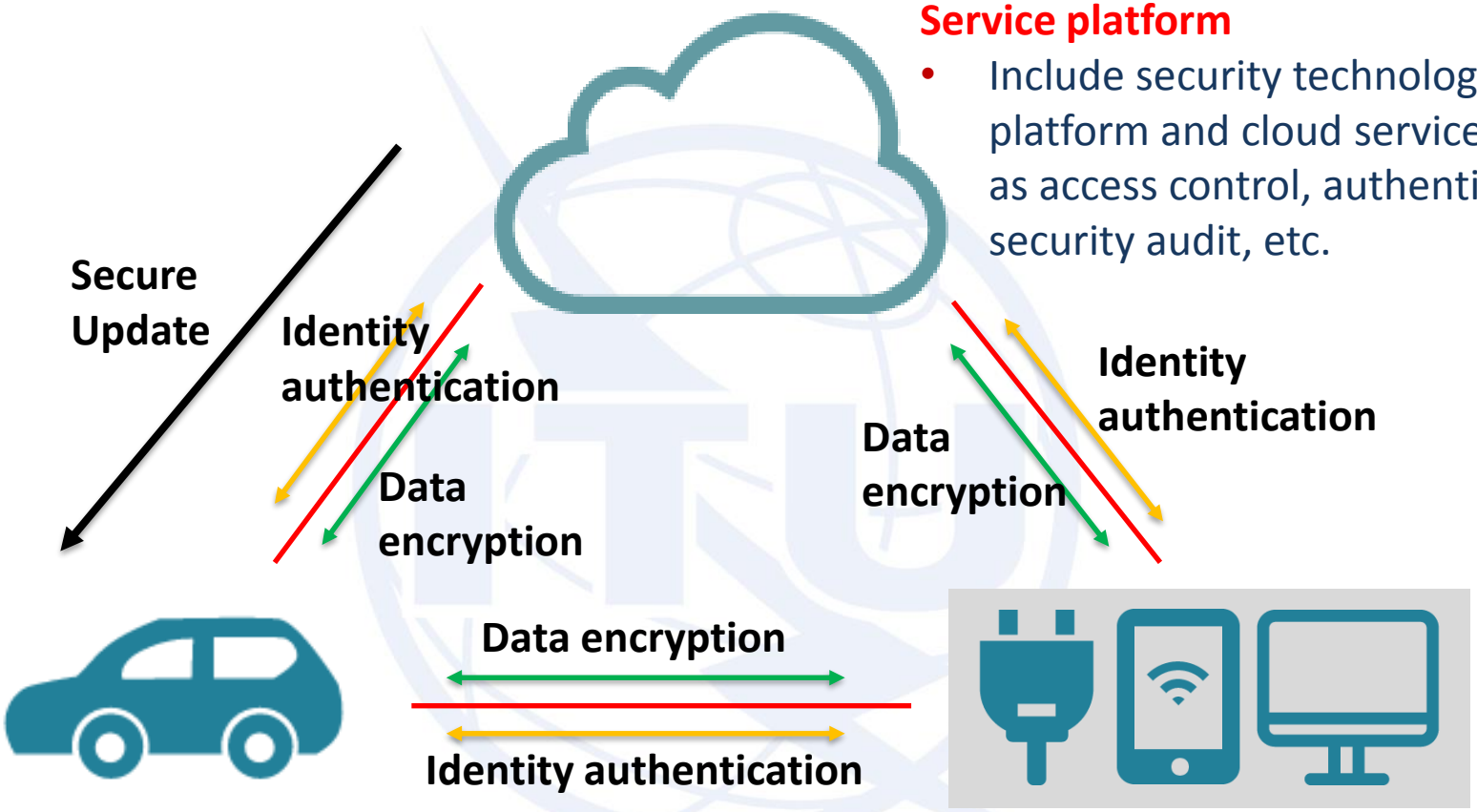
- Data Classification
- Data transmission security
- Data storage security
- Privacy protection in the processes of opening and sharing
- Data security protection for cross border flow



Security solution

Service platform

- Include security technologies of platform and cloud service, such as access control, authentication, security audit, etc.



Connected vehicles

- Lightweight firewall
- Hardware encryption
- Trusted execution environment

Intelligent devices

- Secure application reinforcement
- Secure code check
- Secure application signature

Thanks!

China Academy of Information and Communication Technology

http://www.caict.ac.cn