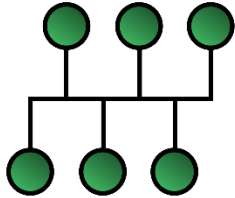


Security of intelligent transportation

Dr. Gábor Fehér

Security of Intelligent Transportation



Car Network (CAN)
+ external connections



VANET security
(Inter-vehicular, road-vehicle)

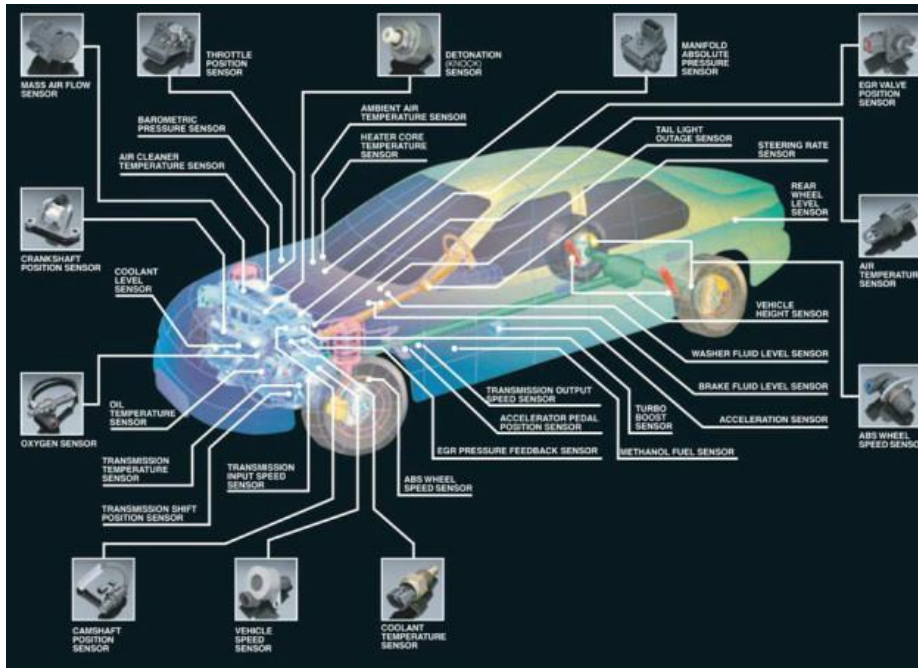


Privacy,
anonymity

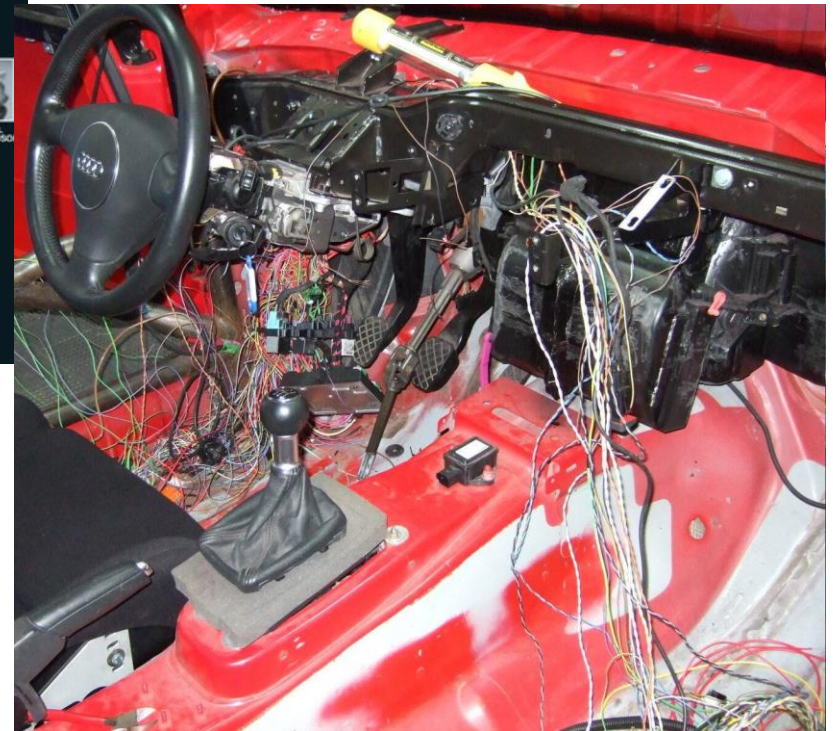
Car network

Wiring in the car 1.

- Sensors and wires in a car



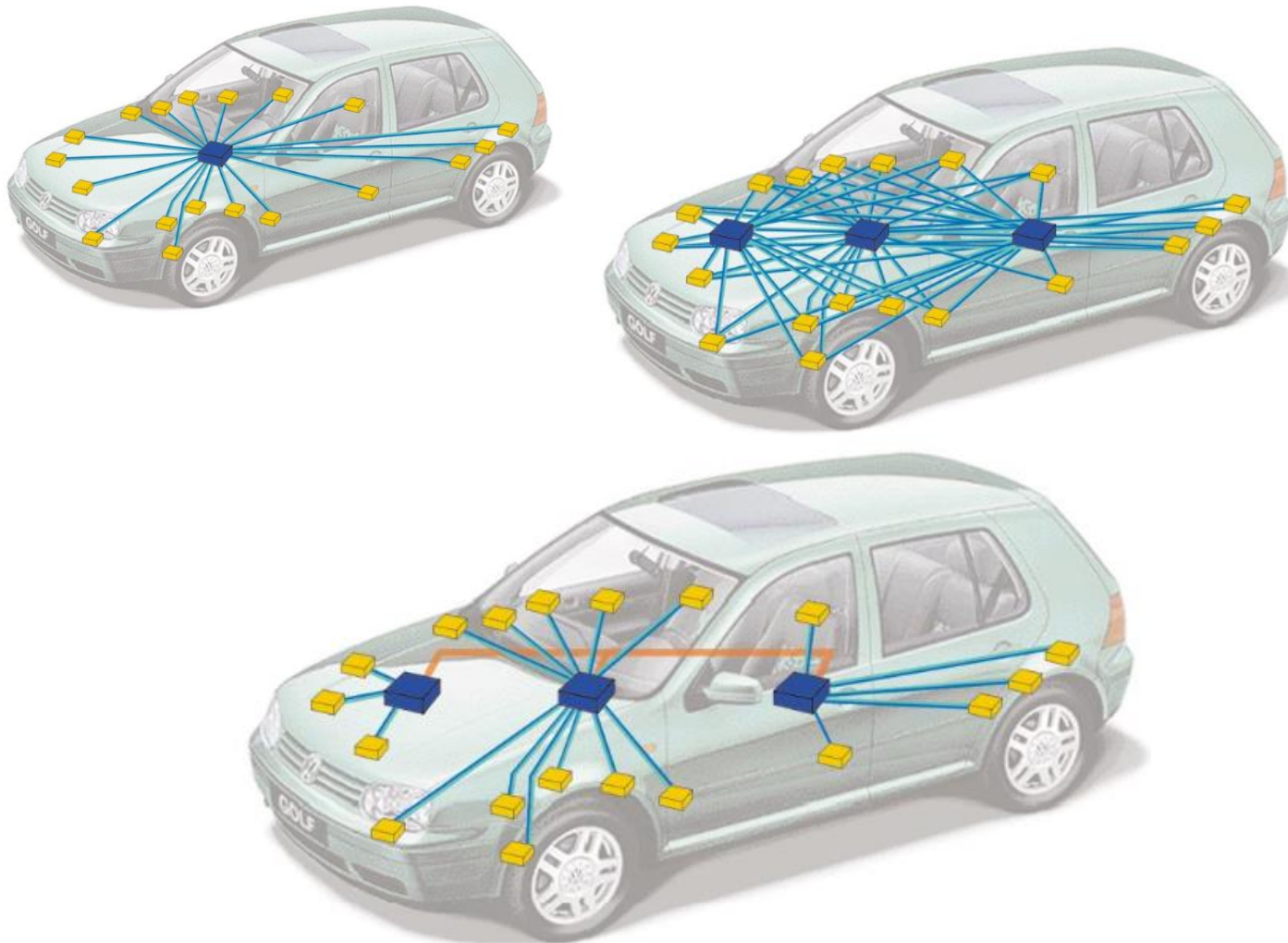
40 to 100 ECUs
[microprocessor-based
electronic control units]



1 km wire,
15-28 kg copper
(250 kg wire ???)

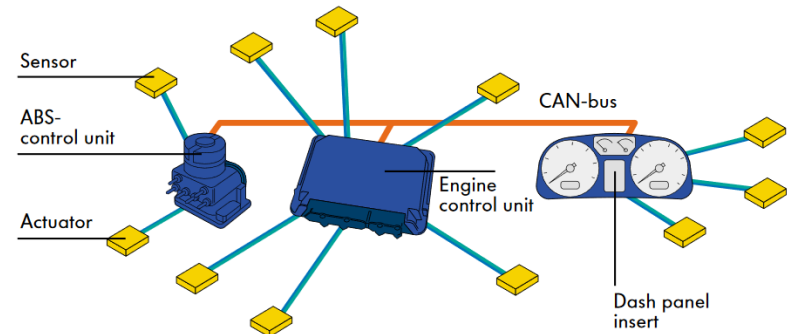
Wiring in the car 2.

- Centralized control vs. bus network



Controller Area Network (CAN)

- 1983- Bosch development
- 1986: Official announcement
- 1991: CAN 2.0 (A and B parts)
- 1993: ISO 11898-1 (data link layer)
ISO 11898-2 (physical layer) fast
ISO 11898-3 (physical layer) slow, fault-tolerant
- 2012: CAN FD (flexible data rate)



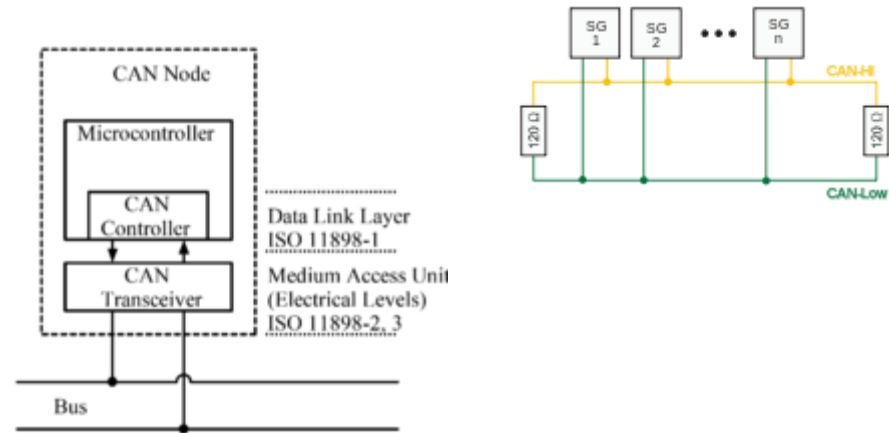
BMW 8xx: The FIRST
CAN bus (1988)

The FIRST “drive by wire”



CAN architecture

- Multi-master serial bus
- Priorities
 - Based on message ID
- CRC protection

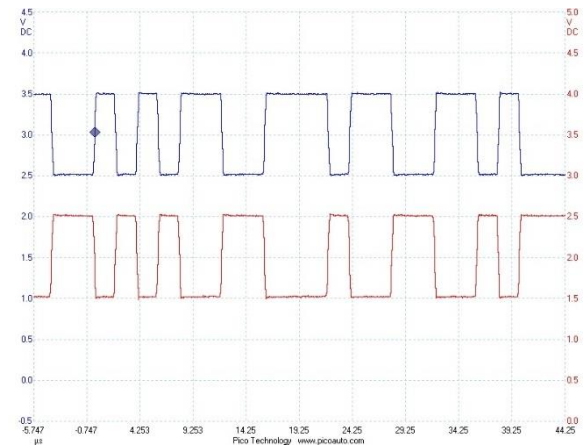


- CAN bus within a car
 - ECU (Electronic Control Unit) connections
 - High and low data rate
 - ECU cooperations

- Data link layer

ABSOLUTELY NO SECURITY !

- Security is based on higher layer protocols by the applications



CAN priority

- Priority based on message ID
 - Lower ID, higher priority

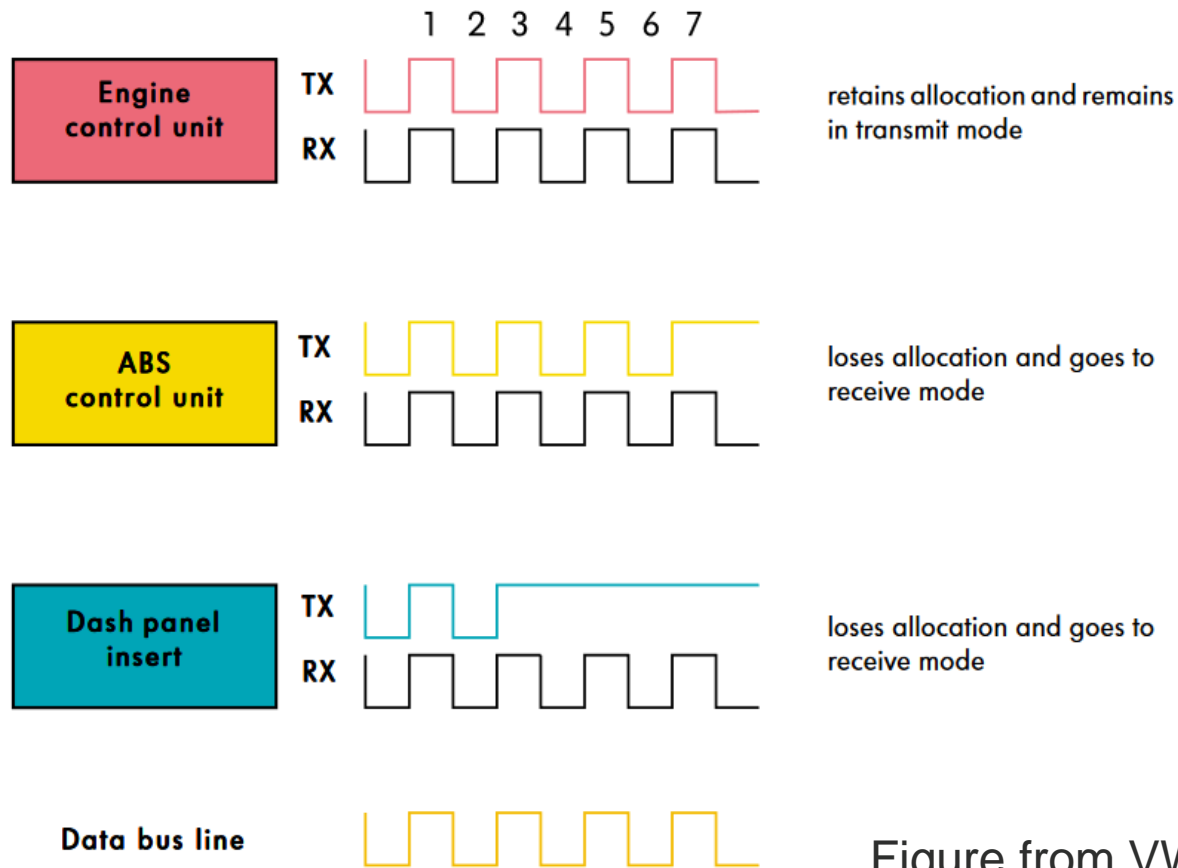
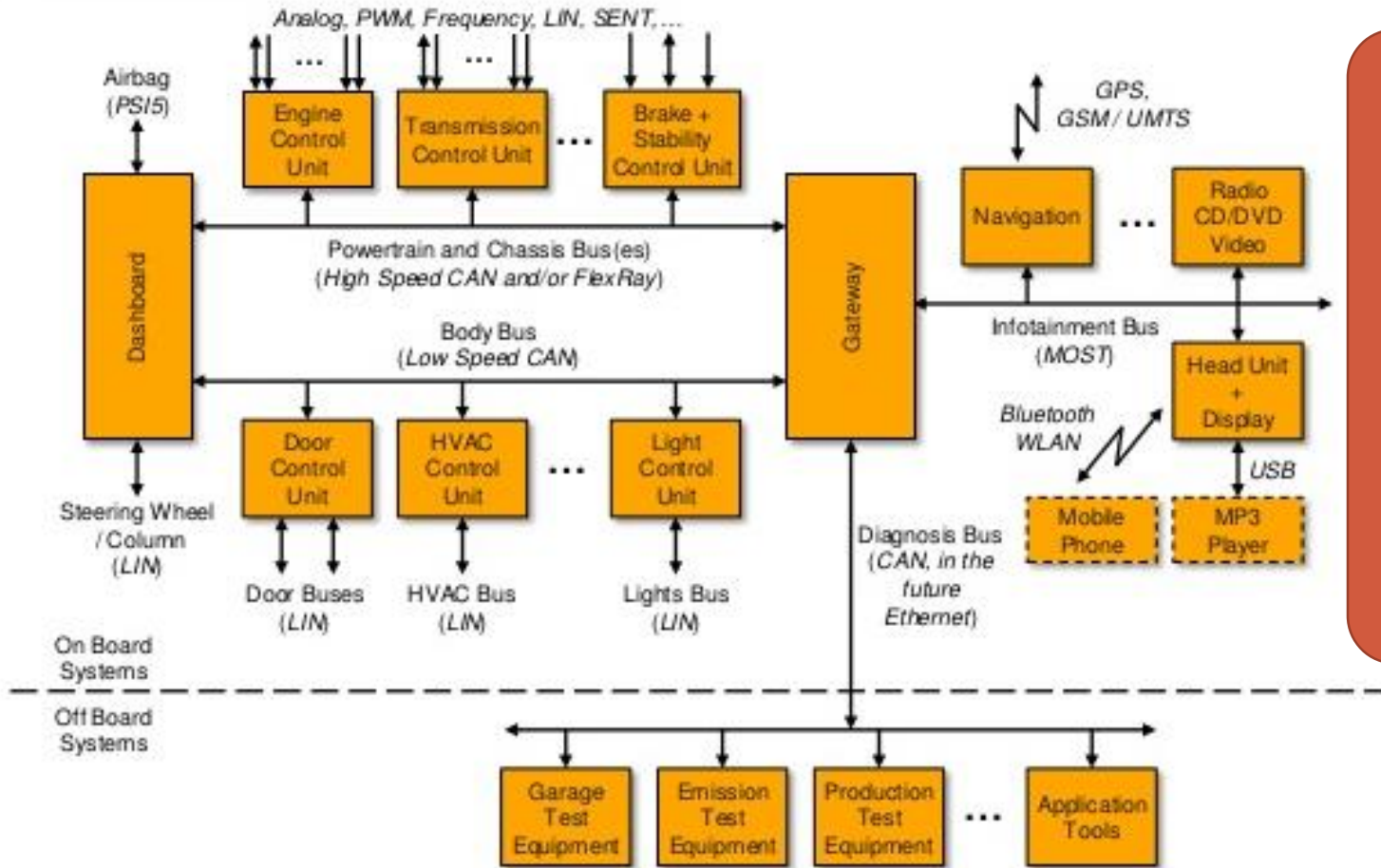


Figure from VW

CAN + LIN + Others

FlexRay
Fast, reliable (expensive)

LIN (Local Interconnect Network)
Cheap alternative (slow)



MOST (Media Oriented Systems Transport)
Plastic Optical Fibre

Picture from Continental

CAN security

- Attack vectors
 - Physical contact
 - Repairman, parking, replacement parts, non factory parts
 - Fitting devices / Reprogramming devices
 - Wireless networks
- Attackers
 - Tuning shops
 - Researchers
 - Joke, „fame”
 - Murder, terrorism
- Challenges
 - Broadcast network
 - Vulnerable to DoS attacks
 - No source identification
 - No source authentication
 - Poor access control (depends on the car make)
 - Non standard implementations

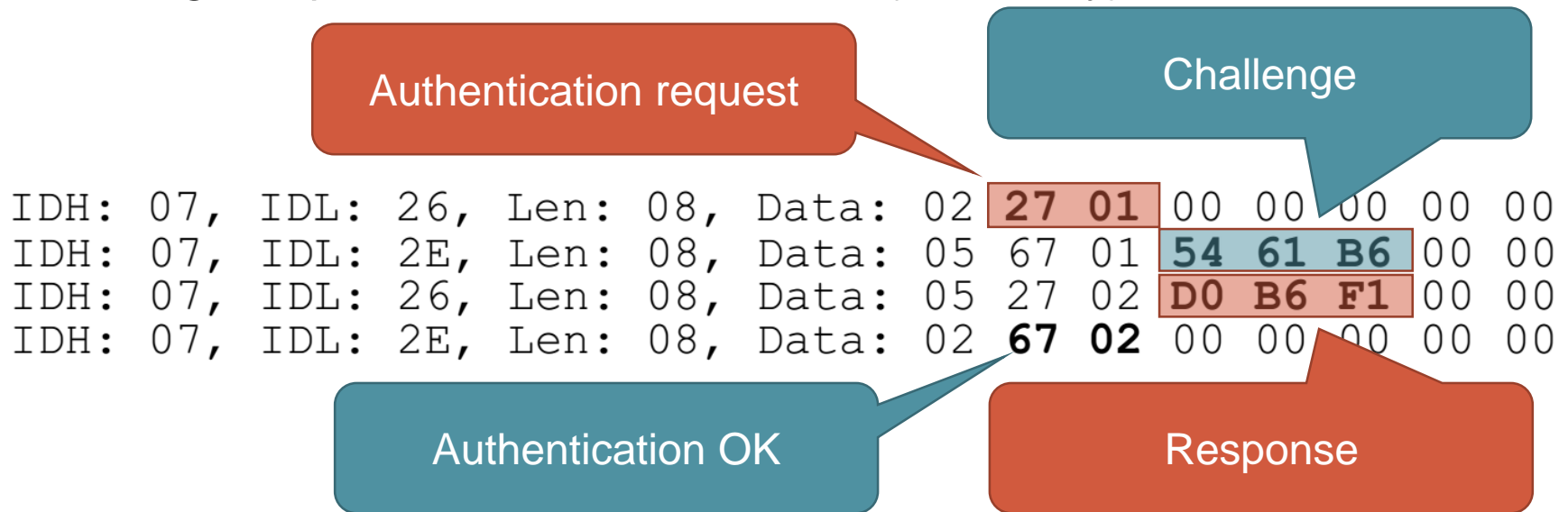


OBD, not CAN, but similar



CAN SecurityAccess

- Service for ECU testing/programming
- Challenge/response based authentication (seed / key)



- The algorithm (challenge -> response) is secret
 - Cannot be stored on the device (could be read out), only the challenges/responses are stored
 - Could be known at the tester
 - You can find some on tuning pages...

CAN SecurityAccess 2.

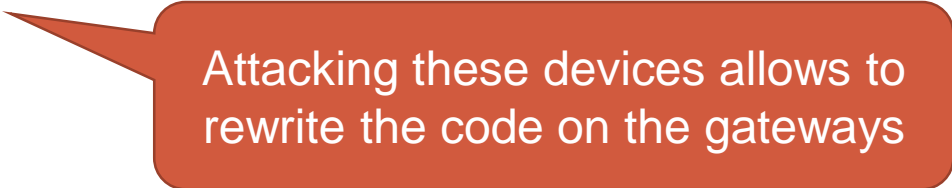
- Brute force attack is possible in feasible! (2-3-4 byte)
 - 2 byte, 10 sec/test: 1 week for the break
 - Break multiple devices at the same time
 - In case of some protection (extra time), the device can be restarted
- Communication can be captured easily
 - The CAN bus is a broadcast channel without any encryption
- Session hijacking: After the authentication, the session can be hijacked
- Some of the possible hacker commands
 - DeviceControl, ECUReset, RequestDownload, RequestUpload, InputOutputControl

CAN Security Access 3.

- The access is often limited while driving due to security reason
 - This is not true for all the cases
 - In the case of firmware rewrite, the engine stops
- In many cases there are alterations to the original protocol
 - The same seed/key in every cases (on all devices)
 - No check on the keys
 - Keys can be read out from the equipment
- The ECU might block dangerous actions
 - Often this is not true (often this rule is ignored during the testing)
 - Moreover, sometimes the authentication is missing

CAN segments

- In most cars, there are minimum 2 CAN bus line
 - High speed CAN bus: Time critical devices (e.g. brake, ABS, engine)
 - Low speed CAN bus: Less critical devices (e.g.: heating, radio)
 - Gateways among the CAN networks
- According to the standard, the high speed bus is more reliable
 - Gateways can be programmed only from the high speed bus
- There are devices, which are on multiple buses (and not gateways)
 - E.g. Telemetric devices



Attacking these devices allows to rewrite the code on the gateways

CAN experiences

- The reverse engineering takes a lots of time, however „fuzzing” are very successful by surprise
- The access control is not (properly) working even in the case of critical ECU devices
- The gateway protection is not satisfactory
- Reprogramming the ECU devices are not easy, however clearing the logs are easy, which makes forensics analysis and finding the responsible people almost impossible

CAN security solutions

- Physical protection for diagnostics and programming
 - Critical operations with physical access only
 - Firewalling external connections (possible?)
 - Truly block diagnostics during driving!
- Mediator
 - The mediator blocks all messages that cannot be associated to the device
 - Requires trusted gateways
- Identification instead of prevention
 - Identify anomalies
 - Can we stop the attack in time?
 - Attacks might not be prevented, but the consequences are less dangerous

Recognizing CAN attacks

- Attack recognition
 - The CAN network is broadcast, so the detector sees all the traffic
 - CAN messages are similar, their content can be predicted
 - The attacks show different behavior, so they can be recognized
 - E.g. the attacker should send more messages in order to cancel the original one
- Steps after an attack recognition
 - Warn the driver
 - Shut down the CAN bus
 - Stop vehicle safely
 - Ignore some CAN messages
- Location of the protection
 - Separate module (IPS ECU) on the CAN bus
 - Extension to the existing software modules
 - OBD II port connection

CAN security solutions 2.

- Using cryptography
 - Encryption in the application layer
 - Often problematic due to the real time requirements
 - Handling/storing keys are critical
 - Possible reverse engineering on the devices
- In many cases there is security by obscurity
 - DOES NOT WORK !!!

Services based on telemetry

- GM OnStar
 - Assistance services (safety)
 - Diagnostics
 - RelayRide (car sharing)
- Ford Sync
- Chrysler Uconnect
- BMW Connected Drive
- Lexus Enform



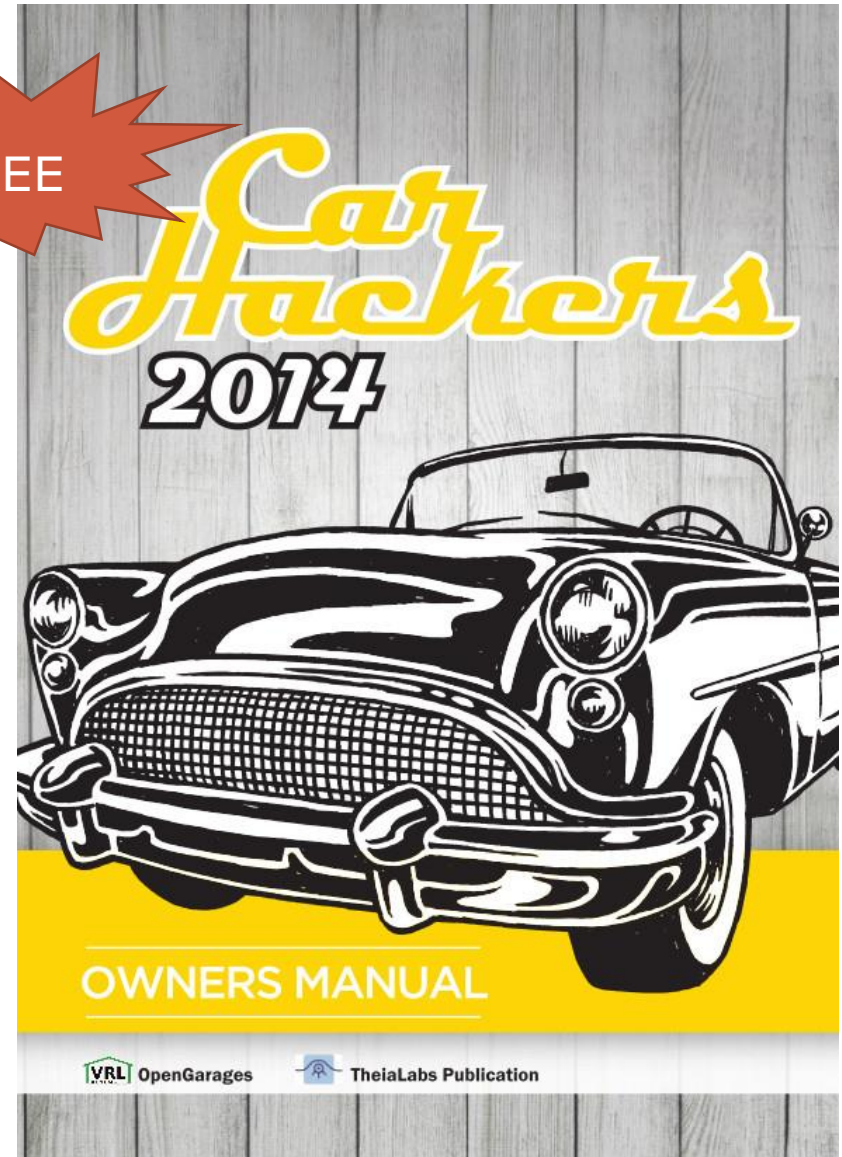
Autonomous cars

- Lane keeping
- Parking
- Driving



Ajánló

- <http://opengarages.org/handbook/>
 - Intro
 - Understanding Attack Surfaces
 - Infotainment Systems
 - Vehicle Communication Systems
 - Engine Control Unit
 - CAN Bus Reversing Methodology
 - Breaking the Vehicle
 - CAN Bus Tools
 - Weaponizing CAN Findings
 - Attacking TPMS
 - Ethernet Attacks
 - Attacking Keyfobs and Immobilizers
 - FLASHBACK - Hotwiring
 - Attacking ECUs and other Embedded Systems
 - What does your hacker garage need?



Network between the cars

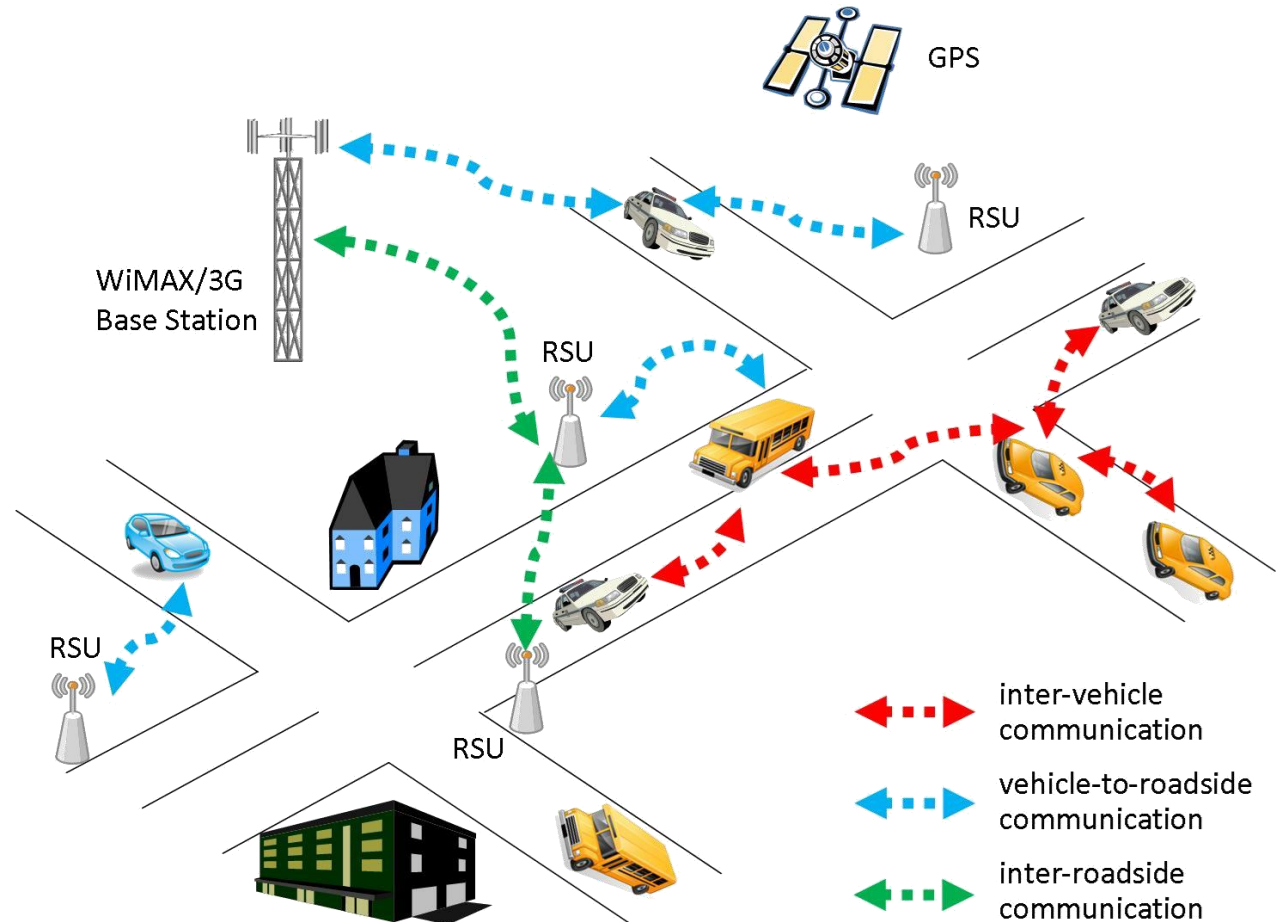
Vehicular Ad Hoc Network - VANET

- Vehicle – Vehicle and Vehicle – Infrastructure communication
 - V2V: Vehicle to Vehicle, V2R: Vehicle to Roadside, IVC: Inter-Vehicle Communications, OBU: On-Board Unit, RSU: Road-Side Unit
- Standards
 - Based on IEEE 802.11p standard
 - Europe: ETSI ITS G5 and USA: IEEE 1609 WAVE (Wireless Access in Vehicular Environments)
 - 5.9 GHz, 5/7 channels
 - Japan: ARIB STD-T109
 - 700 MHz, 1 channel
- Biggest challenges
 - Security
 - Privacy

Vehicular Ad Hoc Network - VANET

- Services

- Safety
- Comfort
- Commerce, Entertainment, Telemetric



Forrás: Jung-Chun Kao's

VANET service examples

- Safety
 - EEBL: Emergency Electronic Brake Light
 - PCN: Post Crash Notification
 - RFN: Road Feature Notificaton
 - LCA Lane Change Assistance, CCW: Cooperative Collision Warning
- Comfort
 - Traffic jam notification
 - Dynamic road planning
 - Parking spot finder
- Commerce, Entertainment, Telemetric
 - Remote diagnostics
 - Advertisements

VANET and MANET

- MANET: Mobile Ad hoc Network
- MANETs are here for a long time, lots of research done
 - Many similarities (solutions can be found)
 - Differences:
 - VANETs are more structured
 - Nodes are more dynamic, moving faster and more
 - Storage and computation capacities in VANETs are not problematic
 - Expecting more nodes in VANETs

VANET security

- DoS attacks
 - Channel jamming
 - The messages cannot reach the car / infrastructure
- Dropped messages
 - Selective forwarding
 - Messages can be used later
- Fake messages
- Modified messages
- Replay messages
- Message multiplication (Sybil attack)
 - The attacker pretends that many cars are in the same situation, hence the information (usually a false one) got higher priority

VANET attackers

- Selfish drivers
 - False information for the driver's advantage
 - E.g.: Simulating a traffic jam in order to empty a road segment
- Avoiding consequences
 - E.g.: Blocking information in order to prevent fines
- Attacks
 - Terrorism
 - E.g.: Creating an accident, and blocking further information
- Jokes and fame

VANET challenges

- Encryption
 - The messages can be seen only for dedicated devices
- Integrity protection
 - Messages cannot be changed
- Authentication
 - Authenticate the source of the messages
 - But RSA is usually slow. Other methods are required

VANET challenges 2.

- Dependability
 - Messages should reach other cars/infrastructure within a given time
- Non repudiation
 - Attackers should be identified by accounting the messages
 - Legal justice, threat attackers
- Privacy
 - Keep out unwanted eyes
 - Anonymity (but with authentication!)
 - Electronic license plate

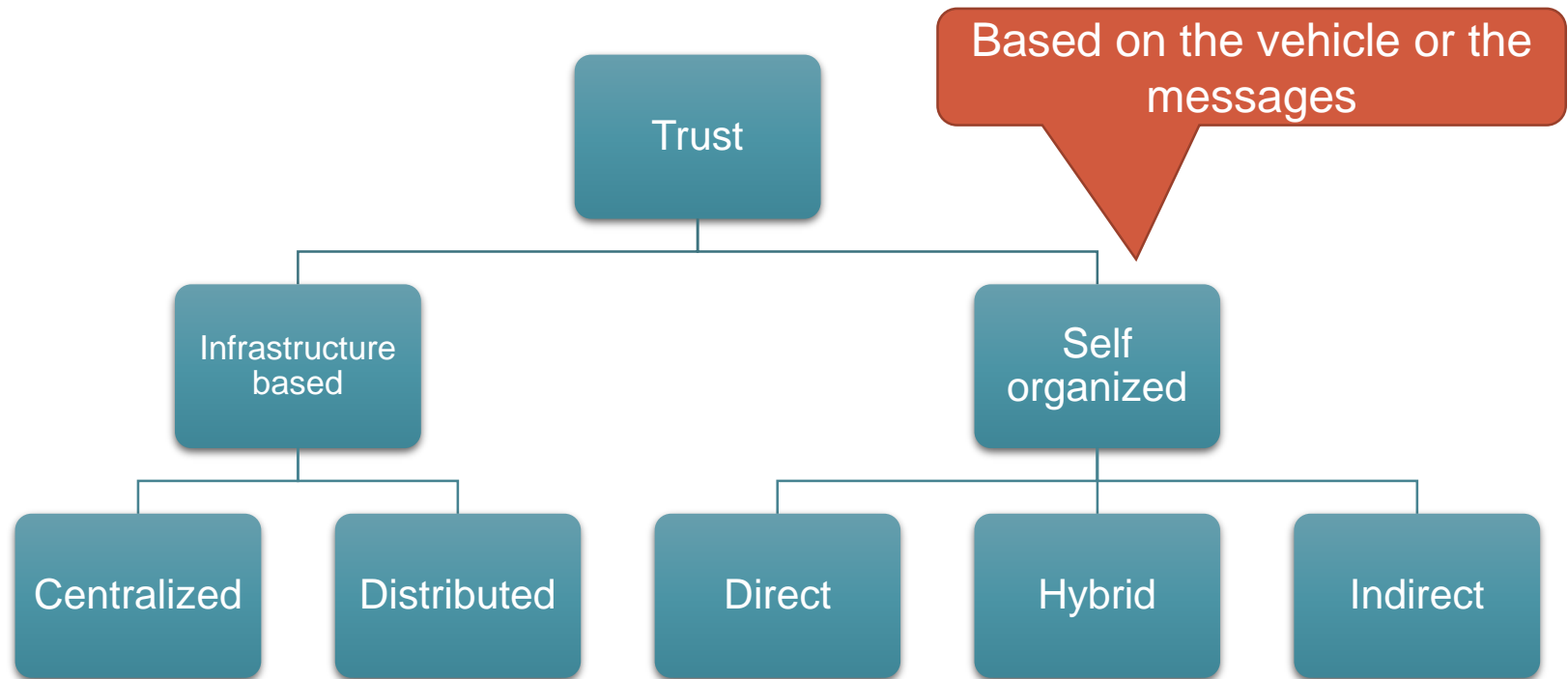
 - Untraceability: The actions of the car cannot be linked together
 - Unlinkability: The driver and the car cannot be linked together

VANET solutions

- Apply existing MANET technologies
- ARAN (Authenticated Routing for Ad hoc network)
 - Secure Ad-Hoc routing using PKI
 - Protects against replay, spoofing + provide non repudiation
- SEAD (Secure and Efficient Ad hoc Distance Vector)
 - Secure routing using one way hash functions
 - Protection against DoS
- SMT (Secure Message Transmission)
 - Secure message transmission using end-to-end authentication based on MAC
- NDM (Non-Disclosure Method)
 - Anonymity provided by an agent. Traffic mix and asymmetric encryption
- ARIADNE
 - Secure routing with MAC and TESLA algorithms, based on symmetric encryption

VANET solutions 2.

- Trust management
 - Trust based on certificate
 - Trust based on reputation



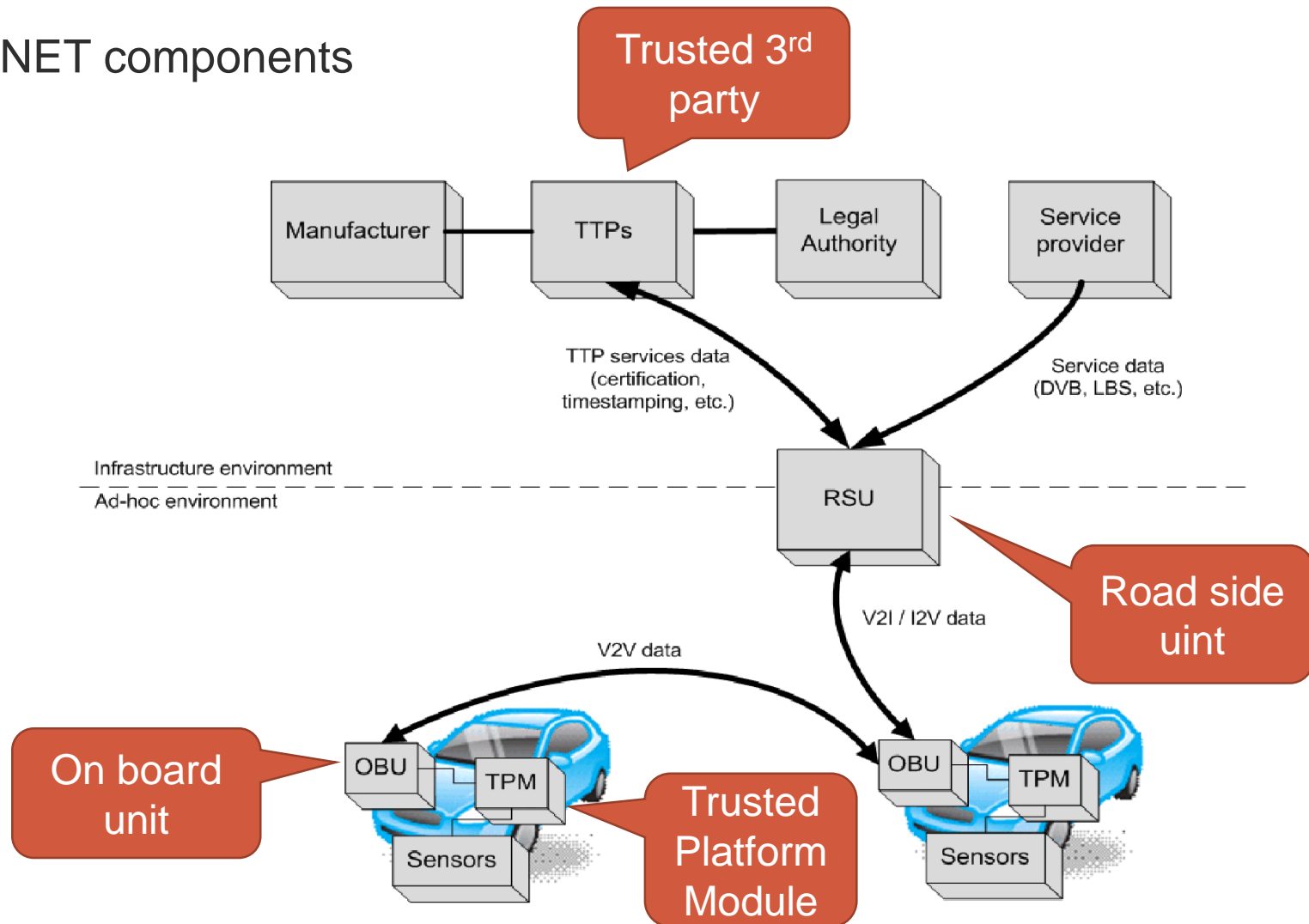
VANET solutions 3. – IEEE 1609.2

- VPKI solutions (Vehicular Public Key Infrastructure)
 - The source digitally signs the message + sends the certificate
 - $V \rightarrow r: M, \text{Sig}_{\text{PrKV}} [M|T], \text{CertV}$
 - Instead of RSA there are better asymmetric ciphers
 - ECC – Elliptic Curve Cryptography
 - NTRU - N-th degree TRUncated polynomial ring
 - Group key and group signature
 - Selected group leader, manages the group and signs. Anonym
 - Questionable efficiency and group leader selection
 - CA (Certificate Authority) is problematic
 - There is no global, worldwide CA
 - Multiple CA
 - Certificate revocation is hard to verify (requires online connection)
- Besides the authentication, encryption is also possible (AES or asymmetric)
- Privacy is not protected here

Timestamp also

VANET solutions 4.

- VANET components



Forrás: Sumegha Sakhreliya, Neha Pandya

Recent researches

- ABE (Attribute Based Encryption)
 - CP-ABE: Cyphertext-Policy Based Encryption (policy in the encrypted data)
 - KP-ABE: Key-Policy Based Encryption (policy in the key)
- Providing access control during the encryption
 - E.g.: encrypted data, but the fireman, police officer can access it (having dedicated attributes)
- Centralized key management
 - Can be hierarchical or distributed