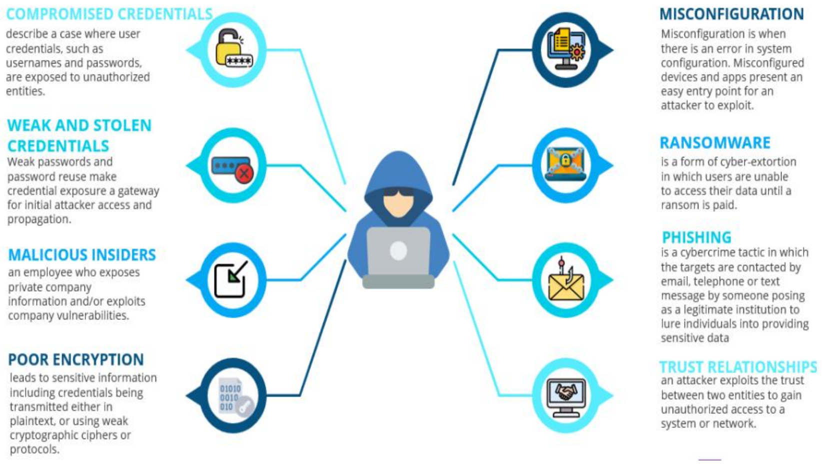
New Requirements and Challenges of Network Link Security

Weiqiang Cheng, China Mobile

Haojie Wang, China Mobile

Jin Yang, China Mobile

Network attacks may be anywhere and anytime



COMPROMISED CREDENTIALS describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities.

WEAK AND STOLEN CREDENTIALS Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation.

MALICIOUS INSIDERS an employee who exposes private company information and/or exploits company vulnerabilities.

POOR ENCRYPTION leads to sensitive information including credentials being transmitted either in plaintext, or using weak cryptographic ciphers or protocols.

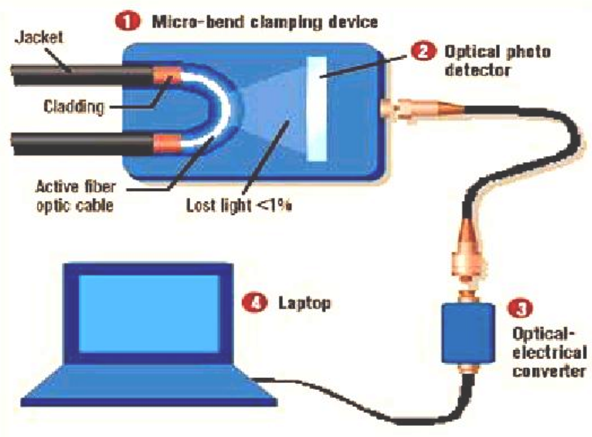
MISCONFIGURATION Misconfiguration is when there is an error in system configuration. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

RANSOMWARE is a form of cyber-extortion in which users are unable to access their data until a ransom is paid.

PHISHING is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data

TRUST RELATIONSHIPS an attacker exploits the trust between two entities to gain unauthorized access to a system or network.

1100+ cyber attacks happened per second [1-2]



Eavesdropping by optical fiber bending [4]

Eavesdropping is easy!

Only 3 steps

① **Interception:** bending to refract light

② **Conversion:** optical signal to electrical signal

③ **Analysis**

- *Network security is essential to protect network links and devices from potential threats. These threats can lead to network outages or sensitive data breaches.*

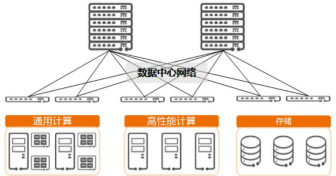
[1] https://www.ciena.com/insights/articles/unlocking-the-macsec-puzzle.html [2] https://www.balbix.com/insights/attack-vectors-and-breach-methods/

[3] https://www.youtube.com/watch?v=0PXJH2UrcPA [4] Securing Fiber Optic Networks and Designed According to the Security Standards

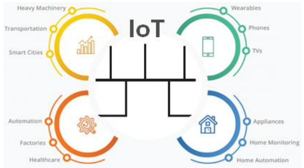
Security requirements of many classical scenarios

- Many classical scenarios such as DCN/DCI， IoT, mobile backhaul, campuses, and telecom networks, etc., need security protection.
- More other scenarios…

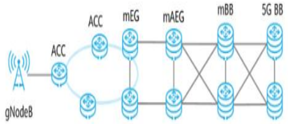
DCN/DCI



IoT



Mobile backhaul

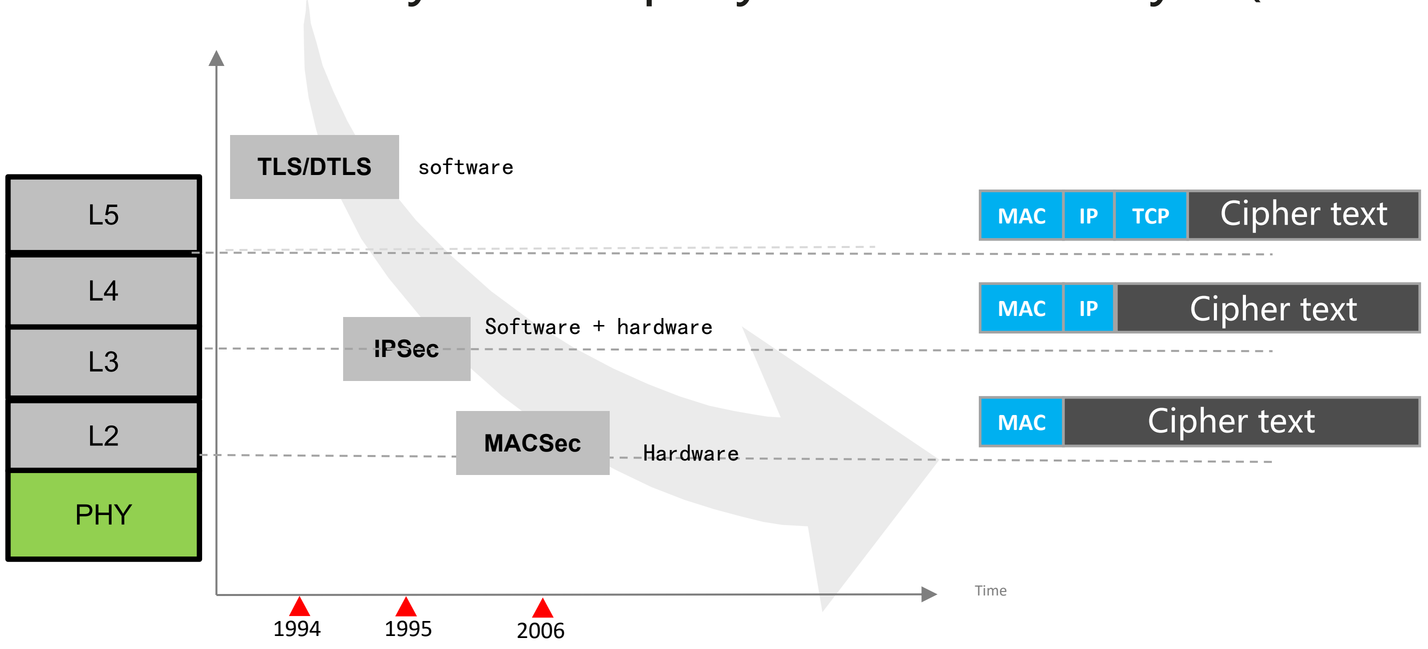


Industrial Network

In-vehicle Network

Existing standard security mechanisms

- Existing standard security mechanisms: TLS、IPSec、MACSec、…
- Trend：
  - ➢ Optimization of security in the same layer (e.g., MACSec, 802.1AE->802.1AEdk)
  - ➢ Implementation of security from top layer to bottom layer (TLS->IPSec->MACSec).



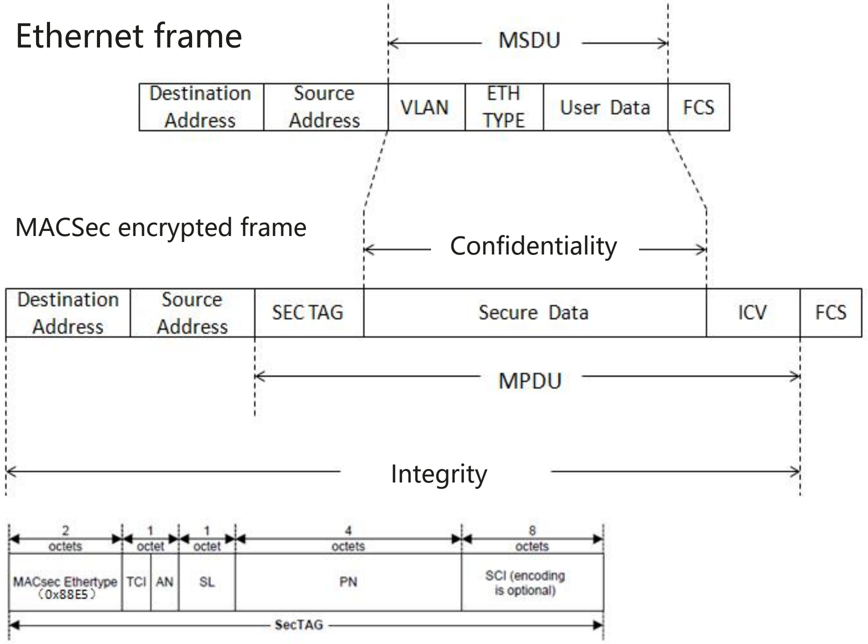
IPSec and TLS

- IPSec/TLS are widely used in end-to-end scenarios.
- Usually software-based implementation. Not easy to chip implementation.
- After the rate reaches 100 Gbit/s+, the encryption capability cannot match the line-rate. The link throughput limitation imposed by encryption has become the biggest bottleneck for encryption application (<70%@1400B packet).

Network Link Security: MACSec

MACSec

- Has been used wildly in Ethernet at layer 2, standardized in 2006. Provides confidentiality，data integrity，replay protection, and data origin authenticity.
- Latest standard amendment of MACSec is 802.1AEdk, published in August 2023, to enhance the privacy protection.



Ethernet frame

MSDU

Destination Address | Source Address | VLAN | ETH TYPE | User Data | FCS

MACSec encrypted frame

Confidentiality

Destination Address | Source Address | SEC TAG | Secure Data | ICV | FCS

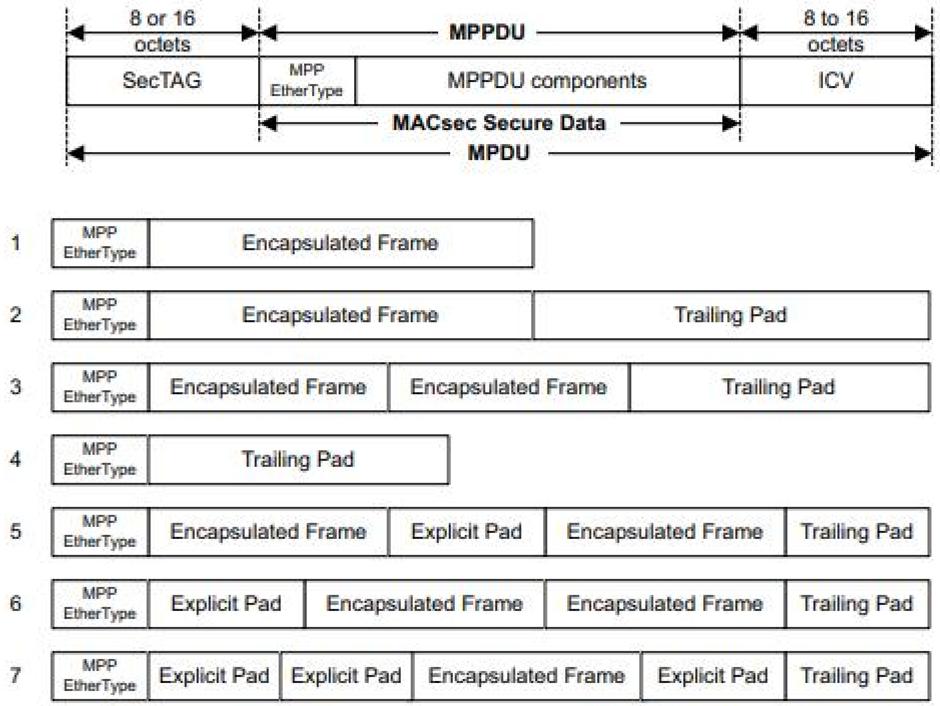
MPDU

Integrity

2 octets | 1 octet | 1 octet | 4 octets | 8 octets

MACsec Ethertype （0x88E5） | TCI | AN | SL | PN | SCI (encoding is optional)

SecTAG



8 or 16 octets | MPPDU | 8 to 16 octets

SecTAG | MPP EtherType | MPPDU components | ICV

MACsec Secure Data

MPDU

1 MPP EtherType | Encapsulated Frame

2 MPP EtherType | Encapsulated Frame | Trailing Pad

3 MPP EtherType | Encapsulated Frame | Encapsulated Frame | Trailing Pad

4 MPP EtherType | Trailing Pad

5 MPP EtherType | Encapsulated Frame | Explicit Pad | Encapsulated Frame | Trailing Pad

6 MPP EtherType | Explicit Pad | Encapsulated Frame | Encapsulated Frame | Trailing Pad

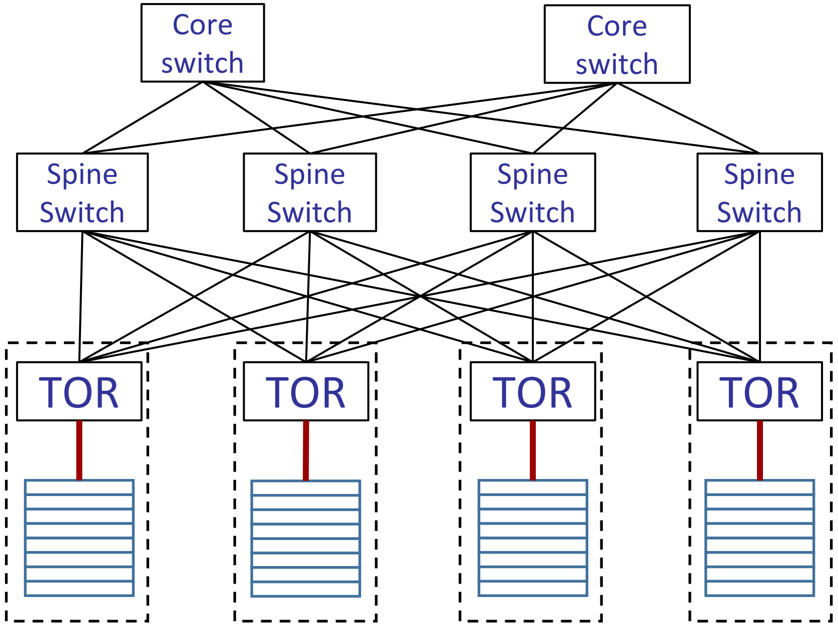
7 MPP EtherType | Explicit Pad | Explicit Pad | Encapsulated Frame | Explicit Pad | Trailing Pad

New security requirements of AI Date center

- Security requirements:
  - Traditional data centers do not have security protection for eastbound-westbound traffic. After evolving to the AI data center, their sensitive assets such as models, parameters, and data may be disclosed.
  - Due to communication link and device port exposure, security protection needs to be enhanced in typical scenarios, such as network expansion and upgrade, frequent O&M, and **multi-tenant networking**.

New scenario: intra-connection of AI Date center

AI date center

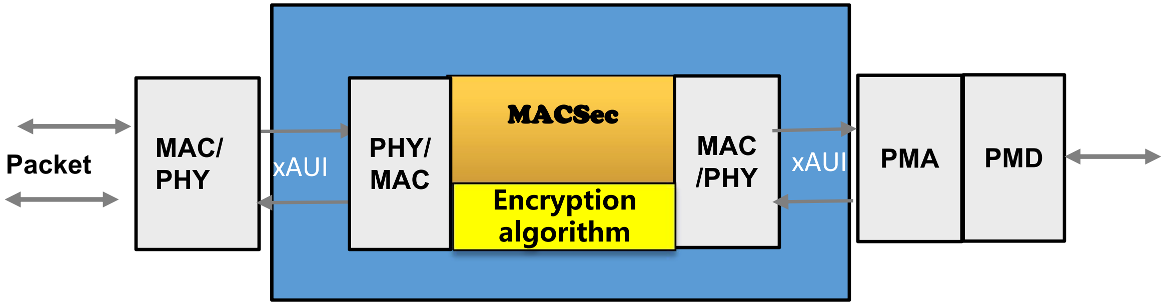


- Performance requirements: **low latency (ns level)** and **high throughput (>95%)**

Challenges

- ✓ MACSec can satisfy the security requirements.
- MACSec cannot satisfy the performance requirements of ICC intra-connection.
  - ➢ Have an impact on computing efficiency. latency >100ns@400G; bandwidth utilization 72.4%@64B
  - ➢ 802.1AEdk hides channel privacy at the cost of some added latency and additional chip resources.

MACSec PHY(BASE-R) chip architecture



Future

- How to solve the link security problem with high performance requirements (such as AI date center, low latency、high throughput、low overhead)?

Thank you !