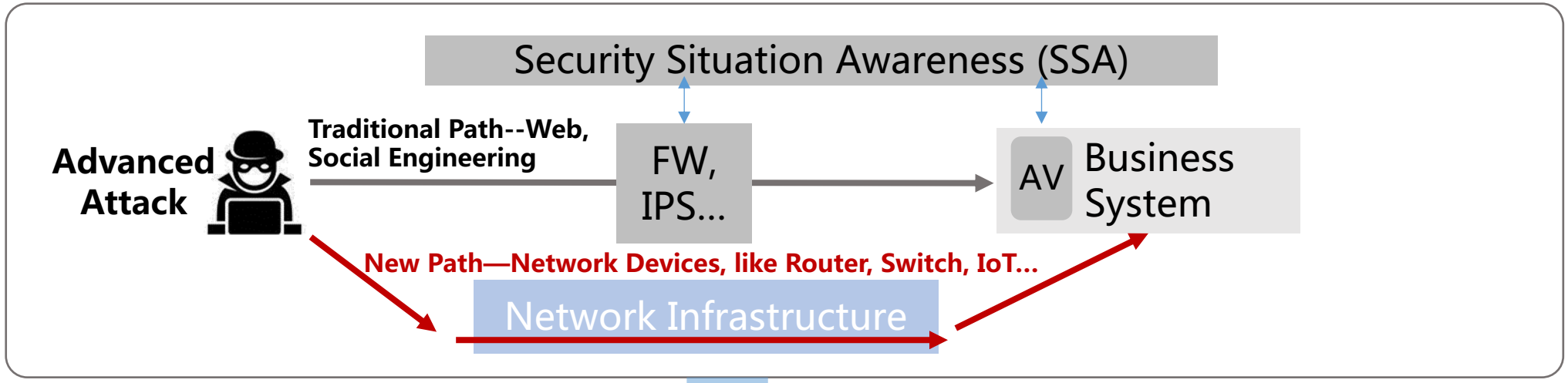
Threat Surface Management of Network Element

Feifei Hu, Danke Deng — China Southern Power Grid
Liang Xia — Huawei

Network Infrastructure Security is Facing Serious Challenge

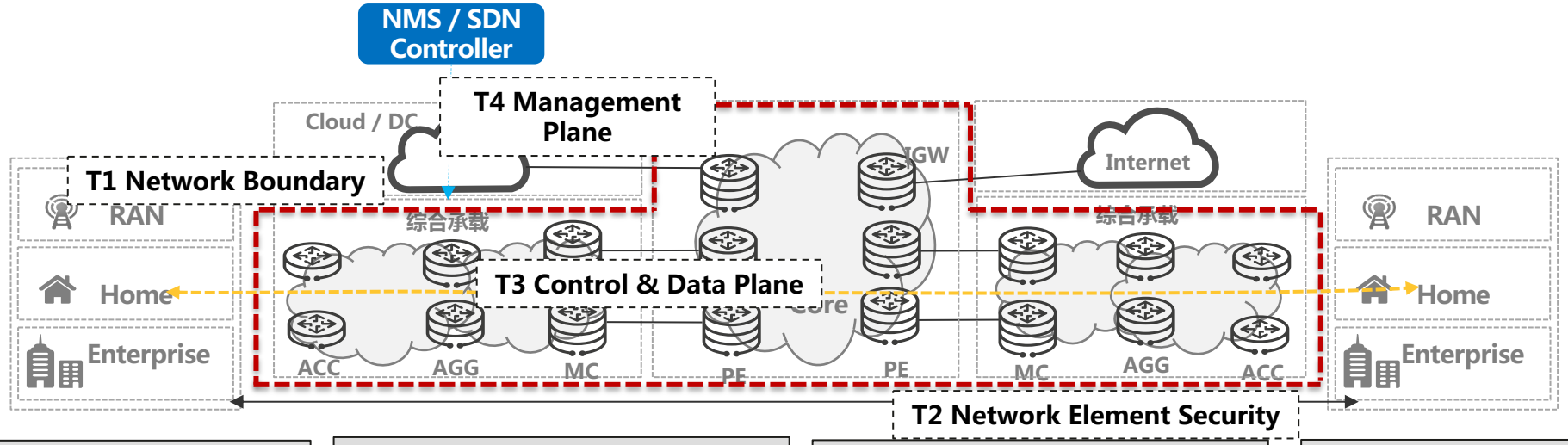


Examples of **Network Infrastructure Attacks**:

- **Operators**: internet outrage, route/data leaking, DDoS, pervasive monitoring …
- **Government, Bank, etc**: data leaking, service outrage, ransomware attack …
- **Energy, Manufacturer, etc**: production network outrage, ransomware attack …
- …

Critical information infrastructure (CII) plays a fundamental role in supporting national economic, social development and people daily life. Network infrastructure security, as the key support, are becoming more and more critical.

A New Standardization Requirement about NE Security Threat Visibility



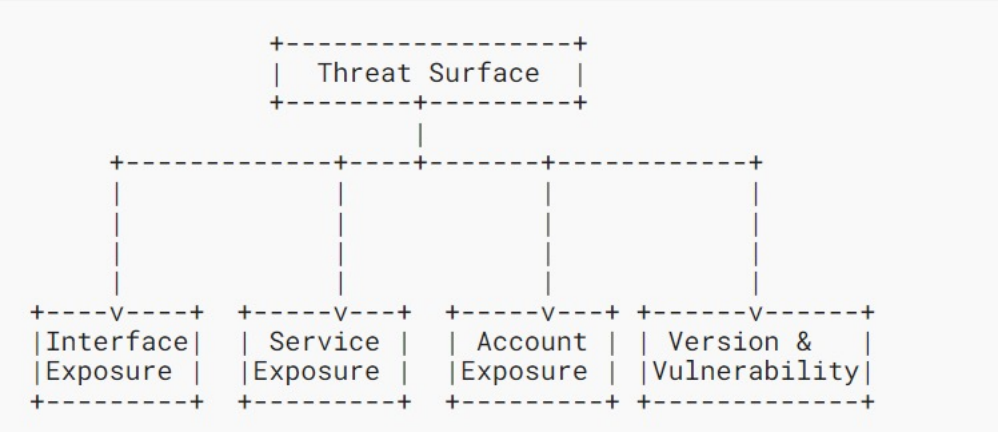
T1. Network Boundary Threat	T2. Network Element Threat	T3. Control & Data Plane Threat	T4. Management Plane Threat
• (T1.1) Illegal Access • (T1.2) DDoS Attacks at boundary • (T1.3) Boundary Invasion • …	• (T2.1) Attacks by vulnerability, external surface… • (T2.2) Weak Config • (T2.3) Availability • (T2.4) Supply Chain Attacks	• (T3.1) Routing Protocol weakness • (T3.2) Traffic interception, theft, and tampering • …	• (T4.1) Attacks of NM Plane • (T4.2) O&M violation operations • (T4.3) Low Visibility • …

IETF is working on (from different perspectives: **network element, network, management & control plane**): RATS, SCITT, IVY, NASR, SCION, SAVNET, GROW, OPSEC, OPSAWG …

Visibility is the key factor for network infrastructure security, we bring one specific standardization requirement: **Network Element Threat Surface Management, and its modelling standardization.**

What is Network Element Threat Surface Management, Why do we need its Modelling Standardization

- **External Attack Surface Management (EASM, Gartner):** refers to the **processes, technology and managed services** deployed to **discover internet-facing enterprise assets and systems and associated exposures** which include misconfigured public cloud services and servers, exposed enterprise data such as credentials and third-party partner software code vulnerabilities that could be exploited by adversaries.
- **Network Element Threat Surface Management:** The threat surface may not have vulnerabilities or be an attack surface. However, it is **exposed to the sight of attackers and faces threats from external attackers. So, Threat Surface is the potential Attack Surface.**



Interface Exposure: Unused Interfaces (physical or logical), IP management interface exposure

Service Exposure: Insecure protocols, Abnormal service IP address, Weak service security configuration, Abnormal Service Port

Account Exposure: …

Standardization Goal: Define the **NE Threat Surface Management Yang Model**, so that **monitor and converge the threat Surface** in real time.

What we are looking for

Collaboration on this specific work, and together look into more potential works related in this direction.

Draft: https://datatracker.ietf.org/doc/draft-hu-network-element-tsm-yang/

Contacts: huff@csg.cn, hongdk@csg.cn, frank.xialiang@huawei.com

Thank you