FIGI Security Clinic: Securing the infrastructure and applications for digital financial services
（Geneva Switzerland, 4-5 December 2019）

SS7 security related standardization activities in ITU-T SG11

INFRASTRUCTURE SECURITY: Securing the DFS Applications and Infrastructure

Xiaojie Zhu
Vice-Chairman of SG11
China Telecom(zhuxiaojie@chinatelecom.cn)

Current issues of SS7 security

□ Technical vulnerabilities

- ISUP
  - Caller ID spoofing: fake calling party identification presentation
  - Abuse of call service
- MAP
  - Location Tracking with call/SMS setup protocol messages
  - Interception of User Traffic including voice call and SMS (e.g. one-time password) with *Update Location/Insert Subscriber Data*
  - Denial of Service (DoS) to specific target user with *Update Location/ Cancel Location/Insert Subscriber Data etc.*
  - Abuse of SMS service: fake, spoof or spam SMS

□ administrative vulnerabilities

- Operators lease SS7 accesses (e.g ISUP/PRI access, SCCP access, etc.) to the third parties and various service providers which are not licensed or regulated.

ITU-T SG11 activities on SS7 security

- □ ITU Workshop on “SS7 Security”(Geneva, Switzerland 29 June 2016)
- □ Presentation at the ITU-T SGs Leadership Assembly, Budapest, 9-10 September 2019
- □ ITU Workshop on Brainstorming session on SS7 vulnerabilities and the impact on different industries including digital financial services”(Geneva, 22 October 2019)

ITU-T SG11 outcomes:

- Revised SS7 related standards– Recommendations ITU-T Q.731.3, Q.731.4, Q.731.5 and Q.731.6 (04/2019) – one of the tools to combat with the spoffing of calling party number
- Technical Report ITU-T TR-SS7-DFS: SS7 vulnerabilities and mitigation measures for digital financial services transactions – the overview of the existing SS7 vulnerabilities

Ongoing activities on SS7 security:

- ITU-T Q.SR-Trust: Signaling requirements and architecture for interconnection between trustable network entities – potential solution to defend business of different stakeholders which use existing telco

ITU-T SG11 activities on SS7 security

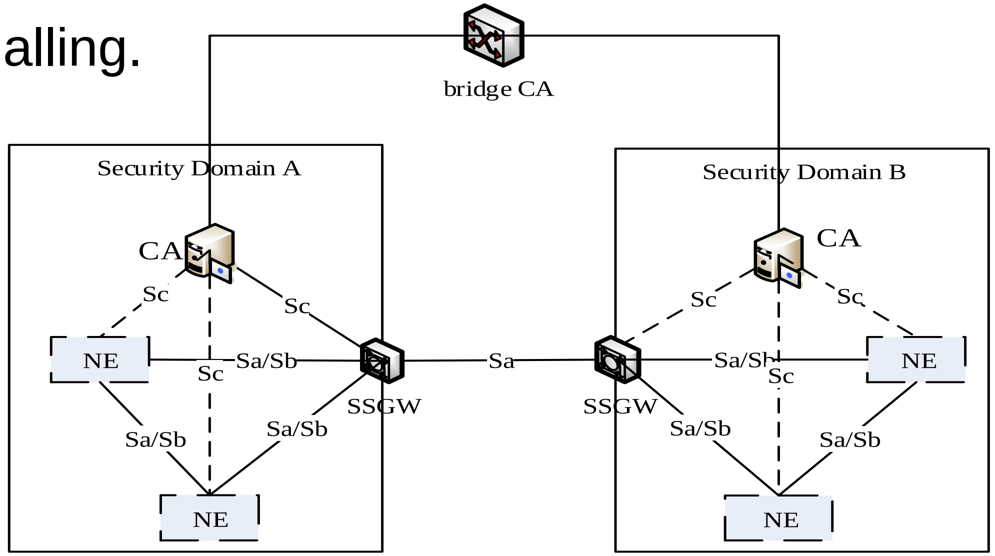
- □ Outcome: Revised ITU-T Q.731.X (04/2019)
  - ✓ to accommodate the urgent demand in dealing with the spoof calling party number problem.
  - ✓ The revised ITU-T Q.731.3 specifies an exceptional procedure for transit exchange in purpose of providing predefined calling party number by the originating operator. The fake caller number from the third parties or service providers which are not licensed or regulated that connect to transit exchange via ISUP shall be replaced with the predefined calling party number.
  - ✓ Some editorial work has been done for Q.731.4, Q.731.5, Q.731.6 to align with this series Recommendation.

ITU-T SG11 activities on SS7 security

- □ Outcome: Technical Report ITU-T TR-SS7-DFS: SS7 vulnerabilities and mitigation measures for digital financial services transactions
    - ✓ result of the Financial Inclusion Global Initiative (FIGI) Security Infrastructure work stream research into SS7 vulnerabilities and their effect on Digital Financial Services (DFS) in the developing world.
    - ✓ describes the researched vulnerabilities, mitigation measures for operators and for DFS providers.
    - ✓ improve the security posture of SS7 towards financial services and other public interest OTT services offered over the telecom infrastructure.

ITU-T SG11 activities on SS7 security

- Ongoing ITU-T Q.SR-Trust: Signaling requirements and architecture for interconnection between trustable network entities
  - ✓ presents the signalling architecture and requirement for interconnection between trustable network entities in support of existing and emerging networks.
  - ✓ specifies the interfaces and signalling requirements between the functional entities. It also presents procedures to be applied for the signalling.
  - ✓ The previous attempt to create an authentication layer for TCAP (TCAPSec - TS29.204/TS33.204) needs to be studied and the lessons learned from it’s lack of adoption integrated into Q.SR-Trust



ITU-T SG11 activities on SS7 security

□ Outcome of ITU Workshop on Brainstorming session on SS7 vulnerabilities and the impact on different industries including digital financial services"(Geneva, 22 October 2019)

—**Potential standardization directions**

In close collaboration between ITU-T SG11 and ITU-T SG2

✓ Integrate the lessons learned from the lack of adoption of TCAPSec into Q.SR-Trust

✓ Devise market economics that will drive the implementation of Q.SR-Trust

✓ Start a work item on drafting requirements for a secure signalling architecture that will enable operators to offer OTT services to public interest services.

✓ Draft a requirement for a SIP-ISUP interworking function to mitigate CLI spoofing by providing origination data to the ISUP IAM request.

✓ Add digital signature (adopt Q.SR-Trust) to ISUP to create attribution of spoofed calls to telcos.

Strategic direction to be taken by ITU-T

- Keep close cooperation among SG11, SG2 and SG17 on this subject
- Invite all ITU Members to implement ITU-T Q.731.X and other mitigation strategies
- Invite all interested stakeholders in the telecommunication, regulatory and financial sectors to join our effort to improve the SS7 security including for digital financial services(e.g. promote via Workshops, trainings)
- Collaborate with GSMA and 3GPP to progress additional mitigation measures to mitigate the vulnerabilities of SS7.

Thank you for your attention!

Xiaojie Zhu

Vice-Chairman of SG11

China Telecom (Email: zhuxiaojie@chinatelecom.cn)