SS7 security related issues

Session 5: Security, privacy and trust

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

ITU-T SG11 activities on SS7 security

ITU Workshop on "SS7 Security"(Geneva, Switzerland 29 June 2016)

Current issues of SS7 security:

- Issues are caused by abuse and misconfiguration of SS7 protocol
- Attacks on SS7 networks include telephone spam, spoofing numbers, intercept calls and messages, etc.
- The risk of illegal usage of customers' applications over SS7-based ICT networks

Operators Challenges:

- the implementation rate of published mitigation measures for SS7 security is extremely low
- affects operators' networks with exposure functionality
- affects subscribers privacy

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)**

Ongoing activities on SS7 security:

- **ITU-T Q.SR-Trust: Signaling requirements and architecture for interconnection between trustable network entities**
- **Technical Report ITU-T TR-SS7-DFS: SS7 vulnerabilities and mitigation measures for digital financial services transactions**

Upcoming activities on SS7 security:

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

Current actions and solutions

- Monitoring and analyse SS7 messages
- Categorize vulnerabilities for different types of attack
- Develop solutions:
  - Signalling network audit
  - Filtering the abusive messages
  - Masking the unnecessary information
  - Improving routing methods (home routing, DPC->GT)
  - Controlling access by authentication and authorization
  - Limiting MAP and SCCP operation to the necessary procedure

The way forward in ITU-T

- **Evaluate the improvement of existing SS7 protocols**
  - To accommodate some Member States' urgent demands relating to the spoofing of calling party number, published the revised ITU-T Q.731.3, Q.731.4, Q.731.5 and Q.731.6
  - Promote the implementation of revised ITU-T Q.731.3, Q.731.4, Q.731.5 and Q.731.6 in SS7 networks
- **Consider to develop standards for new elements or functional entities to enhance security**
  - Progress ITU-T Q.SR-Trust which defines the signaling architecture and requirement for interconnection between trustworthy network entities based on the existing and emerging technologies.
- **Persistently detect and analyze new attack types, develop guidelines to address SS7 vulnerabilities**
  - Progress Technical Report ITU-T TR-SS7-DFS: SS7 vulnerabilities and mitigation measures for digital financial services transactions

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.731.3, Q.731.4, Q.731.5, Q.731.6 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

Questions for SGLA discussion

- Question 1: Are there any additional requirements in terms of SS7 security?
- Question 2: Any suggestions on the cooperation with other SGs and SDOs on this subject?
- Question 3: Any ideas on the implementation of mitigation strategies for SS7 security?
- Question 4-5: Whether the domestic and international legislations need to be changed to facilitate the implementation of mitigation strategies for SS7 security? What actions from ITU are needed?

Welcome to ITU-T SG11 Workshop (Geneva, 22 October 2019)

Brainstorming session on SS7 vulnerabilities and the impact on different industries including digital financial services

Types of attacks using SS7 vulnerabilities:

- telephone spam
- spoofing numbers
- location tracking
- subscriber fraud
- intercept calls and messages
- DoS
- infiltration attacks
- routing attacks, etc.

Objectives

The workshop will be dedicated to brainstorming on the potential way forward to enhance the security mechanisms of SS7 and its adoption rate among telcos in order to defend all stakeholders from related attacks. The key aim of the brainstorming session is to identify the roadmap for fixing these issues