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

(Geneva, Switzerland, 22 October 2019)

Key issues, countermeasures, challenges, and suggestions for SS7 security

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

Key issues on SS7 security

- □ **Technical vulnerabilities**
  - – ISUP
    - 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 with *Update Location/Insert Subscriber Data*
    - Denial of Service (DoS) with *Update Location/ Cancel Location/Insert Subscriber Data etc.*
    - Abuse of SMS service: fake, spoof or spam SMS
- □ **administrate vulnerabilities**
  - – Operators lease SS7 accesses (e.g ISUP access, SCCP access, etc.) to the third parties and various service providers
  - – International roaming related information which should be internal information for exchanging among operators is leaked on the internet. This information may help the criminals perform illegal attacks

Countermeasures for SS7 vulnerabilities

- **Introduce authentication and authorization in the access layer, e.g authenticating caller ID from users even if access with ISUP**
  - None SCCP access permission to third parties
- **Monitor incoming calls from partners**
  - Signaling monitoring and characteristics analysis.
    - Call duration is very short
    - Number of call attempt is large
  - Monitoring behavior of called party： detect dual tone. Fraud calls often play a short voice message which indicate the recipient press “button” to transfer call to manual service.
- **Intercept calls with illegal calling party number**
  - Number format check
  - location check
    - When a call is coming from abroad and the caller ID is a mobile number, check the location of the caller, the call should be blocked if the caller is not outbound roaming.
- **Screening messages of non-roaming-agreement-partners**

Challenges and suggestions on SS7 security improvement

□ Challenges

- Caller ID of the call service abuser is complex and changing all the time
- Upgrading criminal means: criminal illegally obtain personal information, and then making precise calls to reduce the number of call attempts, invalidating the original characteristics of call service abuse, such as large number of call attempts.
- Intercepting calls may infringe on the freedom of communication and must be approved by the regulatory authorities

□ Suggestions to Telcos

- Source controlling: prohibit illegal SS7 access, block fake caller IDs and screen malicious messages.
- Improve SS7 security: implement the standards and measures
- Telecommunication network is a global network, global cooperation is needed.

Thank you for your attention!