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

Outcomes
22 October 2019

Web page
Contacts: tsbsg11@itu.int

Main outputs from Telco discussions

- It was clear that the operators attending the SS7 brainstorming session clearly understood Signalling Vulnerabilities and risks.
    - When asked how many operators were in the audience and how many had deployed signaling firewall 100% had deployed SFW (5 operators – 5 deployments). I was not aware of how many operators were actually in attendance, there could have been more who did not want to be included in the discussion.
    - How do we address the “Non believers” that there are signaling vulnerabilities and risks that could severely affect their brand reputation and share price/churn if they were involved in a High Level (VIP) signalling issue or fraud activity?
- Common requirement between operators for knowledge sharing of signaling firewall attacks, will this ever happen? Doubtful but beneficial if it did.
- Clear requirement for Voice protection (ISUP & SIP) in roadmap.
- Very clear that deployment of SFW and following of GSMA FS11 & FS19 is a good starting point (Foundation) but reliable SFW protection needs daily activity.
- Signalling Threat Intelligence is going to be very important moving forward.
- The audience present appeared reluctant on specific ”DFS-secure” certification for telcos.
- Threats of further DFS deployment via USSD/SMS on 2G/3G networks understood by the audience, at the same time audience is of the opinion that protection of DFS actors from SS7 vulnerabilities is responsibility of financial services providers.

Overview of current standardization activities and other activities related to vulnerabilities of signaling protocols

- SG11 work items: Q.731.x and Q.SR-Trust
- SG2: E.156 & E.157
- Ongoing activities of financial institution (from FIGI)

Main discussion points (1/1)

- **Caller ID spoofing**
  - The main issue is VoIP telephony providers which are not licensed or regulated that connect to the telecom world via SIP trunking or PRI connections and spoof CLI (virtual numbers).
  - Since these VoIP telephony service providers “piggyback” on other telco GTs there is no current method to detect and block the spoofed calls.
  - The leading method today is private / enterprise PBX solutions that run software to detect and block spoofed calls based on proprietary logic.
- **Q.SR-Trust**
  - 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

Main discussion points (2/2)

- **New standardization areas**
  - Try and create new standards that will enable operators to create growth engines, otherwise they may be thinned down like ISPs (the telecom infrastructure will be considered an untrusted infrastructure like the internet).
  - The main issue in creating the signaling infrastructure for secure OTT services that operators can offer is the limitation to their own subscribers, since the OTT applications (financial, ride-sharing, food-delivery, etc.) will want an aggregated service for all of their users regardless of operator affiliation.
- **Adoption rate of signaling security**
  - We need to create market driven incentives for operators to implement signaling security. The demand for more security must generate ROI for the operator, otherwise it will not be implemented widely. Relying on local legislation to enforce the implementation of signalling security will take many years (10+), and we need to move faster than that.

Potential standardization directions

in close collaboration among ITU-T SG11, ITU-T SG2 and ITU-T SG17

1. Integrate the lessons learned from the lack of adoption of TCAPSec into Q.SR-Trust
2. Devise market economics that will drive the implementation of Q.SR-Trust
3. Start a work item on drafting requirements for a secure signalling architecture that will enable operators to offer OTT services to public interest services.
4. Draft a requirement for a SIP-ISUP interworking function to mitigate CLI spoofing by providing origination data to the ISUP IAM request.
5. Add digital signature (adopt Q.SR-Trust) to ISUP to create attribution of spoofed calls to telcos.

Main discussion points – DFS

- **Viability of telco's certification to handle DFS**
  - Certification procedures alike to specific trade certificates (PCI), or non-specific standards (ISO) that would confirm to actors from financial sector that a certain MNO is adhering to security standards and implemented safe environment to handle digital financial services.

- **Counter-actions to increased risk exposure of DFS providers to SS7 vulnerabilities, specifically in developing countries with**
  - Call to suggest specific measures that would protect subscribers/clients of MNOs/MVNOs, using USSD/SMS means to in 2g/3g networks