ITU Workshop on "Improving the security of signalling protocols"

(Virtual, 29 November 2021)

SG11 activities on improving security of signalling protocols

Cheng Li
Rapporteur of ITU-T Q2/11
CAICT(licheng@caict.ac.cn)

Current issues on signalling 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 signalling security

- **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**

ITU-T SG11 activities on improving security of signalling protocol

- 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)
  - —Potential standardization directions
    - ✓ In close collaboration between ITU-T SG11 , ITU-T SG2
    - ✓ 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.
    - ✓ 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 disdinguish spoofed calls.

Terms of Reference of ITU-T Q2/11 related to signaling security

- Q2/11 "Signalling requirements and protocols for services and applications in emerging telecommunication environments" Study Period (2017-2020)

Questions:

- What new recommendations should be made for cloud computing-related services and applications? What associated mechanisms are required to guarantee signalling and control security?
- What enhancements should be made in existing series of ITU-T Recommendations describing signalling system number 7 (SS7) to ensure its security?

Tasks:

- Develop new Recommendations or enhance the existing ITU-T Recommendations to ensure SS7 network's security.

ITU-T SG11 activities on signalling security

- **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 spoofing 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**
  - ✓ **ITU-T Q.3057(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**
- **SG11 ongoing activities on SS7 security:**
  - ✓ **ITU-T Q.Pro-Trust: Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks**
  - ✓ **ITU-T Q.CIDA: Signalling procedures of calling line identification authentication**
  - ✓ **Technical Report ITU-T TR-USSD:Low resource requirement, quantum resistant, encryption of USSD messages for use in Financial services**

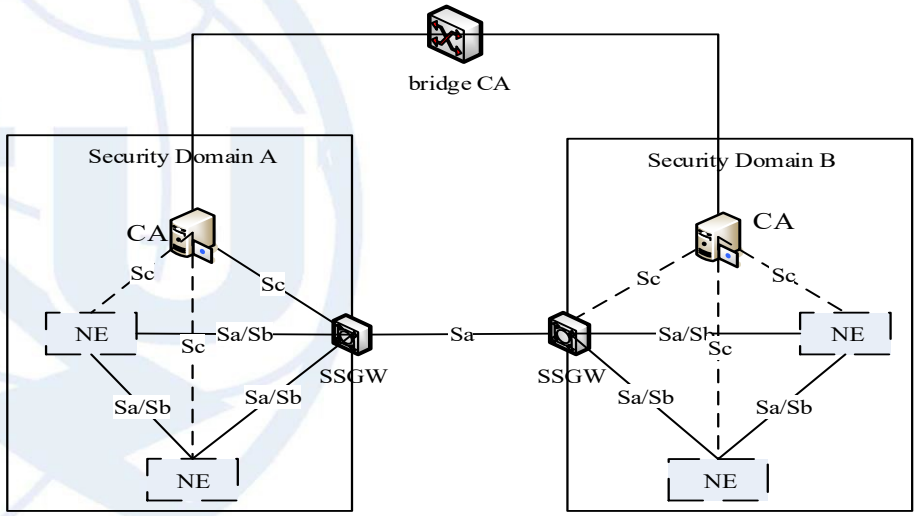
Revised ITU-T Q.731.X

- **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 Q.3057(Q.SR-Trust)

- **Outcome： ITU-T Q.3057(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.

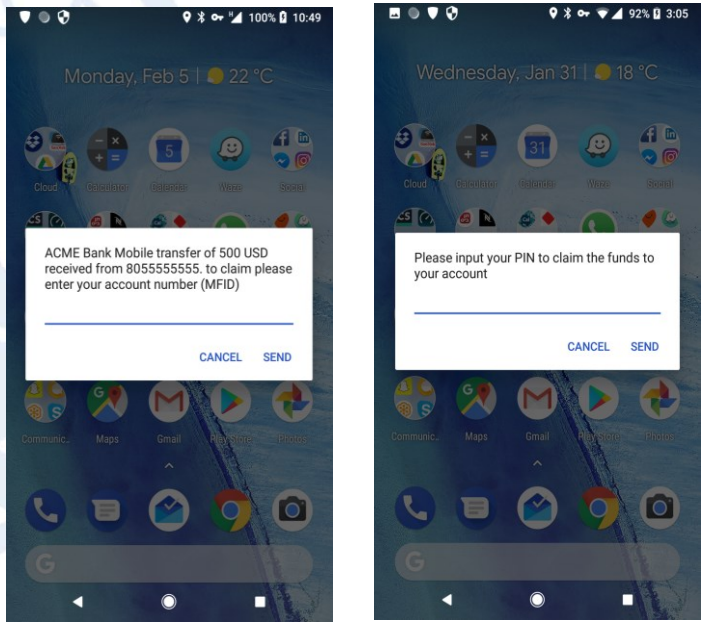


Reference architecture of interconnection between trustable network entities

Technical Report ITU-T TR-SS7-DFS

- **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.

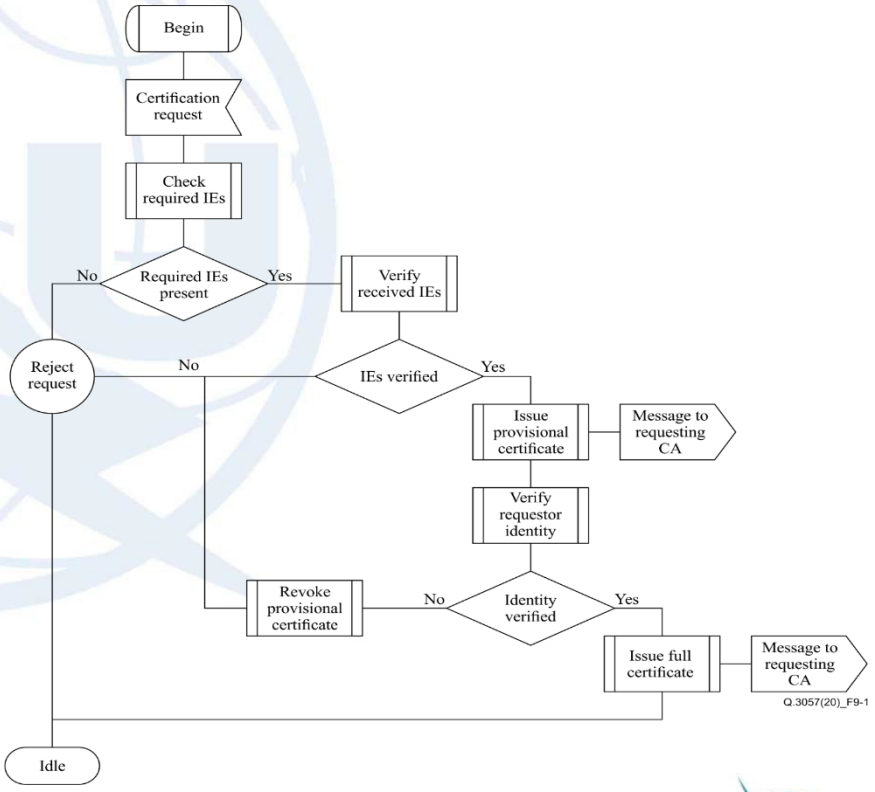


Using USSD to socially engineer the user

ITU-T Q. Pro-Trust

- **Ongoing work item： ITU-T Q. Pro-Trust Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks**

✓ presents the signalling procedures and protocols involved in the application of the signalling requirements and architecture defined in ITU-T Q.3057 for interconnection between trustable network entities in support of existing and emerging networks

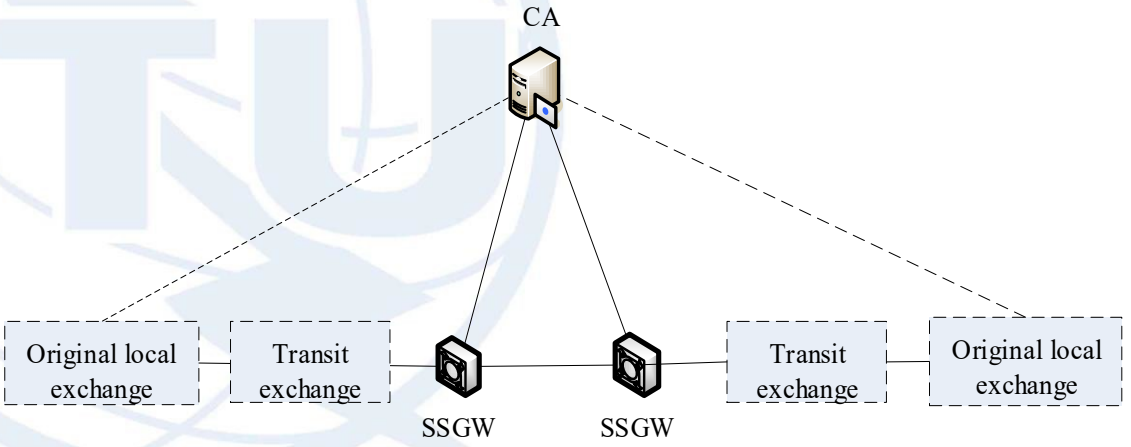


signalling procedures of TSCA
(Trusted Signalling Certificate Authority)

ITU-T Q. CIDA

- **Ongoing work item： ITU-T Q. CIDA Signalling procedures of calling line identification authentication**

- ✓ presents the architecture and signalling procedures of calling line identification authentication in support of existing networks.
- ✓ specifies the procedures of calling line identification authentication.
- ✓ identifies amendments for BICC/ISUP and calling line identification presentation.



reference architecture of
calling line identification authentication

Technical Report ITU-T TR-USSD

- **Ongoing work item： Technical Report ITU-T TR-USSD Low resource requirement, quantum resistant, encryption of USSD messages for use in Financial services**

- ✓ a follow-up study to ITU-T TR-SS7-DFS “SS7 vulnerabilities and mitigation measures for digital financial services transactions”. Clear-text USSD is the most common medium of DFS financial transactions in the developing world, which leads to large scale financial fraud.
- ✓ surveys the available and upcoming encryption technologies that can mitigate this risk of clear-text USSD in DFS.

Content of ITU-T TR-USSD

- How does USSD work
- Examples of exploiting USSD vulnerabilities on to commit DFS fraud
- Quantum resistant cryptography
- The uSIM - a computation platform for post-quantum crypto
- Applicability matrix between USIM platform and post-quantum crypto

Strategic direction to be taken on improving security of signalling protocol 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 signalling security including for digital financial services(e.g. promote via workshops, trainings).
- Collaborate with GSMA, 3GPP and other SDOs to progress additional measures to mitigate the vulnerabilities of signalling system including SS7.
- Consider to develop emerging technologies(e.g. QKDN) enabled architecture and mechanisms to guarantee signalling and control security, including signalling system number 7 (SS7) and emerging signalling systems in next study period.

Thank you for your attention!