Questions transcript provided by moderator

ITU Webinar Series on Signalling Security:
Episode 2: "Securing legacy telecom network services"

7 November 2022

#	Question	Answer
1.	Are there CLI authentication protocols other than STIR/SHAKEN?	The STIR/SHAKEN are basically frameworks for operator authentication but it is not Calling Line Identification (CLI). In general, STIR/SHAKEN does not authenticate the subscriber's phone number while it authenticates the operator on the network. STIR/SHAKEN was designed for VoIP protocols which are widely used over 4G, 5G, etc. However, STIR/SHAKEN is not applicable for legacy networks such as (2G and 3G) which are switched based networks. Those networks utilize different protocols on signalling and payload (audio channel) levels. In this regard, ITU-T SG11 developed number of standards (ITU-T Q.3057, Q.3062 and Q.3063) which define approach on incorporating digital signature (digital certificate) into signalling exchange. This approach might be considered as equivalent to STIR/SHAKEN but can be used on existing and legacy networks as it is applicable to wide number of protocols including SS7, DIAMETER, SIP, etc. STIR/SHAKEN and ITU-T approaches use the same authentication or cryptography scheme, but ITU-T standards define the details on how digitally sign the phone number in signalling exchange.

#	Question	Answer
2.	Do you think that STIR/SHAKEN will be widely deployed outside the US and Canada as a counter-measure to caller ID spoofing? If so, who would provide the global director of certification authorities? Could ITU do that? Regarding your slide 25, Trust Model, could the ITU be the trust anchor?	The deployment of such solutions (STIR/SHAKEN or ITU-based solution) depends on the willingness of the countries. Any country may deploy it locally following implementation of relevant legislation and regulation mechanisms. Some countries may have bilateral agreement on such implementations. As example US and Canada agreed to deploy STIR/SHAKEN together. However, for solving problem on the global level, international deployment is needed and ITU may play a lead role as authority which may provide such globally recognized digital certificates all over the world. Those certificates might be used in all similar solutions such as STIR/SHAKEN or ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063. The global deployment of such solutions may can be interoperable and may mitigate the number of different attacks on existing and legacy networks. In other words, the trust anchor for the trust model for those tokens definitely can be ITU as UN specialized agency which is responsible for International Numbering Resources and it is globally trusted organization.
3.	What is the way forward for implementation of ITU-T Recommendations ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063 which define the usage of digital signatures in the signalling exchange?	In terms of ITU-T SG11, in terms of the technical standards, ITU-T SG11 developed the basic principles and protocols that are required to deploy such solution. Now, ITU-T SG2 may start working on operational procedures and define on how operators may apply for security tokens, where the trusted root is set out and other relevant issues.

#	Question	Answer
4.	Has SG11 sent a liaison statement to SG2 regarding implementation of ITU-T Q.3063 and it's possible relation to E.157?	ITU-T SG11 sent out a LS to SG2 informing about consent of the ITU-T Q.3062 and ITU-T Q.3063 in July 2022. However, it was noted the necessity to send an additional LS which may contain the brief presentation about implementation of ITU-T Q.3063. The ITU-T E.157 then might be revised accordingly. SG11 management and editors of ITU-T Q.3063 will be kept informed.
5.	If Sim Card is 4G, but Telco still using 2G/3G. Is there danger of OTA attack? If yes, how many percent?	In general, it depends on OTA authentication scheme used in SIM card. For 4G-based SIM cards equipped with NFC connectivity feature which utilizes the AES encryption. Therefore, such SIM cards are not vulnerable. If it is an old version of SIM card (without NFC connectivity), then it might be vulnerable. In other words, the vulnerability would depend on the version of SIM cards used by particular operator.

____