Abstract

“Key Trust issues related to

Numbering, Naming, Addressing and Identification (NNAI) and Services”

Communications today is more global than ever before, and as calls pass country borders under increasing number of interconnected networks of different types (e.g. IP based networks), there are increasing challenges to guarantee or verify correctness of electronic communications parameters received, including the received Originating Identification and Calling Line Identification and Calling Party Number Delivery (OI/CLI/CPND), and hence increasing the opportunities for abuse and fraud, including economical fraud and national security breach in addition to consumer inconveniences. For instance, spoofing of OI/CLI/CPND is currently easily attainable e.g. commercially through third parties!

It is also noticed the increased use of shared code global numbering resources to offer global services, mostly including mobility, in such environment trust in the veracity of the resource and the origin of the communication is becoming more intricate.

Increasing trust in OI/CLI/CPND has been addressed by several administrations and regions, but still technical limitations and divergent national regulations and polices currently hinder any effort to achieve trust in the true source or origin of an electronic communication.

ITU-T holds databases of national and international NNAI resources of almost all countries of the world; the Trust in such information and identifiers is crucial to facilitate interworking and interconnection among networks, and to counteract misuse of NNAI resources.

With the expected huge proliferation of IoT and M2M in the coming decades, the role of NNAI for building a trustworthy system is becoming crucial. In such object-wise environment, Trust in identifiers is of great importance. Different divergent IoT identification schemes are currently available, most of them are not intrinsically developed for IoT, where security requirements in IoT IDs is more stringent due to richness in semantics. Building a trustworthy identifiers for the future IoT/M2M systems, either with new Identification Scheme, or through interworking of existing schemes will be a rich are for study in the coming period.

Trust in services is another area that needs careful examination. The advent of social media communications, in particular the OTT communication services, has introduced vulnerabilities, such as spoofing of identity, non-confidentiality of personal directories, hijacking of passwords, masquerading, … etc. Trust in such an open environment is thought to be a basic requirement as well as a right for the end user.

On the operational side, trustworthy network management is an area of concern for network operators; a secure, reliable and resilient management system is essential. Security of the management system is not sufficient, but Trust in that the communication network to perform in the way it was designed for is a global requirement.

The presentation will address the above issues, and will try to identify directions for future studies in the ITU-T.