TRAI Consultation Paper "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communication" from 18 Oct 2016

Date: 9 January 2017

Comments by:

Mr Andreas Sommer
Email a.sommer@sec-sommer.com

Q12 Chapter II
Comment: M2M / IoT require highest level of encryption to be tamper-proof, including end-to-end encryption of devices, data transfer between devices and storage (incl. underlying network), storage on servers (including cloud computing, gateways, various platforms, applications), and data transfer between storages of various servers in various data centers – all India national and international cross border. There might be different national and/or international M2M Service Providers. Current India IT Act does not provide a solid secure basis for national and international end-to-end encryption and storage, including storage on international cloud servers (refer to D. Security and Privacy of Data, all chapters). Sensitive M2M / IoT devices and applications such as health, financial, public infrastructure (smart cities, smart grid), autonomous cars, etc. should not be used unless such IT Act is adapted to new requirements. For example a "four eyes principle", a security precaution that requires at least two people (e.g. judges) to approve interception and to execute interception (e.g. certified engineers only, detailed reports of activities should be mandatory) should be implemented. Furthermore from technical perspective risks of decrypting data should be discussed in more detail. Any backdoor and interim decryption, also those used for lawful interception, will be sooner or later used by criminals[1]. Sensitive M2M / IoT devices and applications should be certified by an independent public authority (e.g. through separate National Trust Center). There should be adequate standards for encryption.

[1] Bleeping Computer: "You Can Now Rent a Mirai Botnet of 400,000 Bots"
https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/

Q13 Chapter II

Comment: End-to-end encryption and data privacy is essential in the world of M2M / IoT. For development and operations of sensitive devices and applications (autonomous cars, health, smart grids) engineers must have adequate education and continued training. A mandatory standardized certification for engineers to be checked and renewed regularly by authorities (e.g. a National Trust Center) should be the right provision to guarantee highest level of security, consumer and data protection, and privacy.

Q13 Chapter II and Q13 Chapter IV

Comment: Liability issues need to be regulated. There should be a "Privacy and Security by Design" principle established, e.g. for RFID-chips (e.g. misuse of data) but also for "dilemma situations", such as pedestrians are overrun by autonomous cars. There shall be appropriate sanctions in case of violation. Furthermore there shall be a clear policy in favor to the injured parties (consumer protection) and disputes should not be left to injured parties battling with operators of devices / autonomous cars, manufacturers, network operators and courts. The government should have a clear protection task for consumers with this regard. Burden of proof shall be with the manufacturer. Critical systems should always be redundant. If for example a camera fails in an autonomous car, other sensor systems must take over the function automatically in milliseconds.

Q16 Chapter II and Q16 Chapter IV

Comment: According recent international studies[2] India has weak telecommunications network infrastructure. Weakness includes coverage; robust, resilient and secure managed backbones considering latency; connection of mobile towers via fiber optic cables (currently about 20% of telecom towers in India are connected via fiber optic cable, in China PR, USA, South Korea it is 65% - 85%); availability of sufficient resilient, secure and well managed resilient data centers / servers; QoS; network congestion; stable power supply; etc. BharatNet is far behind plans improving the network infrastructure[3]. All these are basic requirements for offering, implementing and operating M2M / IoT (including smart cities, smart grids, etc.), but also for example for roll-out of future 5G mobile networks (latency issues, etc.). Are these weaknesses addressed, progress monitored and how they are handled in compliance with M2M /IoT policy? Who has the "umbrella view" national strategy, regulations, legislation, infrastructure, security, skill development, etc.?

---

[2] The World Economic Forum (WEF): "Global Information Technology Report 2016"
www3.weforum.org/docs/GITR2016/GITR_2016_full%20report_final.pdf

Broadband Commission: "Broadband Annual Report 2016"
www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf

ITU: "Measuring the Information Society Report 2016"
www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf

[3] Telegeography: "Slow progress of BharatNet saw just 29% of budget spent over five year-period"
www.telegeography.com/products/commsupdate/articles/2016/10/21/slow-progress-of-bharatnet-saw-just-29-of-budget-spent-over-five-year-period/