Question 6/20 – Security, privacy, trust, and identification for IoT and SC&C

(Continuation of Question 6/20)

1 Motivation

Towards the information society, there are increases in cyber-attacks, cybercrime, and loss of credit or trust. The ICT infrastructure will evolve to provide converged services and applications by accommodating many Internet of Things (IoT) sensors and IoT-related systems. Additionally, the world is experiencing an evolution of Smart Cities. Many stakeholders from various industries are involved in future converged and intelligent services to be deployed using ICT infrastructure. This heterogeneous environment, while it promises great advances in the way the services and applications are provisioned, and in the way systems are managed, administered, and maintained, yet comes with a very wide range of sector-specific risks and threat vectors. Implications for security, privacy[1] and the overall trust of use, adoption, and proliferation of IoT, and smart city devices, systems, services, applications, and platforms could hinder its overall market development. Therefore, it is important that security and privacy concerns are taken into account throughout the design process of products and systems to be used in IoT implementations commonly known as privacy by design and security by design, which emphasize that protection be built into information technologies, business practices, systems, processes, physical design, and networked infrastructure.

The satisfaction of security and privacy requirements plays a fundamental role in the IoT environment and SC&C. Such requirements include data confidentiality and authentication, access control within the IoT network, availability, data integrity, privacy and trust among users and things, and non-repudiation.

Some security measures may not always be directly applied to IoT technologies. Moreover, the high number of interconnected devices raises scalability issues when applying security techniques; therefore, flexible infrastructures are needed, to deal with security threats in such environments. ICT infrastructures should be reliable, safe, confidential, and trustworthy. Therefore, security, privacy and trust provisioning for IoT is one of the outstanding standardization issues of the ITU-T SG20.

On the other hand, various identification technologies have always been regarded as an important enabling technology for IoT implementation. Both physical devices (such as tagged items and products, sensing devices) and virtual entities (such as computational processes, software) could be, or already are, assigned identifiers, in order to be identified and distinguished. It is important for each thing to be addressable, and identifiable in order to tackle, inter alia, privacy, security, trust, and network reachability issues in IoT deployments.

Taking into account the variety of devices, systems, services and applications within IoT and SC&C domains, it is essential to develop trustworthiness models that ensure all physical and virtual things involved are trusted enough to be part of IoT and SC&C environment. Such models should be integrated within IoT and SC&C architectures while defining the set of rules to ensure implementation of trusted IoT systems. The security and trustworthiness architectures should be substantial part of any E2E architectures developed for IoT and SC&C verticals and use-case.

In addition, the adoption of new technologies such as block-chain, big data, quantum computing, machine learning and artificial intelligence (AI) can play important role in developing advanced cost-effective measures and mechanisms to create such trustworthy environment within IoT and SC&C domains.

All above requirement need to be carefully analysed for various IoT verticals and use-cases that may require specific additional demands due to its nature and underlying standards used for IoT and SC&C devices, systems, applications, protocols, platforms, and services.

[1] Consistent with WTSA Resolution 2 (Rev. Geneva, 2022)

2 Questions

Study items to be considered include, but are not limited to:

- What are the possible threats against the compromise of authenticity, confidentiality, integrity, non-repudiation, and availability of IoT and SC&C devices, systems, applications, protocols, platforms, and services?
- What is needed to mitigate and counteract the risks and threats identified in IoT and SC&C systems, and services?
- What are the identification systems capable of fulfilling the requirements of IoT and SC&C including security, privacy and trust?
- What are the requirements and mechanisms for protecting, and preventing disclosure of things' information?
- How can authentication technologies work with identification systems?
- How can security measures be applied in IoT devices to protect identity, privacy, and security of the system, given that the device's environment and resources may be constrained?
- What technical measures are needed to support the protection of privacy in SC&C applications, services, and platforms? How can trust be maintained and supported for the use of such systems?
- What measures can be taken to prevent compromise and protect the integrity and privacy of IoT systems, applications, platforms, and services?
- How to create trustworthiness in IoT & SC&C devices, systems, applications, protocols, platforms, and services?
- How to ensure security, privacy and trustworthiness in data related to IoT & SC&C as well as the relevant data planforms?
- How can block-chain based technologies and mechanisms support security and trustworthiness in IoT & SC&C?
- How to use machine learning and artificial intelligence (AI) technologies for supporting secured interoperability and trustworthiness in IoT & SC&C?
- How can quantum technologies support security and trustworthiness in IoT & SC&C?
- How to apply big data techniques for enhancing security and trustworthiness in IoT & SC&C?
- How Public Key Infrastructure can enhance authentication mechanisms and communication trustworthiness in IoT and SC&C
- What measures can be developed or used to assist with availability and portability of the data in IoT and SC&C platforms, systems, and services?
- What options or measures are available for identification of IoT objects, including non-IP based and non-web-based objects in a heterogeneous IoT system, for SC&C?
- What are identification systems and mechanisms that can be used to support IoT and SC&C?
- How can identification mechanisms support interoperability in IoT and SC&C and mitigate risks?
- How to ensure security and trustworthiness in the interactions through Application Programming Interfaces (API)?
- What options and mechanisms may be used for registering and managing IoT identifiers when appropriate?

- What are the appropriate technical measures needed for identity discovery?
- Which standards development organizations (SDOs), consortia and forums would it be necessary to collaborate with to maximize synergies and harmonize existing standards?

3 Tasks

Tasks include, but are not limited to:

- Developing Recommendations, Reports, Guidelines, etc. as appropriate on:
  - authenticity, confidentiality, integrity, non-repudiation, and availability of IoT devices, systems, applications, protocols, platforms, and services;
  - security and trust provisioning in IoT both at the ICT infrastructure and future heterogeneous converged service environments;
  - security and trust provisioning in IoT services and applications for converged environments among stakeholders of different industries;
  - requirements to mitigate the risks and threats identified in IoT and SC&C systems and services;
  - utilizing security constructs in IoT systems to protect identity, privacy, and security of the system;
  - technical measures to prevent compromise, and protect the integrity and privacy of IoT systems, applications, platforms, and services;
  - technical measures needed to support the protection of privacy in SC&C applications, services, and platforms;
  - identifying the potential risks associated with the different management, administration, maintenance, and service provisioning in SC&C;
  - how to mitigate risks associated with the different management, administration, maintenance, and service provisioning in SC&C;
  - supporting availability and portability of the data in IoT and SC&C platforms, systems, and services;
  - the use of naming, addressing, and identification in IoT and SC&C deployments;
  - identity discovery and identity management in IoT and SC&C;
  - methodologies to create trustworthiness in IoT & SC&C devices, systems, applications, protocols, platforms, and services;
  - security and trustworthiness in using Application Programming Interfaces (API);
  - block-chain based technologies and mechanisms to support security and trustworthiness in IoT & SC&C;
  - machine learning and artificial intelligence (AI) technologies for supporting secured interoperability and trustworthiness in IoT & SC&C;
  - quantum computing mechanisms to support security and trustworthiness in IoT & SC&C;
  - big data techniques for enhancing security and trustworthiness in IoT & SC&C;
  - security architectures for IoT and SC&C;
  - security, privacy and trustworthiness of Data and relevant platforms in IoT and SC&C.
- Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme (https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&q=6/20).

4 Relationships

WSIS Action Lines:

- C5

Sustainable Development Goals:

- 11 and 17

Recommendations:

- Y.4000-series and other Recommendations related to security, privacy, trust and identification

Questions:

- All Questions of ITU-T SG20

Study Groups:

- ITU-T (e.g., considering their lead study group role), ITU-D and ITU-R Study Groups, as appropriate
- This Question will collaborate with ITU-T SG2 and ITU-T SG17 on identification aspects of IoT as per the mandate of each study group.
- This Question will collaborate with ITU-T SG17 on security, privacy and trust issues relating to IoT and SC&C as per the mandate of each study group.

Other bodies:

- ETSI
- ENISA
- AIOTI
- IEEE
- 3GPP
- W3C
- ISO/IEC JCT 1
- Joint IEC-ISO-ITU Smart Cities Task Force
- IETF
- OASIS
- oneM2M