IoT Week 2022

The Role of IoT Standards to help resolve Security Issues.

Rana Kamill, IoT Ecosystems Architecture Solution Manager, BT.

11/10/2022

The growth of IoT

As the world becomes more connected, the number of connected devices is starting to exceed the world's mobile phone population. This wave of hyperconnectivity is transforming the way we live and work. The number of worldwide M2M connections is growing exponentially with some forecasts as high as 50 billion connected devices by 2025.

Various industries from healthcare to transportation and energy to agriculture can benefit from the economic growth and innovation opportunities that M2M communication offers. Standards for the Internet of Things are needed to make innovation more accessible and cost-effective and to turn ideas into scalable solutions that everyone can make the most of.

The growth of IoT

IoT growth has an influence on the way we live and work in various domains such as connected vehicles, eHealth, home automation and energy management, public safety and industrial process control, and smart cities.

The more things are connected, the greater the security risk. So, security standards are also needed to protect the individuals, businesses and governments which will use the IoT.

IoT Security Challenges

One of the challenges in IoT security is the proliferation of connection standards, device operating systems and, use cases. Security has to work across a large number of permutations. IoT users need a standardized and systems-based approach which forms the basis for efficient mixing-and-matching of systems and devices.

Standardization allows better Interoperability. It allows devices and system to work together, making the products work more seamless and efficiently and also more user-friendly for end-users. It creates competition among vendors manufacturers, which reduces prices and gives consumers more choices.

IoT Security Challenges

Most IoT devices and application operate as unattended applications. Designing IoT devices calls for a different mindset to working with human users in the loop, as is common in telephony and many enterprise IT systems, for example. Many security functions that might usually be carried out through human intervention can be automated.

In the IoT scenario, it is important to Detect and eliminate vulnerabilities in IoT components at the outset. Ensuring that security is embedded in designs at the outset .

A very large amount of data can be collected through IoT devices. It is important to make sure that all data is collected, stored, processed, and transferred securely

IoT Security Challenges

IoT devices generally operate with long service lifecycles. There may be limited scope for access or physical replacement. In contrast, user expectations move as fast as the consumer market.

Many of IoT systems are legacy/ older systems which do no receive regular patches and software updates, making the systems vulnerable to new attacks.

Security therefore needs to bridge these timing differences. This requires life-cycle management and cost-efficient security management tools which can be achieved through standardization.

Standardizing IoT

Smart objects produce large volumes of data. This data needs to be managed, processed, transferred and stored securely.

Standardization is key to achieving universally accepted specifications and protocols for true interoperability between devices and applications.

It helps develop cost effective solutions and help make the ecosystem safer and more efficient for consumers.

It opens up new business opportunities in new areas and collaboration possibilities in different markets.

Various applications of IoT/M2M technology addressed in ETSI

• Smart Cities- including networking, energy efficiency and accessibility.

• Smart Energy, Smart Environment, Smart Building, Smart Industry and Manufacturing, Smart Agri-Food, eHealth and Ageing-Well, Wearables, Smart Water, Smart Lift and Smart Escalators.

•Smart appliances.

•Smart grids and meters.

Various applications of IoT/M2M technology addressed in ETSI

- eHealth
  - Telemedicine and the Internet Clinic.
  - Medical implants.
  - Body Area Networks.
  - Pandemic protection, contact tracing.

- Intelligent Transport Systems – including telematics and all types of communications in vehicles, between vehicles and between vehicles and fixed locations. We also address the use of Information and Communications Technologies for rail, water and air transport, including navigation systems.

- Wireless Industrial Automation – standards for radio equipment to be used in factories

ETSI Roles and Actives

The main ETSI IoT standardization activities are conducted at radio layer in 3GPP (LTE-M, NB-IoT and EC-GSM-IoT) and at service layer in oneM2M. A wide range of technologies work together to connect things in the Internet of Things (IoT). ETSI is involved in standardizing many of these technologies.

Smart Machine-to-Machine (M2M) communications

ETSI is one of the founding partners in oneM2M, the global standards initiative that covers requirements, architecture, Application Programming Interface (API) specifications, security solutions and interoperability for M2M and IoT technologies.

IoT Semantic Interoperability

SAREF is our **S**mart **A**pplications **REF**erence ontology that allows connected devices to exchange semantic information in many applications' domains.

Context Information Management (NGSI-LD)

ETSI SG CIM specifies protocols (NGSI-LD API) running 'on top' of IoT platforms and allowing exchange of data together with its context, this includes what is described by the data, what was measured, when, where, by what, the time of validity, ownership, and others. This is dramatically extending the interoperability of applications, helping smart cities (and other areas such as Smart Agriculture and Smart Manufacturing) to integrate their existing services and enable new third-party services.

Example: oneM2M

The challenge of designing effective security solutions for IoT systems has to be situated in the context of a generalized architecture that captures as many use-cases as possible.

oneM2M Partnership Project embarked on a goal of defining the standard for IoT systems in 2012.T his was done with the support of several, national standardization bodies that sought to avoid regional variations and promote a global IoT market on a par with the cellular industry.

Through an analysis of multiple IoT use-cases across different industry verticals, research and commercial representatives identified the elements of a distributed architecture and a set of common services functions involved in deploying IoT systems.

A global partnership among SDOs and Industry Associations/Fora.

Main goal:

- Interoperability.
- Cost-effectiveness / economies of scale.
- Reduced fragmentation.
- Larger market.

Open and transparent: all working documents are public. All deliverables available free of charge.
Detailed scope at http://www.onem2m.org

- Global footprint established through regional presence.
- ETSI is the partner in Europe, your contact point to get involved in oneM2M.
- International recognition with transposition by ITU-T under the Y.4500 series.

oneM2M ITU-T Collaboration

In parallel with standardizing a family of security capabilities for IoT systems, oneM2M is transposing its Security specification TS-003 into an ITU-T SG20 Y series for M2M Security and Privacy protection.

ITU standards are referenced by many countries, government states and corporations. The collaboration between oneM2M and the ITU is therefore very important for establishing common standards that benefit the widest community.

Securing IoT Ecosystems

As long as the IoT Ecosystem continues to grow, security will continue to be a challenge. Standards bodies continue to work on resolving security issues and through collaboration and continuous work from researchers and subject matter experts from all over the world. The standards community stives to develop the best standards to keep IoT ecosystems, users and networks safe.

Thank you!

Questions?

Please email rana.Kamill@bt.com