Orchestrating a brighter world NEC

[NEC Group Internal Use Only]

IoT Security

- Challenges & Standardization status

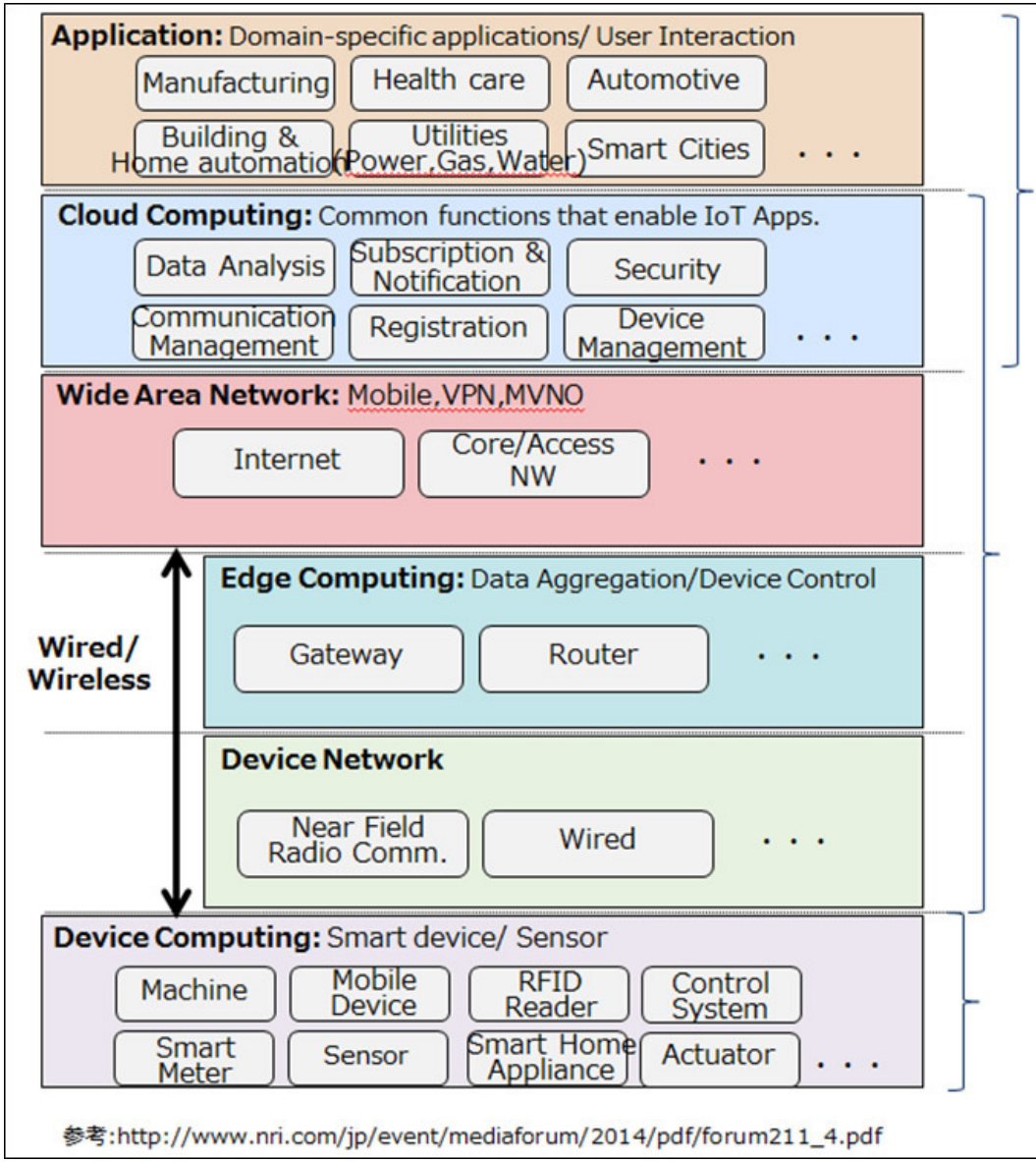
Sivabalan Arumugam

<sivabalan.arumugam@necindia.in>

Outline

- IoT Security Overview
- IoT Security Challenges
- IoT related Threats
- Elements of a Protection Architecture for IoT
- IoT Security Standards
- IoT Security Standards at each Layers
- IoT Security Life Cycle
- Summary

IoT Security Overview



参考:http://www.nri.com/jp/event/mediaforum/2014/pdf/forum211_4.pdf

Linkage with other systems

IoT systems need to work with many other systems such as SCM, CRM, etc.

Secure Data Exchange/ Synchronization between systems

Data Processing at Edge/Device Computing Layer

In order to support numbers of device and ensure near real-time response, many common functions used to be provided at the server might be executed at Edge/Device Layer.

Secure and Real-time Data Linkage

Security for resource-constrained devices

Some devices may lack the capability to perform cryptographic intensive operations and implement lightweight authentication protocols

Endpoint security functions

Secure boot attestation, Remote SW update, Authentication, Access Control, Logging, Data Protection, Endpoint attack response, ..

IOT Security Challenges(1/2)

- Poorly designed and implemented IoT system, using diverse protocols and technologies that create complex configurations.
- Lack of maturity (eg: business processes, technologies).
- Limited guidance for lifecycle maintenance and management of IoT devices.
- Unique physical security concerns.
- Privacy concerns are complex and not always readily evident.
- Limited best practices available for IoT developers.

IOT Security Challenges(2/2)

- Lack of standards for authentication and authorization.
- No best practices for IoT based incident response activities.
- Audit and Logging standards are not defined for IoT components.
- Restricted interfaces available to interact IoT devices with security devices and applications.
- No focus yet on identifying methods for achieving situational awareness of the security posture.
- Security standards for platform configurations involving virtualized IoT platforms supporting multitenancy is immature.

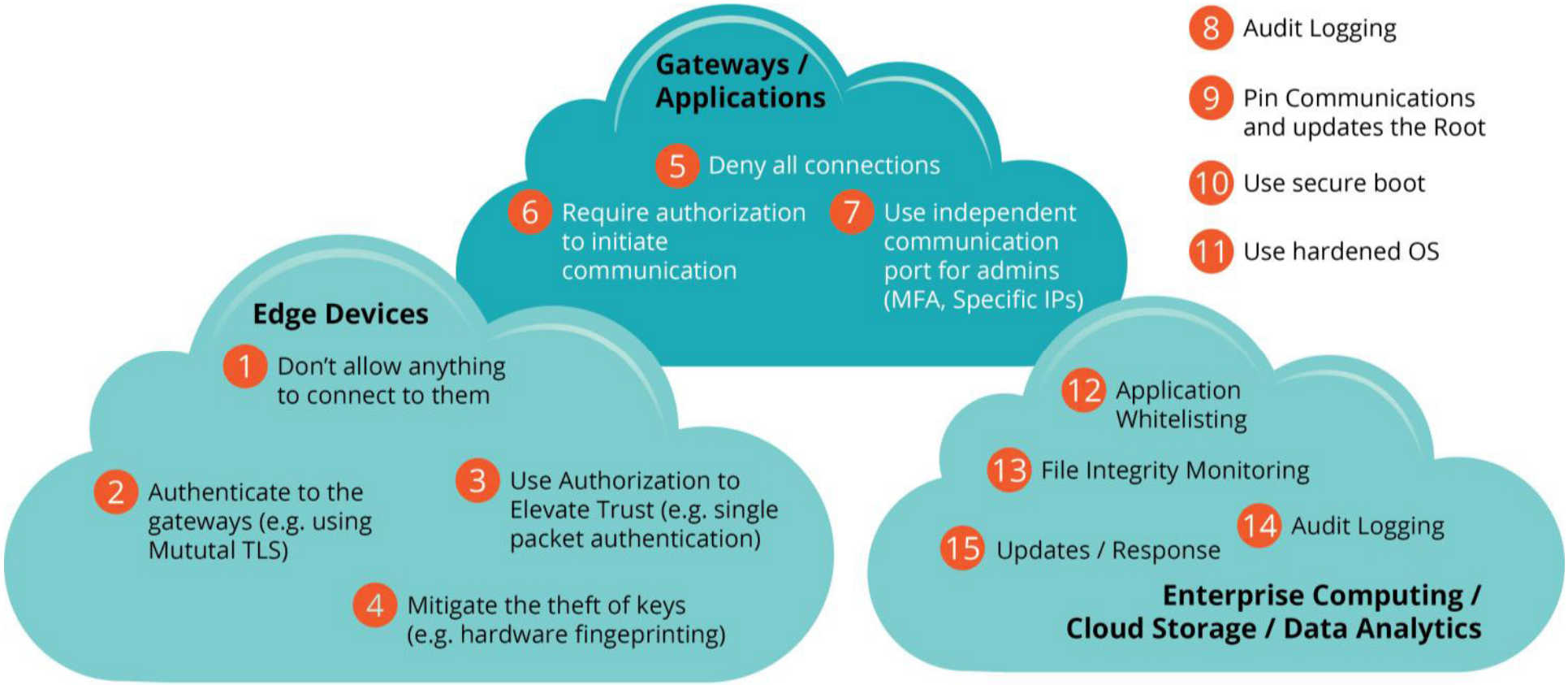
IOT Threats(1/2)

- Control systems, vehicles, and human body can be accessed & manipulated causing injury or worse.
- Health care providers can improperly diagnose and treat patients.
- Loss of vehicle control
- Safety-critical information such as warnings of a broken gas line can go unnoticed
- Critical infrastructure damage can occur
- Malicious parties can steal identities and money
- Unanticipated leakage of personal or sensitive information can occur
- Unauthorized tracking of people’s location behaviors and activities

IOT Threats(2/2)

- Unlawful surveillance
- Inappropriate profiles and categorizations of individuals can be created
- Manipulation of financial transactions
- Vandalism, theft or destruction of IoT assets
- Ability to gain unauthorized access to IoT edge devices and Enterprise network
- Ability to create botnets
- Ability to impersonate IoT devices Unknown fielding of compromised devices

Elements of a Protection Architecture for IoT



IoT Security Standards

An unfortunate characteristic of the current state of the IoT is the lack of standardization across all aspects of the IoT.

But still some standards exists such as

- oneM2M
- 3GPP-MTC
- IEC/TC65, IEC-MSB
- NIST
- NISC
- IoT Acceleration Consortium
- CSA

oneM2M

Release1:

- Released global standards (specification) for deployment in Feb 2015
- Basic framework for authentication and authorization

Release 2

- Interworking framework across IoT protocols including OMA, OIC and ASA
- New Security functions
  - End-to End Security
  - Group authentication
  - Dynamic authorization
- Release 2 planned for delivery in autumn 2016

3GPP-MTC

- 3GPP-MTC specifies the architecture and API to better facilitate machine type communications.

- Resulting from
  - Short packets
  - Large number of nodes
  - Need to support highly energy efficient protocols

- SA WG3 discusses possible security requirements and the possible solutions including secure connection and triggering security.

- Release 13 discuss about the Light weight authentication process to achieve battery efficiency.
  - Group message protection
  - Location management
  - Security for service capability exposure interface

- Release 13 is planned to be fixed in autumn 2016.

IEC/TC65

- IEC/TC65 focuses on industrial-process measurement, control and automation.

- TC65 covers the specific requirements for security in Industrial automation such as
  - Organisation
  - Process
  - Systems
  - Systems components
- ISA introduces cybersecurity certificate programs based on IEC62443.

- Currently IEC discuss about next generation technologies to achieve safe and secure factory operations.

- IEC develops the white papers relating to smart factory/IOT.

NIST (National Institute of Standards and Technology)

- NIST is a unit of the U.S. Commerce Department.
- NIST specifies and publishes security-related documents, SP800/FPS.
  - Used as guidelines for enforcement of security rules and as legal references
- NIST holds open competitions of cryptography primitives.
- Accepted algorithms are widely used as industry standards.
- Cloud System research laboratories submit their authenticated encryption technology to the competition funded by NIST.

NISC (National center of Incident readiness and strategy for Cybersecurity)

- NISC was established as part of the Cabinet Secretariat to form security policy strategies in Japan

- Goal:
  - To protect the information security of government organisations while improving the overall level of information security in Japan.

- NISC develops draft government standards for information security measures.
  - To perform evaluation based on the draft standards, formulate recommendations based on the evaluation results and promotes responses to the recommendations.

- METI and NISC plan to specify the Cyber-Security management Guidelines for certification program on ISMS certificate in 2015

IoT Acceleration Consortium

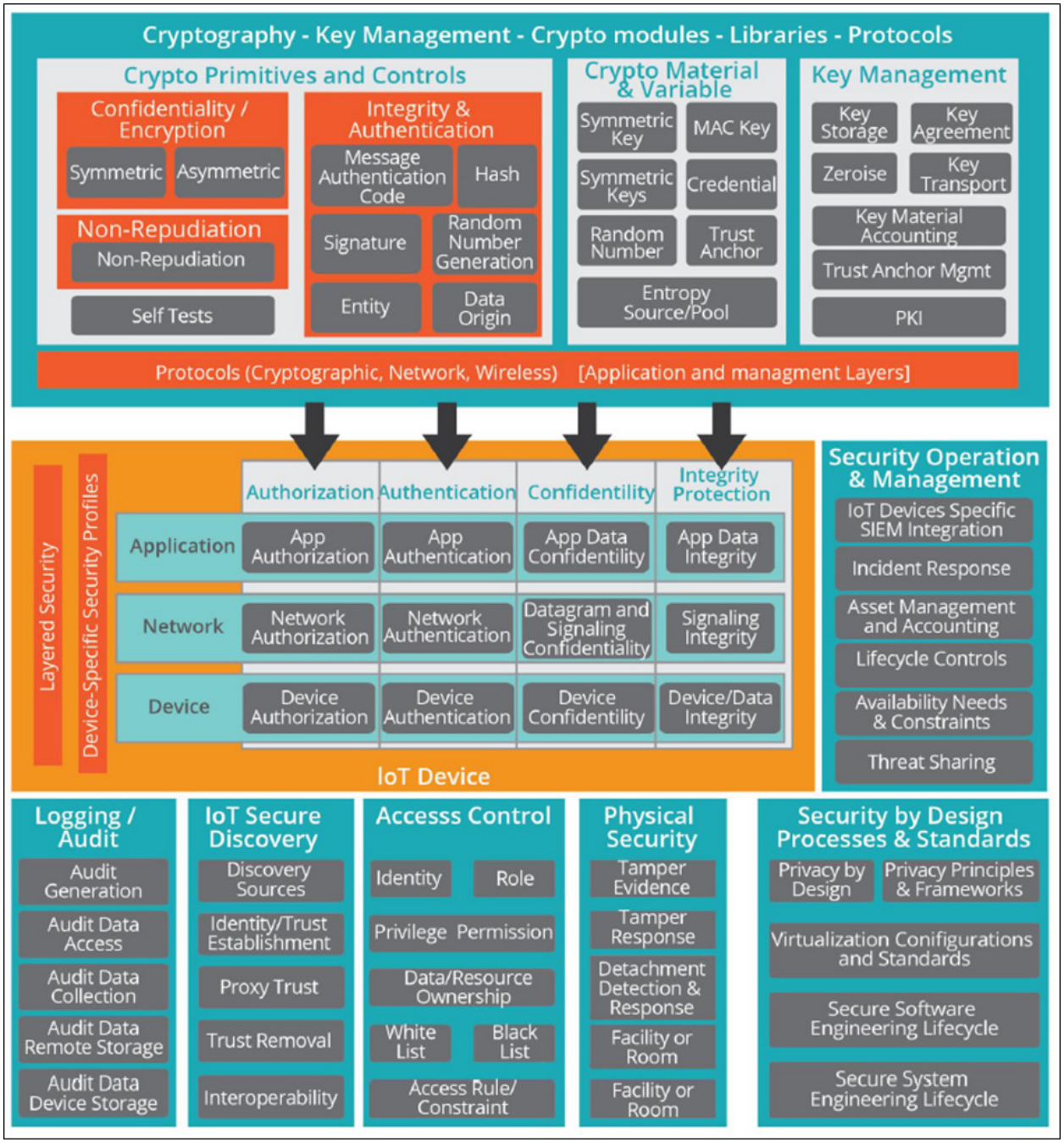
- Aims to combine the strengths of
  - Government
  - Industry
  - Academia
- It build a structure for developing and demonstrating technologies related to the promotion of IoT, as well as creating and facilitating new business mode.

- The Security WG is planned to establish to determine the security policy.

CSA(Cloud Security Alliance)

- It promotes the use of best practices for providing security assurance within Cloud Computing.
- CSA develops the security guidance document to be broad catalog of best practices.
- It operates the popular cloud security provider certification program.
- CSA has launched new security guidance for early adopters of the IoT in April 2015.
- It describes about the key challenges and recommended IoT security controls.

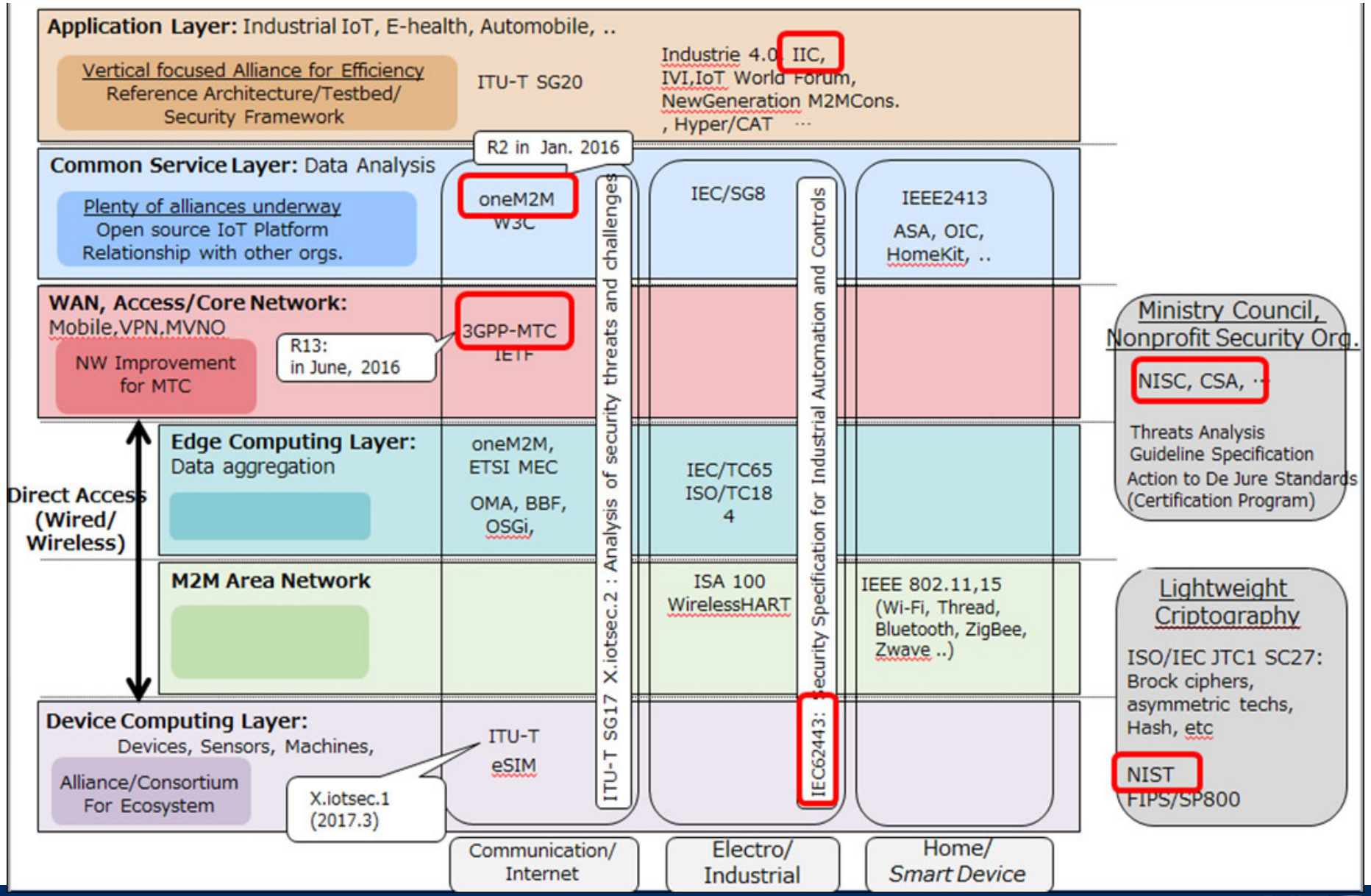
Recommended Security Controls by CSA



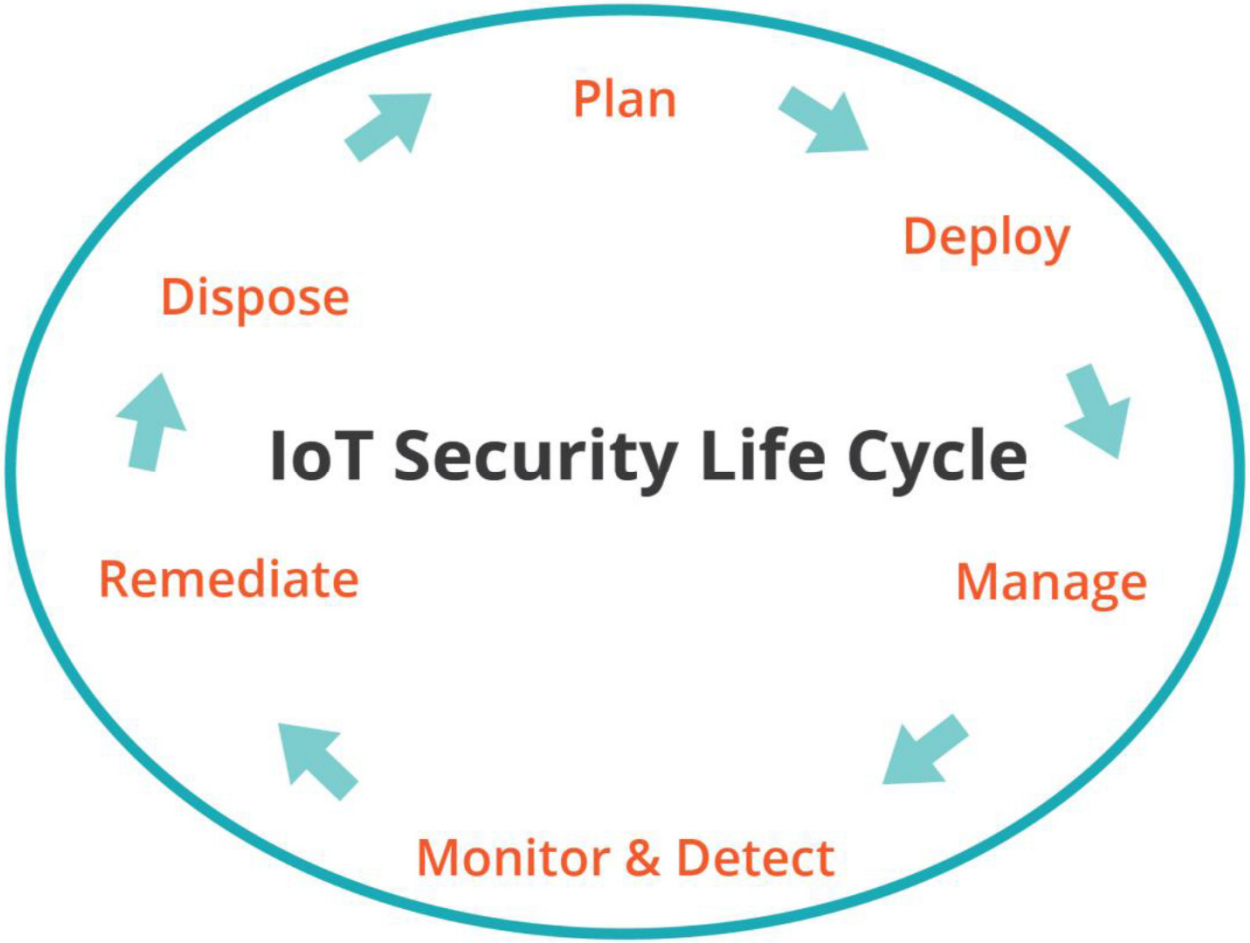
IIC(Industrial Internet Consortium)

- IIC is formed to enable and accelerate creation of the Industrial Internet.
- Not a standard organisation but evaluates existing standards and specifies security and privacy framework based on the open architecture .
- It prepares testbeds to drive new products, processes and services and supports to create ecosystem for new business.
- The Security Working Group defines a security and privacy framework to be applied to technology adopted by the IIC.
- The framework will establish best practices and to be used to identify security gaps in existing technology.
- IIC released Security Framework draft in Oct.2015.

IoT Security Standards at each Layers



IoT Security Life Cycle



Summary

- There many IoT related open security challenges exist
- Since IoT is multi-application/service environments
  - Unified security approach need to be arrived
  - Security need to be considered from the design phase
- IoT Security Life cycle need to be in-place to identify & mitigate the existing and new security

- Collective standardisation effort among different SDOs will make Secure IoT implementation


Orchestrating a brighter world
NEC