Experience on 5G security assessments in Korea (including ITU-T SG17 standardization work)

August 10, 2023

Heung Youl Youm, PhD

Chairman, ITU-T SG17 (Security)

Chairman, Korea 5G security council

Professor, Soonchunhyang University, Korea (Republic of)

Sungchae Park, Ms

Senior researcher, SCH Emerging Cybersecurity Standardization Center, Korea (Republic of)

Contents

- Introduction for 5G network in Korea
- Overview of 5G security council in Korea and its security assessment scheme
- Information security product’s evaluation and certification schemes in Korea
- Security assessment scheme for IoT devices in Korea
- Rapid confirmation scheme for emerging technologies including 5G network equipment
- ITU-T SG17 5G security work
- Concluding remarks

Introduction for 5G network in Korea

Korea (Republic of) to Launch World's First National 5G Networks on April 3, 2019

- Korea launched the world's first nationwide 5G mobile networks.
- The system will bring smartphones near-instantaneous connectivity — 20 times faster than existing 4G — allowing users to download entire movies in less than a second.
- As of March 2023, South Korea had approximately 29.6 million 5G subscribers.

VOA

TECHNOLOGY

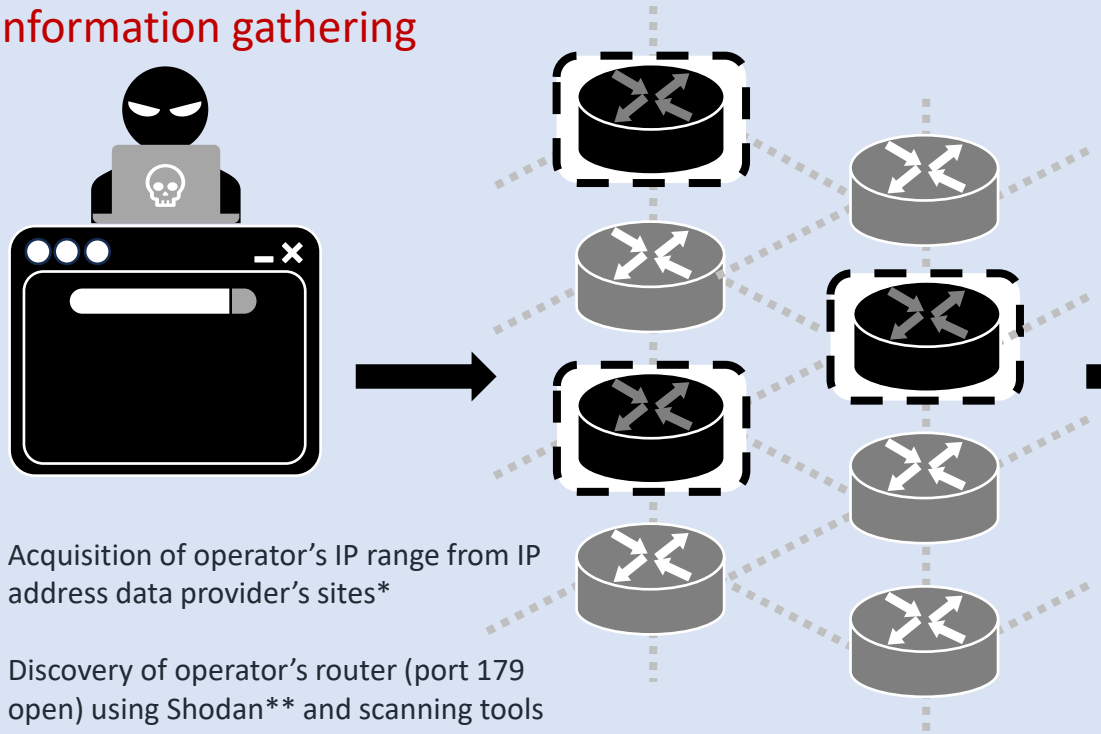
South Korea to Launch World's First National 5G Networks

April 03, 2019 6:39 PM Agence France-Presse

Recent incidents in Korea – DDoS attacks to core network of mobile operator in 2023

- Due to insufficient management, core network's information was exposed to the outside, which became a target for router attacks.
- Nationwide network failure due to DDoS attacks (5 times, 120 minutes) on routers in the broadband network due to insufficient security measures, such as inappropriate operation of access control police and the security equipment (IPS) (Source: KISA)

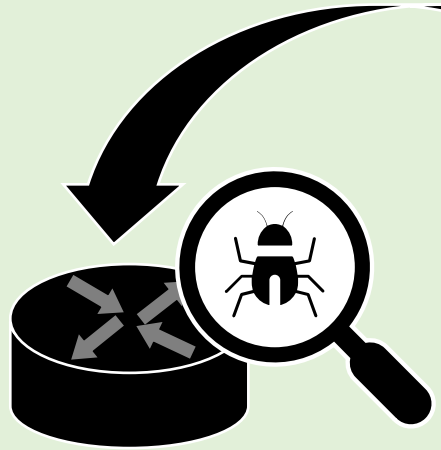
Information gathering



① Acquisition of operator's IP range from IP address data provider's sites*

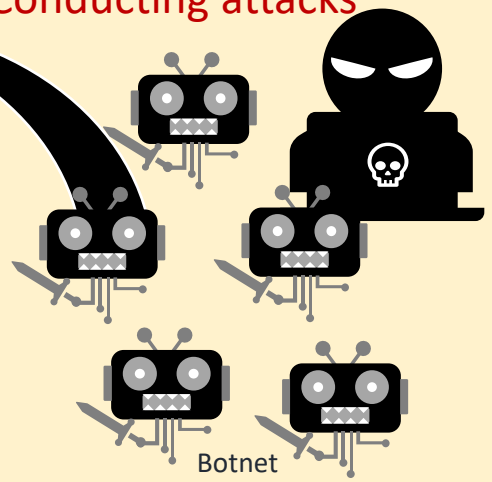
② Discovery of operator's router (port 179 open) using Shodan** and scanning tools

Identifying an attack point



③ Vulnerability check of operator's router 『BGP port*** open (No. 179)』

Conducting attacks



④ DDoS attack carried out against the router with open BGP port (1st, 2nd)

⑤ Additional DDoS attacks (3rd, 4th, 5th)

* National IP address management site and BGP data providing site, etc. (e.g., hxxps://krnic.or.kr/jsp/business/management/isCurrentIpv4.jsp, hxxps://he.net/, etc.)
** Shodan: A search engine that collects information on devices connected to the Internet and provides results, developed for security experts to easily find and address vulnerabilities in devices
*** BGP Port : Boarder Gateway Protocol is a communication protocol for exchanging route data between routers and communicates periodically to update the latest route information.

Overview of 5G security council in Korea and its security assessment scheme

5G security council in Korea

- Objective
  - to identify security issues and develop security measures for safe 5G network implementation, to support the world's first 5G commercialization and expansion strategy
- Established
  - Under the auspicious of Ministry of Science and ICT, Korea (Republic of), in August 2019 (started from November 2018 as 5G security advisory group.)
- The 5G Security Council has
  - three working groups (policy, technology, and standard) were formed, and various stakeholders such as academia, industry, professional organizations, and the Ministry of Science and ICT participated (about 60 people).

Organization of the Korea 5G security council

Ministry of Science and ICT

Steering committee

Policy WG

Secretary: KISA

Analysis of domestic and foreign policy issues related to 5G security and review of policy direction, etc.

Technical WG

Secretary: ETRI

Development and review of technical security requirements for protection of 5G infrastructure and service.

Standardization WG

Secretary: TTA

Development of 5G security standardization roadmap and international standardization activities, etc.

ToR of the 5G security council in Korea

- ToR
  - Identifying and discussing policy issues related to 5G security
  - Policy review and proposals to Government
  - Global networking and information sharing
  - Security checks for 5G network elements in particular, Base Station deployed by 3 local mobile carriers, etc.
- Meetings
  - Each WG meets every quarter.
  - Steering committee meet once a year.

Members of the 5G security council

Ministry of Science and ICT

kt

SK telecom

LG U+

KISA Korea Internet & Security Agency

ETRI

TTA

IITP Institute of Information & Communications Technology Planning & Evaluation

SK shieldus

Penta SECURITY

kani 한국네트워크산업협회 Korea Association of Network Industries

SOON CHUN HYANG UNIVERSITY SCH 순천향대학교

KOREA UNIVERSITY 1905

etc.

Activities of the 5G security council since establishment

- Discussion on 5G security issues
  - Review of overall 5G security issues, including study of security issues in each subdivision, such as 5G security policies, technologies, and standards, and discussions on security enhancement measures
- Security checking
  - Security checking for the 5G Base stations operated by the 3 mobile operators, to check the security and stability and support them to improve through technical consultation.
  - Conducted security checking on the Base Station provided by manufacturers* , which are deployed by three domestic mobile carriers (SKT, KT, LGU+)

    * Samsung, Nokia, Ericsson, Huawei
  - Support for development and improvement of 5G security checking items*, on-site security checking and identification of supplementary items

    * A total of 116 checking items (54 items in the equipment security functions area, 62 items in the equipment operation management area).

- Global Cooperation
  - Hosted a global 5G security workshop to share experience for 5G security issues, response directions and threat response with overseas carriers (2021)

    ※ Held with 4 global operators: Orange (France), KDDI (Japan), Telus (Canada), and Deutsche Telekom (Germany)
- Response to 5G security issues
  - Respond to 5G security issues raised by the Media in relation to the introduction and use of equipment for building 5G networks according to international issues (frequently).

Security checking criteria for 5G Base Station (116 items)

- Items for checking security functions (54)
  - Identification and authentication (9)
    - Mandatory change of default administrator password
    - Secure password setting function …
  - Secure session management (3)
  - Equipment self diagnosis (11)
  - Access control (8)
  - Transmission data protection (4)
  - Audit record (11)
    - Safe storage and management of audit data …
  - Service management (8)
    - Disable unnecessary services

- Items for checking operation (62)
  - Account management (19)
  - File and directory management (4)
  - Service management (31)
  - Log management/security patch/back-up file (7)
    - Secure patch: To check if this security patch uses the integrity verification function when distributing product updates such as equipment firmware (OS) and patches
  - Human/physical security (1)

Review of self assessment report by the 5G security council

- Self assessment conducted by the mobile operators in Korea in support with the team from the Council, and reports of their assessments are submitted and reviewed by the 5G security council.
- Assessment Target: 5G Base Stations (known as Data Unit)
  - Produced by Samsung, Nokia, Ericsson, Huawei
- Several vulnerabilities were identified by the security check, such as vulnerabilities for:
  - Mandatory change of default administrator's password
  - Integrity verification function when distributing updates such as equipment firmware
- Each manufacturer was asked to treat them for their product.

SAMSUNG NOKIA ERICSSON HUAWEI

Future for the assessment for 5G network equipment in Korea

- Plan to consider expanding the evaluation targets to cover all 5G network elements in core network, radio access network, etc., taking into consideration GSMA Network Equipment Security Assurance Scheme (NESAS) by GSMA.
- Plan to continue updates to the security checking criteria of the 5G Base Station, etc.
- Consider the security assessment scheme for IoT devices started December 2017 and Rapid confirmation scheme for equipment's for new and emerging technologies started in 2023.

Information security product's evaluation and certification schemes in Korea

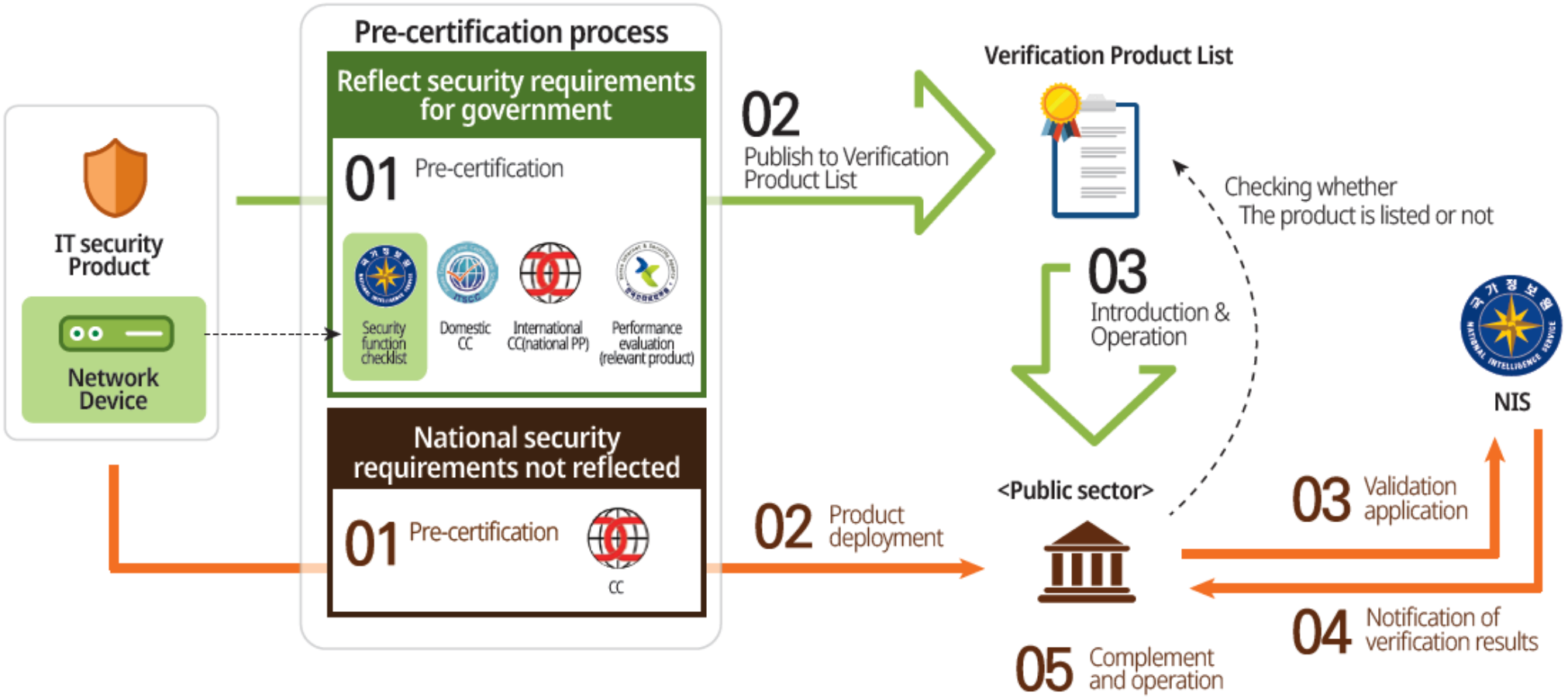
Security conformity verification scheme in Korea

- A scheme to verify the security of IT products with security functions which are introduced by national and public institutions in Korea. There are certification schemes to support this SCVS:
  - Domestic and international CC scheme
  - Security function confirmation scheme
  - Performance evaluation scheme scheme
  - Rapid confirmation scheme (recently started)
- Introduction policy
  - National and public institutions are categorized into 3 groups: Top class(A), Medium class(B), and Low class(C).
  - Organizations belonging to A group can introduce only IT products that have obtained a certificate from CC scheme, security function confirmation scheme, and performance evaluation scheme.
  - Organizations belonging to B group can introduce only IT products that have obtained a certificate from CC scheme, security function confirmation scheme, performance evaluation scheme and rapid confirmation scheme.
  - Organizations belonging to C group can introduce IT products by their own decision.

IT product deployment to national and public institutions

- Government and public institutions may deploy the information security and data communication products in accordance with Article 20 of the 「Basic Guidelines for National Information Security」.
- The followings are the products that satisfy the requirements: the products registered on the safety verification product list through pre-accredited certification tests such as CC certification, security function confirmation, and performance evaluation, and the products that did not comply with national security requirements but obtained CC certification.
- Deployment of products registered on the verification product list confirms that the organization or institute does not need the additional requirement for information security certification.
- However, other products must undergo the process of information security verification before actual deployment and operation.

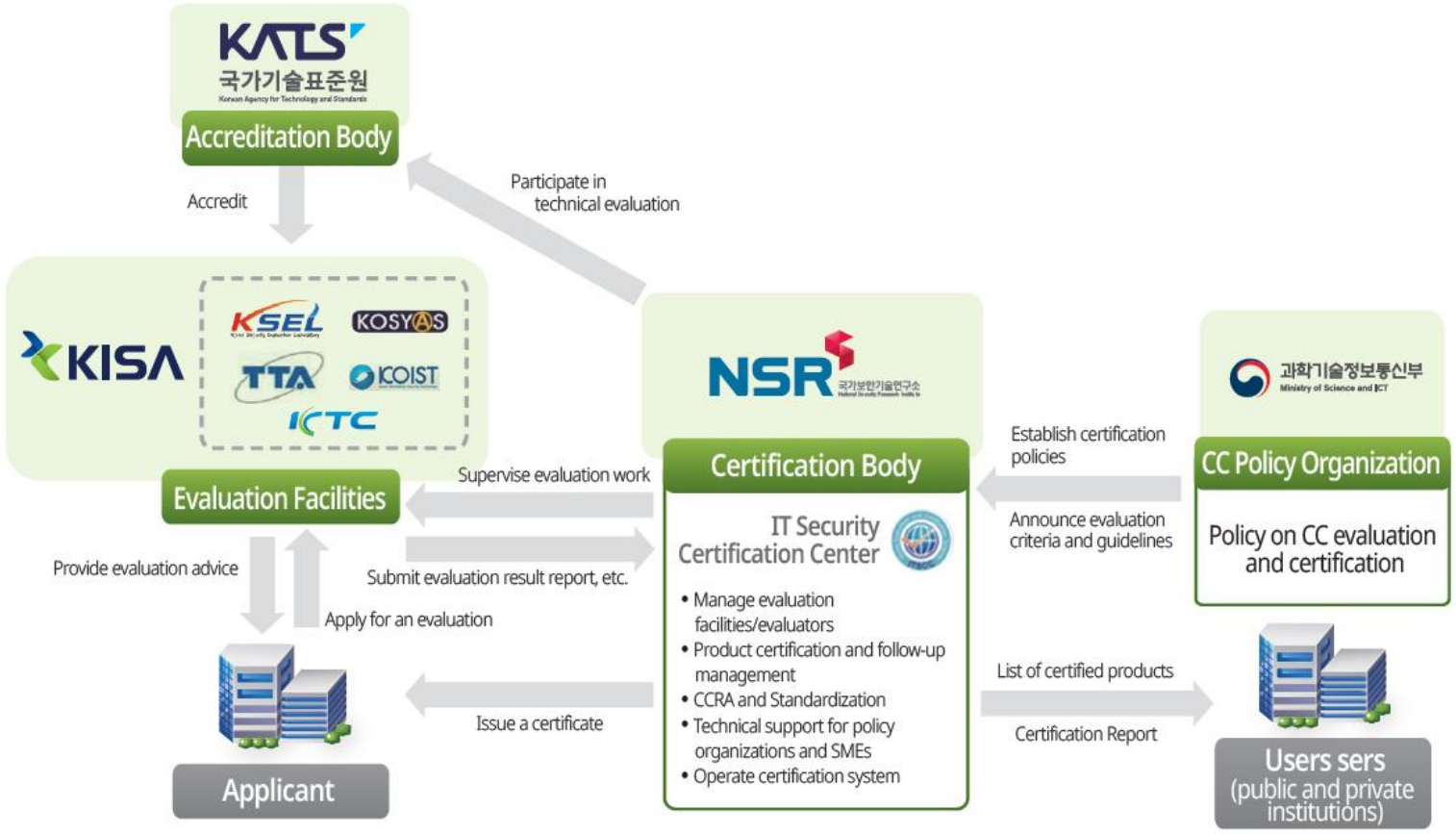
Procedures for introducing IT products by national and public institutions



(Source: White Paper on Information security in Korea in 2022)

Organization of the Information security product's evaluation and certification scheme

- Using Common Criteria (CC), ISO/IEC 15408
- 7 evaluation assurance levels (EAL #1 – EAL #7)
- Examples of Information security products
  - Firewall, Web-firewall
  - Intrusion detection sustem
  - VPN, NAC
  - Spam filter, Host data leakage provention
  - Patch management system
  - Anti-malware system
  - Switch
  - Quantum key management system



(Source: White Paper on Information security in Korea in 2022)

Rapid confirmation scheme for emerging technologies including 5G network equipment

Rapid confirmation scheme (RCS) introduced in 2022

Objective

> “In the existing information security product certification system, to allow entry of new technology and convergence/complex products with no evaluation criteria into the public market”

Scheme overview

Background

Market entry regulation + **Identify business difficulties**

Establishment of a rapid confirmation scheme as an improvement plan for the existing information security product certification system

Rapid confirmation scheme

Notice on information protection system evaluation and certification, etc.” (Ministry of Science and ICT) Article 18-2

“A system that promptly reviews security, etc. based on vulnerability checks, software security weakness diagnosis, and function test results for new technologies and convergence/complex products that cannot be evaluated because national security requirements or national protection profiles are not in place.”

Benefits

Enabling startups or SMEs with new and emerging products to be entered into the public sector, strengthening competitiveness in the information security industry

Security check and function testing in RCS

Security check

- Vulnerability Analysis Evaluation and Software Security Weakness Diagnosis
- Initial inspection test → Complementary measures by company → Implementation inspection test

Security check agency (Notice article 107)

Information security professional service company	Information system supervision corporation
Information security system evaluation agency (CC evaluation agency)	Software Quality Certification Authority (GS Certification Authority)

Function testing

* can be replaced by the GS certificate

- Normal implementation and operation test for major functions (50% of all functions) among all functions

Functional testing agency (Notice article 109)

KOLAS Authorized Testing Institution

Meet requirements in ISO/IEC 25051	Meet requirements in ISO/IEC 25023

Security certification scheme for IoT devices in Korea

Security certification scheme for IoT devices

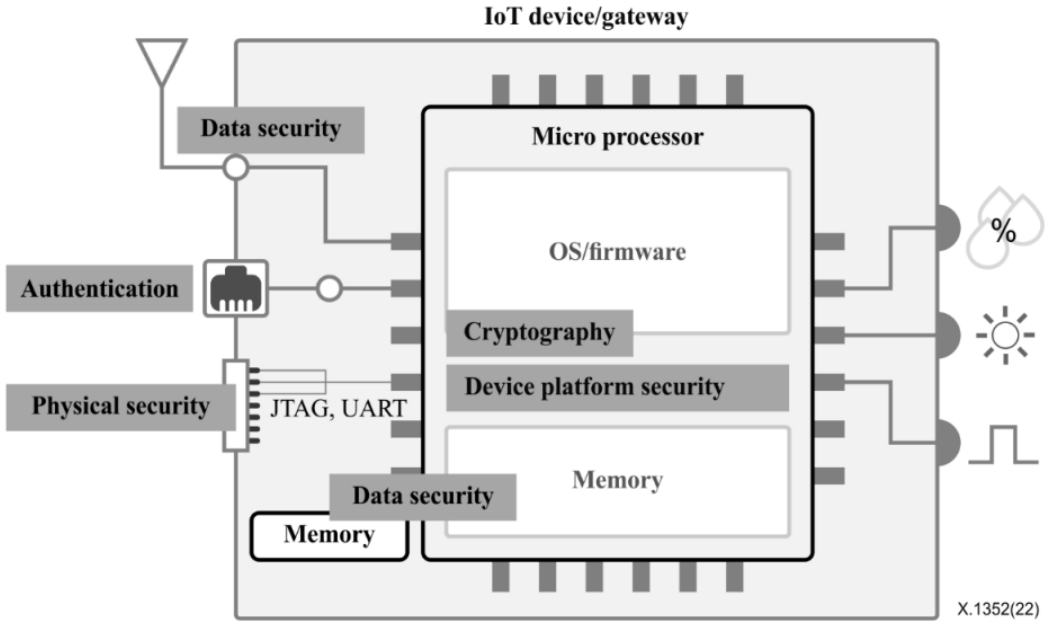
- Overview
  - A scheme to issue a certificate by testing whether IoT products are suitable for information protection certification standards
- Objectives
  - Strengthening the safety of citizens and industrial competitiveness through the operation of the security certification system for IoT devices due to the increase in security threats due to the expansion of the market

- Target of assessment
  - IoT products and mobile apps that work with the products

    * A generic term for devices (including modules) that perform functions such as detection, control, relaying, filming, management, and operation by being connected to a systematically and organically configured network.
- Assurance levels
  - Lite
  - Basic
  - Standard

Example for applied security dimensions on IoT devices and gateways

- In Recommendation ITU-T X.1352 Security requirements for Internet of things devices and gateways,
  - five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security.



Organization for IoT security assessment scheme

Policy agency

Ministry of Science and ICT

Certification agency

KISA Korea Internet & Security Agency

Testing agency

TTA

KTC 한국기계전기전자시험연구원 Korea Testing Certification institute

Testing and certification criteria

7 certification testing areas such as Identification and authentication, data protection, cryptographies, software security, update and technical support, operating system and network security, hardware security

Certification criteria for IoT security assessment

Areas	Components for assessment
Identification and authentication	Use of secure authentication information, user authentication and authority management, restriction of unauthorized mutual authentication, restriction of repeated authentication attempts, prevention of information exposure, safe session management
Data security	Protection of transmitted and stored data, strengthening protection of important information storage areas, legal compliance with personal information, complete deletion of critical information
cryptographies	Use of secure cryptographic algorithms, secure cryptographic key generation, secure cryptographic key management, and secure random number generation
Software protection	Secure coding, source code obfuscation, software security function testing, measures for known vulnerabilities, removal of unnecessary functions and codes, software application security, audit records
Updates and technical support	Check model name and product information, perform safe update, guarantee update file security, recover when update fails, update technical support, provide update information, provide automatic update function
OS and network security	Apply operating system security, control unnecessary accounts/services/ports, disable unnecessary network interfaces, verify integrity of executable code and configuration files, restore system in case of failure, respond to denial of service attacks, protect operating system functions, minimize access rights, block unauthorized software installation/execution, remote access/network traffic control
Hardware security	Safe booting and self-test, self-test failure response, hardware failure response, unauthorized damage prevention, side-channel memory attack response, non-volatile memory protection, external/internal interface protection

Note - Certification criteria is compatible with ITU-T X.1352.

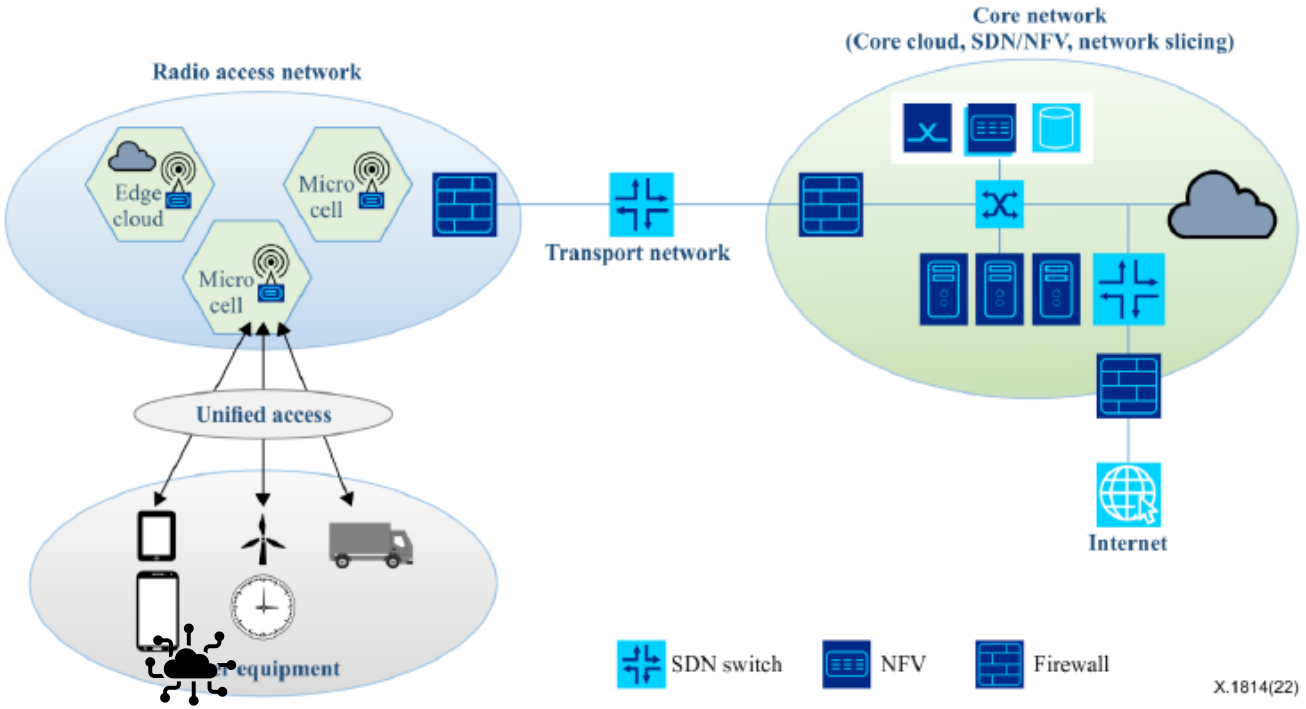
ITU-T SG17 5G security work

ITU-T Recommendations approved for 5G security

- X.1811, Security guidelines for applying quantum-safe algorithms in IMT-2020 systems
- X.1812, Security framework based on trust relationship for the IMT-2020 system
- X.1813, Security and monitoring requirements for operation of vertical services supporting URLLC in IMT-2020 private networks
- X.1814, Security guidelines for IMT-2020 communication system
- X.1815, Security guidelines and requirements for IMT-2020 edge computing services
- X.1816, Security guidelines and requirements for classifying security capabilities in IMT-2020 network slice

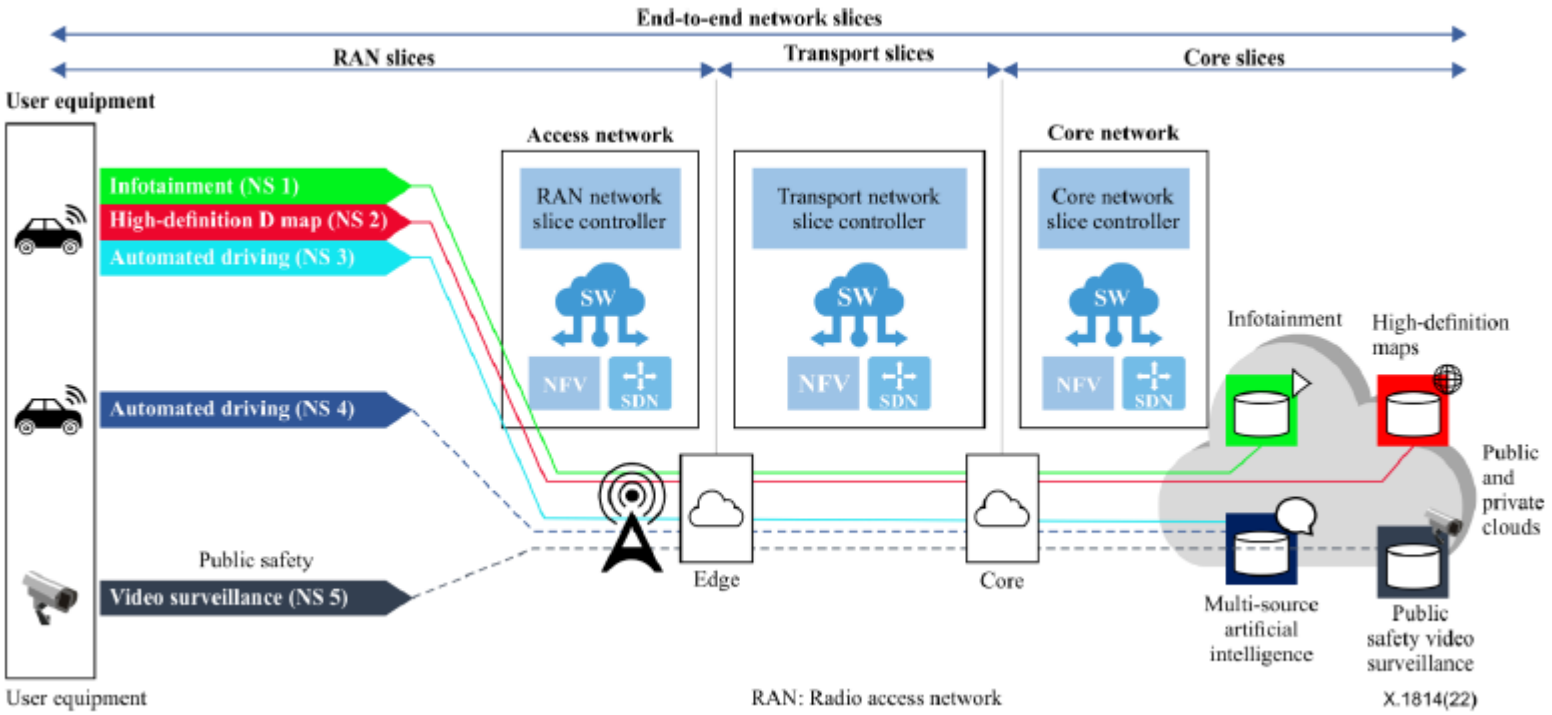
IMT-2020 communication network

- IMT 2020 network in X.1814
  - User equipment including IoT devices
  - Radio access network
  - Core network



IMT-2020 network slices

- End-to-end network slides in X.1814
  - RAN slice
  - Transport slice
  - Core slice



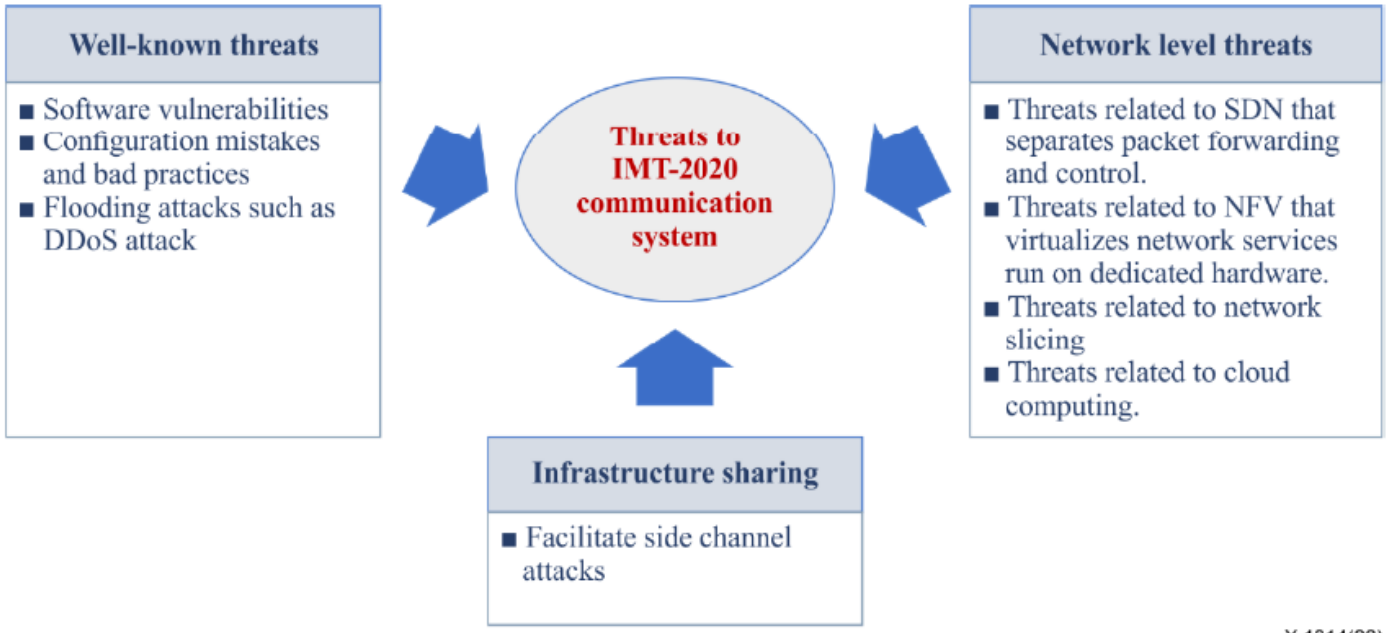
Impact of quantum computing on common cryptographic algorithms and Quantum-safe cryptographic algorithms in X.1811

Cryptographic algorithm	type	use	impact
AES	Symmetric	Encryption	Large key sizes is needed
SHA-2, SHA-3	Hash	Hash function	Larger output is needed
RSA	Public key	Signature, key transport	No longer secure
ECDSA, ECDH	Public key	Signature, key exchange	No longer secure
DSA	Public key	Signature, key exchange	No longer secure

- Quantum-safe symmetric key algorithms
  - basic symmetric cryptosystems with increased key length , such as block ciphers or hash functions are quantum-safe algorithms
- Quantum-safe asymmetric key algorithms
  - Lattice-based algorithms
  - Hash-based algorithms
  - Code-based algorithms
  - Multivariate algorithms
  - Super singular isogeny-based algorithms

Threats for IMT-2020 systems in X.1814

- Generic threats
- Threats to user equipment
- Threats to access network
- Threats to SDN
- Threats to core network
- Threats to network slices
- Threats to network function virtualization
- Threats to management

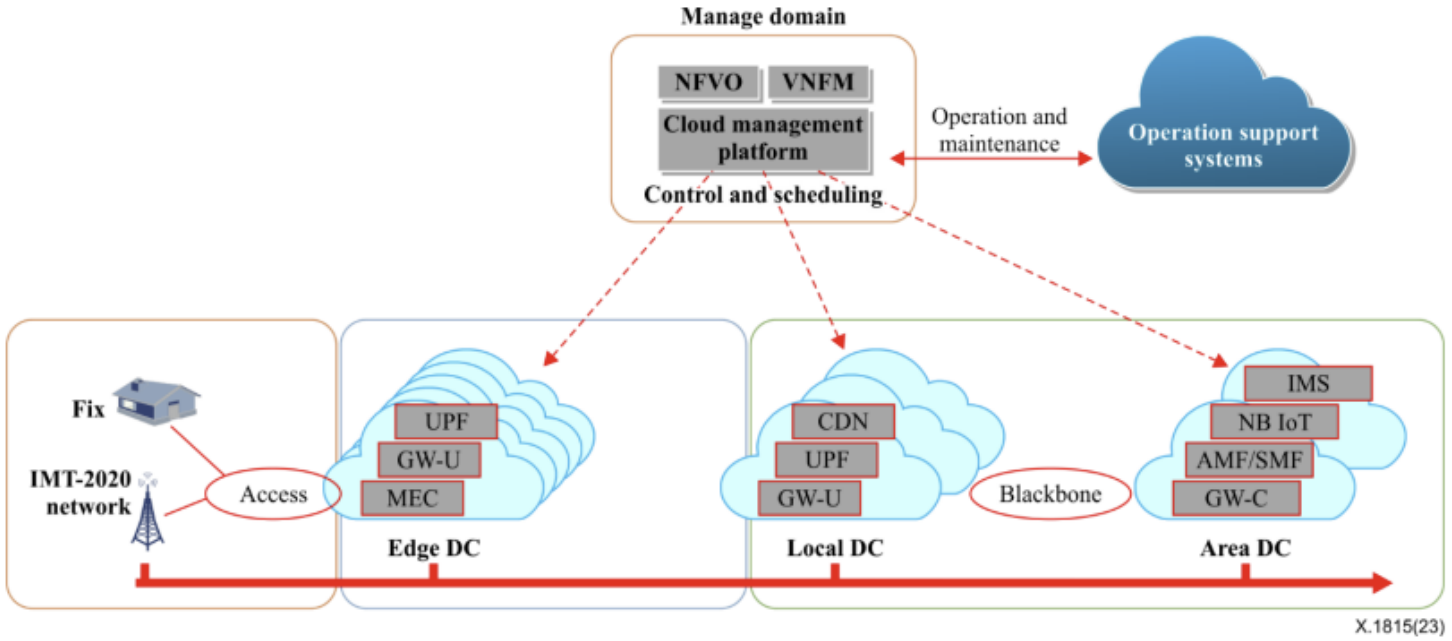


Security capabilities related to components and functions in X.1814

- Security capabilities related to user equipment
- Security capabilities related to access network
- Security capabilities related to software-defined networking
- Security capabilities related to core network
- Security capabilities related to network slicing
- Security capabilities related to multiaccess edge computing
- Security capabilities related to network function virtualization
- Security capabilities related to management function

Deployment scheme of IMT-2020 edge computing services in X.1815

- Edge DC: Provides mobile edge computing (MEC) functionality which enables IMT-2020 edge computing services and gateway-user plane (GW-U) and UPF functionalities.
- Local DC: Provides GW-U, content delivery network (CDN) and UPF functionalities.
- Area DC: Provides gateway-control plane (GW-C), AMF/SMF, NB IoT and IMS etc. functionalities.
- Manage domain: Includes cloud manage platform, network functions virtualization orchestrator (NFVO) and virtualized networ function manager (VNFM).



Security threats, security requirements, and security capability guideline for edge computing service in X.1815

- Security threats to infrastructure layer and network layer,
- security requirements to infrastructure layer and network layer, and application layer
- Security capability guideline to infrastructure layer and network layer, and application layer for edge computing service

Concluding remarks

Concluding remarks

- Security and privacy are critical for building confidence and security of 5G systems.
- Security by design and privacy by design principles should be considered for entire lifecycle of 5G systems.
- Assessment scheme for 5G security and its assessment criteria should be standardized for improving the security level for 5G network elements.
  - National or regional experiences on 5G security assessment should be shared among related stakeholders.
- It is now to start studying IMT-2030 (6G) security, taking onto account experience of 5G security.

Thanks for your attention!