“A Security Architecture for 5G Networks”

IEEE Access, Volume 6, 2018

Presenter:
Sushil Kumar Singh,
2019.09.24
sushil.sngh001007@seoultech.ac.kr
SeoulTech National University and Sciences, Seoul, South Korea

SeoulTech UCS Lab

Table of Contents

I. Introduction

II. Security Architecture and Objectives

III. Security Architecture in Details

IV. Analysis

V. Use Cases (Smart cities and 5G)

VI. Conclusion

VII. References

VIII. Opinion

I. Introduction

- Nowadays, communication is an essential part for everyone.
- Many types of commincations are available such as M2M, H2M and others.
- Challenges of 3G and 4G: Network’s dynamic environment, manages lot of devices, security.
- Concept of network slicing, network softwarization, network function virtualization and software defined network are used in 5G network.
- 5G networks provide opportunities for the creation of new services, new business models to enter the mobile market.
- 5G security architecture is a extension of 3G or 4G architecture.

I. Introduction

❖ Contribution of this research

✓ Provide security architecture for 5G networks that captures the relevant security issues about the use of new technologies.

✓ Proposed security architecture serves as a pre-standardisation effort that aim to be useful for 3GPP.

✓ Present design objectives of a security architecture for 5G.

✓ Describe Architectural concepts with applications (Smart City) and components for 5G networks.

II. Security Architecture and Objectives

The security architecture of 5G networks is devided into four parts:

- Domain: is a grouping of networks entities according to physical or logical aspects that are relevant for 5G networks.
- Stratum (Strata): is a grouping protocols, data and functions related to sevices provided by one or several domain.
- Security Realm (SR): captures security needs of one or several domains.
- Security Control Class(SCC): collection of security functions and mechanisms such as integrity, confidentiality and so on.

III. Security Architectre in Details

A. Domain

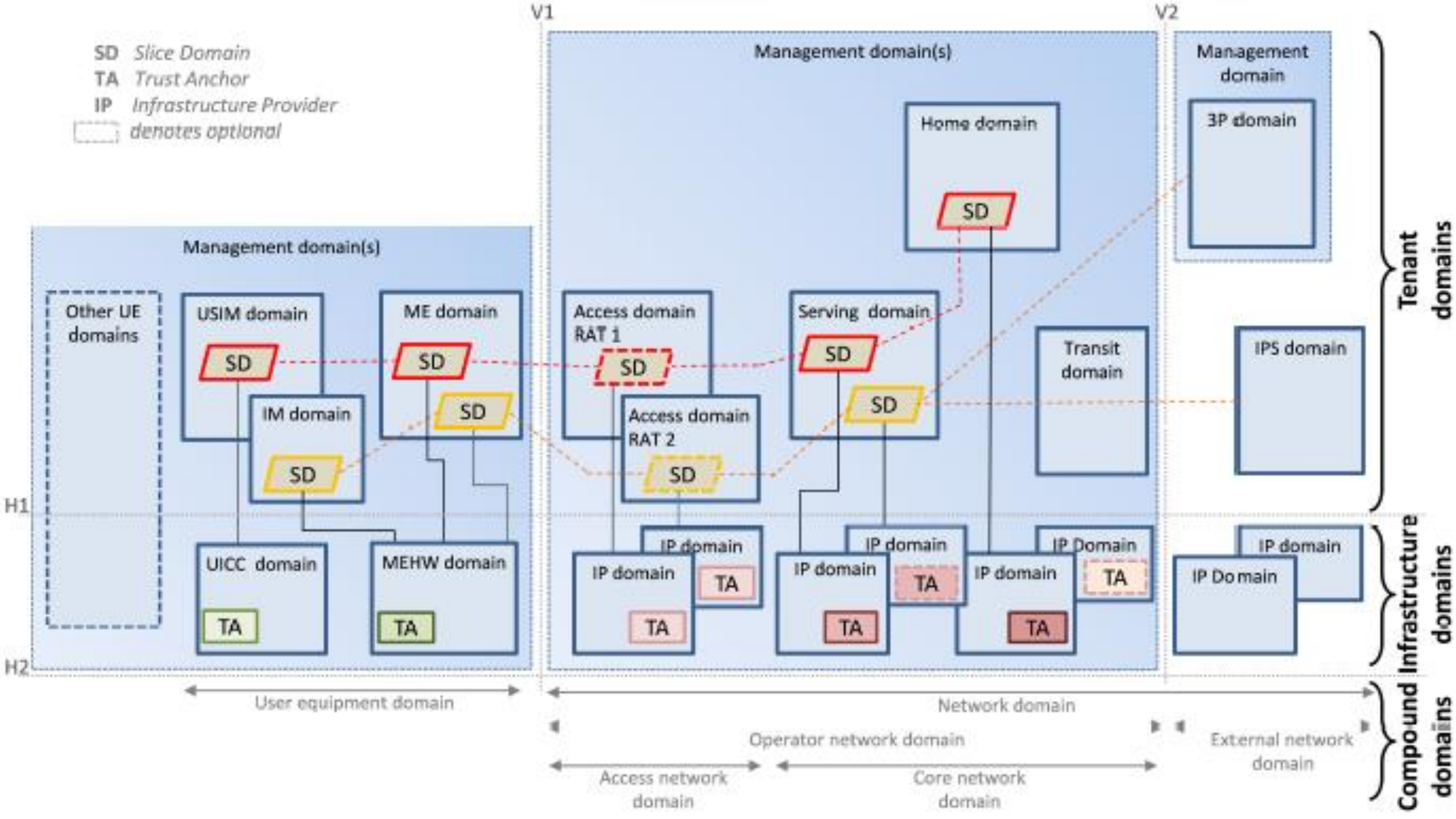


FIGURE 1. 5G domains.

UICC: Universal integrated circuit card

MEHW: Mobile equipment hardware

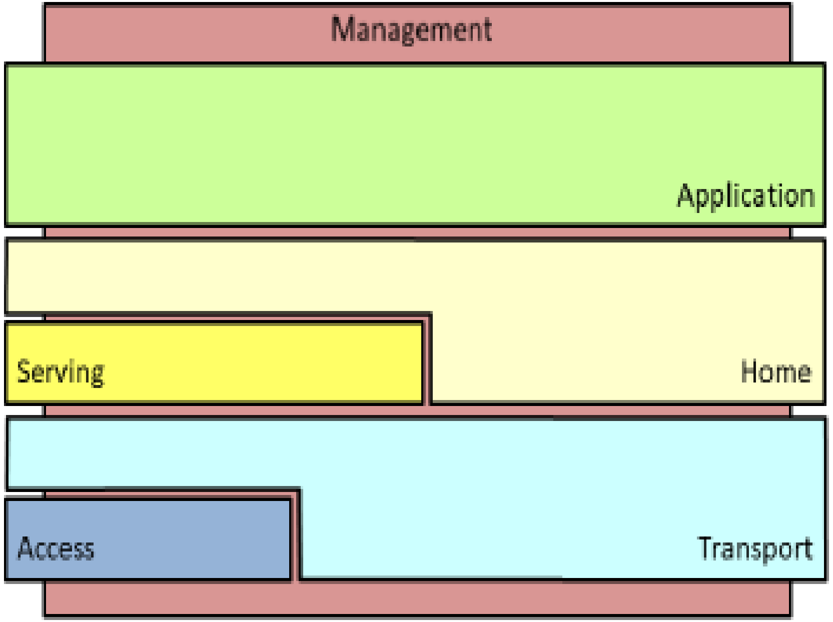
USIM: Universal subscriber identity module

ME: Mobile Equipment

IM: Identity management

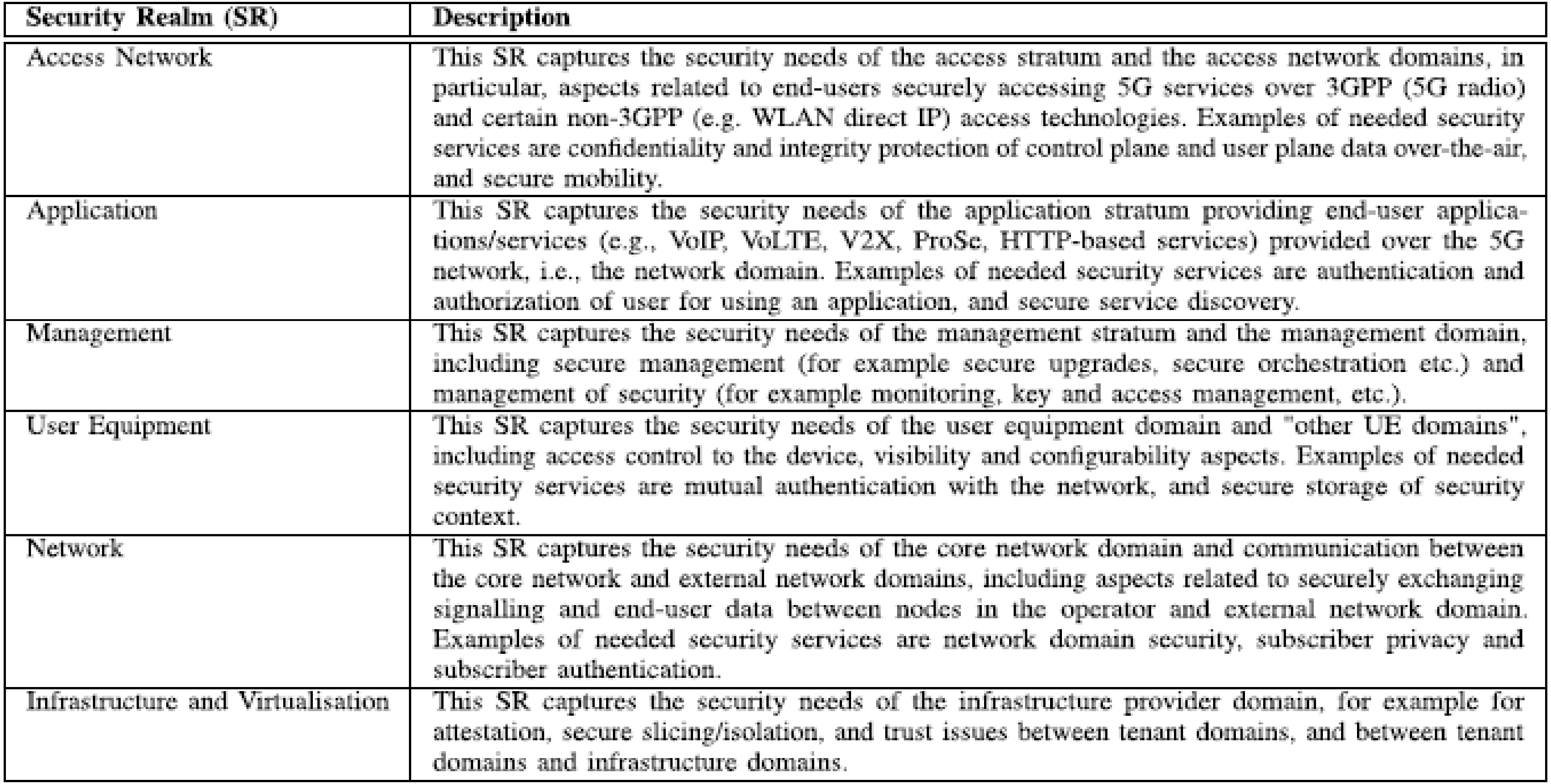
IP: infrastructure provider

B. STRATA (Stratum)



- Provide a high level view of protocols, data and functions.
- Application, Home, Serving, transport and access.
- All parts have protocols and functions related to end to end applications provided to end users.

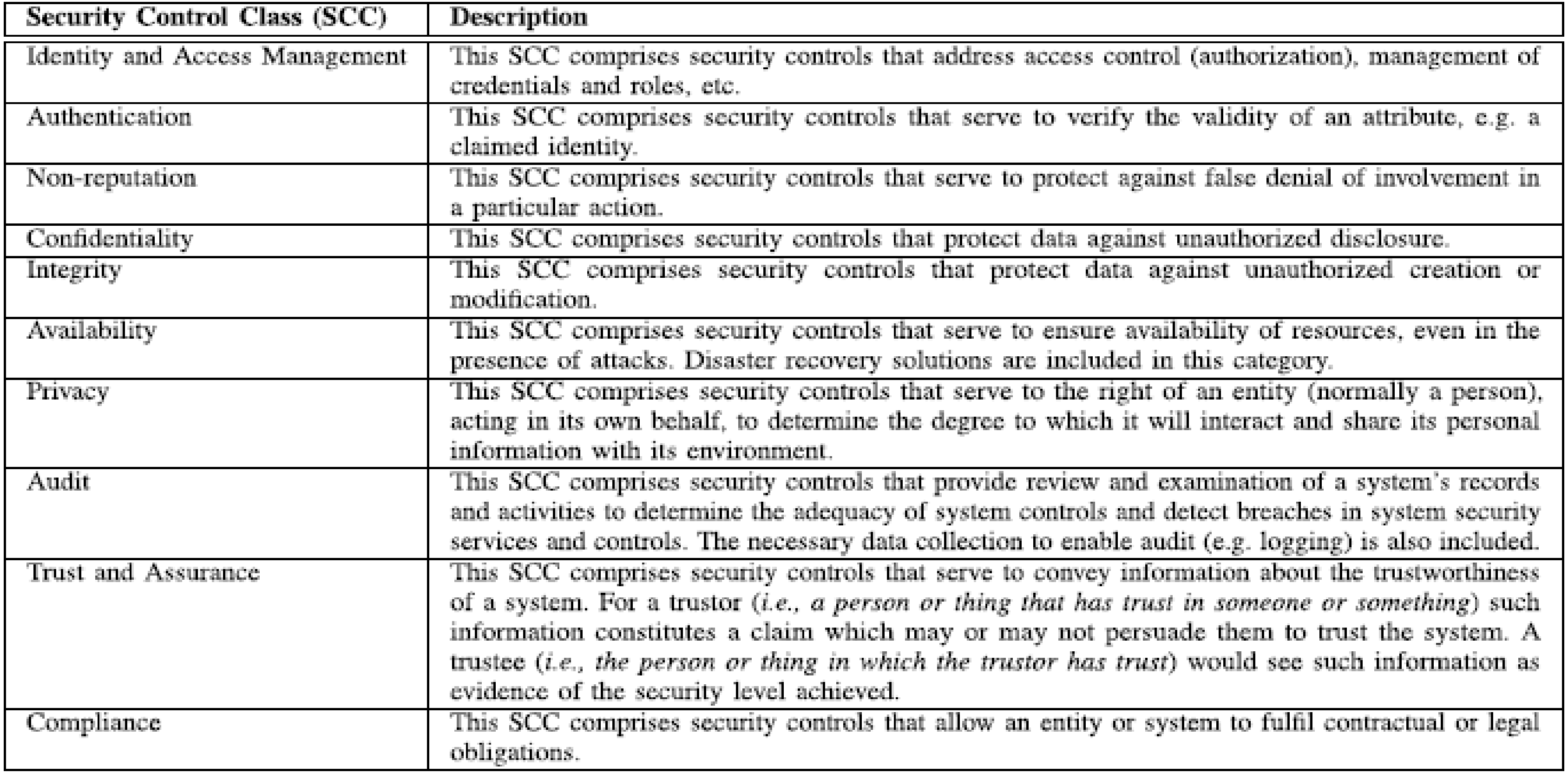
C. SECURITY REALMS



Security Realm (SR)	Description
Access Network	This SR captures the security needs of the access stratum and the access network domains, in particular, aspects related to end-users securely accessing 5G services over 3GPP (5G radio) and certain non-3GPP (e.g. WLAN direct IP) access technologies. Examples of needed security services are confidentiality and integrity protection of control plane and user plane data over-the-air, and secure mobility.
Application	This SR captures the security needs of the application stratum providing end-user applications/services (e.g., VoIP, VoLTE, V2X, ProSe, HTTP-based services) provided over the 5G network, i.e., the network domain. Examples of needed security services are authentication and authorization of user for using an application, and secure service discovery.
Management	This SR captures the security needs of the management stratum and the management domain, including secure management (for example secure upgrades, secure orchestration etc.) and management of security (for example monitoring, key and access management, etc.).
User Equipment	This SR captures the security needs of the user equipment domain and "other UE domains", including access control to the device, visibility and configurability aspects. Examples of needed security services are mutual authentication with the network, and secure storage of security context.
Network	This SR captures the security needs of the core network domain and communication between the core network and external network domains, including aspects related to securely exchanging signalling and end-user data between nodes in the operator and external network domain. Examples of needed security services are network domain security, subscriber privacy and subscriber authentication.
Infrastructure and Virtualisation	This SR captures the security needs of the infrastructure provider domain, for example for attestation, secure slicing/isolation, and trust issues between tenant domains, and between tenant domains and infrastructure domains.

TABLE 1. 5G security realms.

D. SECURITY CONTROL CLASSES



Security Control Class (SCC)	Description
Identity and Access Management	This SCC comprises security controls that address access control (authorization), management of credentials and roles, etc.
Authentication	This SCC comprises security controls that serve to verify the validity of an attribute, e.g. a claimed identity.
Non-reputation	This SCC comprises security controls that serve to protect against false denial of involvement in a particular action.
Confidentiality	This SCC comprises security controls that protect data against unauthorized disclosure.
Integrity	This SCC comprises security controls that protect data against unauthorized creation or modification.
Availability	This SCC comprises security controls that serve to ensure availability of resources, even in the presence of attacks. Disaster recovery solutions are included in this category.
Privacy	This SCC comprises security controls that serve to the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact and share its personal information with its environment.
Audit	This SCC comprises security controls that provide review and examination of a system's records and activities to determine the adequacy of system controls and detect breaches in system security services and controls. The necessary data collection to enable audit (e.g. logging) is also included.
Trust and Assurance	This SCC comprises security controls that serve to convey information about the trustworthiness of a system. For a trustor (*i.e., a person or thing that has trust in someone or something*) such information constitutes a claim which may or may not persuade them to trust the system. A trustee (*i.e., the person or thing in which the trustor has trust*) would see such information as evidence of the security level achieved.
Compliance	This SCC comprises security controls that allow an entity or system to fulfil contractual or legal obligations.

TABLE 2. 5G security control classes.

IV. Analysis

- Backward Compativility
- Flexibility and Adaptability
- Trust Relations
- Virtualisation and Slicing
- Protocol and Network functions
- Security Control Points
- Security Controls
- Network Management

V. Use Cases

A. Smart Cities and 5G

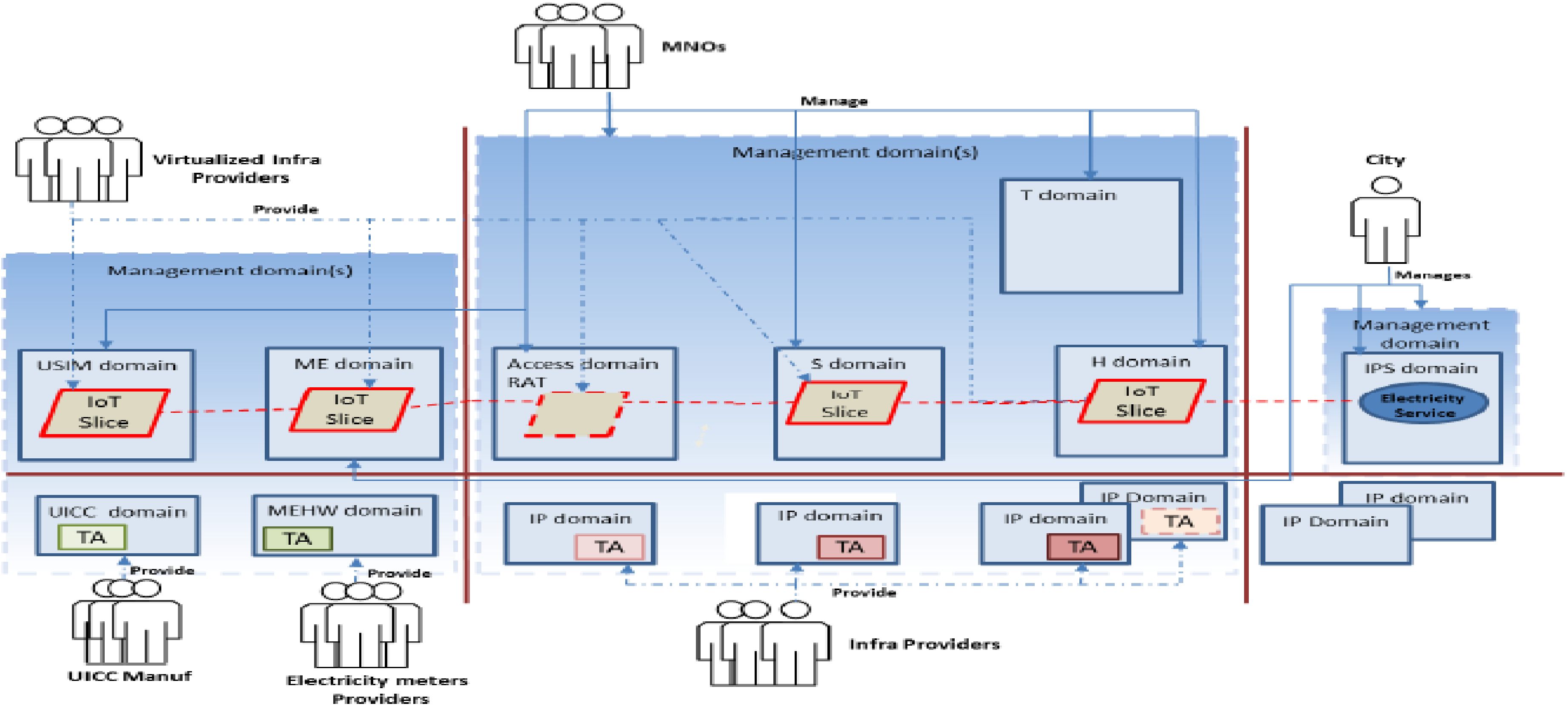
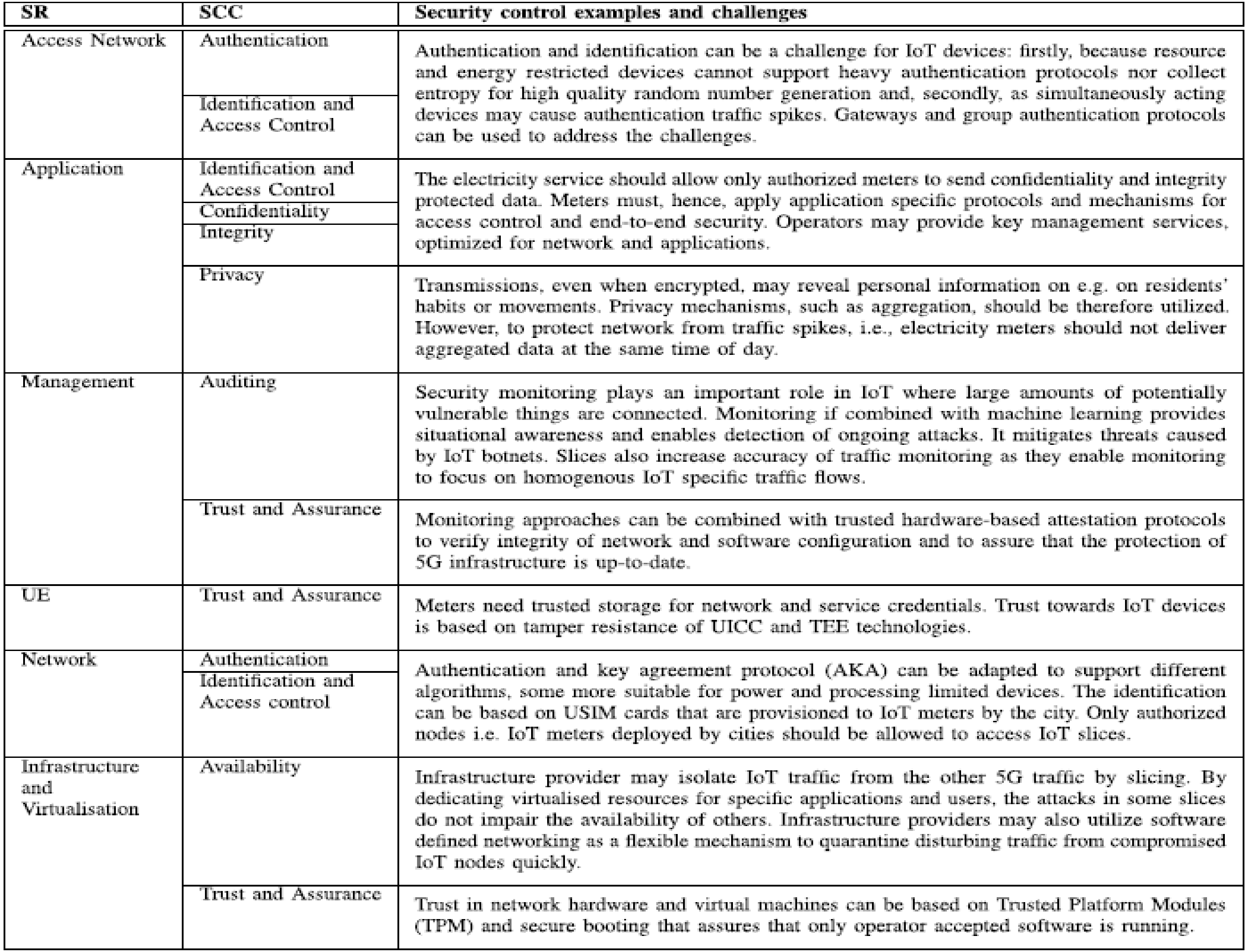


FIGURE 3. Domain view of the smart city use case.



SR	SCC	Security control examples and challenges
Access Network	Authentication	Authentication and identification can be a challenge for IoT devices: firstly, because resource and energy restricted devices cannot support heavy authentication protocols nor collect entropy for high quality random number generation and, secondly, as simultaneously acting devices may cause authentication traffic spikes. Gateways and group authentication protocols can be used to address the challenges.
	Identification and Access Control	
Application	Identification and Access Control	The electricity service should allow only authorized meters to send confidentiality and integrity protected data. Meters must, hence, apply application specific protocols and mechanisms for access control and end-to-end security. Operators may provide key management services, optimized for network and applications.
	Confidentiality	
	Integrity	
	Privacy	Transmissions, even when encrypted, may reveal personal information on e.g. on residents' habits or movements. Privacy mechanisms, such as aggregation, should be therefore utilized. However, to protect network from traffic spikes, i.e., electricity meters should not deliver aggregated data at the same time of day.
Management	Auditing	Security monitoring plays an important role in IoT where large amounts of potentially vulnerable things are connected. Monitoring if combined with machine learning provides situational awareness and enables detection of ongoing attacks. It mitigates threats caused by IoT botnets. Slices also increase accuracy of traffic monitoring as they enable monitoring to focus on homogenous IoT specific traffic flows.
	Trust and Assurance	Monitoring approaches can be combined with trusted hardware-based attestation protocols to verify integrity of network and software configuration and to assure that the protection of 5G infrastructure is up-to-date.
UE	Trust and Assurance	Meters need trusted storage for network and service credentials. Trust towards IoT devices is based on tamper resistance of UICC and TEE technologies.
Network	Authentication	Authentication and key agreement protocol (AKA) can be adapted to support different algorithms, some more suitable for power and processing limited devices. The identification can be based on USIM cards that are provisioned to IoT meters by the city. Only authorized nodes i.e. IoT meters deployed by cities should be allowed to access IoT slices.
	Identification and Access control	
Infrastructure and Virtualisation	Availability	Infrastructure provider may isolate IoT traffic from the other 5G traffic by slicing. By dedicating virtualised resources for specific applications and users, the attacks in some slices do not impair the availability of others. Infrastructure providers may also utilize software defined networking as a flexible mechanism to quarantine disturbing traffic from compromised IoT nodes quickly.
	Trust and Assurance	Trust in network hardware and virtual machines can be based on Trusted Platform Modules (TPM) and secure booting that assures that only operator accepted software is running.

Table3: Mapping of SR to control classes in the smart city

VI. Conclusion

- Proposed 5G security architecture that is combination of domains, strata inherited from 3G, 4G security architecture.
- Introduced set of security realms to capture security needs for domains and strata.
- Security control classess provide security functions and mechnisms in terms of security concerns.
- Finally , studied the mapping of 5G architecture to use case like smart city.

VII. Reference

[1] Arfaoui, Ghada, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix Klaedtke et al. "A security architecture for 5G networks." *IEEE Access* 6 (2018): 22466-22479.

VII. Opinion

- 5G is communication technology based on physical communication.

- When 5G is emerged with IoT, then it has many limitation such as centralization, accuracy, latency, load management.

- To mitigate these limitations, Blockchain and AI are used in 5G network.

- Security architecture of 5G used in many applications such as smart transportation, smart healthcare and CPS (Cyber Physical System) and others.

Thank you for your attention

Sushil Kumar Singh

sushil.sngh001007@seoultech.ac.kr