A SECURITY ARCHITECTURE FOR 5G NETWORK

Seminar Report

submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

In

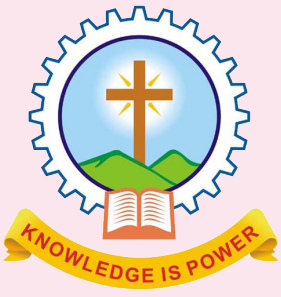
COMPUTER SCIENCE AND ENGINEERING

of

APJ Abdul Kalam Technological University

submitted by

RESHMA JOSHY



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAR ATHANASIUS COLLEGE OF ENGINEERING
KOTHAMANGALAM

A SECURITY ARCHITECTURE FOR 5G NETWORK

Seminar Report

submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

of

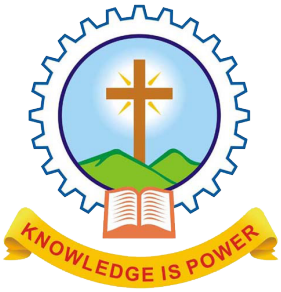
APJ Abdul Kalam Technological University

submitted by

RESHMA JOSHY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAR ATHANASIUS COLLEGE OF ENGINEERING
KOTHAMANGALAM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAR ATHANASIUS COLLEGE OF ENGINEERING
KOTHAMANGALAM



CERTIFICATE

This is to certify that the report entitled **A Security Architecture for 5G Network** *submitted by Ms.* **RESHMA JOSHY** *, Reg. No.* **MAC15CS047** *towards partial fulfillment of the requirement for the award of Degree of Bachelor of Technology in Computer science and Engineering from APJ Abdul Kalam Technological University for december 2018 is a bonafide record of the seminar carried out by her under our supervision and guidance.*

.....	.....	.....
Prof. Joby George	**Prof. Neethu Subash**	**Dr. Surekha Mariam Varghese**
Faculty Guide	***Faculty Guide***	***Head of the Department***

Date: Dept. Seal

ACKNOWLEDGEMENT

First and foremost, I sincerely thank the God Almighty for his grace for the successful and timely completion of the seminar.

I express my sincere gratitude and thanks to Dr. Solly George, Principal and Dr. Surekha Mariam Varghese, Head Of the Department for providing the necessary facilities and their encouragement and support.

I owe special thanks to the staff-in-charge Prof. Joby George , Prof. Neethu Subash and Prof. Joby Anu Mathew for their corrections, suggestions and sincere efforts to co-ordinate the seminar under a tight schedule.

I express my sincere thanks to staff members in the Department of Computer Science and Engineering who have taken sincere efforts in helping me to conduct this seminar.

Finally, I would like to acknowledge the heartfelt efforts, comments, criticisms, co- operation and tremendous support given to me by my dear friends during the preparation of the seminar and also during the presentation without whose support this work would have been all the more difficult to accomplish.

ABSTRACT

5G networks will provide opportunities for the creation of new services and for new players to enter the mobile market. The network will support efficient and cost-effective launch of a multitude of services. Key technology concepts are network slicing and network softwarisation. The technologies include network function virtualisation and software-defined networking. The proposed security architecture builds upon concepts from the 3G and 4G security architectures but extends and enhances them to cover the new 5G environment. The proposed security architecture comprises a toolbox for security relevant modelling of the systems and a set of security functions and security control mechanisms. The use of the proposed 5G security architecture to achieve a systematic treatment of security issues in a smart city use case is also illustrated.

Contents

List of Figures

List of Tables

List of Abbreviations

TVRA	Threat, Vulnerability and Risk Analysis
SDN	Software Defined Networking
NFV	Network Function Virtualisation
VNF	Virtualised Network Functions
SD	Slice Domains
UICC	Universal Integrated Circiut Card
MEHW	Mobile Equipment Hardware
MNO	Mobile Network Operator
IoT	Internet of Things
3GPP	3rd Generation Partnership Project

Introduction

Communication is an essential part of our society. Already today, most of our communication is digital l and includes human-to-machine and machine-to-machine communication. Over the previous decades, we have also experienced a drastic increase in communication traffic carried on standard commercial telecommunications networks. These trends are expected to continue and the forthcoming generation of telecommunication networks, namely 5G networks, aim to provide for this increase. 5G networks should also offer solutions for efcient and cost-effective launch of a multitude of new services, tailored for different vertical markets having varying service requirements, and involving a large number of actors. In particular, an important aim is to support critical services that have strict requirements on security and availability such as network services in Industry 4.0 and e-Health. Secure and reliable network services are also a prerequisite for support of secure digital markets.

5G networks will leverage softwarisation and virtualisation to achieve the service objectives on flexibility, configurability, and scalability[1]. In particular, key design concepts of 5G networks will be network slicing (i.e., dedicating logical networks for isolated applications), mobile edge computing, network function virtualisation (NFV), and software-defined networking (SDN). The vision is that a 5G network will provide a ubiquitous flexible and extensible infrastructure for all types of communication services on top of which a dynamic service and business environment can evolve.

The security of 5G networks and their communication services will be of vital

importance. However, there are a number of challenges to be addressed which are mainly due to the networks dynamic environment and the fact that the security requirements will be much more stringent than in previous network generations since the diverse network services from verticals will be mission critical.

5G will allow the establishment of new business models with new actors in the mobile market. This will give rise to a need to take new types of trust relations between participating actors into account in the security design; whom is to be trusted, in which respect, and to what extent. Furthermore, the use of new technologies like network virtualisation (i.e., decoupling logical networks from networking hardware) and SDN will bring new trust issues; in this case trust between application owners and compute and storage resource providers. In both these cases, the trust relations will manifest themselves in hard security requirements to enforce required service level agreements and to protect information exchange between actors.

A cornerstone in developing secure systems is to apply a security architecture. A security architecture provides a high-level overview of the different entities involved, their relations and interactions. Such a high-level overview is essential for analyzing the security of the developed system as a whole or parts of it, understanding how certain entities impact the systems security, identifying threats, and designing and deploying effective security controls.

The security architectures[2],[3] for previous network generations (i.e., 3G and 4G) fall short for 5G networks. In particular, they do not capture various security issues that originate from the technologies used in 5G and the new use cases stemming from the new business environment offered by 5G. For instance, existing security architectures were not designed for multi-tenancy operation (e.g., shared physical infrastructure used by different providers) and cannot differentiate trust relations between the different tenants. Furthermore, support for network virtualisation and network slicing (i.e., dedicating logical networks for isolated applications) is something that was not part of their requirements. Thus, these existing security architectures need to be updated and extended to include support for such functionalities and technologies in 5G networks.

Related works

Several organizations have been working on designing architectures for telecommunication networks. The 3GPP (3rd Generation Partnership Project) is the standardization body for telecommunication networks. At the time of writing, 3GPP is actively working on release [4] , which includes various requirement and standardization documents for 5G. The 3GPP working groups SA2 and SA3 are of particular relevance for this 5G architecture. SA2 is in charge of the system architecture and identifies the main functions and entities of the network, how these entities are linked to each other, and the information they exchange. SA3 is responsible for determining the networks security and privacy requirements and specifying the security architectures and protocols. SA3 analyses, e.g., in 3GPP TS 33.899 new 5G security issues and proposes individual solutions for each of them but does not provide any overarching architecture that puts the pieces together. Beyond the domain and stratum concepts, the security architecture proposes two transverse concepts namely, security control classes, which are inspired by ITU-T X.805 , and security realms so that requirements can be modelled and traceable through the different views of the proposed security architecture. This architecture enables the description and inclusion of, for example, new requirements for virtualisation and concerns between multiple stakeholders, in particular, the related trust issues . Therefore, architecture covers new and relevant aspects of 5G networks, which are not addressed by the current 3GPP work, e.g., segregation between infrastructure domains and tenant domains, network management and the interface with new domains such as 3P or IPS domains.

The NGMN (Next Generation Mobile Networks) Alliances 5G working programme has identified new threats and security issues that may arise with 5G. In particular, the NGMN Alliance provides 5G security recommendations for network slicing, access network, and low latency use cases. For example, for network slicing, these recommendations express security needs of the infrastructure and virtualisation security realm. The security architecture could be used to improve the precision of the way security controls should be implemented, and where to position security control points on the different domains and their interfaces.

Schneider and Horn discuss potential security requirements and mechanisms for 5G networks. This work is complementary to Schneider and Horns work. In this security architecture, such requirements and mechanisms can be identified and mapped to and clearly positioned within a 5G network. Conduct a threat analysis on a 5G network architecture, giving a description of the threats by network domains. In comparison, security architecture provided is based on a network architecture, which provides a well-suited framework to analyze both security requirements and security threats .

Proposed system

3.1 Security architecture and objectives

In the literature, ready-made security solutions are often labelled as security architectures (e.g. 3GPPP TS 33.401). Such architectures serve a different purpose than this security architecture, namely, they describe implemented security controls and how to assemble those. However, when designing systems like 5G, which have a large variety of different instantiations, a toolbox and guidance is required that allow to model the system itself together with its security and develop security solutions for the designed system from scratch. We therefore define in this paper a security architecture as a methodology for instantiation of secure systems, comprising a toolbox for security relevant modelling of the systems, security design principles, and a set of security functions and mechanisms for implementation of the security controls needed to achieve the systems security objectives. This view of a security architecture is corroborated by the security architecture in ITU-T X.805[3]; in particular, X.805 states that the security architecture logically divides a complex set of end-to-end network security related features into separate architectural components and that this separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

5G (or any other) security architecture in itself does not provide answers to what the security threats to the network are and to which threats that have to be mitigated by

specific countermeasures. The basis for such considerations should be a multi-stakeholder Threat,Vulnerability and Risk Analysis (TVRA) taking the security objectives for the network into account. The TVRA should result in a risk treatment plan stating whether to (a)reduce the risk by implementing specied security controls, (b) accept the risk (i.e., assume it wont happen or wont cause much harm), or (c) transfer responsibility for managing the risk to other stakeholders, either explicitly (by agreement) or implicitly (because they seem trustworthy). The options (b) and (c) involve trust: a stakeholder either trusts that the 5G network will not misbehave or trusts another stakeholder to prevent the risk or mitigate any harm it may cause. These considerations are risk management decisions.

The starting points for new security architecture for 5G are found in the security architectures for previous 3G and 4G network generations. These architectures are extended and revised to cover the specics of 5G networks. since the proposed security architecture needs to comprise additional actors, handle the novel technologies used in 5G, and allow modelling of networks for many new use cases.

The main concepts in the security architecture are domains, strata, security realms, and security control classes.

- A domain is a grouping of network entities according to physical or logical aspects that are relevant for a 5G network. The concept of a slice domain is used to capture network slicing aspects.
- A stratum is a grouping of protocols, data, and functions related to one aspect of the services provided by one or several domains.
- A security realm (SR) captures security needs of one or more strata or domains.
- A security control class (SCC) is a concept that refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for one security aspect, e.g., integrity. Security classes contain security functions and mechanisms to avoid, detect, deter, counteract, or minimize security risks to 5G networks, in particular, risks to a networks physical and logical infrastructure, its services, the user equipment, signalling, and data.

The domain and stratum concepts are leveraged from the corresponding concepts in 3GPP TS 23.101[5] . They are used to logically divide a complex set of end-to-end network security-related features (and entities) into separate architectural components. The security realm concept is similar to the security feature group concept defined in 3GPP TS 33.401[6]. Security realms extend the security feature groups to consider the management and virtualisation aspects. Security realms provide a focus on a specic network aspect and its security. The security control class concept is inspired by the security dimensions in ITU-T X.805[3] and the security controls found in security standards, e.g. by ISO and NIST. The purpose of the security control classes is to provide a breakdown of the needed security functions and mechanisms in terms of security concerns e.g., authentication, condentiality, availability, privacy. Actual controls that are needed depend on the considered domain,stratum, or security realm.

The following is a high-level description of the process to secure a 5G network by applying our security architecture with its security realms and security control classes.

1. Model the 5G network by rst introducing top-level physical and logical domains. These domains should be characterized by ownership, management control, and functional area. Then define the types of slice domains to be supported. This top-level domain model should be based on the networks functional architecture.

2. Introduce reference points (interfaces) between the defined domains. The reference points will dene the dependencies and interactions between the domains. Characterize the information carried over the reference points according to dened strata together with used protocols and assign relevant security realms.

3. For each reference point, define the trust relations between the domains involved.

4. Perform a TVRA and derive a risk treatment plan with required security controls. One step in the TVRA should be to determine where and by whom the required protective measures should be implemented. In the considered multi-stakeholder environment with defined trust relations between actors, trust modelling would constitute a sound basis for such decisions. The analysis in the TVRA should be structured based on domains, strata, and security realms.

5. The definition of required security controls should follow established security-by-design principles and best practises.

6. Implement defined security controls and validate achieved network security objectives.

There are a number of design objectives for the qualitative attributes that a security architecture for 5G should exhibit. These objectives are the result of studying the security architectures from previous mobile network generations and the 5G security use cases.

A. Backward compatibility

It must be possible to use the security architecture to describe and analyze the security of 3G and 4G networks as they will be an integral part of future 5G networks.

B. Flexibility and adaptability

It must be possible to adapt the security architecture to future network solutions with new functionality and services. It must also be possible to use the security architecture and evolve it to cope with new threats and/or security solutions not known or considered at design time.

C. Trust relations

Current mobile networks assume a three-party trust model. Namely, it consists of a mobile network operator, a service provider, and an end user, where the mobile network operator is responsible for the network state.This model is insufcient for 5G. As the use cases show, a 5G network will have more actors with different roles such as Virtualised Infrastructure provider, and VNF provider, etc. Security architecture must be able to make trust relations between these actors explicit.

D. Virtualisation and slicing

5G is expected to be a network that fits all use cases and all requirements. Because 5G use cases have to some extent, contradictory requirements, 5G is supposed to be dynamic and exible. To this end, virtualisation technologies and slicing concepts will be used to provide the required exibility, adaptability and evolvability. That is why our security architecture must capture virtualisation and slicing.

E. Protocols and network functions

As with existing mobile networks, 5G will introduce several new (security and non-security) protocols and network functions. However, 5G networks will need to utilise a multitude of them, as it will also include the ones inherited from previous network generations. The security architecture must identify security relevant protocols and network functions used and offered in a 5G network in order to build effective protection.

F. Security control points

5G networks will be much more complex than 4G and earlier mobile networks. For instance, they will have a large variety of actors, comprise various layers, and different means of accessing the network. Furthermore, they will be dynamic in the sense that new (virtualised) network nodes can automatically be added to and removed from the network, or a slice of it, at any time . Well-dened boundaries and interfaces will be crucial to identify and model attack vectors, which in turn will allow better network protection. Hence, a security architecture must enable depiction of the boundaries and interfaces of a 5G network.

G. Security controls

Along with the new use cases, new trust relations and new technologies that 5G will bring to the table, new security functions and needs will emerge. The security architecture must enable structuring and modelling the mobile network functions and needs into areas with specic security concerns.

H. Network management

Current mobile network generation specications do not formalize network management aspects. It was considered to be implementation dependent. In 5G, technologies will be blended; new roles and actors are emerging. In this context, specifying and defining the network management is important in order to ensure efficient and secure operation of the networks. The security architecture must consider the management aspects.

3.2 Security architecture details

Domains

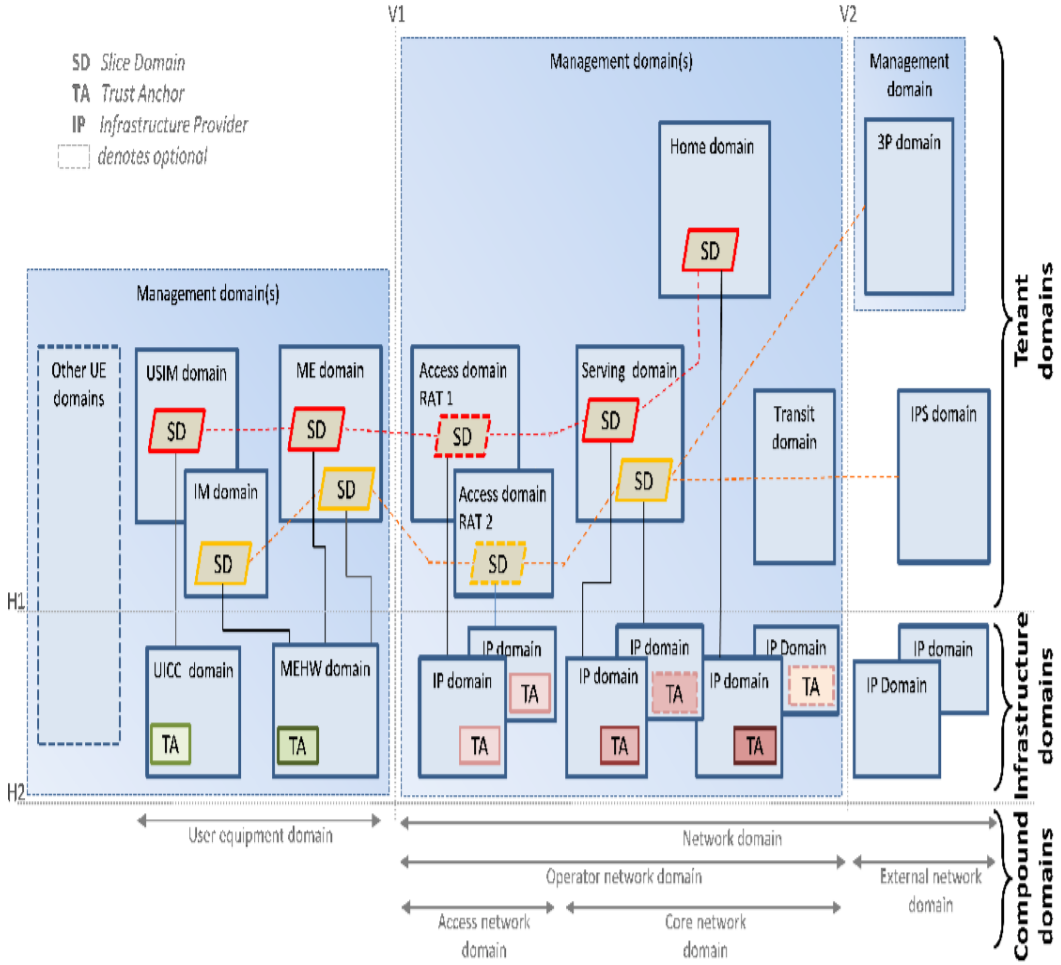


Fig. 3.1: 5G domains

The domain concept is a cornerstone in the 5G security architecture as it makes it possible to represent different functionalities, services, and actors in 5G networks. Figure depicts the 5G domains and illustrates where they are located in 5G networks. In figure, the

horizontal lines H1, H2 and the vertical lines V1, V2 give a first high-level classication of domains. The ones above H1 represent the logical network aspects, called tenant domains;the ones between H1 and H2 represent the physical network aspects, called infrastructure domains; and ones below H2 represent higher order groupings based on several aspects, such as ownership or joint administration, called compound domains. V1 separates the user equipment from the network, and V2 further separates operator network from external network, e.g. Internet services used by the operator network.

Most importantly, for earlier generations of mobile networks,i.e.,2G,3G, and 4G,there was no distinction between the infrastructure and the tenant domains. But this distinction, which is in correspondence with the ETSI NFV work, is fundamental for the next generation 5G networks. This is so because virtualisation, together with SDN, form the basis for the softwarisation of networks for the introduction of such technologies as network slicing and mobile edge computing.

First, the infrastructure domain contains hardware and (low level) software providing infrastructure platform services, including hypervisors and trust anchors (TAs). On the user equipment side, it consists of universal integrated circuit card (UICC) and mobile equipment hardware (MEHW) domains, and on the network side it consists of infrastructure provider (IP) domain. The UICC domain contains a conventional tamper-resistant module offering protected storage and processing of security critical information. The MEHW domain provides hardware support for the mobile equipment and may include trusted execution environments(TEE) supporting,e.g. other forms of credentials such as certicates. Similarly, the IP domain contains the hardware platforms for the compute, storage, and networking resources required in (core) functionality and the access (radio) specic hardware. The figure also shows TAs that capture various trust issues appearing in virtualised systems (therefore various colours/shades), e.g. how to get assurance of tenant domain integrity and that a tenant domain executes on a designated and trusted infrastructure.The TAs can also be used to verify infrastructure domains integrity and to bind tenant domains to infrastructure domains.

Next, the tenant domains contain several logical domains that use infrastructure domains, e.g. to execute their functions.On the user equipment side, it consists of mobile equipment

(ME), universal subscriber identity module (USIM), and identity management (IM) domains. The ME and USIM domains are analogous to the ones in TS 23.101[5] but only contain the logical functionalities required for accessing the network services and using user applications.The IM domain is an important addition to our 5G security architecture which contains functionality to support alternatives to USIM based authentication, e.g. public key certicates for industry automation use cases. The tenant domains on the network side consists of access(A),serving(S),home(H),transit (T), 3rd party (3P), internet protocol service (IPS), and management (M) domains. The domains analogous to the ones in TS 23.101[5] are the A, S, H and T domains which respectively contain the logical functionalities to manage access (radio) network resources; route or transport calls and end-user data; manage end-user subscription data;and provide communication paths between the S domain and external network. The IPS domain represents operator-external Internet protocol networks such as the public Internet and/or various corporate networks. The remaining two domains are an important addition to the 5G security architecture as discussed below. The 3P domain contains functionality for use cases where a trusted(all services are allowed) or semi-trusted(only agreed services are allowed) third party, such as a factory/industry vertical, provides its own authentication services, e.g. to its machine-to-machine(M2M)devices like industry robots and IoT devices.The M domain contains the logical functionality required for management of specific aspects of 5G networks, e.g.,secure management,management of security,traditional network management, orchestration of SDN and virtualised environments, and management of user equipment domains.

Finally, the compound domain consists of a collection of various other domains,grouped together according to 5G relevant aspects,e.g.,ownership,joint administration or the like. On the user equipment side, it comprises a general domain called the user equipment (UE) domain, and on the network side it consists of the network (N), operator network (ON), external network (EN), access network (AN), and core network (CN) domains. The figure illustrates which domains from the infrastructure and tenant domains are grouped by these compound domains. Therefore, no further description will be given for grouping.However,there are two important additions to the 5G security architecture. The first one is called other UE domains that captures

the so-called direct-mode or UE-to-UE type communication. The second one, called slice domain (SD), is of particular importance because it captures network slicing aspects in 5G networks. A slice can cover only some parts of the network, e.g. parts of the CN domain, but are in general dened end-to-end. Slicing may be implemented without relying on a virtualised networking solution, although most 5G networks use such a concept. The SDs shown with solid border lines indicate that they are located in domains that are fully slice aware,i.e.,the domains can fully support exible deployment of different slices. An SD with a dashed border line indicates that it is deployed in a domain which provides some functionality for slicing but is not fully slice aware due to legacy systems.

Strata

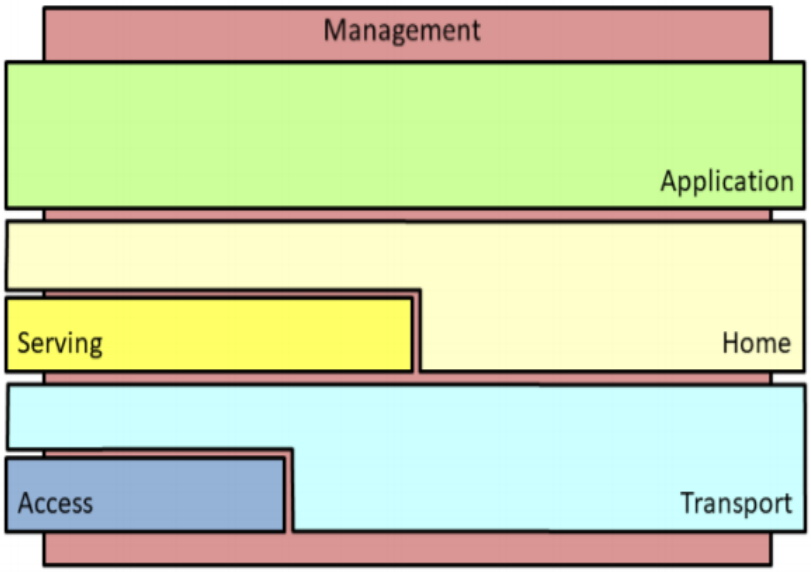


Fig. 3.2: 5G strata

The strata of 5G security architecture provide a high-level view of protocols, data and functions that are related in the sense that they are exposed to a common threat environment and exhibit similar security requirements, e.g., radio jamming, false base station attacks, user plane data injection over-the-air,and spoofed radio resource control messages are common threats to communication between user equipment and a radio access network, while tracking

of subscription identiers, spoong of control plane messages, tampering of security capabilities, etc. are common threats to communication between user equipment and the core network.

The application, home, serving, transport, and access strata are analogous to the ones in 3GPP TS 23.101[5]. They respectively include protocols and functions related to end-to-end applications provided to end-users; handling and storage of subscription data and home network specific services; providing telecommunication services like calls and end-user data; transport of end-user data and network control signalling from other strata through the network; and transmission of data over the radio interface. When end-users are roaming, some protocols and functions belonging to the home stratum are performed by the serving stratum, which is viewed as a sub-stratum of the home stratum. The access stratum is shown as a sub-stratum of the transport stratum because the radio interface is a part of the transport, although very important and with special characteristics.

5G security architecture adds an important stratum which relates to the common threats that management services in 5G networks are exposed to, e.g., unauthorized configuration changes, compromise of network keys and certificates. The new stratum is called the management stratum. It comprises aspects related to conventional network management (configuration, software upgrades, system-user account management, log collection/analysis, etc.) and, in particular, security management aspects (security monitoring audit, key and certificate management, etc.). Further, aspects related to management of virtualisation and service creation/ composition (orchestration, network slice management, isolation and VM management, etc.) belong to this stratum. For instance, the management stratum comprises protocols like OpenFlow for configuring network components. The management stratum carries management operations on network functions in all of the other strata.

Security realms

Domains and strata partition 5G networks at high abstraction levels, but they are not meant to explicitly capture security needs. The concept of security realms is the main tool in the architecture for a focused assessment of the security needs of the different areas of network functionality.

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(3G 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 domain, visibility and configurability aspects. examples of needed security services are mutual authentication with the network, and secure storage of service context.
Network	This SR captures the security needs of 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 domains. Examples of needed security services are network domain security, subscriber privacy and subscriber authentication .
Infrastructure and Virtualization	This SR captures the security needs of the infrastructure provider domain, for example for attestation,secure slicing or isolation and trust issues between tenant domains, and between tenant domains and infrastructure domains.

Table 3.1: Security realms

Table provides a base non-exhaustive list of security realms that we consider of general relevance for 5G networks. By saying non-exhaustive, we mean that new security realms may/should be introduced, in particular for verticals that may have more domain specific important security needs. The management and the infrastructure and virtualisation security realms are important additions in our 5G security architecture. The other security realms are analogous to the security features groups defined in 3GPP TS 33.401[6]. In the following we provide examples of such security needs, corresponding to the threats mentioned in Section III-B on strata. For an access network security realm, example security needs are protection of data storage in base stations, protection from illegitimate user plane data injection over-the-air, detecting cell selection to a false base station, and protection of radio resource control messages. For a (core) network security realm example security needs are privacy protection of subscription identifiers, authentication, authorization, protection of control plane messages, secure mobility, security key distribution, secure algorithm negotiations. And finally, for a management security realm, example security needs are access management and monitoring, secure key management, and secure orchestrations.

Security control classes

The final tool is the concept of security control classes. The purpose of the security control classes is to provide a breakdown of the needed security functions and mechanisms in terms of security concerns. Table depicts security control classes. Seven of them, namely, identity and access management, authentication, non-repudiation, confidentiality, integrity, availability, and privacy are adopted from ITU-T X.805. The other three, namely, audit, trust and assurance, and compliance are important additions in the 5G security architecture.

Security Control Classes(SCC)	Description
Identity and Access Management	This SCC comprises security controls that address ccess control(authorization), managemnt 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 of 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 on 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 systems' 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 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(ie 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(person or thing in which 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 fulfill contractual or legal obligations

Table 3.2: Security control classes

3.3 Analysis

Effectiveness of security architecture depends on how it meets the objectives. The method used is to reason about how the security architecture can be used to describe 5G networks in terms of security relevant groupings of logical and physical entities and subsystems, and how such groupings can be used in the analysis of threats, security requirements and corresponding implementation of protective measures

A. Backward compatibility

The security architecture must apply to 4G networks. The concepts of domain and strata were inherited from 3GPP TS 23.101 and 3GPP TS 33.401 and constitute the basis for 3G and 4G networks security architectures. The security architecture defines (compound) domains and strata corresponding to the ones used in 3G and 4G and can thus model such networks and their security controls.

B. Flexibility and adaptability

The security architecture must be flexible and adaptable to future network solutions with new functionality and services. The security architecture allows definition of new domains, strata, and security realms. The security control classes may also be refined and new ones added. This makes it possible to adapt the framework to capture aspects relevant for new types of threats that need to be considered and to describe future network solutions with new actors, functionalities and services.

C. Trust relations

The security architecture must be able to model the trust relations between 5G actors. A 5G security architecture does not only depend on the security of individual components (domains or strata) but is also impacted by the way actors provide security over the domains and strata that they control. Our security architecture models the different types of domains and strata used to represent the different functionalities, services, and actors in a 5G network. As the defined domains may occur in multiple instances and belong to different actors taking on different roles and responsibilities, they provide a flexible tool for modelling different

5G network configurations and their inherent multi-party trust aspects. By observing inter-dependencies and required interactions between domains, it becomes a straightforward task to model and analyze their trust relations, threat propagation and needed security controls.

D. Virtualization and slicing

Security architecture must capture virtualisation and slicing. The security architecture reflects the important aspect of virtualisation in 5G networks by defining infrastructure and tenant domains giving a clear division between the physical platform offering an execution environment and the logical functions and services in the tenant domain. Trust issues appearing in virtualised systems, i.e., assurance of tenant domain integrity and execution on designated and trusted infrastructure, are captured in the architecture by the introduction of infrastructure trust anchors. These trust anchors can be used to verify infrastructure domains integrity and to bind tenant domains to infrastructure domains. Slicing is explicitly handled by the introduction of slice domains. The use of slice domains also highlights the trust issues appearing between actors controlling a domain and different actors controlling concurrently operating slices in that domain. The requirement on strict isolation between the domains and slices belonging to different actors also becomes clear.

E. Protocols and network functions

The security architecture must enable capturing of the protocols and network functions used and offered in a 5G network in order to build effective protection. The definitions of the different strata in the security architecture provide a high-level view of protocols, data and functions that are related in the sense that they are exposed to a common threat environment and exhibit similar security requirements. The use of strata thus helps in structuring for which purpose and where different security controls are needed.

G. Secutriy controls

The security architecture must enable structuring and modelling the mobile network functions and needs into areas with specific security concerns. The defined security control classes provide a structured way to express security needs of specific data, functions and services in a network. The defined security realms capture needs of one or more strata or domains and are there to group different network aspects with specific security concerns. Bringing these

two concepts together by analyzing which security controls that are required in a given security realm will provide a detailed and structured view of the required security mechanisms to ensure that security requirements are fulfilled.

H. Network management

The security architecture must consider the management aspects. To encompass the important aspects of management in the architecture, management domains, a management stratum and a management security realm have been introduced. These groupings of entities, services and functions enable mapping of different management aspects onto the architecture. In addition to general security management it will allow the mapping of orchestration of SDN functionality and virtualisation platforms in the architecture. Overall, the discussion in this section shows that the objectives for the design of the architecture have been achieved and thus that our security architecture provides a high-level overview of involved entities, their interactions, and their relations, which allow analysis and assessment of the security offered by implemented security mechanisms and protocols.

3.4 Usecases

The use of the proposed 5G security architecture to achieve a systematic treatment of security issues by analyzing the vulnerabilities of individual domains and trust relations between stakeholders is illustrated. In the context of smart cities, we focus on two aspects of 5G communication security for IoT devices. The first aspect is on providing connectivity and the second aspect is a follow-up that is concerned with the softwarisation of 5G networks.

A.Smart Cities and 5G

Smart cities are typically characterized by a large number of low-cost IoT devices. These devices collect data for large scale analysis that enable more efficient and often autonomous control actions. For instance, smart cities may optimize electricity consumption and production as well as rapidly react to malfunctions based on near real time data from electricity meters.

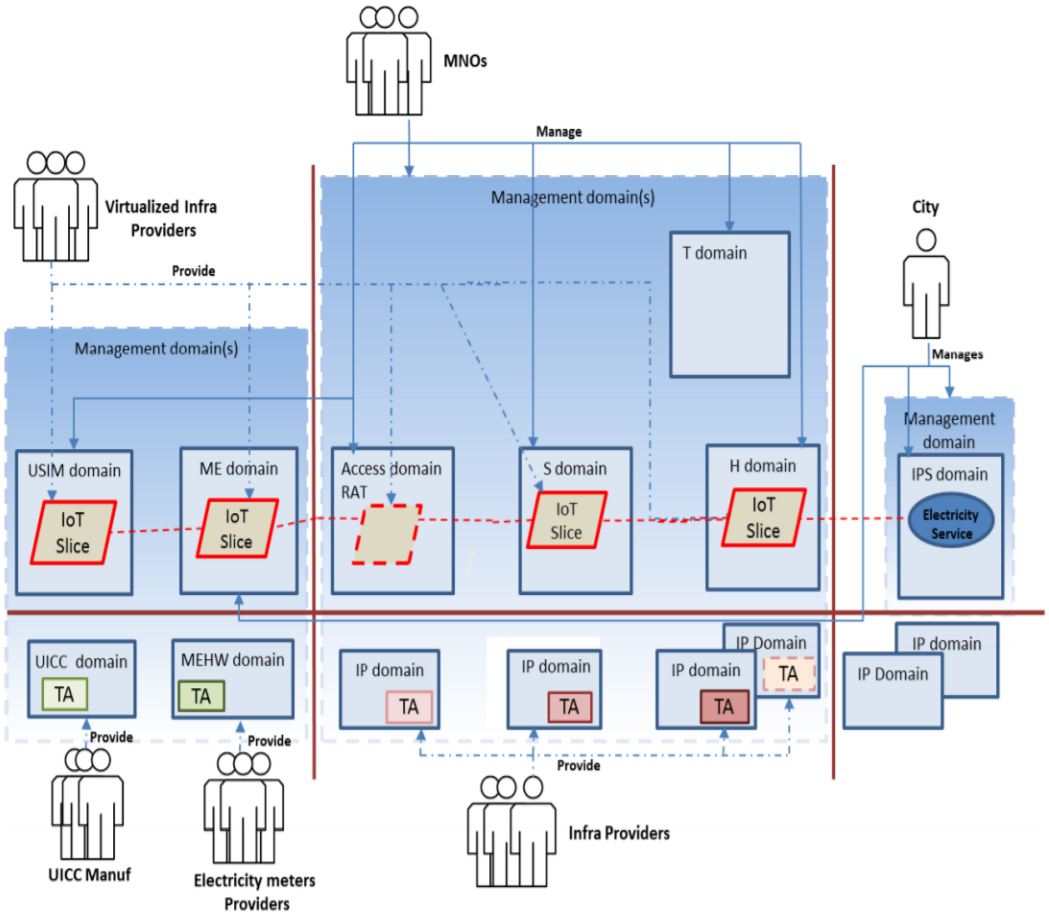


Fig. 3.3: Domain view of the smart city use case

The essential security requirements in this case are connectivity, confidentiality, integrity, and availability. Since IoT devices are geographically distributed and can also be mobile, private physical networks such as WiFi do not provide a suitable solution. 5G technologies, however, can offer a cost-efficient and scalable solution by providing dedicated logical networks (i.e., slices) with guaranteed and customized security properties.

Figure illustrates the relationships within this setting between the stakeholders, processes, and resources by utilizing the various different domains of our security architecture. The stakeholders are the UICC manufacturers, electricity meter providers, 5G infrastructure providers, virtualized infrastructure providers, MNOs (Mobile Network Operators), and the city that manages the electricity service. The dedicated end-to-end slice for IoT traffic flows (red dashed line in Figure) is managed by MNOs

The electricity meter is represented by the UE domain that consists of UICC, USIM, MEHW, and ME domains. The hardware of the operator network is a collection of IP domains. On the networks logical level we can distinguish between access (A), serving (S), home (H), and transit (T) domains. The electricity service is part of the external network domain consisting of IP and IPS domains. The IoT slices are created from VNFs (Virtualized Network Functions). The stakeholders either manage (blue lines) or provide (dashed blue line) the domains. The relationships between the stakeholders can be described by the trust model that states the following:

1. The city trusts the MNOs to enforce that only authorized electricity meters are allowed to access the given slice.
2. The city trusts the MNOs to protect the readings during the transfer from the electricity meter to the electricity service.
3. The users trust the city and the MNOs to securely collect and transfer data.
4. The MNOs trust the UUIC manufacturers to securely store the network key in the UICC.

Table highlights the security control classes that are relevant for the security realms of the 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.

Table 3.3: Mapping of security realms to control classes in the smart city use case

For each realm, which classes are relevant are identified one-by-one and then for each selected class the challenges are analyzed and prominent control technologies. Specific challenges for this use case arise from device-side resource restrictions and unique machine-to-machine traffic patterns that differ from the patterns of user originated communication. To compensate for hardware and power limitations, optimized protocols and solutions are needed in the application, network, and access network realms. Unique traffic patterns and out-of-date security software of IoT may be source of availability challenges in the network, home and access network domains as well as a privacy challenge for the application domain. This motivates the use of slicing technologies that isolate applications and thus better guarantee availability in the infrastructure realm as well as hardware-based trust assurance and monitoring techniques that enable preventive and reactive actions in the UE and management realms.

B. An SDN Attack

The enabling technology that is used in the aforementioned described smart cities scenario relies on NFV (Network Function Virtualization) and SDN (Software Defined Networking). NFV and SDN technologies enable the operators to provide cost-effective means for creating dedicated slices for traffic flows. Mobile network functions are virtualized and the data flows between functions are managed by SDN controllers. SDN also allows for decoupling of the control and data planes by providing programmability of network configuration, evolution, and policy enforcement.

One of the main threats in all mobile networks is the loss of connectivity. This can happen as a result of a DoS (Denial of Service) attack when an adversary overloads SDN controllers in the H, S or access domains. The threat affects a function in the transport stratum (i.e., forwarding function) through a function in the management stratum (e.g. reconfiguration of routing tables). The attack could be carried out by measuring the response times of the network and determining how to trigger the reconfiguration of routing tables. By revealing information about the networks forwarding logic, this fingerprinting attack makes subsequent DoS attacks more powerful. The DoS attack itself is a continuous loop that repeatedly reconfigures the SDN controller until it gets overloaded. The implications of this attack can be summarized as follows:

- The customers (i.e., electricity meters) may lose connectivity and cannot access the electricity service.
- The MNOs will also suffer if the network becomes unavailable. Customers will lose confidence in MNOs. The operator has the responsibility to address this threat on behalf of customers.
- The VNFs will be affected by the degradation of the network. In this case the MNO can either take responsibility for managing this threat or transfer it to the infrastructure providers.

Conclusion

Although 5G networks will be very different compared to their predecessors in some regards, they will still share similarities and they will reuse and extend existing concepts that have proved successful and that are widely adopted. Reusing and building upon the accepted and well-known concepts and terminology in 3GPP TS 23.101 (also 3GPP TS 33.401 and other standards) helps to understand the similarities and differences better, and provides us with the opportunity to clarify or enhance earlier work by eliminating some of its shortcomings that we have identified as part of our work. Towards this, we proposed in this paper a 5G security architecture that builds upon the concepts of domains and strata, inherited from the security architectures of 3G and 4G networks, but adapts to a 5G context. We also introduced a set of security realms to capture security needs of sets of related domains and strata. The means to satisfy these security needs are categorized in a number of security control classes focusing on different security aspects. The security realms are inspired by security feature groups previously defined for 3G and 4G networks. Security control classes find their source in the dimensions defined in ITU-T X.805 . Then, we demonstrated that our security architecture achieves the key objectives of 5G namely by enabling the capture of new trust models, identification of security control points, capture of security related protocols and networks functions, considering network management and, capture of virtualisation and slicing. Finally, we studied the mapping of a major 5G use case, i.e., smart city, to our security architecture. This use case includes IoT and SDN associated requirements which are of wide interest in 5G.

References

[1] 3GPP. (2008). TS 33.401: 3GPP System Architecture Evolution (SAE); Security Architecture

[2] 3GPP. (1999). TS 33.102: 3G Security; Security Architecture. [Online]. Available:https://www.3gpp.org/DynaReport/33102.html.

[3] ITU-T. (2003). X.805: Security Architecture for Systems Providing end-to-end Communications. [Online]. Available: https://www.itu.int/rec/T-RECX.805-200310-I/en

[4] 3GPP. Release 15. Accessed: Oct. 15, 2017. [Online]. Available: http://www.3gpp.org/release-15

[5] 3GPP. (1999). TS 23.101: General Universal Mobile Telecomunications System (UMTS) Architecture. [Online]. Available: http://www.3gpp. org/DynaReport/23101.html

[6] 3GPP. (2008). TS 33.401: 3GPP System Architecture Evolution (SAE); Security Architecture. [Online]. Available: https://www.3gpp.org/