FIFTH GENERATION SECURITY CHARACTERISTICS AND CHALLENGES

Parveen Singla
Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India

Rinkesh Mittal
Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India

Mohit Srivastava
Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India

Abstract*—The two main foundation stones for 5G to become a platform for the networkedsociety are security and privacy. Cellular systems pioneered the creation of security solutions for publiccommunication, providing a vast, trustworthy ecosystem – 5G will drive new requirementsdue to new business and trust models, new service delivery models, an evolved threatlandscape and an increased concern for privacy. Work on the next generation of mobile networks has gained momentum in the last two years. 5G networks will support a variety of use cases with challenging security requirements. This paper summarizes the current status of 5G security and outlines the essential elements of5G security architecture.

Keywords-*5G Networks, Security, Cellular System, Characteristics;*

I. Introduction

Fifth generation based systems are the next step in the evolution of mobile communication. As a fundamental enabler of the Networked Society, 5G networks need to provide capabilities not only for voice and data communication as we know it today, but also for new use cases and new industries, and for a multitude of devices and applications to connect society on the large scale. Research and standardization have started in many technology areas of fundamental importance for 5G such as cloud and the Internet of Things (IoT). These efforts have achieved various degrees of maturity, although the definition of 5G mobile networks has not yet reached standardization phase in the 3GPP.

The evolution of Long Term Evolution (LTE) is a vital part of 5G. However, 5G will include the evolution of all parts of the network, such as core and management systems, as well as all protocol layers ranging from radio to applications. As a result, security is potentially affected everywhere. Current 4G cellular systems provide a high level of security and trustworthiness for users and operators. Second generation (GSM) systems were the first to have standardized, built-in security functions, which then evolved through 3G and now 4G networks. Although the security designs of previous and current systems have provided a platform of undisputed socioeconomic success, with the number of global mobile subscriptions exceeding 7 billion in 2014 [1], 5G introduces many new aspects that require the following important questions to be addressed: Are there fundamentally new security requirements, and if so, how should they be identified?Can 5G securities be a carbon copy of 4G security?Are previous design approaches still valid?

It is easy to think of 5G networks as mainly a quantitative evolution similar to previous transitions, such as higher date rate, lower latency and more devices. 5G security will just provide all services required for networked society in a better way without fear.

II. Security Characteristics Of 5G

A. 5G Security Drivers

The drivers for security haveremained in place to provide a trustworthy basic connectivity service. This basic trust will continueto be a driver for 5G networks as a high data-rate, mobile broadband service. However, additionalkey driving factors will enter the scene.First of all, 5G networks will be designed to serve not only new functions for people and society,but also to connect industries (such as manufacturing and processing, intelligent transport,smart grids and e-health). With 5G, it is possible to foresee new models of how network andcommunication services are provided. For example, a car manufacturer may wish to providemanagement services for cars. Establishing direct roaming agreements with various accessnetwork providers could be a cost-efficient way to achieve this. Similarly, the concept of terminal/device will change: unattended machines and sensors will connect; sometimes entire capillarynetworks comprising tens or hundreds of individual devices will simultaneously attach to the 5Gnetwork.

Next, new service delivery models will be used, involving new actors in the ecosystem. Cloudand virtualization technologies and anything-as-a-service will be used to reduce costs, and todeploy and optimize services more rapidly. Telecom networks will expose application programminginterfaces (APIs) toward users and third-party service providers to a higher degree, for example,for the purpose of optimized delivery using location awareness, content adaptation and caching.Such optimizations will sometimes be provided by third-party software executing on sharedhardware platforms alongside dedicated telecom software.

Furthermore, general awareness of user privacy in society has increased, leading to a greaterfocus on the protection of user metadata and communication. This issue becomes even morecentral with the developments in big data analytics.

What characterizes 5G, even more than 4G, is that it will have a crucial role in the operationof society. The full scope of security, privacy and resilience will be a concern that spans farbeyond technology. It will ultimately impact legal frameworks, regulation and actions by commercialentities and individuals. There will be increased regulatory involvement in how entire 5G systemswill operate.

B. Security Incrimination

The drivers listed above can be grouped into four characteristics of 5G networks and their usage,each with implications for security and privacy. These characteristics are: new trust models, newservice delivery models, an evolved threat landscape, and increased privacy concerns [2].So, how do these characteristics affect the way we need to approach security and privacy in5G?

1. New trust models

Trust models change over time. As a simple example, consider the bring-your-own-device trendin enterprises. Previously, all user devices could be assumed to be trustworthy, as they were allof the same type, all issued and managed by the corporate IT department. Today, users want touse their personal devices instead, posing threats as potential Trojan horses behind corporatefirewalls.

For current mobile systems, the trust model is rather straightforward, involving a subscriber(and their terminal) and two operators (the home and serving networks). Since 5G is aimed atsupporting new business models and involves new actors, trust models will change, giving riseto extended requirements in areas such as authentication between various actors, accountabilityand non-repudiation. For example, for new critical services such as public safety, what securityrequirements will be projected onto the 5G networks?

The new types of devices will span an extremely wide range of security requirements and willat the same time have very different security postures: industry automation control devices,shipping containers, vehicles forming entire capillary networks, tiny climate monitoring sensorsand, next-generation tablets and smartphones.Devices have so far been assumed to comply with standards and not to deliberately attemptto attack networks. But how well protected are very low-cost devices? Can a single connecteddevice be used as a stepping stone for cyber-attacks deep into the system? And what is theattack surface of a 5G system with billions of inexpensive, connected devices?The existing trust model obviously does not capture this evolved business and technologicalscenery of 5G. To ensure that 5G can support the needs of new business models, and ensuresufficient security, the trust model map must be redrawn. As such, this does not necessarilymean completely redesigning security. However, it is crucial to identify any significant shortcomings.This must begin by defining a new trust model.

2. Security for new service delivery models

The use of clouds and virtualization emphasizes the dependency on secure software, and leadsto other effects on security. Current 3GPP-defined systems are based on functional nodespecifications and abstract interfaces (reference points) between them, and as such provide agood starting point for virtualization. Until now, however, dedicated hardware hasstill often been used for these nodes and interfaces. Decoupling software and hardware meansthat telecom software can no longer rely on the specific security attributes of a dedicated telecomhardware platform. For the same reason, standard interfaces to the network platformssuch as those defined by European Telecommunications Standards Institute (ETSI) in theirNetwork Functions Virtualization work – are necessary to ensure a manageable approach tosecurity.

3. Evolved threat landscape

5G networks also play role as critical infrastructure. Many people will havealready experienced occasions when fixed telephone lines, internet access and the TV servicehave all stopped working at the same time during a major network outage. And societies certainlydo not want to lose electrical power, mobile telephony and more at the same time.Today's networks host various values – examples include revenue streams and brand reputation.The accessibility of these values via the internet has already attracted undergroundeconomies, cybercrime and cyber-terrorists. The values hosted in, and generated by the 5Gsystem are estimated to be even higher, and the assets (hardware, software, information andrevenue streams) will be even more attractive for different types of attacks.

Furthermore,considering the possible consequences of an attack, the damage may not be limited to a businessor reputation; it could even have a severe impact on public safety.This leads to a need to strengthen certain security functional areas. Attack resistance needsto be a design consideration when defining new 5G protocols. Questionable authenticationmethods such as username/password need to be phased out. More fundamentally, however,the new threats emphasize the need for measurable security assurance and compliance; in otherwords, verifying the presence, correctness and sufficiency of the security functions. Those using5G will need answers to questions such as: is it safe to deploy a virtual machine on a given pieceof hardware? And what security tests have been applied to the software?A key asset of the Networked Society will be data. The role that data currently plays in processessuch as decision-making and value creation is changing. Being in control of personal data willbe crucial for operational reasons, but this will also increase in importance in order to createcompetitive advantages. As the carriers of this data, 5G networks will need to provide adequateprotection in the form of isolation and efficient transport of protected (encrypted/authenticated)data.The ubiquity of 5G devices and connectivity will not only affect the technological attack surface;the exposure to social engineering attacks will also increase.

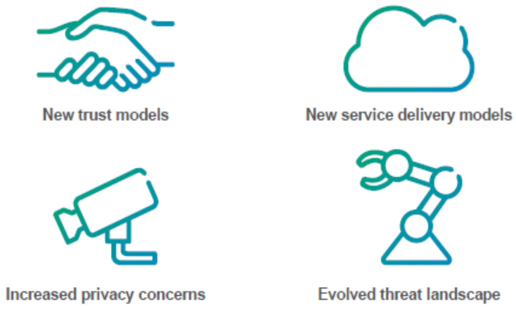

Figure 1. 5G Security Characteristics

4. Increased privacy concerns

There have been several recent news stories related to allegations of mass surveillance. Reportshave also emerged of rogue base stations tracking users in major cities, and of extracting personaldata without user knowledge. The protection of personal data has been discussed within theframework of the EU. It is being reviewed in standardization bodies such as the 3GPP and the Internet Engineering Task Force (IETF), and debated in many other forums.A particularly sensitive asset is the user identifier(s). Ever since 2G, user privacy has been animportant consideration. However, the benefits of full International Mobile Subscriber Identity(IMSI) protection have so far not seemed to outweigh the complexity of implementing it.

III. Elements Of 5G Security Architecture

As the specification work for the overall 5G mobile network architecture is still in an early stage, a 5G security architecture can obviously not yet be given. However, a number of possible elements of this architecture can be anticipated, and are discussed in this section. Figure 2 provides a schematic view of this architecture and depicts possible security architecture elements that are discussed below [3].

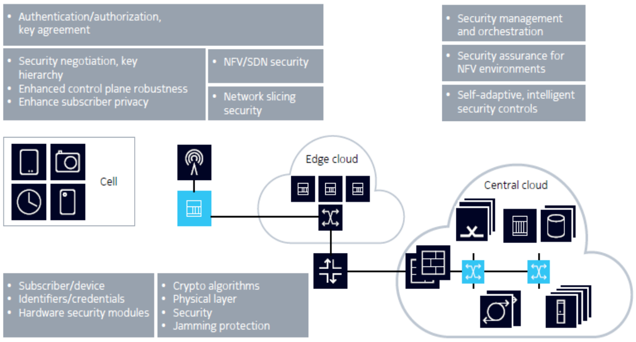
Authentication/authorization, key agreement
Security negotiation, key hierarchy
Enhanced control plane robustness
Enhance subscriber privacy
NFV/SDN security
Network slicing security
Security management and orchestration
Security assurance for NFV environments
Self-adaptive, intelligent security controls
Cell
Edge cloud
Central cloud
Subscriber/device
Identifiers/credentials
Hardware security modules
Crypto algorithms
Physical layer
Security
Jamming protection

Figure 2. Elements of 5G Security architecture

As a basis, a 5G mobile network architecture is assumed wheremost of the network functions run in cloud environments. These cloud environments are not restricted to central clouds, but will comprise a number of highlydistributed edge cloud deployments in order to facilitate mobile edge computing close to the mobile devices. Outside the clouds, “5G Access Points” will be deployed to provide radio coverage to mobile devices. It is assumed that only lower layer functions will be implemented in the 5G Access Points. Using LTE terminology, “lower layer” here means that the Packet Data Convergence Protocol (PDCP) layer that provides the radio interface security will no longer run in a “base station device,” but in the edge cloud.

IV. 5G Security Standarization

The obvious standardization organization for 5G mobile networks is the 3GPP, which has already specified UMTS and LTE. As described, the 3GPP has specified a comprehensive set of potential requirements, including security requirements, for what it calls the “next generation system”. In the context of 3GPP Release 14, studies are being carried out on all important aspects, particularly on the Radio Access Network (RAN) and Service and System Aspects (SA) specification groups. This work is in progress and is being captured in various technical reports [4].

Security work in the 3GPP is carried out in the technical specification group SA3. In the group’s latest meetings, numerous contributions on next generation security have been discussed. In its “Study on the security aspects of the next generation system,” [5]the SA3 has captured many so-called “key issues”, grouped according to security areas, including architectural aspects, authentication, security context and key management, as well as subscriber privacy or network slicing security. Solutions proposed for a variety of key security issues have already been captured. Such solutions provide the input for the normative SA3 work to be started in 2017.

NFV will play a major role in 5G networks, and consequently, also the standards developed by the ETSI ISG NFV[6].In this specification group, security issues are covered by a dedicated security group, which works on topics, such as security management and monitoring for NFV, certificate management guidance, trust/-attestation technologies and practices for secure deployment, specifications for execution of sensitive NFV components, and maintenance host administration, to name a few. In addition, security specifications are being worked out that identify the essential threats for the Management and Orchestration (MANO) components, as well as for the reference points between them.

Besides the 3GPP and the ETSI ISG NFV, other organizations are expected to develop standards relevant for 5G. These include the Open Networking Foundation (ONF)for software defined networking, or the Internet Engineering Task Force (IETF)for multiple kinds of protocols [7-8]. In general, standardization activities outside of the 3GPP will become more relevant for 5G than for previous mobile network generations.

V. CONCLUSION

This paper has provided examination of the security threats associated with 5G networks. As observed by 3GPP today, 5G networks will require complex security requirements at different layers within the system. Moreover, with standardization at an early stage, innovative security solutions proportionate to the threats will have to be built into the network from the very start. This approach will protect subscribers, devices and their communications.

REFERENCES

[1] Ericsson, Ericsson Mobility Report, June 2015, available at: http://www.ericsson.com/ericsson-mobility-report.

[2] 5G Security, Ericsson White Paper, June 2017.

[3] Security challenges and opportunities for 5G mobile networks, Nokia white paper,

[4] "Study on Architecture for Next Generation System", Available at http://www.3gpp.org/DynaReport/23799.htm.

[5] 3GPP TR33.899, "Study on the security aspects of the next generation system", Available at http://www.3gpp.org/DynaReport/33899.htm

[6] http://www.etsi.org/technologies-clusters/technologies/nfv

[7] https://www.opennetworking.org/

[8] https://www.ietf.org/