An Overview of security Scenario for 5G Network

Ms. Uma R. Patil, Dr. V. M. Patil

Abstract— 5G Networks are the next generation in the evolution of mobile communication, related services and a fundamental enabler of the Networked Society. This development creates new security that force to create new security scenarios and requires new security solutions. Security is cornerstones for 5G to become a platform for the Networked Society. Cellular systems pioneered the creation of security solutions for public communication, providing a vast, trustworthy ecosystem 5G will drive new requirements due to new business and trust models, new service delivery models, an evolved threat landscape and an increased concern for privacy and security.

Index Terms— security, 5G mobile network , protections.

1 INTRODUCTION

5G will support a wide range of applications and environments, from human-based to machine-based communication, and thus it should be able to handled with a large amount of sensitive data and that required to be secured and protected against unauthorized access, use, disruption, modification, inspection, attack, etc. Also 5G should be capable to offer services for critical sectors such as Public Safety, Health, and utilities, the importance of providing a comprehensive set of features that forces to required a high level of security in a core for 5G systems. Therefore, 5G should be designed to provide more options beyond node-to-node and end-to-end security available in today's mobile systems. In order to protect users' data, to create new business opportunities required a 5G security design is an all-encompassing one that provides security protection for the everything-connected network. Discussing all this above points, 5G networks security must be "built-in".

2 REQUIREMENTS

2.1 Influence of General 5G Requirements

A significant part of the work on 5G security is naturally dedicated to the discussion of use cases and requirements. General 5G requirements can be highly relevant for the 5G security architecture. For Eg. to initiate communication extremely fast by using authentication and key agreement procedures are executed in the respective use cases. Moreover, a general flexibility requirement could also be applicable to the security mechanisms and procedures supported in 5G.

2.2 Potential Security Requirements

Potential security requirements involve in the following points that consider locations privacy mutual authentications, integrity, platform security.

◎ Confidentiality of user and device identity also providing location privacy

◎ Entity authentication mutual authentication and key agreement between mobiles and the network

◎ Signaling data confidentiality and integrity

◎ User data confidentialitynot in LTE(Long Tern Evolution: integrity)

◎ Security visibility and configurability

◎ Platform security requirements

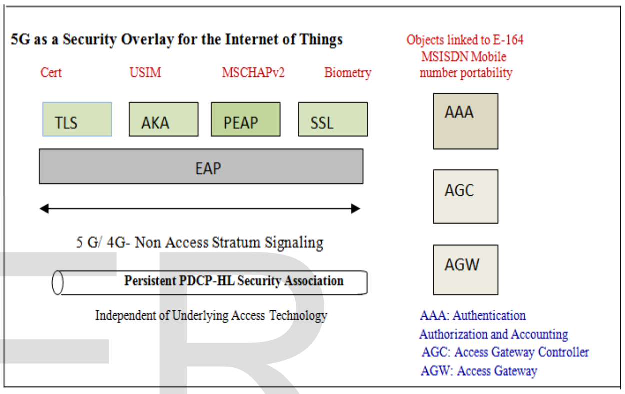
5G as a Security Overlay for the Internet of Things
Cert
USIM
MSCHAPv2
Biometry
Objects linked to E-164 MSISDN Mobile number portability
TLS
AKA
PEAP
SSL
AAA
EAP
AGC
5 G/ 4G- Non Access Stratum Signaling
AGW
Persistent PDCP-HL Security Association
Independent of Underlying Access Technology
AAA: Authentication Authorization and Accounting
AGC: Access Gateway Controller
AGW: Access Gateway

FIGURE 1: 5G AS A SECURITY OVERLAY FOR THE INTERNET OF THINGS

These comprise user data integrity, non-repudiation (e.g. for service requests) and protection against active attacks on the subscriber identity confidentiality (aka "IMSI catching").
Further improvements on the security provided by LTE networks may also be considered, like more robustness against Denial of Service (DoS) attacks in the control plane or against the radio interface. Adoption of new networking paradigms like Network Function Virtualization (NFV) and Software Defined Networking (SDN) may further raise the need of designing secured techniques for the 5 G networks adoptions .

2.3 Flexible Security

Also Flexibility is a general requirement for the 5G to provide the security. Taking user plane security as an example, some applications may not want to rely on security provided by the network, but may rather use end-to-end security. Underlying network-terminated security would not provide a higher degree of security to the applications, but may have an impact on delay or resources on the terminal. Other

Applications, however, may want to rely on user plane security supported by the network, and may even need user plane integrity protection in addition to encryption. To adapt to those varying security requirements, rather than enforcing user plane protection, the network may allow applications to select the way the user plane is protected.

It is clear, however, that it must be guaranteed that the network operator's infrastructure remains protected from abuse even when security can be flexibly selected by the application.

Finally, in addition to the 3GPP (*3rd Generation Partnership Project*) specified radio access technologies, also security concepts from other radio technologies, such as Wi-Fi (i.e. IEEE 802.11), may be relevant for mobile operators, for example for traffic offload. The relevant specification for

Carrier grade deployments is the Wi-Fi Alliance's "HotSpot 2.0" specification which specifies the use of strong security mechanisms.

3 POTENTIAL SECURITY MECHANISMS FOR 5G

The security mechanisms that may be potentially useful to address the security requirements of the 5G networks. Nothing is fundamentally new, and some of it, like public-key based authentication, has even already been discussed during the design of UMTS security in the mid 1990s; but it is certainly worth revisiting the previous arguments in the view of the new architectural and service requirements for 5G and the changed threat landscape.

3.1 User Identity and Device Identity Confidentiality

In GSM, UMTS, and LTE, the permanent user identity is the IMSI (International Mobile Subscriber Identity). The mechanism employed for user identity confidentiality has remained the same across these three technologies: they provide protection against passive, but not active attacks. The situation with the confidentiality of the device identity, the IMEI (International Mobile Equipment Identity), is a little different: in GSM and UMTS, the network, and hence an attacker, may request in an unprotected message that the IMEI be sent in the clear, while the IMEI shall be sent in LTE only in a confidentiality-protected message. This feature is certainly worth keeping in 5G.

3.2 Mutual Authentication and Key Agreement

Authentication corroborates the identity of the other party at the moment the authentication protocol is run. In order to provide continued assurance about the identity of the other party in ongoing communications, authentication between UE (User Equipment) and network has to be always coupled with key agreement. From the agreed keys, further keys have to be derived that are then used to provide confidentiality and integrity for signaling and user data. The possession of the confidentiality and integrity keys then implicitly proves the identity of the other party.

One possible further development would be the use of public-key-based mechanisms for authentication and key agreement in 5G. Advantages of the use of public-key-based authentication and key agreement schemes could include that the home network does not need to be contacted for each authentication or that non-repudiation could be provided, e.g. for the purposes of non-repudiable billing. It was already mentioned in a previous section that the user identity confidentiality could be protected against active attacks in this way.

3.3 Security between Terminal and Network

Signaling integrity is indispensable for preventing impersonation of users and networks. Signaling confidentiality is currently required for providing user identity confidentiality, as discussed in a previous section. The amount of signaling data sent in a mobile system is mostly very small compared to the amount of user data. Therefore, in general, the processing capacity needed for providing signaling data confidentiality and integrity does not seem to have a serious impact on the overall capacity. There may be, however, use cases that may warrant special investigation, e.g. when very small amounts of data are infrequently sent by machine-type applications.

3.4 Security on Network Interfaces

Currently, 3GPP specifications mandate (under certain conditions) using IPsec to protect core and backhaul interfaces. For the core network interfaces, only signaling protection is addressed while the protection of the backhaul link is also specified for the user plane as of yet, it is not fully clear whether the distinction between backhaul and core network interfaces still makes sense in 5G, which non-IP protocols would be used on which interfaces, and whether these interfaces would require separate protection.

3.5 Security Visibility and Configurability

In existing mobile networks, it is the network that decides on the security features and algorithms applied. The choice typically applies to all users in the same way (providing the UE capabilities support it). Further forms of security visibility have been envisaged, but never implemented, such as the use of certain strong or weak algorithms (which would matter especially for GSM where some algorithms still in use have been badly broken).

3.6 Platform Security

The LTE specifications mention the need for secure execution environments and trusted platforms in two places: in TS 33.401 for eNBs, and, in a much more detailed way, for Home eNBs in TS 33.320. It needs to be discussed what type of platform requirements would be appropriate for 5G. Furthermore, also platforms for network functions in the core may require secure execution requirements, which is particularly critical in virtualized environments.

3.7 Protection against Denial-Of-Service Attacks

Denial-of-Service (DoS) attacks aiming at exhausting resources at the victim are very common in the Internet today, targeted mostly against web services. As mobile networks become increasingly important as parts of the critical infrastructure, they are also becoming a very relevant potential target for DoS attacks as acts of cyber crime, cyber terrorism or even cyber warfare.

4 USAGE OF NFV AND SDN

There is a clear trend visible in the evolution of mobile networks towards the adoption of the concepts of NFV (Network Functions Visualization) and SDN(Software Defined Networking). These techniques are already being applied to existing mobile networks, but in 5G, much stronger adoption in all areas of the network, including the radio access network, can be expected. Virtualization technologies using software-defined networking and network functions virtualization are expected to play a significant role in the development of next-generation mobile technology standards expected to rollout under the "5G" banner
With NFV, network functions become virtual network functions (VNFs) and are no longer isolated from each other in dedicated hardware. Instead, isolation fully relies on the virtualization layer, which, as a complex software system, cannot be expected to be flawless. So it may be useful to investigate, design and implement ways to control the allocation of software components to physical computing resources, in a way that retains the capability to use available hardware efficiently and be able to dynamically scale VNFs according to changing capacity demands. Such an approach would for example allow isolating certain VNFs by preventing other software components to run on the same physical computing blade.

5 CONCLUSION

Security features need to be built into the system design for 5G-connected digital society. Identification of the major security requirements and concerns around future 5G systems from different perspectives play an important role between security community and all other parties who contribute for 5G technology. Work towards the fifth generation of mobile networks has gained a lot of momentum recently. It is important to start also the work on the security architecture, in order to ensure that security is built into 5G networks right from the start.

REFERENCES

1. Larsson, E.; Edfors, O.; Tufvesson, F.; Marzetta, T., "Massive MIMO for next generation wireless systems," in *Communications Magazine, IEEE*, vol.52, no.2, pp.186-195, February.

2. Gushing Cao Jean-Pierre Hubaux Yongdae Kim Yanchao Zhang, "Security and Privacy in Emerging Wireless Networks", IEEE Wireless Communications • October 2010.

3. Huawei White Paper, "5G Security: Forward Thinking",Huwai Publications, July 2014.

4. Günther Horn, Peter Schneider, Nokia Networks, München, Germany, "Towards 5G Security" "IEEE Access August 2015.

5. A. Gupta, R. K. Jha: "Survey of 5G Network: Architecture and Emerging Technologies", IEEE Access, Aug-2015.

6. Mohsen Guizani, Daojing He, "Security and Privacy in Emerging Wireless Networks: part 1 ", IEEE Communications Magazine, Issue, June 2015.

7. European Commission, Digital Agenda for Europe, "Towards a 5G Connected World: A Security' Insight, Oct 20, 2015.

8. 5G – ENSURE ,"5G -ENSURE launches to make 5G networks and systems secure and trustworthy", The 5G Infrastructure public private Partnership.