Towards 5G Security

Erzhena Tcydenova
Department of Computer Science & Engineering
Seoul National University of Science & Technology
CIS (Cryptography and Information Security) Lab
2019. 11. 12.

I. INTRODUCTION

❖ This paper discusses potential security requirements and mechanisms for 5G mobile networks. It does not intend to do so exhaustively, but rather aims at initiating and spurring the work towards a 5G security architecture.

❖ When designing 5G networks, architectural considerations must be accompanied with respective security considerations, and such security considerations are expected to influence architectural decisions. In line with this goal, this paper raises a number of questions that need to be addressed in the design of 5G networks.

II. REQUIREMENTS

A. Influence of General 5G Requirements

❖ General 5G requirements can be highly relevant for the 5G security architecture.

❖ A requirement to initiate communication extremely fast will have impact on how and how often authentication and key agreement procedures are executed in the respective use cases.

❖ A general flexibility requirement could also be applicable to the security mechanisms and procedures supported in 5G.

- 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 confidentiality (not in LTE: integrity)
- Security visibility and configurability
- Platform security requirements

- Security requirements that were discussed, but not adopted, for UMTS or LTE may be rediscussed.

- Further improvements on the security provided by LTE networks may also be considered.

- Adoption of new networking paradigms like Network Function Virtualization (NFV) and Software Defined Networking (SDN) may further raise requirements aiming at properly securing these techniques.

- Flexibility is a general 5G requirement that could apply also to security.
- 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 may want to rely on user plane security supported by the network, and may even need user plane integrity protection in addition to encryption.

III. SHOULD 5G SECURITY BUILD ON LTE?

- LTE has so far not exhibited any significant security weaknesses, so it seems natural to use LTE security.
- The 5G security architecture will critically depend on the overall 5G system architecture.
- For security, it may not matter so much whether the 5G (physical layer) radio interface follows a clean slate approach or not, as security is likely to be provided above the physical layer also in 5G.
- Backwards compatibility requirements, regarding the access of legacy terminals to 5G networks will also have a strong influence on the 5G security design, complexity and mobility.
- Security concepts from other radio technologies, such as Wi-Fi, may be relevant for mobile operators.

IV. DISCUSSION OF POTENTIAL SECURITY MECHANISMS FOR 5G

A. User Identity and Device Identity Confidentiality

- In GSM, UMTS, and LTE, the permanent user identity is the IMSI (International Mobile Subscriber Identity).
- 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.
- The protection against passive attacks on the IMSI is achieved through the use of temporary identities.
- IMSI catching, i.e. harvest the IMSIs of all subscribers in the vicinity of the attacker's false base station.
- Public key, symmetric key methods and the use of pseudonyms are mentioned as potential countermeasures.

- 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 and network has to be always coupled with key agreement.
- The authentication and key agreement protocols used in UMTS and LTE are called AKA.
  - UMTS AKA provides a guarantee to the subscriber that it is connected to a network entity authorized by the home Network;
- EPS AKA, which is used in LTE, is almost identical to UMTS AKA, except that EPS AKA provides an additional guarantee to the subscriber about the identity of the serving network.

- No security vulnerabilities of UMTS AKA or EPS AKA have become known since.
- Besides being secure, UMTS AKA and EPS AKA are also efficient:
  - The messages are short compared to other authentication protocols;
  - Only one handshake between UE and serving network and between serving network and home network is required;
  - The HSS does not need to keep protocol state as the HSS just responds to a request from the serving network and updates its data base;
  - The protocol is symmetric-key-based; this makes the computations required in the Authentication Centre.

❖ One possible further development would be the use of public-key-based mechanisms for authentication and key agreement in 5G.

❖ The home network does not need to be contacted for each authentication or that non-repudiation could be provided.

❖ The use of permanent symmetric keys as a basis for authentication and key agreement in mobile networks was questioned as a result of the alleged attacks by powerful agencies against the SIM provision process.

- It was claimed that a property called Perfect Forward Secrecy (PFS) could have helped in thwarting these attacks.
- PFS is typically provided using a form of the Diffie-Hellman (DH) mechanims.
- The use of DH would force an attacker to play man-in-the-middle at the time of eavesdropping.

- Another aspect that needs to be considered in 5G is the storage of credentials on the UE side.
- The long-term credentials, permanent authentication keys, are stored in the USIM, which is an application on the UICC (Universal Integrated Circuit Card), a smart card platform.
- Present UICCs are removable and pre-provisioned with credentials for one operator.
- This may be cumbersome or even prohibitive especially for devices used for machine-type communication.
- Embedded UICCs may further ease the implementation of the UE as there no longer is the requirement of removability of the smart card.

- Signalling integrity is indispensable for preventing impersonation of users and networks.
- Signalling confidentiality is currently required for providing user identity confidentiality.
- The amount of signalling data sent in a mobile system is mostly very small compared to the amount of user data.
- The processing capacity needed for providing signalling data confidentiality and integrity does not seem to have a serious impact on the overall capacity.

- There is a distinction in LTE, as opposed to UMTS, between NAS layer signalling and AS layer signalling.
- This prevents base stations that may have been compromised by a physical attack, from accessing the NAS signalling.
- A threat that was not present in UMTS, as UMTS radio interface security reaches beyond the UMTS base stations, up to the radio network controller.
- This division also provides a strengthening of security in LTE over UMTS
- NAS security context may be always available in the UE and the network, even when the UE is deregistered, while the AS security context is only available when the UE is in connected mode.

D. Security on Network Interfaces

- Currently, 3GPP specifications mandate using IPsec to protect core and backhaul interfaces.
- For the core network interfaces, only signalling protection is addressed while the protection of the backhaul link is also specified for the user plane.
- Questions to be discussed here for 5G include:
  - whether this different treatment of the user plane for backhaul and core network interfaces is still justified in 5G.
  - whether protection mechanisms at layers different from the IP layer would be needed.

E. Security Visibility and Configurability

- In existing mobile networks, it is the network that decides on the security features and algorithms applied.
  - the network may choose to not activate encryption due to legal constraints in the country of operation;
  - or the network may support only certain algorithms.
- Since GSM, specifications therefore demand that the user shall have the possibility to see whether encryption is applied.
- The number of terminal types supporting a ciphering indicator is decreasing.

E. Security Visibility and Configurability

- Security configurability is a property that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation.
- However, the only use case explicitly is “enabling/disabling user-USIM authentication”.
- The questions includes whether users have sufficient awareness of consequences of security decisions or whether security should be rather transparent to users.

F. 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 for Home eNBs in TS 33.320.
- It needs to be discussed what type of platform requirements would be appropriate for 5G.
- Platforms for network functions in the core may require secure execution requirements, which is particularly critical in virtualized environments.

- Denial-of-Service (DoS) attacks aiming at exhausting resources at the victim are very common in the Internet today.
- Better availability of protocol stacks (in form of OpenSource software) will further lower the hurdles for external attackers and thus increase the likelihood of serious DoS attacks carried out by mobile botnets.
- Another type of DoS attack that is specific to wireless communication is radio interface jamming.
- Control plane protocols between mobiles and the network should be designed.
- Overload protection mechanisms must be implemented.

V. USAGE OF NFV AND SDN

- There is a clear trend visible in the evolution of mobile networks towards the adoption of the concepts of Network Functions Virtualization and 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.

V. USAGE OF NFV AND SDN

- With NFV, network functions become virtual network functions (VNFs) and are no longer isolated from each other in dedicated hardware.
- Isolation fully relies on the virtualization layer, which, as a complex software system, cannot be expected to be flawless.
- Network security concepts typically rely on separating traffic types, such as user, control and management traffic.
- Such concepts can clearly be transferred into an NFV environment.
- A relevant issue with NFV is software integrity protection. Integrity and confidentiality protection is for sure a requirement here.

V. USAGE OF NFV AND SDN

- Within a datacenter, connectivity may be enabled by means of SDN.
- SDN may apply to fronthaul or backhaul networks, to wide area networks interconnecting the various, distributed sites implementing the radio access network and core clouds.
- SDN comprises the separation of the control plane from the forwarding plane, allowing to implement SDN controllers as logically centralized network functions within a cloud and also comprises programmability.
- While SDN is supposed to bring significant advantages in terms of flexibility, agility, automation and efficiency of network control, possible security threats must be mitigated by protection measures.

VI. CONCLUSION.

- This paper was written before the 5G revealed itself.
- There were discussed security requirements that 5G has to face.
- Most of these requirements were considered in 5G network, for example:
  - Usage of public-key certificated has been started for authentication
  - NVF and SDN is being applied more widely.

CIS LAB

Thank you for your attention