5G Security: Forward Thinking

Huawei White Paper

HUAWEI

Content

1 Foreword

As vertical industries are thriving —Vehicle Network, Internet of Things (IoT), AR/VR, and high speed railways, just to name a few — they all demand fast yet ubiquitous network access to gain a new momentum. The rise of new business, new architecture, and new technologies in 5G will present new challenges to security and privacy protection.

In 5G business environment, security is a necessary enabler for continuity of the business. Users already realize that security and privacy are important, and they could be aware of the security/privacy service provided to them. It is believed that the extent and strength of the security mechanisms provided correlate with the perceived security level, at least in the long run. Perception is closely related to trust, hence negative changes may happen very quickly (e.g. because of front-page news about observed attacks).

In the 5G context, users may already have some perception of provided security level based on experience with earlier generations. To provide continuity of perceived security, it is important that security and privacy features that exist in earlier generations are also present in 5G, although the actual technical security mechanisms may be different.

On the other hand, it is clear that it is not sufficient just to provide the same security features as in the legacy systems because there may be new security requirements and challenges. 5G systems are going to be service-oriented. This implies there will be a special emphasis on security and privacy requirements that stem from the angle of services.

2 5G Security Challenges

Traditional Security Practice

Mobile communications systems have evolved through wireless technology innovation into 2G, 3G, and then 4G to keep pace with ever increasing voice and data traffic. Tougher security mechanisms are in place to safeguard today's mobile communication systems. For instance, one-way authentication in 2G has been elevated to mutual authentication in 3G & 4G; key length and algorithms are becoming more robust; as mobility management is improving, a forward key separation in handovers has been added in 4G; also more effective privacy protection is considered.

Traditional security architectures focus on protection of voice and data, and they all have the following security features in common:

- User identity management based on (U)SIM
- Mutual authentication between networks and users
- Securing the path between communicating parties hop-by-hop

Security Challenges Ahead of 5G

New Business Models

In traditional mobile communications networks, the primary goal is to enrich people's life through communication. Users may communicate by text messages, voice calls, and video calls, or surf Internet or access app services using smart phones. However, 5G is no longer confined to individual customers. It's not simply about having a faster mobile network or richer functions in smart phones. 5G will also serve vertical industries, from which a diversity of new services are going to stem.

In the context of vertical industry, security demands could vary significantly among services. For instance, mobile Internet of Things (IoT) devices require lightweight security while high-speed mobile services demand high efficient mobile security. The network based hop-by-hop security approach may not be efficient enough to build differentiated end-to-end (E2E) security for different services. As IoT is gaining momentum, more people will be able to remotely operate or "talk" to networked devices, for instance, instructing facilities at a smart home to get up. Therefore, there is a need of a more stringent authentication method to prevent unauthorized access to IoT devices. For example, biometric identification could be part of the authentication in smart homes.

IT-Driven Network Architecture

New IT technologies, like virtualization and Software Defined Network (SDN)/Network Functions Virtualization (NFV), are seen as a way to make 5G networks more nimble and efficient, yet less costly. While CT are happy to see IT injecting new vigor into their networks, new security concerns are emerging.

Security cannot be built for 5G services unless the network infrastructure is robust. In legacy networks, security of function network elements (NEs) relies largely on how well their physical entities could be isolated from each other. However, in 5G, the isolation will work differently as virtual NEs on cloud-based infrastructure. It's likely that time is right to take 5G infrastructure security into consideration.

SDN is proved to be of help in improving transmission efficiency and resource configuration. On the other hand, it is important to consider in the 5G security design that it could be managed in terms of the isolation for network nodes such as control nodes and forwarding nodes, and the secure and correct enforcement of the SDN flow table.

Based on network virtualization technology, a network could build different virtual network slices. Each virtual network slice could accommodate a particular service requirement and thereby may require differentiated security capabilities. 5G security design may need to consider issues of how to isolate, deploy, and manage virtual network slices securely.

Heterogeneous Access

Heterogeneous will be one of the network features of next-generation access networks. The heterogeneous nature comes not only from the use of different access technologies (WiFi and LTE), but also from multi-network environment, which might imply that the access network architecture from different networks are different. So a consideration for security designers is building security architecture suitable for different access technologies.

IoT devices have many choices in the way they access networks. For instance, they may connect to networks directly, or via a gateway, or in the D2D or Relay fashion. Comparing to mobile handset, security management of IOT device in 5G may be efficient and lightweight in order to establish trust relationships between devices and networks.

Privacy Protection

With the advances of mobile Internet, more and more vertical industries, including health care, smart home, and smart transport, will resort to 5G networks. As open network platforms, 5G networks raise serious concerns on privacy leakage. In many cases, privacy leakage can cause serious consequences.

As primary method for network accessing, mobile networks carries data and signaling that contains many personal privacy information (for instance, identity, position, and private content). In order to offer differentiated quality of service, networks may need to sense what type of service a user is using. The service type sensing may involve user privacy. Add all this together, privacy protection in 5G is more challenging.

3 5G Security Blueprint

5G Security Goals

As the 5G era is drawing near, the volume of data traffic and variety of services will increase to unseen-before levels. IoT service is just one of the many. When it comes to 5G, it is not simply about being a medium for communication. It can be seen as a catalyst for minimizing the boundary between the digital world and physical world. 5G security design is an all-encompassing one that provides security protection for the everything-connected world.

E2E Security for Vertical Industries

- Differentiated security protection
  E2E security design caters to different vertical industries. In that case, the design of security protection needs to consider how to fulfils various security requirements.

- Flexibility
  In order to provide better support and rapid response to the vertical industry requirement, it is nice that E2E security capabilities could be rapidly aligned with business changes. In that case. it would request flexible and high efficient E2E security deployment and adaptation.

- Privacy protection
  5G will see APP services thriving vigorously. Along with this thriving, personal privacy data is growing massively also, including device identifiers, user IDs, and user preference. Considering that, privacy protection could be built end to end, leaving no part of the security chain vulnerable to privacy leaks.

- Security as service
  In face of convergence of IT and CT, telecom industry is seeking to boost their strength and better serve vertical industries. Tele communications systems have done well in protecting user privacy, and users have built relatively good level of trust with security strength of the communication systems. 5G could continue to extend the user trust by opening up security capabilities as a service to individual users and vertical industries.

Secure Infrastructure

- Diversified system level protection of IT-aware infrastructure
  after IT technologies (e.g. NFV and SDN) are put into use, a vast array of system-level protections is in place to defend against distributed denial of service (DDoS) and other active attacks that may increase.

- Identity management
  Both software and hardware infrastructures run in multi-vendor environment. In order to mitigate unauthorized access to network resources, stringent identity management is a possible need.

- Data protection
  Integrity and confidentiality protection are provided throughout data transmission to prevent data from being intercepted or re-routed to unauthorized destinations.

5G Security Perspectives

New Trust Model and Identity Management

In legacy mobile communications networks, Telecom networks are responsible for authenticating user for network access only. A trust model with two elements, between users and networks, is formed. The authentication between user and services are not covered by the networks. However, in 5G networks, a trust model with an additional element, the vertical service provider, is favored possible design. Networks may cooperate with service providers to carry out an even secure and more efficient identity management.

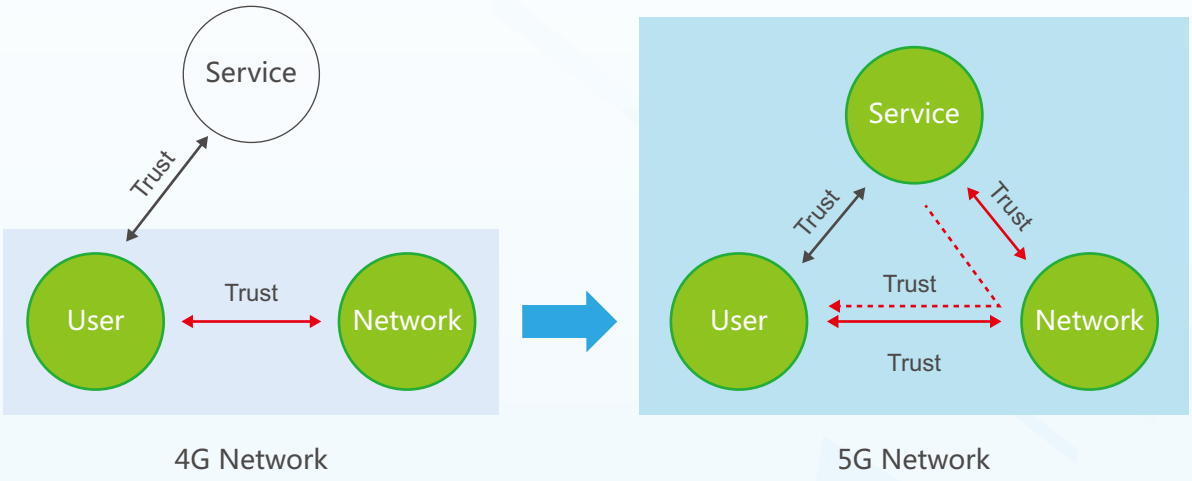

Figure 3-1 Evolution in trust model

- **Hybrid Authentication Management**

5G networks are open platforms with a plethora of services. Smart transport, smart grid, industrial IoT are some of them. Both networks and service providers face challenges in making access & service authentication simpler and less costly. Three authentication models would possibly co-exist in 5G to address needs of different businesses.

- Authentication by networks only
  Service authentication incurs significant amount of costs to service providers. Service providers can pay networks for service authentication so users will be able to access multiple services once they complete a single authentication. This frees users from the cumbersome task of getting service grant repeatedly when accessing different services.

- Authentication by service providers only
  On the other hand, networks may rely on the proven authentication capabilities from vertical industries and exempt devices from radio network access authentication, which can help the networks lower down operating cost.

- Authentication by both networks and service providers
  For some of the services, a legacy model might be adopted. Networks take care of network access, and service providers deal with service access.

• Diversified Identity Management

Legacy cellular networks rely on (U)SIM cards to manage user identities and keys. In 5G, equipments such as sensors, wearable devices, and smart home devices are possibly either too small or too cheap to accommodate (U)SIM. Now the time has come to find a new way of managing device identities, for instance, produce, assign, and apply lifecycle management on device identities.

- Combination of device identity and service identity
  In the new identity management framework, an identity consists of a device identity and a service identity. Each device identity (also called physical identity) is globally unique and may be assigned to a device at the manufacturing phase. Service identities are assigned by service providers or networks. A physical identity may correspond to one or more service identities.

- From device-based management to user-based management
  It leaves to users to decide which of their devices is allowed to access the network and which service is allowed to use. As an example, devices of a same user may share bandwidth quotas with each other in either online or offline manner.

Service-oriented Security

• Build E2E Security

Differentiated security for different services

5G systems are going to be service-oriented. This implies that there will be a special emphasis on security requirements that stem from the angle of services. For instance, remote health care requires resilient security while IoT requires lightweight security. It is quite reasonable to offer differentiated security to different services.

Flexible security architecture to support security attributes for different network slices

If differentiated security is offered, then flexible security architecture is needed to support E2E protection for different service, based on network slicing architecture. Network manages different E2E security capabilities, including strength of security algorithms, ways to derive and negotiate secret keys, and mechanisms for protecting confidentiality and integrity. Within a virtual network slice, security capabilities could further be distributed.

A Uniformed security management framework for multi-vendor environment

In cloud environment, software and equipments of network infrastructure come from more than one equipment vendors, which relatively complicate the security issues. For the services and users, building an E2E data security chain could be a way to reduce the reliance on individual link security and simplifies security management.

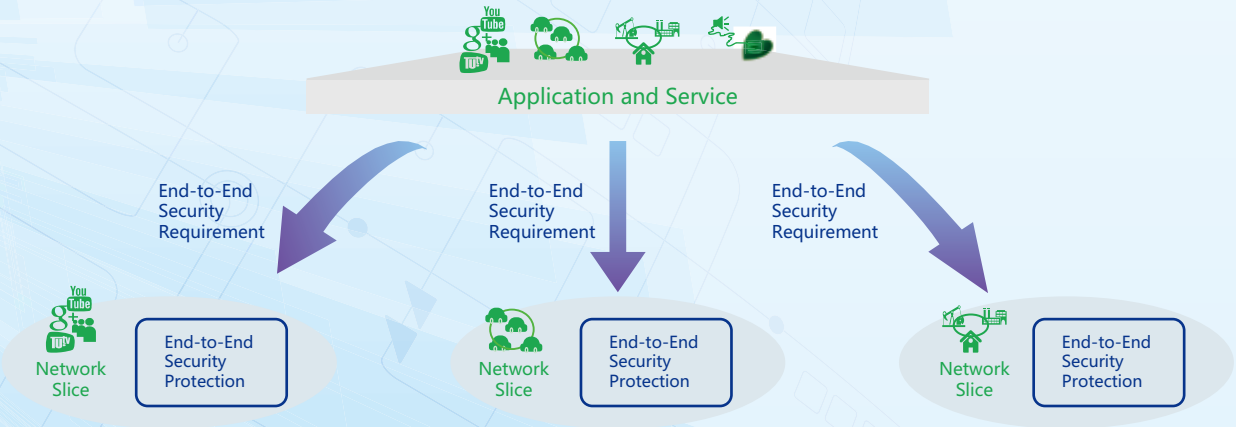

Figure 3-2 E2E security protection

- **Open Up Security Capabilities, and provide security as a Service**

Security management, for instance, managing identities, performing authentication, defending against denial of service (DoS) attacks, and protecting confidentiality and integrity of service traffic, is a general request to vertical industries. However, perhaps not all industry players have the capabilities to build security management on their own, either due to economic burdens or technical challenges, etc. Utilizing security service could be a good choice to these players.

On the other hand, Telecom networks have relatively nice work in the security capabilities (i.e. authentication, identity & key management) and are trusted by users after years of commitment in services. It is a good opportunity for networks to provide their security capabilities as a service to vertical industries. For instance, networks could authenticate service access and return the authentication result to vertical industries.

It is the network's choice either to deploy the security service on a cloud platform or simply built it into a virtual network slice of the vertical industry who has bought the security service from networks. Security capabilities can be seamlessly built into business flows of vertical industries.

- **Isolate Virtual Network Slices**

For virtual network slices, each of which handles a different type of application service to facilitate flexible resource orchestration and scheduling, there is a need to isolate slices from each other to prevent their resources from being accessed by network nodes in other slices. For instance, patients in a health care slice desire to allow only doctors access their health data, and they are reluctant to see their data accessed by someone in other slices.

The isolation statement is also applicable to virtual network slices with the same type of application service. For instance, enterprise A may hope to block other enterprises from using its resources, although these enterprises are served by a same type of virtual network slices.

The isolation effect for service and data in the virtual network slices could approach to the user experience in traditional private network, only in this way the users are willing to store the private data on cloud, and then they could freely access their private data without concern about the security risk on the data.

Security Assessment

5G needs an open platform to support a vast array of services from vertical industries, for instance, remote health care, Internet of Vehicle (IoV), and IoT. The platform can be further divided into units based on the functions. Different software or hardware vendors can contribute their own strength in the development of the units. In this way, the service deployment can be more rapid and the operating cost can be reduced.

To build an open software & hardware ecosystem, it is essential that network function units from different vendors are interoperable via standard interfaces. All network function units may need to attest to each other that they are secure, so that when they are integrated into a platform, a high level of platform security could be achieved. A traditional way to assess their security strength is that vendors sign a trust agreement and then test security performance of each other. However, the testing model is expensive and impedes the growth of the open software & hardware ecosystem. Therefore, a well-received assessment procedure and tools are seemed to be possible approaching, by which all vendors could follow a standard procedure to test their network function units.

Security assessment is feasible only if specific and measurable security metrics are figured out for each network function unit. For instance, the metrics could be the password length and its complexity. An important point to note is that the way for defining and

measuring these security metrics. Security metrics that are standardized and well received could help in the case that even third-party test bodies can effectively assess network function units.

To support dynamic service deployment as well as automatic service rollout, deployment, and management, network units that pass the security assessment can be granted a certificate and an electric signature for automatic verification upon integration. To keep track of security risks, it is nice that security management maintenance be performed on a regular basis during business operations that security measures can be taken on a timely manner in the event of an incident.

Low-Delay Mobility Security

Emerging of delay-sensitive applications such as vehicles network and remote surgery have communication scenarios characterized by low-delay and high-security. In these scenarios, the 5G network may need to support high reliability while providing QoS guarantee with a delay not more than 1 millisecond, so as to prevent accidents such as vehicle collision and surgical operation errors. Further, with the deploymentof ultra-dense deployment technologies in the 5G network, when a vehicle is on the move, mobility management procedure can occur frequently. Considering the delay requirement, the mobility management-specific functional entities and processes need to be optimized.

To address these new challenges, mobility security may be redesigned and optimized for the 5G network to build an efficient, lightweight, and compatible mobility management mechanism to meet the more stringent delay requirements.

User Privacy Protection

As 5G networks will serve a large number of vertical industries. This indicates that a great amount of user privacy information will be carried over the 5G network also. Any information leak may lead to severe consequences. With advancements in data mining technologies, retrieval of user privacy information has been made easier. Therefore, user privacy information must be securely protected in the 5G network so that users and vertical industries can use the network without worrying about information leakage.

- ### Usage management of privacy information in 5G network.

  The 5G network provides customized network services (including slice customization or selection) for users by sensing their service features. However, privacy information, such as user health information and location, may be utilized in the service type sensing process. To protect user privacy, a service sensing rule must be clearly defined for the 5G network to address users' concerns about privacy. The method must stipulate how the privacy information is used and how it is handled after being used.

- ### More rigorous privacy protection scheme in 5G network.

  In a heterogeneous network where multiple access technologies are used, the protection for user privacy information varies depending on the access technology. In addition, the 5G network is one that runs over multiple types of network. User data may traverse various access networks and network functional entities supplied by different vendors. As a result, it’s possible that user privacy information could exist in any corner of the networks. With data mining technologies, a 3rd-party may be able to derive detailed user privacy information through analysis on the disperse user privacy data. Therefore, it’s time to have privacy information exposure risks thoroughly considered in the 5G network.

4 Summary

Security and privacy for a large system such as 5G cannot be properly built after other parts of the system design have already been completed. Instead, security and privacy features need to be built into the system design. This goal requires an active dialogue between security and privacy community and all other parties who contribute for 5G technology.

At the moment, many aspects of 5G are still uncertain but certain high level decisions about security and privacy principles could already be agreed between the stakeholders. For instance, it could be agreed whether or not 5G security and privacy solutions would cover the service layer in addition to the access layer. As another example, time is right to agree whether to extend the role of end-to-end protection mechanisms from what they have had in previous generations.

Similarly, it could be already agreed now whether to aim for extended protection of identity and location privacy against active attackers.

All these principles, if adopted, would have an impact on 5G system design and they could be taken into account in the design from the early phases, and the dialogue could begin. All issues we have discussed in this paper would be solved at some stage of the dialogue, once it has started.

Security and privacy requirements are often seen as obstacles or burden in the system design but ignoring them in the beginning is not cost-efficient in the long run. Adding features afterwards is less effective and often more costly than including proper mechanisms from the beginning. In long term, security is a driving factor for service and network evolution. Since the service and network architecture of 5G is going through dramatic remodeling, it will improve the feature and competitive strength for 5G if security protection and privacy consideration is included at early stage of 5G.

Huawei 5G website

Trademark Notice

NO WARRANTY

HUAWEI TECHNOLOGIES CO., LTD.
Bantian, Longgang District
Shenzhen518129, P. R. China
Tel:+86-755-28780808

www.huawei.com