12

User Privacy, Identity and Trust in 5G

Tanesh Kumar[1], Madhusanka Liyanage[1], Ijaz Ahmad[1], An Braeken[2], and Mika Ylianttila[1]

[1] *Centre for Wireless Communications (CWC), University of Oulu, Finland*
[2] *Industrial Engineering INDI, Vrije Universiteit Brussel VUB, Nijverheidskaai, Brussels*

12.1 Introduction

5G systems are the next major transition in the way of future mobile communications. 5G technology promises to provide higher bandwidth and lower latency. Unlike the traditional mobile technologies, which are mainly meant for voice and data communications, 5G ensures to provide much more. 5G technology has the great potential to enable services for new use cases and vertical industries, for example, in the healthcare, transportation and smart homes. It provides opportunities for companies to build new business models to deliver novel services to consumers in more improved and efficient ways, as well as to increase their revenue. This rise in new business models, architecture and technological changes in 5G will bring new challenges to the user's privacy. The privacy requirements is one of the crucial elements to consider in the discussion of 5G technology as it is of utmost importance to balance the privacy requirements of users with respect to the services offered.

The on-going mobile networks mainly consider four security aspects, that are; authentication, integrity, confidentiality and availability. However, the privacy requirements are not at all (not only) taken into account from the infrastructure and but architecture's perspective as well. As 5G will produce novel and critical applications, it is therefore vital to consider the privacy characteristics from the architecture's point of view, such as observability, anonymity, unlinkability and pseudonymity. This will also ensure the strong trust relationship of the consumer with mobile operators and with the third parties, which are providing the various services. Also, not all privacy aspects can be included while addressing the architecture of the network, due to the lawful and privacy regulatory policies [1,14,15].

5G technology predicts the vision of "always available", where the services are available to users anytime and anywhere. This 24/7 connectivity with other devices may originate a number of attacks such as impersonation, Denial-of-Services (DoS), and replay attacks among others. 5G technology is also considered the key enabling technology for providing ubiquitous connectivity for smart objects. The immersive experiences, such as context

A Comprehensive Guide to 5G Security, First Edition. Edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila.

aware services, augmented reality, and concepts of anything as a service and user personalization will be a major vital force behind the massive adoption of 5G technology. 5G is also the main driver for Internet of Things (IoTs)-based applications, where things are connected through this technology and services will be delivered by more efficient and faster means. This means that 5G requires special consideration on privacy requirements from various perspectives of technologies and services [14,15].

Moreover, due to recent advancements in sensing and communication technologies such as smartphones and wearables, the general awareness of privacy in current society has increased, and thus this encourages higher protection of user's metadata and communications. With the kind of capabilities 5G would possess, it is expected that novel use cases and applications will come into the real-time actions. Service-oriented privacy mechanism would be a more preferable way to protect the privacy. Also, in the case of 5G, security- and privacy-based solutions need to be focused from scratch. Therefore, it must add the security and privacy features built in to the system design from the start.

The continuous improvements in mobile communication technologies also require enhancement in identity management techniques. 5G technology will bring an enormous number of users and devices together and they will be connected in a ubiquitously manner, therefore it is crucial to protect the identities of subscribers as well as of devices. It is important to make sure that no any adversary or third party can steal the subscriber's real identity without his/her consent. Similar kinds of secure approaches are needed for building and maintaining the strong trust relationship among subscribers and various stakeholders, such as service provider, enterprises, etc.

This chapter mainly highlights the potential privacy, identity and trust challenges for future 5G technology from the user's point of view. Section 12.2 gives some background knowledge regarding security and privacy issues about previous generations. Section 12.3 elaborates on the user's perspective on privacy, which is further expanded into three sub-parts, that are; data, location and identity privacy. Identity management mechanism and its related challenges are explained in Sections 12.4, and Section 12.5 presents the trust issues and elements required for developing the business models in the 5G system. Finally, we discuss the overall aspects in Section 12.6 and conclude in Section 12.7.

12.2 Background

Over the last two decades, smart devices such as smartphones and tablets have provided more ubiquitous and persuasive types of services to consumers. The initiation of mobile communication systems, starting from the second-generation Global System for Mobile Communications (2G/GSM) and heading towards the third-generation Universal Mobile Telecommunication Systems (3G/UMTS), has expanded widely into all parts of the world. The next major transition is this evolution was the latest generation, "Long Term Evolution" (4G/LTE) systems, which are being broadly deployed.

Right from the start, there have been numerous threats faced by 2G systems, such as no mutual authentication mechanisms available between mobile phone users and the networks. It means that with these limited resources, it was easy for an attacker to launch a fake base station and assure the mobile devices that it is a valid base station and that it can connect to it. Fake base stations can also act as International Mobile Subscriber

Identity (IMSI) catchers, due to lack of authentication mechanisms and thus can be used to trace and monitor users. The next major transition is the 3GPP (Third Generation Partnership Project), which increased the level of security as compared to the 2G systems. The security specifications in 3GPP also included the mutual authentication mechanisms [2,3]. Furthermore, with the increase in the amount of mobile data, along with the evolution of new applications, the motivation growed to move from 3GPP towards the fourth-generation. LTE is designed to allow strong cryptographic, encryption and mutual authentication mechanisms [3,4].

The techniques to tackle the identity management challenges are an essential part of 5G, due to the fact that the security requirements will be high in this case. Threats such as International Mobile Subscriber Identity (IMSI) catching were also discussed during the standardization of 3G and 4G and thus it is also considered as a focal point in 5G systems [5]. There is not yet any complete or exact document/specification available (at least not in the technical specification for 3GPP) regarding trust models for on-going mobile networks (2G-4G). But considering the trend of security requirements, which has evolved from 2G-4G, the current trust model for mobile networks can also be analyzed. However, in the case of 5G networks, the trust model among various stakeholders would be even more complex, because additional entities will also become involved.

12.3 User Privacy

5G technology will enable several novel applications that will potentially open doors for a large number of vertical industries. This leads us to the fact that a large amount of personal information will be carried out over the 5G networks. With the introduction of data-mining techniques, it is easier to retrieve the data privacy information and thus the data is at huge risk. The 5G system must provide security mechanisms for protection of a variety of trusted information, regarding humans as well as for machine-users (e.g. identity, subscribed services, location/presence information, mobility patterns, network usage behavior, commonly invoked applications, etc.).

5G technology would also offer customized network services for consumers by realizing the characteristics of particular services. Thus, the privacy requirements in the 5G network may vary from service to service. 5G technology will also enable service-oriented privacy requirements. For example, health information of the users in certain healthcare applications will require a higher degree of privacy. Also in the case of some critical industrial tasks, equally higher level of privacy protection is required. But applications like searching for some kind of location information may require a smaller degree of privacy. For more focused understanding, we have split the user privacy concepts into three parts, that are; data, location and identity privacy, as shown in Figure 12.1.

12.3.1 Data Privacy

There will be heaps of smart and heterogeneous devices connected through 5G technology, thus the chances of leakage of the user's personal data is very high. Service providers/companies store and use the private information of consumers without their permission. In some cases, the service provider stores the user data for their own product, but later shares them with other companies so that they can analyze the data and find some trends that, which of their own product is more suitable for that particular

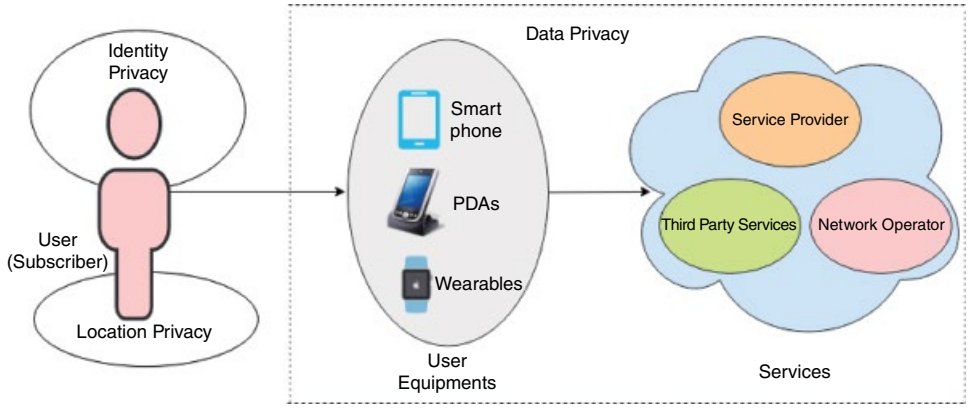

Figure 12.1 Various elements in user privacy.

user. In certain cases, it is even useful to take some of the user's personal data, and based on that, the company can build new products and services. But companies/service providers need to provide a clearer explanation regarding for what purpose their data have been used. They must also answer questions like what data has been taken and how and where they stored it.

Several smartphone applications (Apps) for example in android, ask for certain information before the installation. Mostly, the information for which the App wants permission does not have any direct relation to service of that particular App. This data can be used for other purposes, which are undefined by the Apps developers [6]. Nowadays, social media sites are the most common ways to share public and private information among various users. These are the frequent ways of updating others about your current activates, share/upload personal pictures and even can have live text, audio and video conversations. 5G is supposed to enable this kind of communication seamlessly and continually. But still many people raise doubts over the leakage of their personal information by various means, which are of real concern for our current society.

5G-based IoT systems are the crucial part of future technologies for providing numerous digital services. This will eventually generate massive amounts of data all the times. Since IoT is becoming omnipresent, large amounts of data will be coming into action. 5G will assure the increase in data transfer speeds and thus have a higher risk of malicious attacks. In a similar way, wearable devices produce an explosive quantity of data, because sensors/chips attached to wearables are continuously monitoring and gathering user personal information such as fitness, pulse rate, etc. This data may be analyzed by a third party, who can extract other features from them without asking permission of the user.

Data privacy risks arise when the third party/service provider or any malicious attacker wants to access the user's personal data without their consent. For example, by monitoring the activities of someone using its personal data, one can easily predict the daily routine of that particular consumer. This can be harmful in some cases, because if somebody wants to observe/guess the activities of a person, they can easily do so. The other critical example can be that of healthcare, where the medical data is very sensitive.

In many cases, the patient wants to restrict some particular information to certain people such as doctors, specific family members or friends. But malicious users or unauthorized persons may access the information and use it for unethical purposes. Another such example of privacy breaches can be the purchasing of anything on a consistent basis, like any particular type of food that may reveal religion or health information.

In 5G networks, for many cases, the privacy protection requirements are also dependent on the usage of the particular access technology. Because the element of heterogeneity will be available at much higher rates, along with multiple access technologies it will be used to obtain the required services. User data will be traversed in various access networks in 5G and different vendors will provide the functional entities for the network. As a possibility, by using data-mining methodologies, a third party can derive user personal information by analyzing the user disperse data, which might be available on any part of the network. Because of the risk of such scenarios, more rigorous data privacy protection schemes are required for 5G networks [7].

It is important to formulate strong data protection mechanisms while discussing standardization and policy-making for 5G technology. The service providers must also explain ways of data collection and its use for various services. There should be a balance between the user privacy and data used by the service providers, so that companies can build novel and useful applications for the user and at the same time, user privacy should not be affected. Accountability mechanisms should be involved so that monitoring of each action by various entities will be easy. Data minimization techniques should also take into account such that companies/service providers/third parties limit the data they collect and retain, and dispose it once they no longer need it.

12.3.2 Location Privacy

Nowadays, several smart devices such as smartphones, tablets and wearables, which have powerful computational and storage capabilities along with positioning technology, can request services at anytime and anywhere. Location Based Services (LBS) are popularly used with respect to the development of future wireless technology. With the introduction of 5G, which will enable seamless and continuous availability of services, the location of the user is also continuously monitored in such cases. In order to provide improved services, various companies have also started to track the current location of the user. From this information, they are constantly monitoring the habits and routine of the user. At one hand, this kind of tracking service helps companies to improve their services and to build new user-friendly services. However, on the other hand, it raises serious concerns over user privacy.

Also, many online apps on mobile devices require location information along with their personal information. In some cases, location information of the user is taken, no matter whether it is to be used or not. These online apps want more and more information with each of their updates. Nowadays, the social media applications like Facebook also have the option "check-in", where users are sharing their current locations. This will raise concerns over tracking of user movements by observing the location information constantly. Recently, wearable devices are also actively used for tracking purposes, such as tracking children and pets. These wearable devices are tracking the respective user every second and that also raised huge privacy concerns.

There are few existing techniques available for preserving the location privacy that can also be useful in the context of location privacy protection in 5G applications/technology. Common methods used to protect the location privacy of the user may include anonymization, pseudonym change and path perturbation [8]. Regulatory approaches are also needed, so that strong rules, regulations and legislation can be designed for proper usage of the network, putting the awareness over of the specification of internet and network security [9]. Encryption-based techniques are among other available ways to protect the user's location privacy. The message is encrypted by the user before sending it to the LBS provider. Once the message is received by the LBS provider, it will be decrypted. This approach includes relatively more intensity of anonymity, but it has high computational and communication costs, which is one of the disadvantages of using this approach [9].

Anonymity-based approaches hide the user's real identity and replace it with pseudonyms. In this case, a trusted middleware is used to generate the fake information (being the pseudonym), which is then sent to the LBS provider for particular location service. There is also another approach, in which the quality of user location information downgrades in order to preserve the location privacy; this is known as obfuscation. For example, one spatial cloaking-based technique is formulated that enlarges the location point of the user to a region called ASR which contains the location of the user, where a typical k-anonymity technique is mostly utilized. Then the trusted third party sends the ASR to the LBS provider to complete the LBS query. And finally, some privacy policy-based approaches are required to ensure that it can restrict the misuse of location information in certain ways, for example, by protecting the user privacy through information retrieval methods [9].

12.3.3 Identity Privacy

While acquiring digital services on certain occasions, consumers do not want to reveal their original identity to other users or to service providers. For example, when asking any queries online or giving feedback on the website of companies, users prefer to remain anonymous. In some situations, users might use temporary or fake identities and discard them when the required task is completed. Knowledge of permanent identity of a user may permit an adversary to track and amass comprehensive profiles about individuals. The trend of stealing online identities is more common nowadays. There are numerous online applications such as shopping and banking that would require online ways of payment through credit cards. This information may lead to revealing the real identity and can cause possible risks to the user's privacy. Usually, anonymity-based approaches are used to hide the real identity. Identity privacy can be further divided into subscriber and device identity privacy:

- *Subscriber Identity Privacy*: In this case, threats can arise when users are tracked or monitored by the subscriber's identifier or may be through a temporary identifier. Users also generally do not want any kind of linkage/connection between their subscriber's identity and device identity. The possible solution to protect the subscriber's identity privacy would be through encryption of the IMSI and usage of enhanced pseudo-identifier. In order to guarantee the unlinkability of the subscriber and device identifier, an anonymization system might be one of the potential approaches to consider [10].

- *Device Identity Privacy*: The vulnerabilities that could exist concerning device identity privacy are that, subscribers do not wish to be tracked by their UE identifiers. Likewise, as with subscriber identity privacy, users also do not want linkage between their subscriber's identifiers with device identifiers. This can be resolved by studying the possible end-to-end anonymization approaches that provide a guard against the unauthorized tracking of devices and preserve the disclosure of device identity. 5G also ensures that only through a confidential protected message, the International Mobile Equipment Identity (IMEI) should be sent [10].

12.4 Identity Management

The mechanism of handling the identity in a 5G system would be a crucial task for certain reasons, such as keeping a high degree of security to ensure mutual authentication along with maintaining the user's friendliness and privacy. As 5G technology will become a more multi-vendor environment and comprise of various stakeholders, a strong identity management mechanism is needed to protect the identity and network from unauthorized access of users. During the standardization process of 3G and 4G, when equipment such as mobile devices show their specific identities, there is a serious threat regarding International Mobile Subscriber Identity (IMSI) catching. At the moment, there is no protection mechanism proposed, because that particular threat has not caused any serious trouble to the access network. It is not completely clear yet that whether this attack is still valid for 5G technology and needs any further consideration [8].

The core reason behind an IMSI catching attack is that while in the unavailability of Temporary International Subscription Identity (TMSI), User Equipment (UE) might be unable to use IMSI as its identifiers. IMSI catching attacks can be both active and passive. In passive attacks, all IMSI can be captured and gathered by the IMSI catcher when it eavesdrops in the neighborhood of the wireless traffic. On the other hand, in active attacks, a fake base station is established that has strong signal strength and might be considered as a legitimate base station. Mobile devices usually prefer the base station with the highest signal strength. A message requesting the identity is sent to all mobile devices within the specific area through this fake base station. Mobile devices send their IMSI, as they consider it a valid base station, which have lost the connection to TMSI. Catching IMSI is often supposed to be a starting point for more detailed eavesdropping attacks in GSM [12]. An enhancement technique is mentioned in [12], which allows home network operators to place their trust less on serving networks and guard against IMSI catchers. The idea is to enhance the handling of identifiers and protocols, so that the UE and home network can see IMSI in clear text.

The on-going privacy preserving mechanisms do not guarantee protection against the threats on air interface, because they act as a valid network that has lost temporary identity and also when the request for IMSI is made, there is no proper protection for passive eavesdroppers that possibly could be available there [12]. Several privacy related attacks have been reported, such as in some cases when a fake base station is plotted leading to the derivation of user's personal information. IMSI attacks are mainly focused on stealing IMSI of a mobile subscriber. The IMSI catcher requests the subscriber's identity from the mobile subscriber for the longer term. This is considered as a normal routine request and in reply, mobile devices send its IMSI using standard

security mechanisms. Hence the IMSI catchers are also used to monitor and track the locations of specific subscribers.

The traditional cellular systems are usually dependent on Universal Subscriber Identity Module (USIM) cards, to manage user's identities and keys. In the case of 5G systems, devices and equipments such as smartphones, wearables and smart sensors would be comparatively smaller in size and too economical to accommodate USIM. Therefore, novel methods are required in this case to manage the device identities [7]. There is possibility of a framework that can comprise the device and service identities together. During the manufacturing phase, the device identity can be allocated and is considered as a unique global identity. On the other hand, the service provider offers the service identities. Device identity is also referred to as the physical identity and may address single or multiple service identities. It allows users to make their decision regarding which particular device can be permitted to access the network and utilize the assigned services [7].

The 5G ecosystem would need more flexible, general and open identity management infrastructure, which should have the scope for various alternatives and be able to give permission for that. One way of proceeding for companies is that, they might allow the existing ID management mechanism to reuse it for 5G access. In 5G, there would be an immense number of hand-held devices that may include smartphones and tablets, as well as wearables; therefore it is important to find ways on how to handle these devices and at the same time maintain the subscribers' identities. It is also crucial to think about novel trust models for 5G networks. There are also some key concepts such as network slicing and virtualization, which must be considered when proposing the secure identity management solutions for such scenarios [11].

12.5 Trust Models

Trust models change with respect to the time and improvements in technology. Previously, for companies, the mobile devices of all users are considered to be more trustworthy, because they were issued and managed by their own IT department. But recently, every user in the company/enterprise wants their own personal gadgets, which can eventually lead to a number of security threats to firewalls of the company [11]. Trust includes capabilities such as security, identity management and privacy. Even with to date, there are no standard trust models available for current networks (2G-4G). The current (2G-4G) trust model mainly comprises of the entities, such as user (subscriber), service provider, network operator, Virtual Mobile Network Operator (VMNO), and equipment manufacturer among others, as shown in Figure 12.2 [1]. Usually, the subscribers keep their trust over the service provider and assume that the rules and regulations written in the service subscription contract/billing must be followed, and this trust is then further developed based on experience, reputation and the legal framework. It is assumed that the end-to-end path between subscribers and service providers are secured during any communication (may be voice), and users trust that their critical data is secure with operators.

The service provider is responsible for providing the required services to subscribers through some kind of user device or equipment, such as a mobile phone or tablet. The trust which service providers mostly seek from the subscribers is that they must

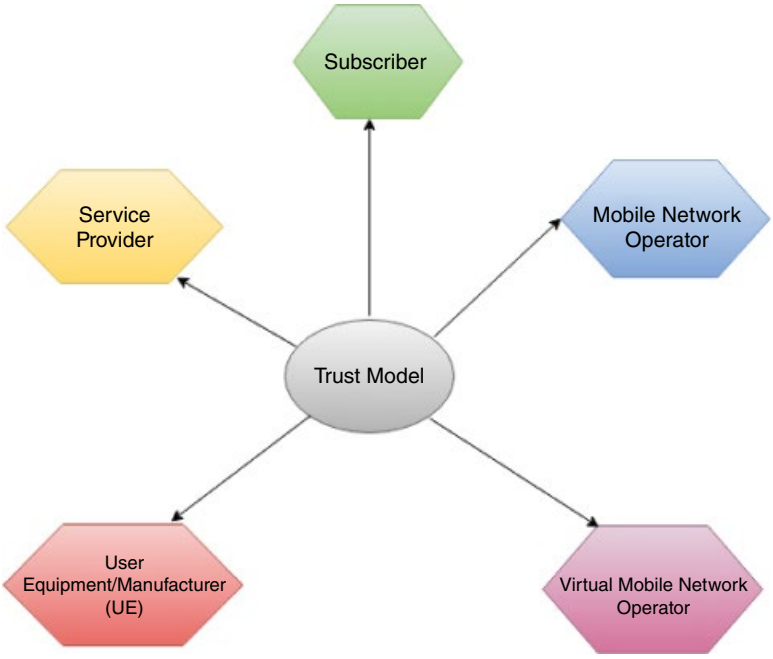

Figure 12.2 Actors/Entities in the trust model.

be able to pay the billing/charging or subscription price well within the predefined time. Although service providers do not have much trust that the subscribers will maintain strong passwords for their authentication to the services and therefore, in order to authenticate securely, it offers the subscriber an UICC. In some scenarios, the two terms, provider and network operator are used in the same context. The network operator is known to be the central element and provides a trust relationship with various other elements in the network. For example, Mobile Network Operators (MNOs) or Satellite Network Operators (SNOs) perform operations such as deploying, maintaining and managing the network (Satellite). Up to now, there are no such standardized security procedures available, which can highlight the network operators sharing certain information. In the current scenario, the trust relationship among various network operators is strong and regulated by contract. However, there can be untrustworthy network operators, who can misuse the personal data, and that can be a serious threat for such networks [1].

VMNO is based on one of the special forms of network operator. It does not contain the mobile network, but instead borrows some virtual space from the database of that network operator. Therefore, it follows almost the same trust model and entities as assigned for the network operators. It keeps the trust between VMNO and its infrastructure elements and can utilize the various resources as agreed in the contract between both of them. Regarding the (UE), it was assumed that this entity does not need to be included in trust models, because the network operator is the one who chooses which manufacturer is trustworthy and which equipment should be used. But there are some cases such as for USIM manufacturer, where it is

required to consider the higher level of trust because of the special requirements for USIM/UICC [10].

From the network operator perspective, Next Generation Mobile Networks (NGMN) [13] presented three types of business models, that is the Asset provider, Connectivity Provider and Partner Services Provider. For Asset, XaaS and network-sharing models are the most important. The Connectivity provider relies on two business models, that is basic (projection of current 4G business) and enhanced. There are also two business models for partner service providers. The first is "operator offer enriched by partner", which deals with the services provided by the mobile network operator using the unique capabilities of third-party resources. The second one is "partner offer enriched by operator", where unique capabilities of an operator is utilized to deliver the services directly to subscribers.

The existing trust models might not be fully applicable for 5G networks, as in the case of 5G, where there will be additional entities and actors coming into action to provide and support numerous novel services. Thus, building the trust model will not be straightforward and will include far more complexities than one could ever have imagined. For example, one of the possibilities could be to introduce a new entity, such as the external cloud infrastructure. This is because through virtualization, network operators can run some operations and applications of the network on the external cloud. Furthermore, these external clouds might also have their own data centers at different jurisdictions. Other possibilities to improve the services delivery in 5G are by in sourcing some of the network functionalities, which can be performed by the third party. As Content Distribution Network (CDN) providers integrate catches in the network operator, it is crucial to consider the fact that the network should not become affected by the addition of these new functionalities. In traditional mobile communication architectures, telecom authorities are responsible for giving access to valid users for specific networks only. There is no trust model available between the authentication of users with their services. However, in 5G networks, this shortcoming would also be resolved, as networks can authenticate the service providers to have even more secure and efficient identity management, as shown in Figure 12.3 [7].

Service providers do not actually trust subscribers to authenticate themselves; instead they are dependent on IMSI stored in the USIM. Hence, IMSI and IMEI are used to

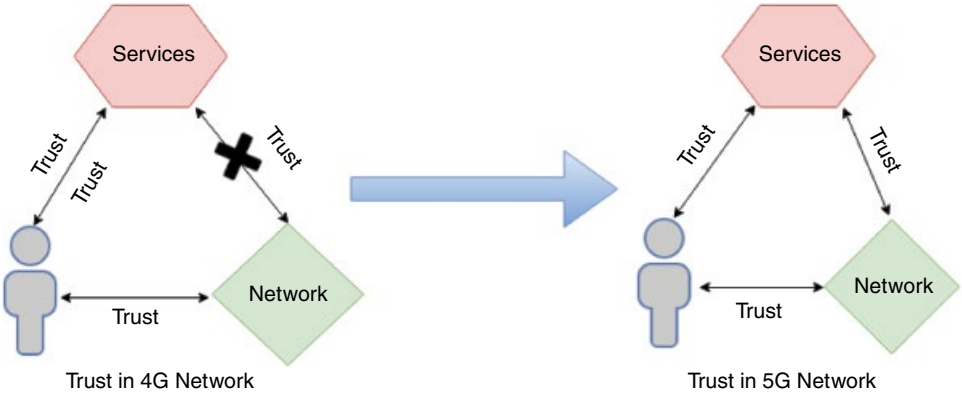

Figure 12.3 Evolution in the trust model.

Table 12.1 Potential threats between stakeholders.

Type of threat	Detail
Malicious stakeholders	One stakeholder might work against another's interests
Non-malicious actions	Caused by actions of stakeholders technological proxies, user errors
Malicious attacks	External attacker may subvert technology of stakeholders, which lead to act against other stakeholders
Internal failures	Caused by internal faults in system leads to detriment of the stakeholders
External disasters	Caused by external sources, such as natural disaster
Threat to stakeholder trust	Stakeholder continues trusting and using system
Threat to stakeholder distrust	Stakeholder loses trust and withdraws from system

detect the attempts of attacks by or against stakeholders. Therefore, subscribers and service providers put their trust in the manufacturers of USIM and Mobile Equipment (ME) domain equipment. Equipment operators are mainly responsible for its behavior, whereas the manufacturer has less responsibility. In some cases, contracts reflect the trust between various stakeholders, such as a roaming agreement of the service provider with other roaming providers, which can permit users to connect to their respective domains. Both the service and roaming providers must have agreements with other providers (services) to establish a communication path for subscribers. In the 5G (4G) network, trust relationships exist between various stakeholders, but there may be certain attacks in which trustworthiness of the equipment may not stay according to expectations [1]. Table 12.1 highlights such kind of threats.

12.6 Discussion

5G technology will dramatically change the current way of acquiring digital services. At this moment, it is hard to elaborate on the complete picture as to how 5G will benefit different vertical industries. However, 5G has promised to do a lot for industries such as automation, healthcare and transportation among others. It is assumed that services will get delivered in a continuous and seamless manner. However, this vision can only be achieved by giving proper attention to security, privacy, identity and trust issues for 5G technology.

In the beginning, we focused from the user's privacy perspective and divided this idea into three key elements; data, location and identity privacy. Huge quantity of personal data is generated by various devices, which are being processed by a service provider/third party. The main issue is that personal information of a subscriber is being used without their permission. In some cases, one company shares the personal information with other companies, so that they can analyze the data and make the relevant new product to generate higher revenues. Hence, strong accountability and transparency is required in such cases. Strong data protection and privacy regulations should be considered in 5G systems. Similar in the case of location privacy, companies through various location-based applications track the user's location without informing them. This raises

privacy concerns for the subscribers. The subscribers may even not want to reveal his/her real identity in environments that are unfamiliar to them. An anonymity-based solution is preferable in such scenarios.

Then identity management mechanisms are discussed, which is another key area to focus while designing the standards and regulation for 5G. New 5G radio access technologies for certain applications, such as industry automation, can be beneficial in terms of low cost and high quality of services. In such cases, it is required to have device identity management for 5G access in various industries. Also, similar kinds of identity mechanisms are needed in situations involving satellite networks and dual satellite and terrestrial 5G access.

Finally, trust is as equally important as privacy and should be taken care of properly in parallel. The trust must cover both human and machine perspectives and trustworthiness by design methodologies. We have explained the entities and elements involved in current 4G networks and highlighted the trust aspects among them. There are no complete standardized trust models available for 4G networks, but various concepts from them can be useful in building the trust among various stakeholders in 5G. The role of privacy would be considered vital in defining the actors for modelling the trust in 5G networks. The ideal trust model for 5G network should be able to answer the questions such as "for what one does on trust?", "how much should one trust?", and "how much anyone can trust?"

12.7 Conclusion

This chapter primarily focused on privacy, identity and trust challenges of the user in future 5G systems. It is undoubtedly agreed by all entities and actors involved in 5G technology that without handling the privacy properly, 5G would face larger obstacles in the way of complete acceptance, adoption and success among their users. From the user's point of view, data, location and identity privacy are the basic-key elements to consider. In the 5G system, privacy features must be considered right from the designing phase and some of them should be built into the system. Furthermore, the system should be intelligent enough and can adopt the privacy accordingly to the degree of importance of services. The context aware applications and services would also require more focused privacy solutions.

5G will be the driving force of many other technologies, such as IoT and therefore an enormous number of users and smart devices would come into action. It is necessary to have a secure identity management mechanism for both subscriber and device. The privacy sometimes has a conflicting relationship with trust, as more trust on service provider can increase the risk of privacy violations. Future 5G systems will introduce new business models that will eventually increase the number of stakeholders and therefore trust association among each of them will be crucial. 5G technology might use some similar concepts to existing trust models, along with the addition of few new actors and entities.

References

1 Deliverable D2.2 Trust model, 5G-ENSURE. Available at: http://www.5gensure.eu/sites/default/files/5G-ENSURE_D2.2%20Trust%20model%20%28draft%29_v1.1.pdf
2 Shaik, B.A. *et al*. (2015) Practical attacks against privacy and availability in 4G/LTE mobile communication systems, Computing Research Repository, October.
3 Gindraux, S. (2002) From 2G to 3G: a guide to mobile security. *Proceedings of the Third International Conference on 3G Mobile Communication Technologies*, p. 308–311.
4 Seddigh, N., Makkar, N.R. and Beaumont, J.F. (2010) Security advances and challenges in 4G wireless networks. *Proceedings of the Eighth Annual International Conference on Privacy, Security and Trust*, pp. 62–71.
5 Rannenberg, K. (2004) Identity management in mobile cellular networks and related applications. *Information Security Technical Report*, 9(1), 77–85.
6 Sørensen, L.T., Khajuria, S. and Skouby, K.E. (2015) 5G visions of user privacy. *Proceedings of the IEEE 81st Vehicular Technology Conference (VTC Spring)*.
7 5G Security: Forward Thinking Huawei, White paper. Available at: http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf
8 Sadegh, F. *et al*. (2015) PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks. *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*.
9 Yu, R. *et al*. (2016) A location cloaking algorithm based on combinatorial optimization for location-based services in 5G Networks. *IEEE Access*, 4, 6515–6527.
10 Deliverable D2.1 Trust model, 5G-ENSURE. Available at: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf
11 5G Security, Ericsson, White paper, June 2015. Available at: https://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf
12 Norrman, K. *et al*. (2016) Protecting IMSI and user privacy in 5G networks. MobiMedia, Xi'an, China, June 18–20, pp. 159–166,.
13 NGMN 5G, White paper. Available at: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
14 Ijaz, A., Namal, S., Ylianttila, M. and Gurtov, A. (2015) Security in software defined networks: a survey. *Proceedings of the IEEE Communications Surveys and Tutorials*, 17(4), 2317–2346
15 Securing the future of mobile services. An analysis of the security needs of the 5G market: a SIMalliance 5G Working Group marketing white paper. Available at: http://simalliance.org/wp-content/uploads/2016/02/SIMalliance_5GWhitepaper_FINAL.pdf