Ericsson white paper
GFMC-18:000078
March 2021; originally published March 28, 2018

ERICSSON

5G security – enabling a trustworthy 5G system

Connected devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy, and the 5G system is designed with these requirements in mind. This white paper provides an overview of the five core properties that contribute to the trustworthiness of the 5G system: resilience, communication security, identity management, privacy and security assurance. Ericsson believes that these properties of the 5G system contribute toward creating a trustworthy communications platform that is an ideal foundation on which to build large-scale, security-sensitive systems, including those used in industrial settings.

Introduction

Ericsson's longstanding vision of a connected society has become a reality in recent years, with mobile systems acting as a backbone for both the Internet of Things (IoT) and a rapidly expanding range of digital services. We believe that digitalization will continue to transform our industries, lives and society. The 5G system will enable many new use cases [1] that will make the critical role of mobile systems even more apparent than it is now.

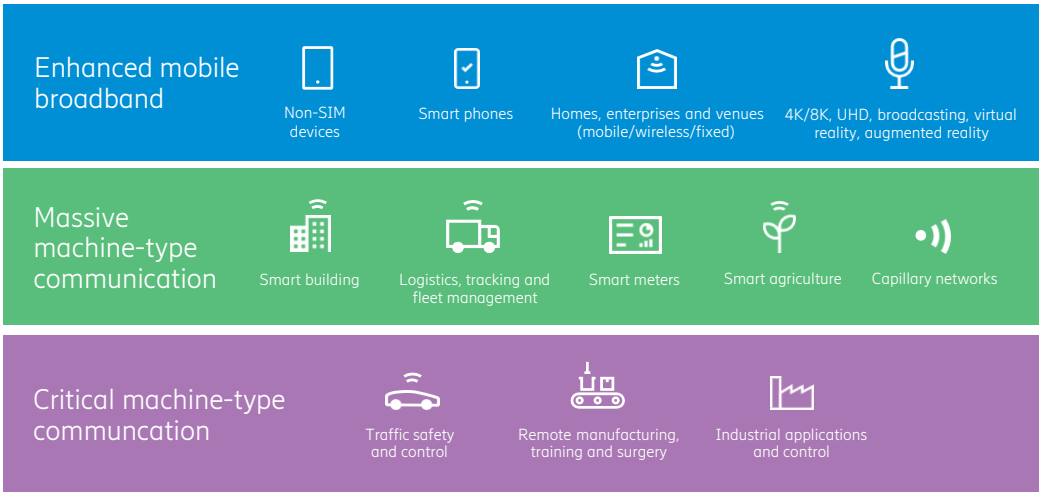

Figure 1: 5G use cases

Figure 1 illustrates the wide variety of use cases and applications that will rely on 5G mobile networks for communication. Some of the applications are simple over-the-top (OTT) applications, which require only best effort communications. Others demand a complete vertical perspective and have stringent requirements on the underlying communication platform [2, 3]. Examples of the latter are medical applications, factory automation use cases and telecommunication services. Because these different use cases may share resources in the mobile network, cyberattacks against one may affect others. The more society depends on digitalized services, the more cyber threats against these services increase.

It is important to realize that OTT security solutions – such as a secure session between an industrial process remote monitoring camera and a control server, for example – are insufficient by themselves regardless of how strong the end-to-end encryption is. Several security aspects cannot be adequately handled on the application layer. One concrete example in this context is availability, defined here as the average percentage of time a certain service is available for use. The camera and the control server could be using secure encryption of the media on the application layer. The availability of the camera service would still suffer if the underlying communications network fails to deliver data due to a cyberattack.

In light of this, it is clear that there are characteristics of the underlying communication infrastructure that, if not properly taken care of, introduce weaknesses in a system taken as a whole. Therefore, for systems to be resilient, secure and privacy-preserving, one needs to take the environment they operate in, specifically the trustworthiness of the underlying communication system, into account.

Context

When discussing security, encryption – and often end-to-end encryption specifically – is the first topic that comes up. While encryption is certainly an important tool, it is just one of the many tools needed to ensure the security of a system.

To build secure systems it is important to take a holistic view and not only focus on individual parts in isolation. For example, interactions between user authentication, traffic encryption, mobility, overload situations, and network resilience aspects need to be considered together. It is also important to understand relevant risks and how to appropriately deal with them; threats need to be weighed against the cost of them materializing and the cost of applying countermeasures. This is what 3GPP does when developing the specifications that constitute the basis for the security of the 5G systems [4].

The holistic mindset is also manifested in the many organizations that are jointly developing the 5G system, each covering different aspects and/or focusing on specific parts. Relevant specifications and supporting studies and functions are produced by such organizations as the Internet Engineering Task Force (IETF), GSM Association (GSMA), European Telecommunications Standards Institute Network Function Virtualization (ETSI NFV) working group, and Open Network Automation Platform (ONAP), to mention a few.

The security and resilience of the 5G system rest on continuous threat and risk analysis as well as more dedicated efforts [5, 6]. The purpose of this is to introduce a balanced set of countermeasures that appropriately match identified threats and risks.

On a high level, a 5G system comprises a device connected to a 5G access network, which in turn is connected to the rest of the system called a 5G core network. **Figure 2** shows a simplified 3GPP 5G system architecture. The 5G access network may include 3GPP radio base stations and/or a non-3GPP access network. The 5G core network architecture is significantly better than 4G in terms of being able to support cloud implementation and the IoT, with major improvements in network slicing and service-based architecture (SBA), in particular.

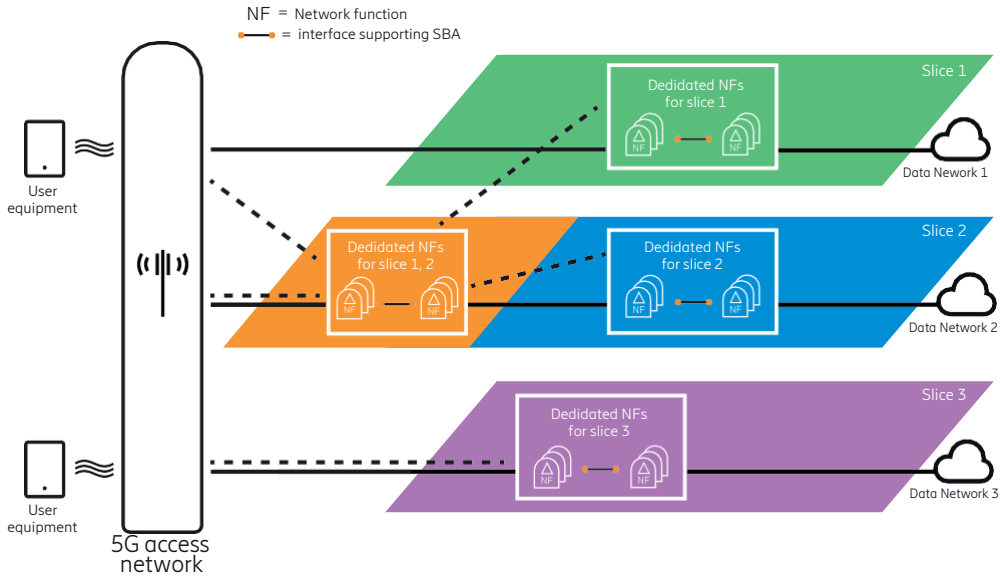

Figure 2: Simplified 3GPP 5G architecture

The 5G system also expands on 4G by adding new radio (NR) capabilities, doing so in such a way that LTE and NR will be able to jointly evolve in complementary ways. This development makes it possible for the 5G system to take advantage of important new 4G system concepts, including energy-saving narrowband IoT (NB-IoT) radio, secure low-latency small data transmission for low-power devices, and devices using energy preserving dormant states when possible. In this white paper, however, we focus on the security of the NR radio and the 5G core network.

Five properties that ensure trustworthiness

On top of the state-of-the-art encryption that is included in 5G, the trustworthiness of the 5G system is the result of the five properties illustrated in Figure 3, namely: resilience, communication security, identity management, privacy and security assurance. These properties make the 5G system a trustworthy platform that enables many new services to be created.

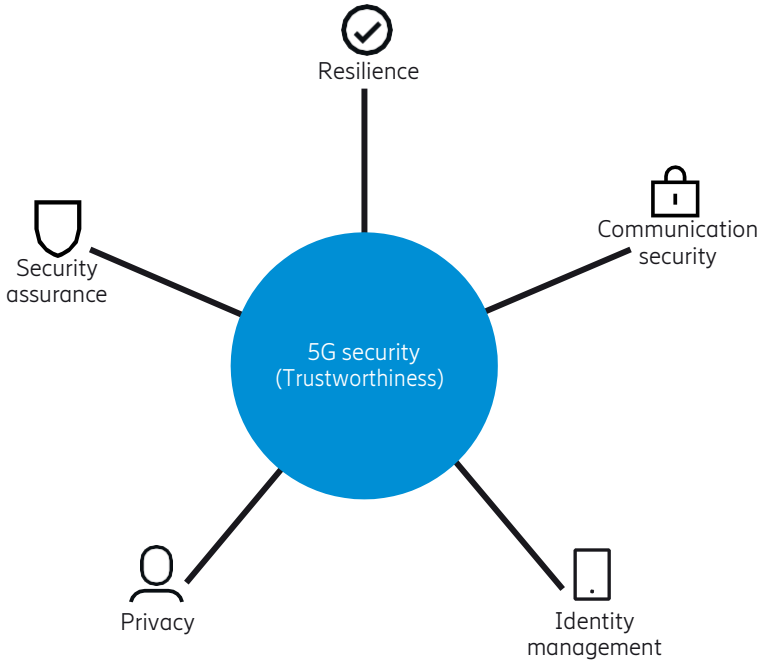

Figure 3: Five properties that contribute to the trustworthiness of the 5G system

1. Resilience

The 5G system's resilience to cyberattacks and non-malicious incidents comes through a variety of complementary and partially overlapping features. First, the 5G NR access was developed with many different use cases in mind from the start, and some of them were collected in one class under the umbrella term ultra-reliable low latency communications (URLLC). The features 5G NR provides for use cases of this class are ideal for industrial control, critical infrastructure and public safety applications. Even greater resilience against failures and attacks can be obtained by deploying a single base station as two split units, called a central unit and a distributed unit. This split also facilitates customizable deployment of security sensitive functions of the 5G NR access, such as user plane encryption, in a secure central location while keeping non-security sensitive functions in less secure distributed locations.

Next, the 5G core network architecture itself is designed around resilience concepts. For example, network slicing isolates groups of network functions from other functions. At one extreme, a public safety organization can use a dedicated complete mobile network (slice 3 in **Figure 2,** for example). An operator may also isolate low-priority IoT devices on a separate slice to ensure that these will not interfere with other users should a problem occur with large quantities of IoT devices.

SBA principles are another architectural concept that enhances resilience. These principles make use of software and cloud-based technologies that improve on the more static and node-centric designs of previous generation networks. This design shift creates functions that can easily be scaled depending on traffic load, and can be independently replaced, restarted, or isolated when failing or under attack.

The resilience of the 5G system also stems from the strong mobility support that it shares with previous generation 3GPP networks, which ensures continuous secure connectivity for devices moving from one location to another. This feature can also be used to let more stationary devices connect to another base station should the current radio conditions become unsuitable due to changes in the environment such as vehicles passing by. This is an example of how added redundancy increases the resilience of the air interface. The 5G system has lower latency at mobility compared to legacy systems. In contrast to 4G mobility, where security is re-configured at handovers to ensure security (causing a small transmission interruption and more complex implementations), the 5G system can reuse the same configuration across handovers. This is because the security sensitive functions are processed in the central unit of the base station.

In addition to these general features providing resilience, there are more specialized functions introduced to operate a radio access network in extreme situations, such as when it has become separated from its core network. This is called isolated E-UTRAN operation for public safety in 4G and is very useful in disaster areas, for example. The same principles can be applied to 5G.

Finally, partly due to strong regulations and associated high fines, cellular networks have long adhered to high carrier-grade availability requirements. This is reflected in the many strong features described in this section that provide resilience at a system level, as well as in implementations, as explained in the security assurance section below.

2. Communication security

Overall, the 5G system provides secure communication for devices and for its own infrastructure. The latter includes links such as front haul between distributed and central units of base stations, backhaul between access and core network, and network domain links between core network nodes. The security design follows principles similar to those used in the 4G system but has been evolved to better meet the needs of new use cases. In particular, the new SBA for core network communication takes threats from the interconnect network into account from the start.

The 5G system includes protection against eavesdropping and modification attacks. Signaling traffic is encrypted and integrity protected. User plane traffic is encrypted and can be integrity protected. User plane integrity protection is a new feature that is valuable for small data transmissions, particularly for constrained IoT devices.

The strong and well-proven security algorithms from the 4G system are reused. These are encryption algorithms based on SNOW 3G, AES-CTR, and ZUC; and integrity algorithms based on SNOW 3G, AES-CMAC, and ZUC. The main key derivation function is based on the secure HMAC-SHA-256.

Mobility in the 5G system also inherits security features from the 4G system, such as separation of keys for specific purposes, backward and forward security for keys at handovers and idle mode mobility, and secure algorithm negotiation. On top of this, there are new security features like automatic recovery from malicious security algorithm mismatches, security key separation between core network functions, and fast synchronization of security contexts in access and core networks.

3. Identity management

At its heart, the 5G system has secure identity management for identifying and authenticating subscribers, roaming or not, ensuring that only the genuine subscribers can access network services. It builds on strong cryptographic primitives and security characteristics that already exist in the 4G system. Examples of primitives include strong cryptographic algorithm sets and key generation functions, and mutual authentication between device and network.

One of the most valuable new security features in the 5G system is the new authentication framework where mobile operators can flexibly choose authentication credentials, identifier formats and authentication methods for subscribers and IoT devices. Previous mobile network generations required physical SIM cards for credentials, but the 5G system also allows other types of credentials such as certificates, pre-shared keys and token cards. The different authentication methods that mobile operators can choose from are called the 5G authentication and key agreement (5G AKA) protocol and the extensible authentication protocol (EAP) framework. A key feature of EAP is the flexible way in which different authentication protocols and credential types can be used without affecting intermediate nodes.

This flexibility opens up for many new use cases. For instance, SIM cards would still continue to be useful for mobile broadband subscribers with smartphones. Non-SIM-card-based credentials would be useful for very cheap IoT devices, like small temperature sensors, in which requiring implementation and deployment of SIM cards would be prohibitively expensive. Further, the 5G system can be used as Wi-Fi replacement in an enterprise or factory setting, reusing an existing public key and certificate infrastructure for network access authentication.

Another valuable new security feature is the ability of a subscriber's operator to determine the presence of the subscriber during an authentication procedure – even when roaming. This feature enables the subscriber's operator to mitigate potential fraud and prevent security and privacy attacks against the subscriber or operator.

The 5G system also inherits a mechanism from legacy systems, called equipment identity register (EIR) check, which can be used to prevent stolen devices from using the network services, thereby discouraging device theft.

4. Privacy

In the context of this white paper, privacy relates to protection of information that can be used by unauthorized parties to identify subscribers. In recent years, much has been written about so-called IMSI catchers and false base stations that can be used to identify and track subscribers, and even eavesdrop on 2G phone calls. To address growing concern and privacy legislation, such as the General Data Protection Regulation (GDPR) [7] and the ongoing review of ePrivacy Directive [8] in Europe, addressing the issue of privacy has been a high priority in the 5G system from the beginning so that subscribers' privacy is included by design.

Data traffic, including phone calls, internet traffic and text messages, is protected using state-of-the-art encryption. The devices and the network mutually authenticate each other and use integrity-protected signaling. This setup makes it infeasible for an unauthorized party to decrypt and read the information that is communicated over the air.

Another privacy enhancement is protection of subscriber identifiers, both long-term and temporary. 3GPP has defined a mechanism that enables a home operator to conceal a subscriber's long-term identifier, roaming or not, while simultaneously complying with regulatory duties. The concealment mechanism is based on the Elliptic Curve Integrated Encryption Scheme (ECIES) [9] and uses the home operator's public key. When enabled, this feature makes active attacks and the infamous IMSI catchers – ineffective in a 5G-only system. In addition, the 5G system enforces a stricter policy for update of temporary identifiers. This guarantees that temporary identifiers are refreshed regularly which makes passive attacks impractical.

Further, the 5G system is also able to detect false base stations that are the root cause of IMSI or TMSI catchers. From data in the measurement reports collected from devices, the 5G system can detect the presence of false base stations. For example, when a 2G base station is detected in a system without any 2G deployment, it is certainly a true positive. Similarly, when the received signal strength of a base station does not match the expected signal strength at a particular location, the reported base station is likely a true positive. The detection mechanism makes it easy to execute configurable actions (e.g., informing subscribers and contacting legal authorities) when detections are made.

5. Security assurance

In 3GPP, security assurance is a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes. This assurance is especially important for mobile systems, as they form the backbone of the connected society and are even classified as critical infrastructure in some jurisdictions. Early on the telecom industry realized the need to ensure secure implementations in addition to the secure standardized system and protocols. Therefore, 3GPP and GSMA took the initiative to create a security assurance scheme called the network equipment security assurance scheme (NESAS), which is suitable to the telecom equipment lifecycle [10, 11]. Ericsson strongly and actively supports the initiative in both 3GPP and GSMA by feeding the strongest parts of our own Security Reliability Model (SRM) into the scheme, ensuring the other parts are covered by the scheme, and aligning the two.

NESAS comprises two main components: security requirements and an auditing infrastructure. The security requirements are defined jointly by operators and vendors in 3GPP. These requirements are currently defined on a node basis and collected in so-called SeCurity Assurance Specifications (SCAS). There is, for example, one specification defining security requirements for 4G base stations. Various types of requirements exist, including the use of a general security policy, such as minimum length of management passwords, but also hardening and penetration testing requirements. The auditing infrastructure is governed by the GSMA, the global mobile operator organization. The GSMA appoints audit firms that perform the audits of vendors' development and testing processes. The GSMA also publish information on the vendors that pass audit.

NESAS aims to meet the needs of many national and international cybersecurity regulations, such as the EU cybersecurity certification framework. The move towards larger portions of products being software – as we can see with SBA and cloud-based implementations – also offers the possibility for faster update cycles if vulnerabilities are discovered.

The way forward

The 5G system will continue to evolve beyond the current release (called 3GPP Rel 15) with new and enhanced features for various use cases such as NR vehicle-to-everything (V2X), voice-over-NR (VoNR), and enhanced NR LTE coexistence. Of course, 5G security will evolve in concert with and as an integral part of the 5G system's features.

Ericsson continues to work on the resilience of the 5G system. As a general principle, automatic recovery mechanisms will be increasingly inherent so that the system recovers from and avoids faulty situations to an even higher degree than today. Resilience against (smart) radio jamming and the protection of broadcast system information over radio also demand continued research and consideration. Security and privacy aspects of network slicing life cycle management will be further scrutinized while taking into account progress made in other organizations, especially IETF, ETSI NFV and NGMN. Similarly, necessary adjustments to SBA to support new use cases and developments in virtualization technology will be made.

In terms of communication security, it has been debated whether or not quantum computers will pose a threat to 128-bit symmetric algorithms in the foreseeable future. The current prevailing understanding is that they will not. Even so, Ericsson believes it is important to verify that the 5G system can easily use 256-bit symmetric cryptography mechanisms inherited from the design of the 4G system. 3GPP has already started to look into this issue and will continue to do so. The legacy security visibility and configurability functionality will evolve, and devices will become more aware and responsive to different security configurations.

Identity management will be studied further to mitigate the risk of mass compromise of long-term subscription credentials [10]. Potential mitigations are remote update of long-term subscription credentials and the addition of perfect forward secrecy of session keys. With IoT the relationship between the device and the subscriber changes and it is important to follow up on this evolution to ensure that the 5G system provides appropriate identity management for IoT use cases.

We will also continue to prioritize the privacy considerations related to new services and features. Similarly, the SCAS work will continue for new network functions introduced by the 5G system. Ericsson firmly supports the assurance efforts.

Conclusion

Like its predecessors, the 5G system will soon be an indispensable part of our connected society. A variety of use cases, some finally being possible thanks to 5G and others not yet imagined, will soon see the light of day. Ericsson believes that 5G security provides a level of trustworthiness that enables the 5G system to meet the requirements of the vast majority of these use cases from the end user, service provider and regulatory perspectives. The trustworthiness not only originates from a set of security features, but also from system design principles and implementation considerations that have all been applied with a holistic and risk-based mindset.

References

1. 5G open for business (2018), available at: https://www.ericsson.com/5g

2. 5G security – scenarios and solutions (first published 2015, re-published 2017), available at: https://www.ericsson.com/en/white-papers/5g-security-scenarios-and-solutions

3. Protecting digital business (2018), available at: https://www.ericsson.com/en/security

4. TS 33.501 – Security architecture and procedures for 5G System (2018), 3GPP technical specification, available at: http://www.3gpp.org/DynaReport/33501.htm

5. TR 33.899 – Study on the security aspects of the next generation system (2017), 3GPP technical report, available at: http://www.3gpp.org/DynaReport/33899.htm

6. 5G enablers for network and system security and resilience (2017), available at: http://www.5gensure.eu/

7. GDPR – General Data Protection Regulation (2016), European Union, available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32016R0679

8. ePrivacy – Directive on privacy and electronic communications (2002), European Union, available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058

9. Elliptic Curve Cryptography Version 2.0 (2009), SECG SEC 1 specification, available at: http://www.secg.org/sec1-v2.pdf

10. Setting the standard: methodology counters security threats (2014), available at: https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2014/er-security-assurance-3gpp.pdf

11. NESAS – Network Equipment Security Assurance Scheme (2018), GSMA, available at: https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme

12. The Great SIM Heist (2015), available at: https://theintercept.com/2015/02/19/great-sim-heist/

Abbreviations

EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access
GDPR	General Data Protection Regulation
GSMA	GSM Association
IETF	Internet Engineering Task Force
NESAS	Network Equipment Security Assurance Scheme
NB-IoT	Narrowband IoT
NR	New Radio
NFV	Network Function Virtualization
SBA	Service Based Architecture
SCAS	SeCurity Assurance Specifications
URLLC	Ultra-Reliable Low Latency Communications

Contributors

The contributors to Ericsson's opinion on this topic are Karl Norrman, Prajwol Kumar Nakarmi and Eva Fogelström.

Karl Norrman
Karl holds an M.Sc. in computer science from Stockholm University and has been with the Security Research department within Ericsson Research since 2001. He was actively involved in the LTE security standardization and was Ericsson's security coordinator in 3GPP. He currently works as a master researcher focusing on 5G security and automated cryptographic protocol verification.

Prajwol Kumar Nakarmi
Prajwol is a senior security researcher at the Security Research department within Ericsson Research. He joined the company in 2011 and is currently focusing on 5G security standardization. He has worked on a number of projects related to anomaly detection/prevention in mobile networks. Prajwol holds a Master's degree in Security and Mobile Computing (Erasmus Mundus Programme) from KTH Royal Institute of Technology in Stockholm, Sweden, and Aalto University in Finland.

Eva Fogelström
Eva Fogelström is director of the Security Research department within Ericsson Research. She holds a Ph.D. in Telecommunications and an M.Sc. in Electrical Engineering, both from KTH Royal Institute of Technology in Stockholm, Sweden. Eva has been with Ericsson since 1997, working in the fields of security, mobility and standardization.