5G SECURITY ISSUES

Positive Technologies

2019

positive-tech.com

Contents

Executive summary

5G Non-Standalone is vulnerable to denial of service. Transitioning to 5G will involve multiple stages, according to the 3GPP roadmap. One of these stages, 5G Non-Standalone, combines use of 5G New Radio and an LTE network core. As a result, these networks inherit all the vulnerabilities of LTE networks from the get-go. Research indicates that 100 percent of LTE networks are vulnerable to denial of service (DoS) through Diameter exploitation. This means that 100 percent of 5G Non-Standalone networks will be vulnerable to DoS, too.

Hacking 5G could become as simple as hacking the web. The 5G network core will be based on software-defined networking (SDN) and network function virtualization (NFV). SDN and NFV make heavy use of the HTTP and REST API protocols. These protocols are well known and widely used on the Internet. Tools for finding and exploiting vulnerabilities are available to any adversary. And now, these protocols will also be used on 5G networks. Consider the current situation with web security: despite the best efforts of the IT and security industries, well-protected websites are the exception rather than the rule. Software development is rife with mistakes that impact security. The average web application contains 33 vulnerabilities and 67 percent of web applications contain high-risk vulnerabilities. Lowering the barrier to entry will pave the way for an upswing in attacks on 5G networks.

More flexibility. More configurations. More errors. When performing security analysis of mobile operator networks and corporate information systems, our experts routinely find dangerous configuration flaws. Even with today's 4G networks, not every operator succeeds in securely configuring the core network and protecting it from all angles. As SDN and NFV are implemented for network slicing in 5G, administration will become even more difficult. Flexibility in 5G networks comes at the cost of increased complexity and settings to monitor. This flexibility means a higher likelihood of security-busting configuration mistakes.

Millions of connected IoT devices offer a bonanza for botnets. Most user equipment on 5G networks will not be consumer phones or computers, but IoT devices. By 2020, there will be about 20 billion such devices. The number of attacks on the IoT is increasing. Device protection is poor and malware distribution is easily scalable. In the last year alone, our experts found 800,000 vulnerable devices. Mirai was an example of the destructive capacity of a large botnet. To avoid a new Mirai and the threat of disruption of user service, 5G network operators will have to develop new threat models more attuned to these realities.

Introduction

Each new generation of mobile standards since 2G has been designed for one and the same goal: to boost bandwidth on packet networks. Faster Internet access is the name of the game. Other changes have been minimal. The voice codec in 3G changed only slightly. On 4G networks, voice traffic is transmitted over packet data using the IP Multimedia Subsystem (IMS), which many operators have not deployed. The 4G network may not transmit voice at all, instead falling back on 2G/3G to make calls. Yet recent mobile networks have certain drawbacks compared to their predecessors. 3G and 4G in particular are a less-than-ideal fit for the IoT: compatible devices need to have high performance and corresponding high energy consumption. As a result, devices require frequent charging or battery swaps. This is unacceptable for many IoT devices, which may require battery life of up to 10 years without swapping or charging batteries.

5G networks are designed to account for such diverse needs. They can provide superfast access with minimal latency. At the same time, they retain the flexibility to provision slower speeds with lower device resource requirements.

According to 3GPP Release 15 for 5G, which came out in summer 2018, the first wave of 5G networks and devices is classified as Non-Standalone (NSA). 5G radios will be supported by existing 4G infrastructure. In other words, devices will connect to 5G frequencies for data transmission when needing greater bandwidth and lower latency (such as for communication between smart cars), or to reduce power draw on IoT-enabled devices, but will still rely on 4G and even 2G/3G networks for voice calls and SMS messaging. So, at least during the transition period, future 5G networks will inherit all the vulnerabilities of previous generations.

5G Standalone networks may add new types of security flaws, because the entire packet core and additional services will depend on virtualization. Technologies such as NFV and SDN will make deployment simpler, faster, and more flexible. But replacing dedicated hardware with software-defined systems (some of them based on open-source code) may prove a double-edged sword that makes mobile networks more vulnerable to attacks.

One thing is for certain: availability, integrity, and confidentiality will remain the foremost concerns. As 5G begins to penetrate every area of life—such as manufacturing, healthcare, and transport—emboldened malefactors will surely follow with close interest.

[1] gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf

[2] portal.3gpp.org/#55934-releases

5G overview

The transition to 5G will be gradual. Standards have not been fully finalized yet and 5G networks are expected to initially rely on and integrate with previous-generation networks, slowly displacing them over time.

5G standardization

Standards-making for 5G networks, including development of plans for future specifications, kicked off at the September 2015 workshop held by 3GPP. As planned, Phase 1 specifications were to describe the architecture for meeting service requirements, with Phase 2 detailing protocols for implementing that architecture.

During preparation, it was decided to split Phase 1 into two parts. In December 2017, standardization of the non-autonomous, or Non-Standalone, architecture for 5G New Radio (NR) was completed. This first official set of 5G standards defines the wireless air interface for interworking with existing LTE base networks. This has allowed operators to combine 4G LTE networks with 5G NR, improving the latency and bandwidth of user data transmission.

In July 2018, the first stage of standardization for 5G Phase 1 was completed. As part of 3GPP Release 15, NR Standalone architecture specifications were released, indicating how the proposed 5G radio network will work with a 5G network core. In addition to radio network standardization, work was also done in 3GPP Release 15 to define the structure of most of the 5G network core.

Phase 2 of standardization of the 5G network core structure and use cases is the priority for current work on 3GPP Release 16, which should be completed by December 2019.

Because the 5G network core is still being standardized, nobody has a full picture yet of 5G network security. However, the standards released so far allow us to make some early assessments. To understand the issues at play, it is worth first reviewing the key use cases contemplated by 5G standards.

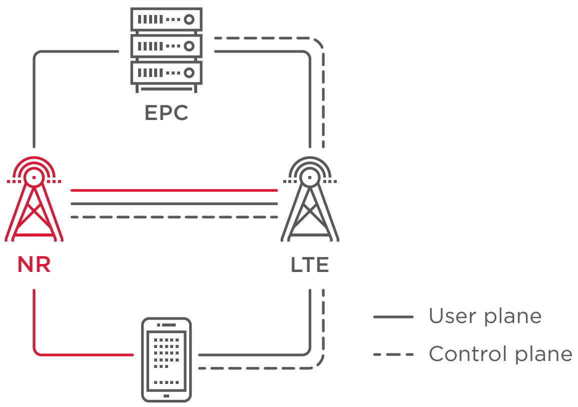


Figure 1. Using 4G infrastructure in 5G networks[1]

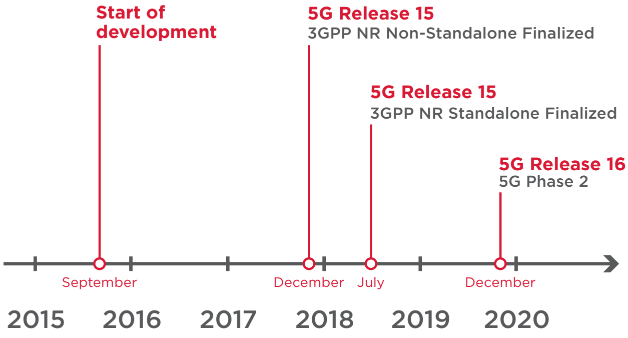
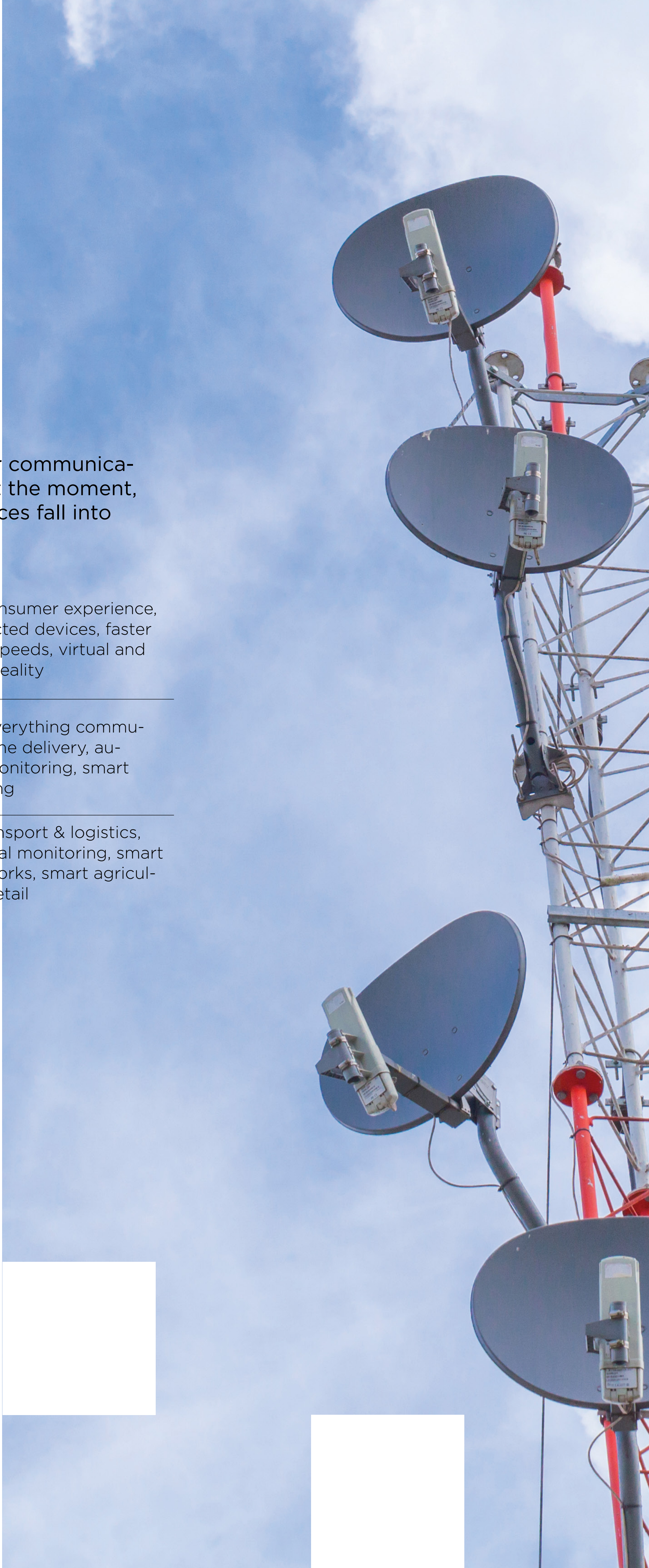


Figure 2. Current schedule for 5G standardization[2]



Use cases

5G promises to be the standard for communication between billions of devices. At the moment, these devices and associated services fall into three main 5G use cases:

Enhanced Mobile Broadband (eMBB)	Improved consumer experience, more connected devices, faster connection speeds, virtual and augmented reality
Ultra-Reliable and Low-Latency Communications (URLLC)	Vehicle-to-everything communication, drone delivery, autonomous monitoring, smart manufacturing
Massive Machine-Type Communications (mMTC)	E-health, transport & logistics, environmental monitoring, smart energy networks, smart agriculture, smart retail

Enhanced Mobile Broadband (eMBB)

eMBB is an evolution of existing wireless broadband access services, with an emphasis on greater speed for consumer needs.

Key network requirements: data transmission speed up to 20 Gbps and latency less than 7 ms.

Examples include:

- High-speed Internet access
- HD video streaming
- AR and VR services
- Support for large numbers of subscribers in a single location

Ultra-Reliable and Low-Latency Communications (URLLC)

Quick and consistent data transmission is attractive to manufacturing, transport, healthcare, and other industries. URLLC services have strict requirements regarding network reliability and quality, prioritizing low latency, reliability, and low probability of error.

Key network requirements: probability of error from 10^{-5} to 10^{-8} and latency less than 3 ms.

Examples include:

- Self-driving vehicles
- Telemedicine, including remote diagnostics and robotic surgery
- Remote control of industrial processes

Massive Machine-Type Communications (mMTC)

mMTC takes the IoT to the next level by bringing an even larger number of devices into the fold. This use case centers on high reliability, low power consumption, and support for high device densities in a given area.

Key network requirements: density of up to 1 million devices per square kilometer and battery life of up to 10 years without recharging.

Examples include:

- Smart City systems
- Transport and logistics
- Production and staff monitoring
- Other scenarios with exceptionally high concentrations of IoT sensors

5G use cases are shown |in the following graphic[3]

Naturally, this description of 5G use cases is not exhaustive. Communication technologies are always put to use in novel and unexpected ways. This is why the 5G network architecture has been designed with the capacity to adapt to new use cases with divergent requirements.

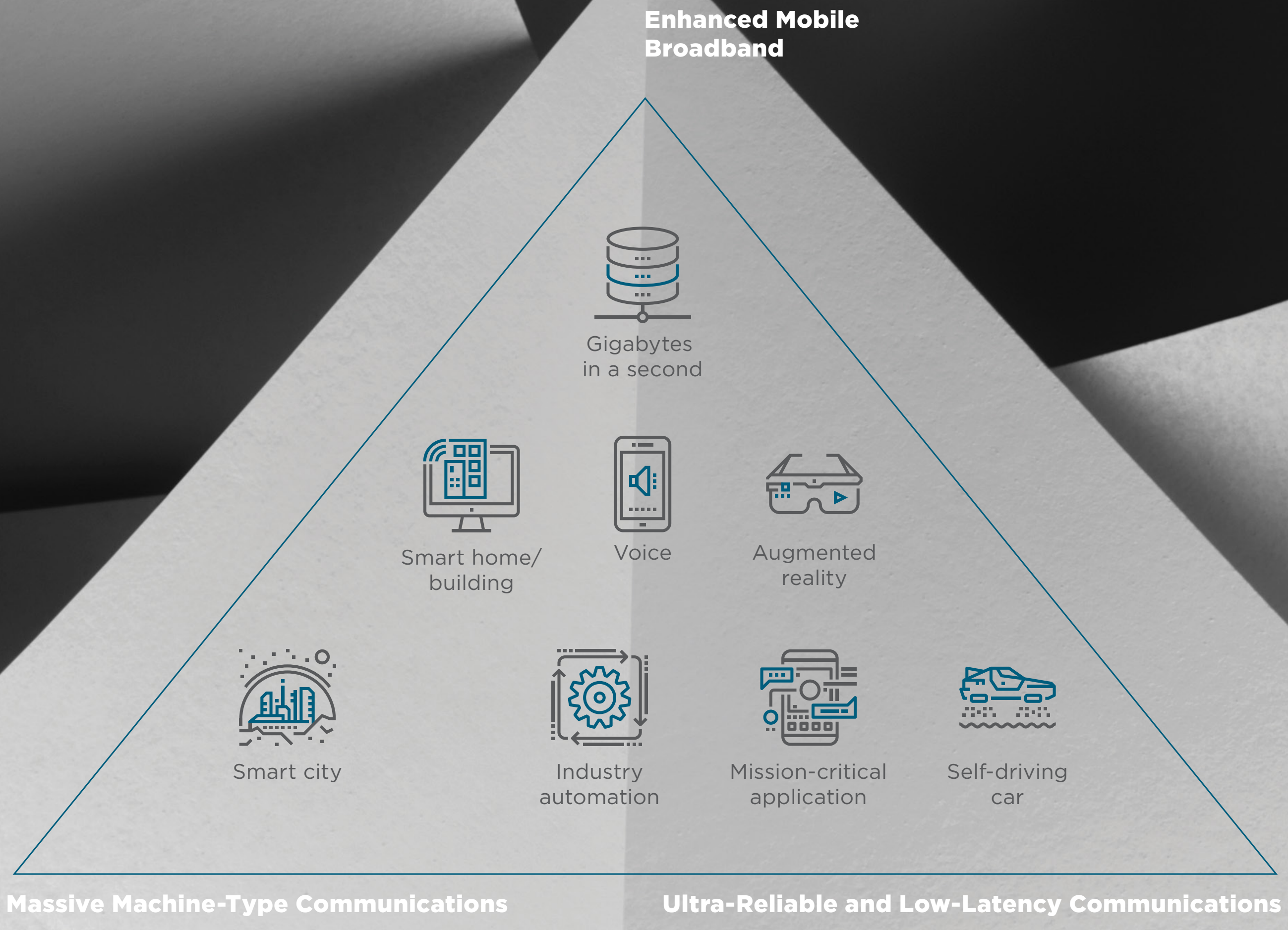

Enhanced Mobile Broadband
Gigabytes in a second
Smart home/ building
Voice
Augmented reality
Smart city
Industry automation
Mission-critical application
Self-driving car
Massive Machine-Type Communications
Ultra-Reliable and Low-Latency Communications

Figure 3. Anticipated 5G use cases

[3] itu.int/rec/R-REC-M.2083

Architecture

Implementing 5G will leave no part of the network untouched. The growing number of connected devices, plus the different demands placed on services under each use case, require new technologies both in the radio network and in the network core.

Radio network

5G networks require a wide band of frequencies. The main difficulty for operators was that available spectrum is very limited. Suitable bands were already allocated for other uses. Ultimately, 5G networks were assigned new millimeter-wave and centimeter-wave bands never used before for mobile communications. But the new frequency bands brought a new problem: short millimeter waves do not travel well through obstacles.

To compensate, a solution was devised with massive MIMO (Multiple Input Multiple Output) antennae comprised of hundreds of elements working in concert. Beamforming creates directional beams to efficiently serve individual subscribers. Each 5G network subscriber receives a spatially and temporally tailored signal from the base station antenna, which provides only the service needed by that particular subscriber. This technology allows using the base station more efficiently and increasing 5G radio bandwidth. And with multi-connectivity, user equipment can connect to multiple base stations simultaneously.

Core network

Networks must serve devices and applications with varying traffic profiles. As such, it is important to accommodate the needs of applications and allocate network resources based on these diverse requirements. The 5G network flexibly allocates its resources, based on rules defined in software, for optimal service. This flexibility is achieved with the help of software-defined networking and network function virtualization.

Software-defined networking

SDN abstracts the network control level from data transmission devices, allowing implementation in software.

Key principles of SDN:

- Data transmission is separate from data management.
- Unified software centralizes network management.
- Physical network resources are virtualized.

The result for operators is consistent automated control of network parameters, which allows the following:

- Centralized application of policies
- Easy and quick configuration by managing at the level of networks, as opposed to network elements
- Optimization of traffic (L2/L3) transmission thanks to a larger number of routing paths

Network function virtualization

With NFV, it is possible to mix and match network functions on the software level to create unique telecommunication services without making changes at the hardware level. So an operator could launch a new service without purchasing new equipment or having to verify compatibility with what is already installed. NFV underpins network slicing, which splits a single physical network into multiple virtual networks (slices) so that a particular device can access only certain services with certain parameters at the right time.

Each slice in the network is allocated its own resources, such as bandwidth and service quality. By design, all slices are isolated from each other. Errors or failures in one slice should not affect services in the other slices. Network slicing improves the efficiency of mobile networks and quality of service.

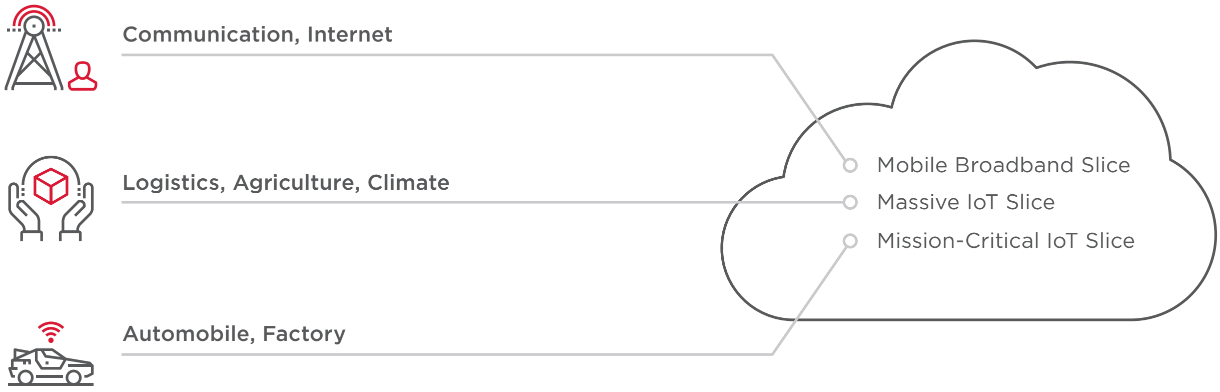


Figure 4. An example of network slicing[4]

[4] 3gpp.org/NEWS-EVENTS/3GPP-NEWS/1930-SYS_ARCHITECTURE
[5] Anand R. Prasad, Sivabalan Arumugam, Sheeba B, and Alf Zugenmaier, "3GPP 5G Security", Journal of ICT Standardization (River Publishers, Vol. 6, Iss. 1&2)
[6] ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/
[7] ptsecurity.com/ww-en/analytics/diameter-2018/
[8] ptsecurity.com/ww-en/analytics/epc-research/

Securing 5G

The architecture of 2G, 3G, and 4G networks did not account for the possibility of an intruder inside the network or even one on a roaming network. The model of trust was absolute. Anyone with access to the inter-operator network can gain access to the network of any operator—a serious security flaw.

The key security change in 5G is the new trust model. In essence, the farther equipment is from the subscriber's SIM card (Universal Subscriber Identity Module, or uSIM) and network core (Unified Data Management, or UDM; Authentication Credential Repository and Processing Function, or ARPF), the lower the trust in that equipment.[5] Now only the subscriber's uSIM and UDM with ARPF are trusted; all intermediate network hosts are considered untrusted.

A number of new security features ensure that the subscriber and the network interact in a verifiable and authenticated way, according to the updated model of trust:

- **Inter-operator security.** Owing to fundamental vulnerabilities in the architecture of the SS7 and Diameter protocols, a number of security issues have been identified in 2G/3G and 4G networks.[6, 7, 8] Inter-operator security in 5G will be provided by security proxy servers, which are essentially an evolution of 2G, 3G, and 4G signaling firewalls.
- **Privacy.** To prevent disclosure of subscriber identifiers, 5G networks will use the home network public key for asymmetric encryption.
- **Primary authentication.** Network and devices in 5G are mutually authenticated.
- **Secondary authentication.** Data transmission networks outside the mobile operator domain, such as Wi-Fi calling, undergo secondary authentication.
- **Key hierarchy.** To implement the updated trust model, 5G employs key separation. This limits the damage if a part of the infrastructure is compromised and protects the integrity of data transmitted by the user.
- **Radio network protection.** In the base station (gNB) in 5G, the data processing module (Central Unit, or CU) and the radio module (Distributed Unit, or DU) are separated at the architecture level. The CU and DU interact via a secure interface. Such separation prevents the attacker from breaching the operator's network, even if successful in gaining access to the radio module.

Taken together, these changes reflect how 5G networks are designed with robust security compared to previous-generation networks. Known security issues in SS7 and Diameter signaling networks have been considered and addressed in 5G. This does not mean, however, that 5G networks are unhackable. At this point, we will discuss potential security issues with 5G. Integration of 5G networks into new areas—such as remote surgery, self-driving cars, and automated production processes—makes these networks a very tempting target, multiplying the potential damage and consequences.

Integration of 5G networks into new areas makes these networks a very tempting target, multiplying the potential damage and consequences

Security issues

Compatibility with previous-generation networks

Telecom networks are slow to change. The transition to a new generation usually occurs in several stages and takes years. For a long while, 5G networks will be used side by side with 4G, and even 3G and 2G networks. We must also keep in mind that different operators and different countries will move from 4G to 5G at their own speeds. Mobile operators will have to take care of security not only for 5G, but for the transition and interworking with previous-generation networks.

As we know, previous-generation networks are prone to vulnerabilities allowing an adversary to implement attacks such as call and SMS interception, geotracking, and denial of service.[9, 10] For instance, in 2018 our experts managed to intercept voice calls on all tested 3G networks, and successfully intercepted SMS messages on 94 percent of tested networks. On all tested 4G networks it was possible to cause denial of service. Because of 4G's role during the transition period, these threats will remain even after 5G reaches the public.

It is also possible to attack from the radio interface. One of the latest examples was demonstrated by a group of researchers from the Korea Advanced Institute of Science and Technology[11] who ran a fuzzing test of a 4G network by sending specially crafted messages to check how equipment handles non-standard data. Analysis of two mobility management entities (MMEs) revealed 51 vulnerabilities caused by incorrect protocol implementation by equipment manufacturers. The same test can be done for 5G, which has the potential to contain similar issues.

Security threats associated with 3G and 4G will remain after 5G reaches the public and will heavily influence NR deployments on the horizon of three to five years

[9] ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/
[10] ptsecurity.com/ww-en/analytics/diameter-2018/
[11] syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf
[12] ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018/
[13] ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/
[14] cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8046
[15] cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17485

Use of Internet technologies

New-generation mobile networks require new signaling protocols in the network core. Telecom operators will now have to contend with the wider range of threats already facing Internet systems.

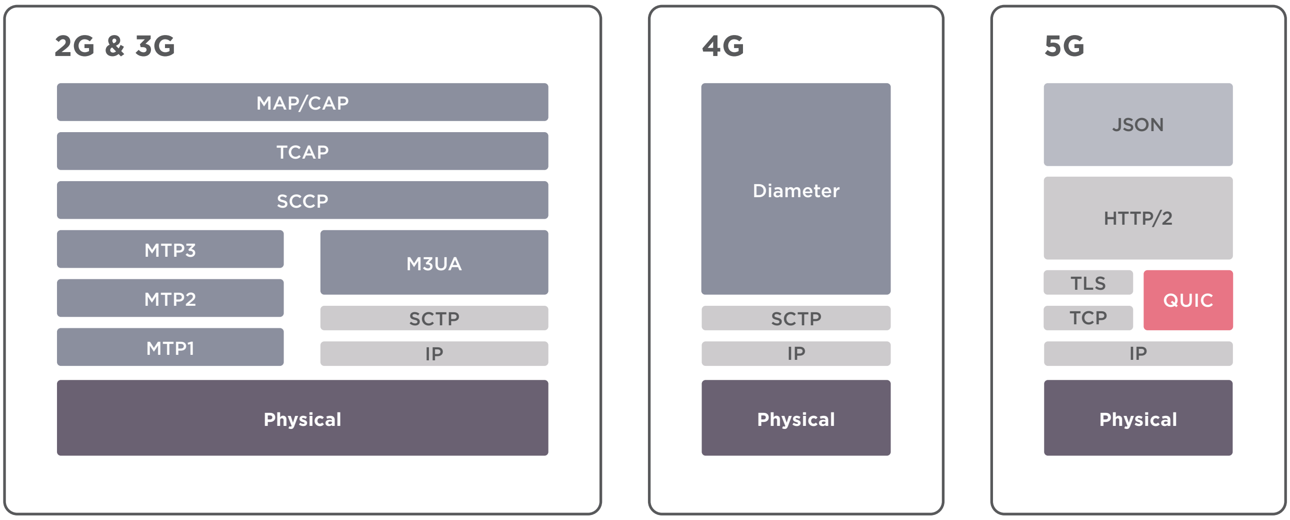


Figure 5. Evolution of network core signaling protocols

Previous generations relied on the niche SS7 and Diameter protocols. The 5G network core is built on well-known Internet protocols such as HTTP and TLS. This change gives some reason for anxiety because the closed nature of telecom protocols acted as a sort of entry barrier to attackers. By contrast, Internet technologies are open and well known to attackers: there are a lot of techniques to search for vulnerabilities in them, and there are many tools available for easy exploitation.

So how risky is use of Internet technologies, from a security standpoint? We know that hackers love to target web resources, where these protocols are currently used. In 2018, web attacks accounted for a quarter of all security incidents.[12] Software development is rife with mistakes that impact security. Our latest study shows that 67 percent of web applications contain high-risk vulnerabilities.[13] Due to failure to correctly handle or sanitize inputs, a specially crafted JSON object may cause denial of service or allow the attacker to execute arbitrary code and get control of equipment (see, for instance, vulnerabilities CVE-2017-8046[14] and CVE-2017-17485[15]).

Lowering the entry barrier will inevitably create more permissive conditions for attacks on 5G networks. Attackers who previously were deterred by complex telecom-specific protocols will target 5G networks built on the technologies they already know how to hack.

Network slicing

As described already, network slicing splits a network into isolated slices. Each slice is allocated its own resources (bandwidth, service quality, and so on) and has unique security policies. In theory, every network slice is isolated from the others. Therefore a compromise of any one slice should not impact the other slices or the network as a whole. But now instead of configuring just one network, operators will have to configure a larger number of slices with greater complexity and service requirements. This has significant security implications. As the configuration burden and number of parameters increase, so does the probability of a security slipup. This may be especially true when 5G network infrastructure is built jointly by several operators or when a single 5G network is shared by several virtual mobile operators.

Even today's systems often find operators unable to cope with their complexity. As indicated by our study of security of 3G[16] and 4G[17] networks, as well as corporate information systems,[18] configuration errors are very common. For instance, in 2018 one out of every three successful attacks during 4G network testing resulted from incorrect settings of network equipment and equipment responsible for security of signaling networks. Configuration flaws were found in all corporate systems tested by our company, and 75 percent of systems harbored critical or high-severity vulnerabilities based on CVSS v3.0 scoring. Moreover, in one out of every four external penetration testing projects, configuration flaws allowed pursuing the attack vector until access to the internal network was successfully obtained.

Paradoxically, the effect is that although network slicing is supposed to promote security, increasing the number of slices on a 5G network may lead to more configuration errors and even deterioration of operator awareness, adversely impacting security overall.

One out of every three successful attacks on 4G networks was resulted from incorrect configuration of equipment

[16] ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/
[17] ptsecurity.com/ww-en/analytics/diameter-2018/
[18] ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/

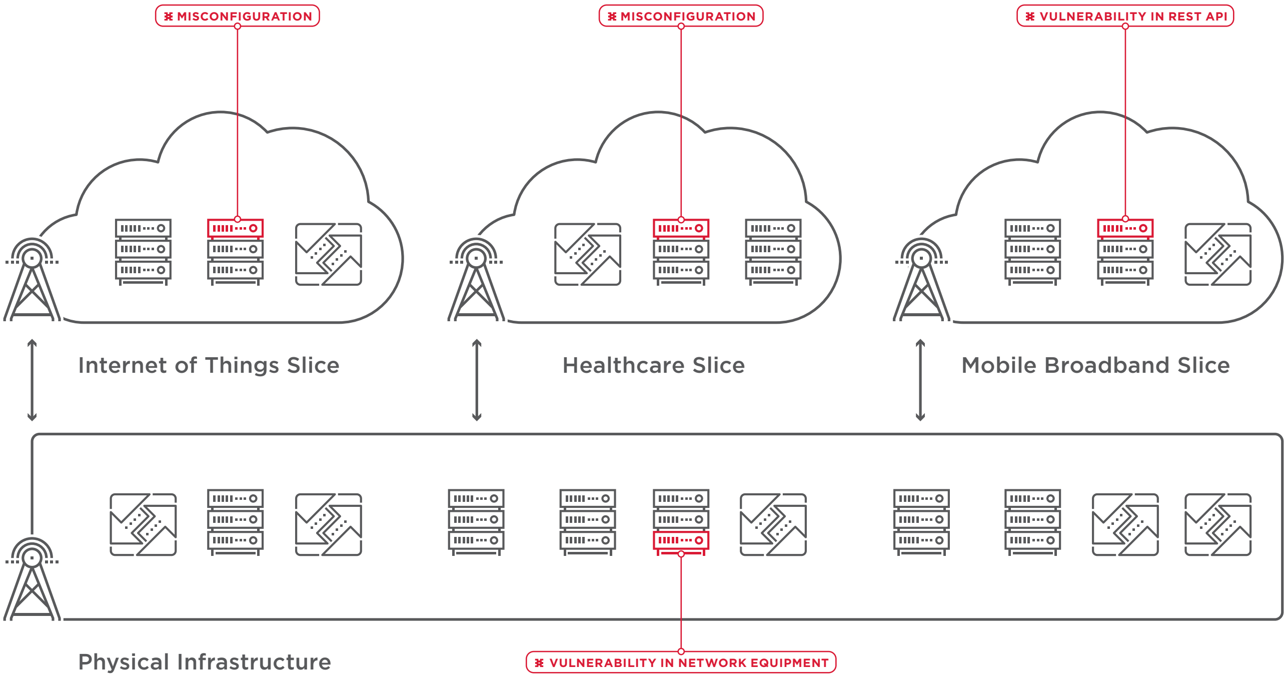


Figure 6. Increase in number of vulnerabilities

Proliferation of network slices makes proper configuration more difficult

SDN and NFV

Networks built on SDN and NFV differ from traditional networks. For instance, on a traditional network, the task of copying signaling traffic for monitoring is handled by special hardware subsystems (ASICs) with no appreciable impact on network performance. On SDN/NFV networks, this task inevitably increases the CPU and memory burden on the virtual network because infrastructure is pooled. Also, some hardware components may communicate with each other directly, which precludes mirroring of traffic. All this may cause operators to try to reduce the number of monitoring points and, as a result, blind spots may appear and make it impossible to detect malicious activity.

Switching to SDN/NFV entails a change in network infrastructure and appearance of new elements, such as an orchestrator and various control components. This lengthens the chain of trust and brings new risks.

Reduced isolation. With NFV, most components can communicate with each other directly, at least on a physical level. On traditional networks they are physically isolated.

Risk of sharing resources. A number of non-related components can draw on the same hardware resources, impacting each other's performance. Attack on any virtual function can impact other virtual machines running on the same physical server.

Access control issues. How can credentials and access keys be distributed between functions to prevent access by an intruder?

All of these issues complicate efforts to detect, localize, and resolve security issues on 5G networks.

Internet of Things

Gartner analysts expect that by 2020, there will be about 20 billion IoT devices worldwide. By the time 5G makes its mass debut, most subscribers will not be consumers per se as was the case with previous-generation networks. The bulk of 5G users will consist of IoT devices, such as industrial monitoring systems, or smart city and smart home elements. 5G use cases for IoT devices (URLLC and mMTC) anticipate needs quite different from those of human subscribers.

The patterns of human subscribers are more or less consistent; network activity and movement usually vary based on the time of day. But the behavior of IoT devices is absolutely different from device to device. For instance, sensors communicate and exchange data periodically regardless of the time of day, but they may remain entirely stationary. By contrast, other devices—for car sharing or any kind of logistics—are constantly moving. So the existing threat model, developed for identification of suspicious activity in the context of a human subscriber, will not work for the IoT.

The threat model for identifying suspicious activity in the context of a human subscriber will not work for IoT devices, which are the majority of 5G users

At the same time, the number of malware campaigns targeting IoT devices has boomed by 50 percent in the last year.[19] Perhaps the best-known example of the destructive capacity of such attacks is the Mirai botnet, which included over half a million devices. This botnet was responsible for a series of powerful DDoS attacks in 2016. These include an attack on the equipment of Deutsche Telekom[20] that affected about 900,000 devices and caused mass disruption of communications in Europe, as well as an attack on DNS provider Dyn,[21] which cut off access for U.S. and European users to major web services such as Amazon, GitHub, and PayPal. New variations of Mirai are still being discovered today, such as the IoTroop/Reaper botnet, which struck financial institutions in 2018, and Yowai, discovered in early 2019.

The security of IoT devices is still poor. Malware distribution is easily scalable, because users rarely update device firmware and seldom change factory passwords. In 2018, Positive Technologies experts found vulnerabilities in ZTE CPE terminals allowing to remotely execute arbitrary code.[22] At that time, on the Shodan search engine one could find over a million devices vulnerable to incorporation in a new botnet potentially even larger than Mirai.

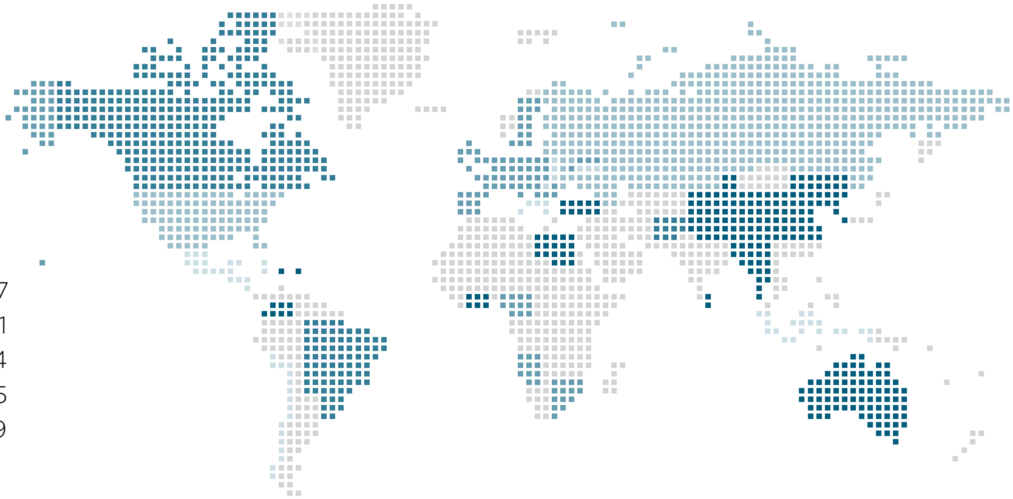
There are many types of IoT devices and new ones appear every year. 5G network operators will have to develop new threat models more attuned to diverse device types.

Vulnerable ZTE devices

Total results:
1,079,593

Top countries:

Thailand	501,977
Egypt	117,841
Turkey	80,344
Sri Lanka	58,055
El Salvador	51,589



[19] ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018/
[20] threatpost.com/hacker-admits-to-mirai-attack-against-deutsche-telekom/127001/
[21] dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[22] support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1009383

Responses for operators

Unfortunately, very often during testing and even during implementation operators build their networks with little or no thought to security. Security policies are applied only once the network is in use by paying subscribers. This expedites network deployment and may save some money initially, but in the long run ends up causing large financial headaches. Operators are forced to spring for equipment not in their original budget. Bought in haste, the new solutions often integrate poorly with the existing network architecture. In such cases, fully meeting security requirements can become nearly impossible.

Based on our experience studying the security of previous-generation networks, as well as the potential security problems with 5G networks described already, we can provide some high-level recommendations for future 5G network operators.

Network protection: comprehensive approach

At first, 5G networks will be based on the 4G network core, thus inheriting the vulnerabilities of 4G networks. One threat is a cross-protocol attack, when hackers exploit vulnerabilities in multiple protocols at the same time. An attack can begin with exploitation of 4G or even 3G vulnerabilities, with the resulting information then used against 5G networks. For instance, the attacker can learn a subscriber's IMSI by exploiting vulnerabilities in 3G networks. In 2018, such vulnerabilities were found on 74 percent of tested networks. In addition, every tested 4G network allowed obtaining data about the operator's network configuration.

This means that to build adequate protection for 5G networks, operators need to start with securing previous-generation networks.[23] Operators should immediately start analysis of all signaling information crossing the border of their home network in order to ensure security and block illegitimate traffic. This analysis provides the data needed to keep security policies up to date. This comprehensive and systematic approach can enable securing 5G networks from day one.

Auditing

The service-oriented 5G network architecture with SDN, NFV, and network slicing affords operators the flexibility needed to quickly adapt their networks to market requirements. But the downside is the difficulty of managing everything. This heightens the importance of security audits to spot vulnerabilities and check whether security policies have been correctly configured and applied. Security auditing should be performed periodically, both during initial 5G network deployment and during regular operation.[24] This allows monitoring changes in network security and taking timely countermeasures.

Attacks on 5G networks can begin with exploitation of vulnerabilities in previous-generation networks

[23] positive-tech.com/products/signalling-firewall/
[24] positive-tech.com/services/telecom-security/

Conclusion

Security as a process

Security is a process, not a one-and-done event. Despite a great deal of 5G security work at the standards level, major unknowns still remain.

Operators must regularly study and implement 3GPP and GSMA recommendations for protecting their 5G networks. Recommendations must be implemented in a thoughtful way. They are usually generic, but every network is unique. Changes in security policies—whether based on recommendations, audits, or monitoring—need to be part of an overall process. Verification must be performed before and after implementation.

In other words, 5G security is not just about having the right architecture or security equipment. It requires building workflows, procedures, and collaboration across teams.

Each new generation of mobile networks has tended to reduce information security risks. Known issues with SS7 and Diameter security have been taken into account during development of the 5G network architecture. However, new 5G technologies such as virtualization and novel use cases bring new kinds of risks for network operators. Despite all the security mechanisms in 5G networks, achieving durable security will require the diligent efforts of telecom vendors, responsible for standards implementation, and of the operators themselves, responsible for proper configuration and compliance with recommendations.

Ensuring 5G security is all about establishing an effective security management process