Cyber Risk

Tue, Mar 22, 2022

A 5G Security Overview: Features, Rewards, and Risks of 5G Technology

Alex Cowperthwaite

Realizing Science Fiction — The Features of 5G Technology

The fifth-generation (5G) of cellular communication will revolutionize the world. This new standard is not a mere technological upgrade from 4G/LTE, but an entirely new way for technological devices to interact with each other, which means that 5G security architecture will have to be built from the ground up as well. Examples of how 5G will change society are limitless, but the Alliance for IoT Innovation (AIOTI) has collected a number of use cases.[1] Some examples include:

- With Unmanned Aerial Vehicles (UAVs), imagine farmers leveraging a suite of drones equipped with sensors to ensure their crops and livestock are all provided the exact treatment they need. Automatically.

- With Automated Valet Parking (AVP), imagine driving to a concert, a sporting event, or any other crowded place, stepping out at the front gates, and letting your car find a parking spot itself. No more fighting for a parking spot.

- With Intelligent Emergency Response Systems, the elderly can be equipped with a device that can detect falls as soon as they happen. Relaying the precise location to emergency services in real-time.

It is possible for the above examples to be implemented with existing cellular networks. Companies may even exist today that sell those products. However, if those examples are implemented on a grand scale, problems will occur.

Let us take a look at the existing wireless technologies that we leverage today. Bluetooth, Zigbee, and Wi-Fi are all relatively secure (if implemented correctly) protocols and sufficient for most use cases you may come across. But they possess extremely limited range. Cellular networks can have massive range but are limited to 4,000 devices per square kilometer.[2] That capability is likely reached during your average sporting event in a major city with cell phone usage alone. 5G can handle one million devices per square kilometer which will help to facilitate a smart city full of IoT devices.

The last major case study as to why 5G infrastructure is needed is video streaming. According to Cisco, video traffic will account for 82% of all internet traffic in 2022.[3] Naturally, people will want to do this on their phones and 4G's speeds just won't cut it. 5G expands the bandwidth by 20 times where users can theoretically obtain peak speeds of 20 gigabytes per second.

Unlike 4G/LTE, where voice, MMS, and data, all possess the same quality of service, network latency, security controls, etc. 5G was designed with much greater flexibility in mind so it can handle all manner of use cases in appropriate ways. Adjusting latency, bandwidth, and even security as needed.

The Evolution of Cellular Technology Standards — The History of 5G Technology

The 3rd Generation Partnership Project (3GPP) is a group of standards organizations that develop and maintain various cellular and telecommunications standards around the world — consider them the United Nations of the telecom industry. 3GPP is the organizational body that has defined the 5G standard.

Since 1992, the group has proposed various standards in a series of Releases. 5G was introduced in Release 15 as "5G Release 15," but this does not mean there were 14 other 5G-related standards before it. Release 15 is technically the 17th release (this is not a mistake) that the body has proposed. Other notable releases include: Phase 1 in 1992 for GSM, Release 99 in the year 2000 for 3G, and Release 8 in 2008 for the introduction of LTE. The release schedule certainly is not consistent with naming. Thanks to electronics-notes.com ,who proposed the following chronological account of 3GPP releases, you can see for yourself[4]:

3GPP Release	Release Date	Details
Phase 1	1992	Basic GSM
Phase 2	1995	GSM features including EFR Codec
Release 96	Q1 1997	GSM Updates, 14.4 kbps user data
Release 97	Q1 1998	GSM additional features, GPRS
Release 98	Q1 1999	GSM additional features, GPRS for PCS 1900, AMR, EDGE
Release 99	Q1 2000	3G UMTS incorporating WCDMA radio access
Release 4	Q2 2001	UMTS all-IP Core Network
Release 5	Q1 2002	IMS and HSDPA
Release 6	Q4 2004	HSUPA, MBMS, IMS enhancements, Push to Talk over Cellular, operation with WLAN
Release 7	Q4 2007	Improvements in QoS & latency, VoIP, HSPA+, NFC integration, EDGE Evolution
Release 8	Q4 2008	Introduction of LTE, SAE, OFDMA, MIMO, Dual Cell HSDPA
Release 9	Q4 2009	WiMAX / LTE / UMTS interoperability, Dual Cell HSDPA with MIMO, Dual Cell HSUPA, LTE HeNB
Release 10	Q1 2011	LTE-Advanced, Backwards compatibility with Release 8 (LTE), Multi-Cell HSDPA
Release 11	Q3 2012	Heterogeneous networks (HetNet), Coordinated Multipoint (CoMP), In device Coexistence (IDC), Advanced IP interconnection of Services,
Release 12	March 2015	Enhanced Small Cells operation, Carrier Aggregation (2 uplink carriers, 3 downlink carriers, FDD/TDD carrier aggregation), MIMO (3D channel modelling, elevation beamforming, massive MIMO), MTC - UE Cat 0 introduced, D2D communication, eMBMS enhancements.
Release 13	Q1 2016	LTE-U / LTE-LAA, LTE-M, Elevation beamforming / Full Dimension MIMO, Indoor positioning, LTE-M Cat 1.4MHz & Cat 200kHz introduced
Release 14	Mid 2017	Elements on road to 5G
Release 15	End 2018	5G Phase 1 specification

Release 16	2020	5G Phase 2 specification
Release 17	~Sept 2021	

Release 15 – 5G Phase 1

At the end of 2018, 3GPP released the full design specifications for implementing 5G infrastructure. These specifications include two different types of 5G implementations: Standalone (SA) and Non-standalone (NSA). Standalone is where 5G is implemented without any reliance on previous cellular generations. Non-Standalone is a way for entities to implement 5G from 4G/LTE in a phased approach. Hannes Ekström, Head of the 5G product line from Ericsson, describes the difference between the two as "it is not an 'either-or' selection between NSA and SA but rather a matter-of-time perspective"[5].

This standard also discusses the three main use-cases that the system was designed for. All 5G implementations, from healthcare IoT and smart cars to smart cities and everything in between, fall into one of the following categories:

- **Ultra-reliable Low-latency Communication (URLLC)**: URLLC is designed with ultra-responsiveness for mission-critical data transmission such as a fast-moving vehicle or drone
- **Enhanced Mobile Broadband (eMBB)**: eMBB supports extreme throughput such as streaming 4K video content or cloud-based gaming
- **Massive Machine-type Communications (mMTC)**: mMTC is optimized for geographical areas that have a large number of low complexity devices like a smart city (which could have internet-connected devices in everything from street lights to sidewalks).

Release 15 also introduces the components of a 5G System. A full standalone 5G system is composed of User Equipment, the Radio Access Network (either abbreviated as RAN or AN), the Core Network, and the Radio Communication itself.

User Equipment

User equipment (UE) can be any device that leverages the 5G network. Examples include cell phones, vehicles, 5G IoT and more. Because the next generation of cellular telecommunications will touch so many different industries, the entire spectrum of user equipment most likely will not be fully realized for many years after 5G is released.

Radio Access Network

The Radio Access Network is the gateway used to access the 5G network. The Radio Access Network is a series of base stations (and supporting infrastructure) that act as an intermediary between UE and the Core Network. This area of the 5G system is focused on setting up connections, routing data, session management, quality of service, and numerous other attributes.

Core Network

The Core Network is where all the processing occurs within 5G. This system is entirely virtualized in the cloud. Virtualizing the standard with on-premises server infrastructure is possible, but typically only used for implementing private 5G, like one could leverage to run a production line.

Implementing 5G in the cloud is beneficial because it not only allows a 5G cellular stack to grow and expand as required, but also enables mobile edge computing/multi-access edge computing (MEC). MEC is where the 5G core attempts to have cloud computing close in proximity to a given user or device. MEC helps to enable the ultra-low latency that 5G was designed for.

With the 5G use cases described above, there may be times when low latency is not a requirement. Instead, it might be more beneficial to have high throughput (maybe a user is streaming 4K video), or maybe even additional security protections in place (perhaps healthcare data is being transmitted). In these cases, 5G leverages a technology called network slices to determine how best to treat a device's data. Depending on how the device's data is classified, it will be given its own network slice implemented via software-defined networking (SDN).

Radio Communication

5G operates across a massive electromagnetic spectrum. Radio waves on the lower end of the spectrum travel farther but cannot transmit as much information. At the higher end of the spectrum, faster data transmission speeds can be achieved, but coverage is reduced because the radio waves cannot travel as far.

VentureBeat reports that telecom companies in the United States are embracing a multi-tier implementation of the 5G radio spectrum. This multi-tier implementation of frequencies can be broken into the following three areas[6]:

- **Low Band**: Transmitting around the 600-megahertz frequency, this band is used primarily for coverage as one 5G tower can enable coverage across hundreds of square miles. These frequencies are also leveraged by 3G/4G
- **Mid Band**: Used to service major areas, this band transmits around the 2GHz to 6GHz range. The data transmission in range is higher but the service area is much smaller than the low band. Wi-Fi also occupies this frequency range. In the future there may be a convergence between Wi-Fi and 5G in some areas.
- **High Band**: This band operates in the 30 and 300 gigahertz spectrum, for incredibly fast transmission speeds over a tiny transmission area. The radio waves in this spectrum are called millimeter and centimeter waves because their lengths are either in the millimeters or centimeters.

Millimeter waves (mmWave) and centimeter waves operate best when two devices that are trying to communicate are in an unobstructed path. This means that areas with a large concentration of objects (such as a city) will have poor cellular coverage. To compensate for this, Small Cells were added to the 5G specification. Small Cells are low powered base stations and can be placed anywhere (inside or

outside) to increase cellular coverage. A city might have 10s or even 100s of these placed throughout its area.

5G networks require a lot of sending and receiving wireless signals. To help facilitate that, 5G leverages Massive Multiple-Input Multiple-Output (abbreviated as either Massive MIMO or MIMO). MIMO is a wireless system that leverages multiple transmitters to send and receive data at once. MIMO by itself is not a new concept. With 5G, MIMO has been scaled up with a massive number of antennas for drastic improvements on cellular throughput.

One key component of massive MIMO is Beamforming. Beamforming is a wireless transmission technique that focuses a wireless signal in a single area as opposed to typical cellular antennas that broadcast over a large area. The beam is not owned by a single individual device, but rather all devices within the beam's radius, enabling even more efficient use of the technology.

Release 16 – 5G Phase 2

This iteration of the 5G standard, labeled "The 5G System – Phase 2," builds upon and enhances the already defined technologies and provides more support for companies transitioning from 4G/LTE. The specification also provides new deployment scenarios like Integrated access and backhauling (IAB). Instead of connecting small cells and base stations with fiber optic cables, IAB enables those cells to communicate wirelessly. In addition to simplifying deployment, this allows for extending coverage in the event of an emergency or a city expecting a large influx of people.

Other big improvements included in this release are changes made to vehicle-to-anything (V2X) communications by implementing intelligent transportation systems (ITS). ITS is a catch-all term to describe IoT devices embedded within vehicles that can communicate directly to each other or through an intermediary like a base station. ITS is the mechanism that will help improve the efficiency of driving in cities, on the highway, in parking lots, etc. The goal is to leverage ITS to help reduce traffic congestion, decrease fuel consumption, and reduce environmental impacts.

Release 17

Scheduled for delivery in 2022, Release 17 further enhances many of the technologies mentioned so far in releases 15 and 16. According to the proposed features released by 3GPP, Release 17 will include a study that describes the use of 5G with both eXtended Reality (XR) and virtual reality.

5G Security Architecture

Despite the fact that countries are adopting 5G, the standard is still in active development, and the security of the standard is still being worked out. That said, researchers from across the globe have spent time putting together an assessment of the 5G security protocol's security posture. The

following sections will first discuss the security architecture of 5G and then discuss the concerns not addressed by the specification.

Security Overview

In addition to all the performance improvements, 5G was designed with an updated security model. In summary, the security features of 5G include:

Zero-Trust

Since the 3rd Generation (3G) of telecommunications was implemented, mutual authentication between user devices and base stations have been implemented. 5G continues with this trend of distrust. In previous cellular generations, within the internal cellular network, when a mobile network received data from another network carrier, it would accept it as fact. 5G has implemented the Security Edge Protection Proxy (SEPP), a gatekeeper that prevents any traffic that isn't authorized and verified from entering the network carrier's network.

Another example of how zero-trust has been implemented within 5G is through the separation of duties. Components from previous cellular standards have been broken up with gateways in between them to ensure that the data received is valid. To help facilitate this is an updated cryptographic key hierarchy. Effectively, these sub-components now have specific encryption keys between them. In the event that one sub-key is compromised, the rest of the 5G environment remains protected.

Data Transmission Security

As the cellular generations have developed over time, the encryption and integrity controls have slowly been increasing. With the first generation (1G), anyone tuned into the frequency that a cellular device operated on could listen in on the conversation. The second-generation (2G) added encryption between a user device and base station but left the rest of the network lacking. The 3rd and 4th generations effectively added another hop of encryption to their standards.

The situation was made worse by the fact that critical vulnerabilities due to lack of cryptographic and integrity controls were found in the signaling protocols leveraged by those cellular generations. Signaling protocols are what's leveraged to manage telephone calls, route text messages, and perform roaming. The abuse of these protocols allow adversaries to intercept and listen in to phone calls, perform fraudulent cellular activity, track users, and more.

With 5G, the standard has finally reached a point where all signaling traffic is encrypted and integrity protected. And user traffic is encrypted with optional integrity protection. The SEPP ensures that traffic sent from one network operator to another is encrypted.

Privacy

The previously discussed enhanced authentication, encryption, and integrity controls help to address privacy concerns. But 5G also directly addresses privacy concerns discovered with the 4G/LTE standard.

In order for a device to leverage the cellular network, it has to perform an attaching procedure. In 4G/LTE, the device will continuously beacon out an identifier that the cellular network uses to identify and authorize the user. This value is called the International Mobile Subscriber Identity (IMSI). During the attachment procedure, the device and base station authenticate each other and agree on security controls they will use to communicate.

Because the IMSI is beaconed out before security controls are agreed upon, the attribute is transmitted in plaintext, allowing users to be tracked and, in some cases, even for adversaries to perform fraudulent cellular activity on a victim's behalf. Vulnerabilities related to the IMSI have been discussed in many security conferences around the world[7,8,9].

5G addresses the weaknesses of the plaintext IMSI by taking the 5G equivalent, now called the Subscription Permanent Identifier (SUPI), and encrypting it with that device's home carrier's public key. The encrypted SUPI is called a Subscription Concealed Identifier (SUCI). The SUCI is then leveraged to initiate the attachment procedure.

Virtualization and Software-Defined Networking — 5G Deployment Dangers

Because 5G is implemented in the cloud, all components are virtualized. As such, 5G networks can be constructed like Lego pieces, hot-swapping components as needed. Instead of having a flat network where all internal components can talk to each other, 5G can ensure that the only areas of a network that should be able to communicate can. Also, in the case where vulnerabilities are found, machines can be updated or mitigations can be put in place instantly to address the concerns. The cloud also enables resiliency not found in previous generations of cellular technologies. Cellular components can scale to address communication surges.

On top of the overall virtualization that's achieved by being in the cloud, internal networks are similarly virtualized with network slicing. Network slicing enables mobile network operators to ensure that each type of data flowing through the mobile network is treated in the way that best suits it. For example, payment card data flowing over the cellular network can be configured with more secure encryption and integrity algorithms. In cases where availability is more important than security, network slicing can ensure that fast response times are enforced.

5G Security Risks and Concerns

As 5G becomes more ubiquitous across the globe, the security community is taking the opportunity to review and understand the potential security risks associated with implementing the standard. These security risks fall into the following categories:

- Inherited flaws
- Out-of-specification issues

Inherited Flaws

Bloomberg reports that it will cost hundreds of billions of dollars to upgrade from 4G/LTE to 5G[10]. This is a massive cost for any company or nation to bear, requiring many companies to slowly phase in the next generation of cellular technology over the next decade. Because these partial 5G networks rely heavily on pre-existing 4G/LTE technology, they will also absorb their vulnerabilities.

Legacy Protocols

The legacy protocols that possess the most vulnerabilities are the aforementioned signaling protocols. A brief summary of what each protocol does and its vulnerabilities are summarized below:

- **SS7**: Used in 2G/3G to exchange information needed to transmit voice and text messages between parties. This protocol lacks authentication and integrity controls resulting in any party being able to establish man-in-the-middle connections, allowing communications to be intercepted. Abusing this protocol also allows an attacker to perform telephone spam, spoof numbers, and track a user's location[11].
- **Diameter**: With the transition from 3G to 4G/LTE, the Diameter protocol was brought in to replace SS7. Diameter provides authentication, authorization, and even encryption. Weaknesses were discovered in this protocol that allow adversaries to send spoofed messages that can leak information about a cellular user such as their location[12,13].
- **GTP**: Recently, Positive Technologies released research into another vulnerable protocol leveraged in 4G/LTE and 5G: GTP [14]. GTP is used to transmit user traffic on all generations of mobile technologies from 2G to 5G. Abusing this protocol can result in a bad actor being able to impersonate a user, perform fraudulent cellular activity, and achieve denial of service.

Unlike the other two protocols, GTP is defined for use in 5G standalone architectures.

Downgrade Attacks

Because of how fast technology moves forward, it can be difficult even for tech enthusiasts to keep up-to-date, let alone non-technical people. To ensure that everyone has sufficient time to upgrade, new standards are typically made to support older ones as well. However, in allowing support for older generations, there's the potential that downgrade attacks can be performed.

Downgrade attacks trick users into leveraging the insecure and out-of-date versions of a protocol. These types of attacks can be found everywhere. For instance, the Transport Layer Security (TLS) protocol that a browser leverages to securely surf the internet. Even the latest TLS version published in 2018 has been found to be vulnerable to downgrade attacks[15]. But, there's an easy fix. A web browser can be configured to limit access to websites that leverage the latest, most secure protocols, disabling anything deemed insecure. With those protocols disabled, if someone attempts a downgrade attack against it, the browser will simply refuse.

Cellular devices don't have the same flexibility that web browsers do. When a mobile device connects to a cellular network, the user has no control over the process. There's no setting in an iPhone or a Pixel that can be configured to prevent a phone from connecting to out of date and insecure cellular networks (like 2G). The Electronic Frontier Foundation (EFF) is actively lobbying tech giants, namely Apple, Samsung, and Google, to allow users the ability to disable insecure cellular standards within their devices[16]. Until these changes are implemented, adversaries have the potential to side-step all the security controls implemented by 5G by performing downgrade attacks.

Out-of-specification Issues

3GPP has defined very explicit details on the 5G standard in their releases, but there's a number of areas of 5G that they deem out-of-scope. It's these areas that companies and network operators have to figure out on their own and therefore where there is the highest probability of something going wrong. This includes security problems with the cloud, web application vulnerabilities, and privacy concerns.

Cloud Computing Vulnerabilities

To enable the flexibility of virtualization and network slicing, many companies will push their 5G environments into the cloud. Empowering 5G deployments with cloud capabilities will result in many benefits. However, these benefits come at a cost. Cloud misconfigurations are frequently cited in the news, such as storage services left open for anyone to browse or management interfaces exposed with default credentials. Telecom companies will need to ensure their cloud environments are completely secure before going live.

Another consideration is attacks from inside the 5G network. Unlike previous generations of cellular standards, 5G will be required to execute potentially untrusted 3rd party code within its environment. With multi-access edge computing, companies will be able to run applications in edge locations all around the world. Despite the fact that, by design, this should be segmented entirely from the internal core network, this still presents a number of concerns:

How will 5G managed network operators ensure that the 3rd party code does not include malware or exploits? A code review process similar to the one used by the Google Play Store or Apple's App Store will need to be implemented

If Company A and Company B both have applications within an edge computing environment, what is stopping one from attacking another? Telecoms will need to treat all non-telecom related code as untrusted, ensuring it is executed only in application-specific segmented environments.

Web Application Issues

With 4G/LTE, rather than having separate protocols for voice, text messages, and data, all communications are treated as Internet Protocol (IP) packets. On top of IP, custom telecommunications protocols were built. 5G eliminates these custom protocols and instead leverages HTTP for internal network communication.

The adoption of such a well-known standard will enable flexibility in the future for upgrading or changing components. However, it will also lower the bar considerably from a security perspective, allowing adversaries to attack core infrastructure. Web-related vulnerabilities are thoroughly documented by organizations such as OWASP, and can allow anyone to understand and attack the next generation of wireless technology.

One particular area of focus will be the way in which internal authentication from one mobile operator to another is implemented – a use case that will play out over and over as a user roams, or finds themself on a network owned by another carrier in their country. Internal authentication leverages OAuth2, JSON, JSON Web Signatures, and JSON Web Encryption. These technologies possess well-known implementation flaws, which creates the potential for interesting authentication, authorization, and data validation vulnerabilities (like JSON deserialization attacks).

Complications Managing User Privacy

In recent years, end-user privacy has become a focus around the world. Researchers are examining the controls within 5G and looking to identify improvements to the standard before the design is finalized. In the whitepaper "5G Privacy Scenarios and Solutions," researchers identified that one of the main privacy concerns relates to responsibility ambiguity[17].

Mobile network operators will need to work with cloud providers and third-party developers to define who has what responsibilities in terms of user privacy, and how each player will be held responsible. One might suspect that current privacy regulations help provide assurance here. But 5G networks do not stop at a country's border since radio waves have no comprehension of political jurisdictions. So it is entirely possible for overlapping laws to conflict. The situation becomes even more convoluted when an incident occurs because it's not possible to predict which law(s) will take precedence when a victim, an attacker, and the service provider are from different locations.

And all of this is assuming that a nation-state has implemented 5G with industry best practices. To ensure confidentiality and integrity of over-the-air communication, 5G leverages the New Radio Encryption Algorithm (NEA) and New Radio Integrity Algorithm (NIA), respectively. Both algorithms support the highly secure Advanced Encryption Standard (AES). However, in both cases, these

algorithms also support weaker algorithms (like SNOW 3G[18]) and can be disabled entirely so no protections are in place.

As 5G becomes ubiquitous, lawmakers around the world will need to devise adequate policies to address security concerns to ensure there are no gaps in protecting end-user data.

Conclusion — The Fate of 5G Technology

The emergence of the fifth generation of cellular technology will revolutionize the world and facilitate unprecedented use of internet-connected devices. As it stands, the security of the protocol is not only a concern of 3GPP and the researchers developing the standard, but also of the lawmakers developing policies that pertain to 5G. Ultimately, the responsibility for implementing adequate 5G security rests in the hands of the entities that build and deploy the technology.

Contact us to learn more about Kroll's technical expertise with 5G.

Abbreviations

1G – first generation of wireless cellular technologies

2G – second generation of wireless cellular technologies

3G – third generation of wireless cellular technologies

4G – fourth generation of wireless cellular technologies also known as LTE

5G – fifth generation of wireless cellular technologies

3GPP – The 3rd Generation Partnership Project

AES – Advanced encryption standard

AIOTI – Alliance for IoT Innovation

AVP – Automated Valet Parking

EFF – Electronic Frontier Foundation

eMBB – enhanced mobile broadband

IAB – Integrated access and backhauling

IMSI – International Mobile Subscriber Identity

IP – Internet protocol

ITS – Intelligent transportation systems

JSON – JavaScript Object Notation

LTE – Long term evolution also known as 4G

MEC – mobile edge computing / multi-access edge computing

MIMO – Multiple-Input Multiple-Output

mMTC – massive machine-type communications

mmWave – millimeter waves

NEA – New radio encryption algorithm

NIA – New radio integrity algorithm

NSA – Non-standalone

RAN – Radio access network

SA – Standalone

SDN – Software defined networking

SEPP – Security edge protection proxy

SUCI – Subscription Concealed Identifier

SUPI – Subscription Permanent Identifier

TLS – Transport layer security

UAV – Unmanned Aerial Vehicles

UE – User equipment

URLLC – Ultra-reliable low-latency communication

V2X – Vehicle to everything communication

XR – eXtended Reality

Sources

[1]G. Karagiannis and T. Klein, "[PDF] IoT Relation and Impact on 5G," AIOTI, 01-Feb-2019. [Online]. Available: https://aioti.eu/wp-content/uploads/2019/03/AIOTI-IoT-relation-and-impact-on-5G-190308-R2-published.pdf. [Accessed: 27-Aug-2020]..

[2]H. Vella, "5G vs 4G: what is the real difference between them?," Raconteur, 08-Jul-2020. [Online]. Available: https://www.raconteur.net/technology/4g-vs-5g-mobile-technology. [Accessed: 27-Aug-2020].

[3]T. Spangler, "Netflix Bandwidth Consumption Eclipsed by Web Media Streaming Applications," Variety, 12-Sep-2019. [Online]. Available: https://variety.com/2019/digital/news/netflix-loses-title-top-downstream-bandwidth-application-1203330313/. [Accessed: 27-Aug-2020].

[4]"3GPP 3GPP Specification Release Numbers," Electronics Notes. [Online]. Available: https://www.electronics-notes.com/articles/connectivity/3gpp/standards-releases.php. [Accessed: 27-Aug-2020].

[5]H. Ekström, "Non-standalone and Standalone: two paths to 5G," Ericsson.com, 11-Jul-2019. [Online]. Available: https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks. [Accessed: 27-Aug-2020].

[6]J. Horwitz, "The definitive guide to 5G low, mid, and high band speeds," VentureBeat, 10-Dec-2019. [Online]. Available: https://venturebeat.com/2019/12/10/the-definitive-guide-to-5g-low-mid-and-high-band-speeds/. [Accessed: 27-Aug-2020].

[7]R. Borgaonkar and S. Udar, "Blackhat – Understanding IMSI Privacy," Youtube, 19-Mar-2015. [Online]. Available: https://www.youtube.com/watch?v=E-IPzIptM1A. [Accessed: 27-Aug-2020].

[8]F. Martinez, "DEF CON 23 – Crypto and Privacy Village – Freddy Martinez – IMSI Catchers," Youtube, 07-Dec-2015. [Online]. Available: https://www.youtube.com/watch?v=JyTb5mJOYLo. [Accessed: 27-Aug-2020].

[9]C. Quinton, "DEF CON Safe Mode – Cooper Quintin – Detecting Fake 4G Base Stations in Real Time," Youtube, 05-Aug-2020. [Online]. Available: https://www.youtube.com/watch?v=siCk4pGGcqA. [Accessed: 27-Aug-2020].

[10]O. Kharif, S. Moritz, "Upgrade to 5G Costs $200 Billion a Year, May Not Be Worth It," Bloomberg, 18-Dec-2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-12-18/upgrade-to-5g-costs-200-billion-a-year-and-may-not-be-worth-it. [Accessed: 27-Aug-2020].

[11]T. Engel, "CCC – Tobias Engel: SS7: Locate. Track. Manipulate.," Youtube, 28-Dec-2014. [Online]. Available: https://www.youtube.com/watch?v=-wu_pO5Z7Pk. [Accessed: 27-Aug-2020]

[12]H. Schmidt and D. Mende and E. Rey, "Blackhat – Attacking NextGen Roaming Networks," Youtube, 08-Jan-2020. [Online]. Available: https://www.youtube.com/watch?v=AySWvrpj9s8. [Accessed: 27-Aug-2020]

[13]N/A, "Security assessment of Diameter networks," Positive Technologies, 2020. [Online]. Available: https://positive-tech.com/storage/articles/diameter-2020/diameter-2020-eng.pdf. [Accessed: 27-Aug-2020]

[14]N/A, "Threat vector: GTP," Positive Technologies, 2020. [Online]. Available: https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf. [Accessed: 27-Aug-2020]

[15]D. Wong, "Downgrade Attack on TLS 1.3 and Vulnerabilities in Major TLS Libraries," NCC Group, 07-Feb-2019. [Online]. Available: https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2019/february/downgrade-attack-on-tls-1.3-and-vulnerabilities-in-major-tls-libraries/. [Accessed: 27-Aug-2020].

[16]C. Quinton and A. Arrieta, "Your Phone Is Vulnerable Because of 2G, But it Doesn't Have to Be," Electronic Frontier Foundation, 29-Jun-2020. [Online]. Available: https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be. [Accessed: 27-Aug-2020].

[17]M. Liyanage and J. Salo and A. Braeken and T. Kumarand S. Seneviratne and M. Ylianttila, "[PDF] 5G Privacy: Scenarios and Solutions," Research Gate, 01-Jul-2018. [Online]. Available: https://www.researchgate.net/publication/324683290_5G_Privacy_Scenarios_and_Solutions. [Accessed: 27-Aug-2020].

[18]F. Nilofer and J. Qaddour, "[PDF] Comparative Study of Vulnerabilities in Lte Cryptographic Algorithm: Semantic Scholar," Semantic Scholar, 01-Jan-2018. [Online]. Available: https://www.semanticscholar.org/paper/Comparative-Study-of-Vulnerabilities-in-Lte-Nilofer-Qaddour/8c7a8dcf180950a481f56b53ee47209bc98fd17e. [Accessed: 27-Aug-2020].

Share

Stay Ahead with Kroll

System Assessments and Testing

Kroll's field-proven cyber security assessment and testing solutions help identify, evaluate and prioritize risks to people, data, operations and technologies worldwide.

Penetration Testing Services

Malware. Ransomware. Social engineering schemes. Brute force attacks. How confident are you that your protective measures are effective against current and emerging cyberattacks?

Cloud Security Services

Kroll's multi-layered approach to cloud security consulting services merges our industry-leading team of AWS and Azure-certified architects, cloud security experts and unrivaled incident expertise.