Chapter 8

SECURITY, PRIVACY & TRUST IN 5G WIRELESS MOBILE COMMUNICATIONS

A. Yarali, R. Yedla, S. Almalki, K. Covey, and M. Almohana
Telecommunications Systems Management
Murray State University, Murray, KY

ABSTRACT

The main purpose of this chapter is to identify the potential threats that can occur in 5G mobile communications systems and to discuss the possible techniques that can be implemented to avoid these threats. The design of the 5G networks must be scrutinized at the beginning phase of its implementation considering massive connectivity of M2M, D2D and new applications and services. The migration from 4G to 5G is not just a quantative transition because this generation of mobile communication expected to integrate and to connect various sectors such as smart grid, health, transportation and manufacturing. To counter such threats in 5G, cryptographic techniques

Corresponding Author address
Email: ayarali@murraystate.edu

Every service they provide should be technologically secured; the security service should be integrated within the cellular technology. With every generation of the new invoked cellular technology, they create a better prominent technique that makes the data more secured. 5th Generation cellular technology is totally dependent on TCP/IP layered model. 5G is broader than the previous versions of cellular technology, and technically making it different from the previous versions (4G and 3G). In simple words, the paper first gives an overview about the next generation of mobile communications, second, about the 2020 agenda from 3GPP, third, about the threats 5G wireless mobile communications could face, fourth, techniques involved in cryptography to secure the user data, fifth, about the trust model and ends with a conclusion.

WIRELESS ANONYMITY

Anonymity is a relatively new concept in the wireless world. Over the past decade, the public has become increasingly concerned about the privacy of their communication methods. Due to events, such as whistleblowing, hacking, and governmental corruption, society is becoming aware of malicious attackers, and their policy makers pulling the wool over their eyes. Because of this, citizens are taking certain measures to ensure that their telecommunications remain private. Whether the government likes it or not, people are not going to be as easily fooled as they once were. Luckily, there are many software and hardware engineers who have taken the task of keeping the wireless world anonymous and secure, upon themselves as their personal mission. Therefore, there have been so many accomplishments in the world of security because of these volunteers. Hence, this paper will only be scratching the surface. In this study, we will see how the public views their privacy and the steps they are taking to remain hidden - and safe - in the wireless world.

Wireless anonymity, put plainly, is ensuring by any necessary means that guarantee all information you are sending over a network remains private between you and your endpoint. All over the country, people are continuing to funnel money into programs dedicated to helping them retain their privacy online. There are solely set up communities that instruct people on how to remain anonymous over their networks. Websites, such as the Information Security section of StackExchange, are flooded with questions about remaining anonymous over the internet daily. Google is certainly searching the terms ñwireless anonymityò to bring results from the aforementioned site. This goes to show that people are indeed interested in remaining private.

Companies have begun to take advantage of this recent privacy trend as well. One such company, Anonabox, has created a hardware router that connects to the Tor network so that they can keep your communications secure (explained later, for now just think of it as the ultimate private network) (Anonabox). This device is for sale on their website for $99. Any person can purchase this device in

is mentioned first because it is the easiest for people to wrap their head around. In essence, it is just a piece of hardware that you plug into your computerôs USB ports (which almost all computer users are familiar with). The device then acts as your own personal computer and private router; accordingly, rerouting all of your communication messages to a separate global network before going to your destination, thus, protecting your online identity. This is a remarkable achievement towards everyday privacy. Consumers with a little knowledge of the information technology industry can ensure that their communications stay private just by purchasing a convenient and pluggable device, and running it alongside their everyday computer tasks. In the not-so-distant past, this would have only been attainable by a programmer or information technology professional manually setting up such a system catered to each individual. As you can see, however, this is no longer the case. Wireless

made to the opposite end of the spectrum designed to hinder your everyday life and communications. Have you ever wondered how easy it is for an attacker to retrieve your information over an insecure connection? It is as easy as downloading the right software, telling it where to listen, and relaxing in your chair while you sneakily eavesdrop on someone

Security, Privacy & Trust in 5G Wireless Mobile Communication

the development community do not know that it is also open source software. Chromium is made to be safe, secure foundation for other software (particularly web browsers). Anyone can go and use the Chromium project as the foundation for their own web browser if they wish. A large part of Chromiumôs success as a secure and a reliable piece of software is due to the fact that it is an open source. Without such an idea, and a community, there is no way to tell how far along secure software would be today. As citizens who are concerned about our privacy and security, we owe many thanks to the open source community (The Chromium Projects).

As a person who is aware of the importance of wireless anonymity and security, I am glad to see that there is a rapid growth being made in the information technology industry. Thanks to large companies who have considerable influence in the software development industry spreading the importance of such awareness (such as. Google, Mozilla, etc.), more big players are starting to pay attention and give citizens what they deserve. The events that people, such as Edward Snowden, brought to light are inexcusable. No government should ever be allowed to spy on their people without proper cause, especially, a government built upon the foundation of freedom and democracy. It is despicable to think that our own policy makers are citizens themselves, and would do such a thing to their country. Because of open source security projects, we are beginning to get past this phase of wireless privacy infringement. Eventually, people will no longer be able to snoop in on other peopleôs communications. We owe our thanks to these teams that have made such a thing possible, lest we take them and their service for granted.

3RD GENERATION PARTNERSHIP PROJECT

3rd

Broadband, Critical Communications, and Network Operations. Like, 3GPP other bodies which are working towards the 5G are: NGMN (Next Generation Mobile Networks): it associates leading operators, vendors, manufacturers, and universities. GSMA, 5G-PPP ópublic private partnershipô initialized by European Commission, IETF, and IEEE. 3GPP believes that LTE (Long-Term Evolution) will only be the standard that they are depending on. There is a possibility that they are going to reach the maximum limits of LTE, but they must improvise the current standard of LTE, such that they are compatible with the 5th Generation Mobile Communication. LTE will remain as a key factor for wide area broadband coverage of 5G era.

5G: THE NEXT GENERATION MOBILE COMMUNICATION

The next generation of mobile communication is about the connectivity to every electronic device. Unlike the predecessors of the cellular communications the main agenda that the 5G cellular communication is considering is to: provide better coverage, greater connectivity, higher reliability, greater mobility range, higher throughput, and lower latency. These features will be featured by different network layers, implies directly to the need of provision of an identity, security, trust, and privacy. Currently, we have IMT-Advanced/4G

the world-

recognized as: Security of service layer, Privacy, Integrity & Authenticity of transmission of data over different network layers, Security of network application.

Technological changes, abilities, services, regulatory requirements, and new security concerns will surface with a new beginning of 5G just as every new product in the market. More and more security standards will be under developing stage until a standard of good security ability is finalized. The current 4G security standards are confined to 4G itself since the use of virtualization and cloud in 5G encourages the telecommunication industry to develop a better secured and trusted model to be developed. The whole agenda again must consider the efficiency and performance since it should degrade the efficiency and performance of the system. The security should be considered between end to end communication, such as machine to machine and not just confining to one device alone.

DENIAL OF SERVICE ATTACKS & DISTRIBUTED DENIAL OF SERVICE IN 5G

It is an attack on the network, which floods the networks with unwanted traffic and making the network congested. Teardrop and Ping of Death attacks are examples of DoS

Protection towards user data,
Assuring security,
Strong monitoring,
Security update and management mechanisms.

CRYPTOGRAPHIC TECHNIQUES

With few resources in hand, building a security standard for 5G is a difficult task, for example, the system built should be compact, sleek, efficient, and powerful, building a cryptographic system with limited resources is a complex job and difficult to estimate. The data traffic is set to increase in the coming years as more and more number of device connectivity is expected in the coming years. 5G has greater data speed (in Gbps) and expecting higher traffic, for example, something around thousand times greater than that of the present LTE, and low latency should be considered in building a secure system. In general, there will be a tradeoff between speed and size of hardware for building a secure system which is a severe setback. Ciphers like óGrainô has high propagation delay and Ciphers like óTriviumô use too many óflip flopsô to maintain the security level, such as cryptography must compromise w.r.t speed or size of the hardware.

In cryptography for encryption purpose, there are different types of cyphers and those are categorized as stream and block ciphers. Block ciphers research started some fifty years back, and the development led to Advanced Encryption Standard (AES) algorithm, which is secured and it can withstand different kinds of attacks. The most recent ciphers are known as Stream ciphers as binary additive stream ciphers. At this point, the plain text, the key, and the cipher text are all in binary sequences. The key is generated by a keystream generator in which it attains a secret key and initial value as a source, and these generate a random sequence of 1ôs and 0ôs. The ultimate cipher text is, thus, attained by the bit-wise addition of the generated key and the plain text. Stream ciphers are sleeker and faster than block ciphers as in the case of Trivium and Grain.

Recent innovations and research made the block ciphers too in the size of Trivium and Grain. Examples of block ciphers which are almost the same capabilities as Grain and Trivium are Piccolo, LED, PRESENT, TWINE, and KATAN. The block codes are mostly for radio frequency identification tags and they can be clocked at frequencies of 100KHz, yet some of them can be clocked even faster up to 1Gbps. However, stream ciphers are naturally the best choice when considering compact size and higher throughput. Global System for Mobile Communications (GSM) ciphers A5/1 and A5/2 belong to stream ciphers category. As we have seen that the stream ciphers are sleek and fast, yet they were found susceptible to attacks. So, later they were replaced with more secure stream cipher A5/3 in place of A5/1 and A5/2 was restricted from any further use.

KASUMI belongs to the block cipher category which is used in GPRS, UMTS and GSM cellular mobile communication systems. GPRS uses óGEA3ô as ókeystream generatorô; GSM uses óKASUMIô in óA5/3ô keystream generator and UMTS where KASUMI is used for

AUTHENTICATION MODEL

The 5G era would change the businesses around the world with abundant of services they provide. Different businesses require different authentication techniques. The service providers try their best to provide their service at lower costs with simplicity. The possible authentication models that could exist in the 5G era for different business needs:

Network Authentication:

Service providers must first pay to the networks, and then the service authentication will be granted so that the users can access through the services through single authentication. This procedure incurs costs on service providers.

Service Provider Authentication:

Networks relay on the authentication from the service providers, and there is no necessity for any network access authentication. It implies the incurred costs on operating the networks are lowered.

Service Provider and Network Authentication:

In this case, networks are undertaken by the network access and services providers stick with the service access.

CONCLUSION

5G security and privacy design must be integrated along with 5G system, moreover, 5G cellular mobile communications is vast, and it can encounter more threats from the third-party intruders. The need for stable cryptographic techniques is necessary when developing 5G mobile communication. The researchers and many academic institutions have a keen interest in the prospering field of 5G. As we can

Service ProvreW*nBT/F1 10.56 s. er30( )-211(G)-4(or)3(e 332.n Tm0 gonospe)3(r)3(i)5(n)6(c1 10(o)11(r)-3( )-101(st)8(abl)ns)-212(hav)12(e)-

REFERENCES

"Anonabox | Tor Hardware Plug and Play Onion Router." Anonabox. Web. 16 June 2015.

Geier, Eric. "Here's What an Eavesdropper Sees When You Use an Unsecured Wi-Fi Hotspot." PCWorld. PCWorld. Web. 17 June 2015.

"What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?" What Is SSL (Secure Sockets Layer)? Digicert. Web. 17 June 2015.

"Tor: Overview." Project: Overview. Tor. Web. 18 June 2015.

"RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2." RFC 5246