Mobile Security

Cassandra McCandless

With mobile security, the hope is that with each new generation, security will become better. 2G, 3G, 4G, LTE, and 5G are all generations of mobile devices that have different features, security, and even flaws. We all use mobile devices these days, but most of us do not understand how the mobile security on these devices actually works. It is important to know what each generation does and can do so that we can understand mobile security better.

2G is the second generation of digital cellular phone communication. Seeing as it is one of the first generations ever created, it has some of the most security flaws. First of all the encryption scheme that is used for 2G mobile devices can be attacked pretty easily. This is done by exploiting weaknesses and using common hardware. The benefit of 2G networks with phone conversations is that the communications are digitally encrypted, but the main security issues are that the crypto algorithms which are A3 for authentication, A5 for encryption, and A8 for key generation have weaknesses that can be exploited. A5 is vulnerable to a real-time and a ciphertext-only attack, and it is also vulnerable to a rainbow table attack. Some of the major security concerns are that communications and signaling traffic in a fix network are not protected, terminal identity cannot be trusted, and it is really only as secure as the fixed network it is connected to. Because of some of these security concerns, 3G was created. 3G is more secure for a variety of reasons. First, it provides better security because it allows mutual authentication between terminals and networks. 3G also makes cellular devices more similar to a computer which means that if someone is going to hack a cell phone, they are going to need to use the same types of methods they would use in hacking a computer. This is a good and bad

thing because it does give hackers more access to information that is stored on mobile devices like being able to spy on our movements, listen to phone calls, and read messages. 3G networks use the KASUMI block crypto instead of the A5/1 stream cipher like 2G does. Some of the security problems with KASUMI is that IMSI is sent in cleartext when allocating TMSI to a user and hijacking outgoing and incoming calls in the networks with disabled encryption is possible. This is done when a hacker facilitates a man in the middle attack and drops the user once the call is connected. Unauthorized access to sensitive data is also possible.

4G allows users to connect to the Internet through a provider's cellular connection. Instead of getting the connection from an internet provider like a user would at home, they actually get it from the cellphone company. Data that is sent over 4G is encrypted, and this actually makes it safer than just using public Wi-Fi. Now, 4G is more secure than the previous generations of 2G and 3G, but anything that is connecting to the Internet is not totally secure. There have been a couple of successful cases of people hacking into 4G devices by using a man in the middle attack, but overall this is much more difficult on a 4G network than it even is on Wi-Fi. 4G also offers users greater speed, and when 4G was first announced, the speeds that were being discussed were unheard of.

LTE is another generation of mobile data technology, and it stands for long-term evolution. The whole goal of LTE was to improve wireless broadband speeds because with more people using mobile devices the demand needed to be met. LTE really is what is bringing mobile data technology closer to the speed of what 4G really should be. LTE offers greater speed and stability to its users. By using LTE, a user can also download data from many sources at once by aggregating channels instead of just connecting to the strongest signal nearby.

On a 4G LTE network connection, data is encrypted, and a users identity must be authenticated and protected. 4G LTE is considered more secure than previous generations, too. LTE security is based on a shared secret key K between the USIM and the HSS. The UE and the eNodeB and MME derive keys for the encryption and integrity protection from K. These derived keys then use NAS encryption and integrity protection, RRC encryption and identity protection, and user plane encryption. The purpose of NAS security is to securely deliver NAS signaling messages. These messages go between a UE and MME in the control plane by using the NAS security keys. These security keys come from K_{asme}, and new keys are generated every time EPS AKA is performed. This is every time a new K_{asme} is generated. After this security setup is finished the UE and the MME get to share a NAS encryption key and a NAS integrity key. These are then used for encryption and integrity protection of NAS messages before they are transmitted. For AS security the purpose is the be able to deliver RRC messages between a UE and eNB in the control plane of the IP packets in the user plane by using the AS security keys. The security keys come from the K_{enb} and new keys are generated every time there is a new radio link established. After this setup is done, the UE and the eNB get to share the RRC integrity key, RRC encryption, and the user plane encryption key.

With 4G LTE there is some problems with weaknesses in authentication and key agreement. This is problematic because it can lead to data leaks. Also, with inexpensive hardware, hackers have the ability to intercept calls and track where users are at. Another attack that can be carried out on devices using 4G LTE is connecting to networks without authorized usernames and passwords. This can lead to user's identities being stolen, forcing devices off the network, and even sending fake messages from somebody else's device. Hackers are even able to do things with spoofing where they are committing a cybercrime in the United States, but they

can make it look like they are somewhere else in the world. Overall, spoofing and fake messages are two of the biggest security risks when it comes to 4G LTE. The hope is that once 5G is really up and running well, these attacks will be able to be mitigated.

There are also attacks that can happen using 4G LTE called protocol attacks. This is done by forging attach_request messages from a malicious device. This can block a user's phone from attaching and can track a user through a malicious node. There is another protocol attack that also works by injecting malicious control panel commands, and this can cause service disruption. To mitigate this type of attack there is something that has been created called the LTEInspector. It is a symbolic model checker and a cryptographic protocol verifier. It examines the order of events and actions. This includes cryptographically protected messages. LTEInspector aims to verify authenticity, availability, integrity, and secrecy of user's sensitive information. This will disallow impersonation, prevent service disruption from happening, stop unauthorized billing, and prevent activity profiling.

Now, 5G is the next generation of mobile connectivity. Just like with 3G, 4G, and LTE, the whole goal is to make connectivity better and more secure. Just like LTE, 5G is going to offer even faster speeds and better and more reliable connections. The average download speed with 5G is going to be about 1GBps. It is also going to be able to carry so much more data, and this is going to lead to a more connected world which is important with the growing and growing use of mobile devices. With 5G the hope is that it will serve critical infrastructures like automation, connectivity to machines, robots, and transport solutions. Because the use is going to be even more widespread security is even more important. 5G is going to utilize IMSI encryption. All traffic data that is sent over 5G networks will be encrypted. There will also be integrity

protection and mutual authentication put into place. 5G will also have what is called end to end encryption. This is just one of the tools that will be used to bring security to 5G. 5G will also have 5 components that make it more secure. These include resilience, communication security, identity management, privacy, and security assurance. 5G will be resilient to cyberattacks and non malicious incidents. This is because it has overlapping features that will protect against these types of things. 5G NR provides industrial control, critical infrastructure, and public safety applications. Even more resiliency can be put into place if needed by deploying single base station as two split units that are called a central unit and a distributed unit. This will be able to deploy security sensitive functions of the 5G NR access that include features like user plane encryption. It will also be done in a secure central location that keeps non security sensitive functions in less secure locations in other places. When it comes to communication security, 5G is going to include protection against eavesdropping and modification attacks. This is possible because signaling traffic is encrypted and integrity protected. User plane traffic is encrypted and integrity protected, too. User plane integrity protection is actually a brand new feature, and it is really good for small data transmissions which is great for the everyday user. For identity protection there is a new authentication framework. It allows user to choose their own authentication credentials. It will allow for certificates, pre-shared keys, and token cards. In the past SIM cards were required for credentials. It will also use EAP. For privacy, data traffic like phone calls, internet traffic, and text messages will be protected with the new, state of the art encryption. Devices and the network will mutually authenticate making it impossible for an unauthorized party to decrypt and gain access to information that is communicated over the network. Finally, 5G meets security assurance. This means that it meets all security requirements

and is implemented following secure development and product lifecycle processes. This is great for mobile security!

Works Cited

"5G Security - Enabling a Trustworthy 5G System - Ericsson." *Ericsson.com*, 18 Sept. 2019, www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system?gclid=EAIaIQobChMI6MD1lv-g5QIVyP_jBx3DsQ2SEAAYBCAAEgI_v_D_BwE.

Chirgwin, Richard. "4G LTE Pried Open to Reveal a Slew of New Protocol-Level Attacks." *The Register® - Biting the Hand That Feeds IT*, The Register, 7 Apr. 2018, www.theregister.co.uk/2018/03/05/4g_lte_protocol_vulnerabilities/.

"Critical Infrastructures – Main Threats for 2G and 3G Mobile Networks." *Security Affairs*, 25 Oct. 2016, securityaffairs.co/wordpress/1603/security/gsm-mobile-networks.html.

EventHelix. "LTE Security: Encryption and Integrity Protection Presentation and Call Flow." *Medium*, LTE - Long Term Evolution, 4 June 2017, medium.com/long-term-evolution/lte-security-encryption-and-integrity-protection-presentation-and-call-flow-dd407bbc1889.

"How Safe Is Surfing on 4G vs. Wi-Fi?" *How Safe Is Surfing on 4G vs. Wi-Fi?*, us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html.

"LTE Security II: NAS and AS Security." *Network Manias*, www.netmanias.com/en/post/techdocs/5903/lte-security/lte-security-ii-nas-and-as-security.

McCann, John. "5G: Everything You Need to Know." *TechRadar*, TechRadar, 1 Oct. 2019, www.techradar.com/news/what-is-5g-everything-you-need-to-know.

Schick, Shane. "Security Flaw Spawns 10 New Kinds of 4G LTE Attacks, Researchers Report." *Security Intelligence*, securityintelligence.com/news/security-flaw-spawns-10-new-kinds-of-4g-lte-attacks-researchers-report/.

"What's the Difference between 4G and LTE ... and Does It Even Matter?" *Digital Trends*, 18 July 2019, www.digitaltrends.com/mobile/4g-vs-lte/.