Security in Cellular Networks

Syed Muhammad Ali Nawazish, 18030007

February 2020

1 Introduction

Cellular Networks have become an integral part of everyone's life throughout the world. In fact, they are a key component in making a digital society. The rise of the Fourth Generation Cellular network (4G/LTE) furthered the progress in achieving an interconnected world. With improved assurances provided by the 4G/LTE, it is being widely embraced by the network operators, making it a dominant mobile access technology in recent times. According to an estimate by Ericsson Mobility Report, June 2017, 4G/LTE is projected to reach 5 billion subscriptions by the end of 2022 [1]. The reason for 4G/LTE success lies in its performance goals of providing lower latencies and higher bandwidth capabilities than its predecessors, 2G/3G, which makes it a preferred choice for the network operators.

Another essential ingredient to the success of 4G/LTE is the strengthening of its authentication and encryption. The previous 2G/3G mobile systems were vulnerable to various network attacks. The 2G lacked mutual authentication, which allowed the adversaries to set up fake base stations. The 3G systems introduced authentication and the use of cryptographic algorithms, but the usage of ciphering was still limited. 4G/LTE not only further solidified the security but also introduced it in more scenarios, making 4G/LTE more secure. However, it was found out that 4G/LTE is still prone to network attacks [2][3][4]. Known attacks such as "IMSI-Catching" are still possible, although there have been multiple studies conducted to defeat the attack[5]. The network operators, unfortunately, have to be more vigilant, as they do not have an automated security solution at hand. Thus, these security issues not only inflate the cost of operating 4G/LTE networks, but also make them more difficult to manage.

2 Related Work

This section classifies some attacks that still prevail in 4G/LTE networks and need to be handled.

Attacks against control procedures. Control procedures are an essential part of 4G/LTE networks. They are responsible for performing multiple tasks ranging from service establishment, authentication and session/bearer creation. Most important control procedures are attach, detach and paging procedures. ToRPEDO[6] located a vulnerability in paging protocol and demonstrated that since paging requests only arrive in a specific time period (called paging occasions), it is easy to exploit the fixed occasions. They showed that this exploit can result in the device's persistent identity(IMSI) being revealed. Another system, LTEInspector[7], found through formal analysis ten new attacks against attach, detach and paging procedures. The most notable attack they discussed is the *authentication relay attack*, that allows the attacker to modify the location of a user without owning their credentials.

Attacks against pseudonyms. Pseudonyms(temporary and randomized identifiers) such as TMSI and GUTI are used to hide the actual identity (IMSI) of a subscriber. According to 3GPP, it is essential to hide IMSI because an attacker can take advantage of it to locate a user. However, many network operators use predictable temporary identifiers, which may allow an adversary to link the temporary identifier to IMSI. [8] showed that in 4G/LTE, GUTI can only be changed by reallocation procedure, but it is not enough to change it – An unpredictable and frequently changing GUTI is required. They conducted a study to find out that out of 11 countries, 28 carriers were using insecure temporary identifiers. [9] found a similar flaw in using temporary identifiers. They also mentioned that network operators reuse the temporary identifiers frequently, which defeats the purpose of using them.

Rogue eNodeBs. 4G/LTE introduced an authentication protocol known as AKA protocol. It allows a user to make sure that the other entity it is communicating to is genuine. However, [10] showed that some procedures message such as *Service Reject / Attach Reject* are transferred without mutual authentication. This flaw allows the attacker to place a rouge eNodeB that can decode messages and dictate the user. Such privilege lets the rogue eNodeB downgrade or even deny services to the users.

3 Proposed Approach

It has been established from the existing literature that every known solution caters to a specific vulnerability. That is, the researchers first model the 4G/LTE protocols, identify problematic interactions and propose fixes that are specific to that vulnerability. Therefore, it is impractical to enumerate every potential vulnerability in 4G/LTE specifications given the sheer number of interactions in 4G/LTE protocols. Keeping in view the limitations of existing approaches, we are going to develop a distributed anomaly detection system, that leverages the power of Machine Learning to learn about existing as well as zero-day attacks. It will not only detect the attacks, but it will also take appropriate measures to quarantine those attacks.

Fundamentally, we will develop our module as a sub-component for Mobility Management Entity (MME). The control-traffic of every MME will be used for training and inference. In the first step, every sub-component will perform the local computation to understand the patterns local to that component. Then, in the second step, every component will send the summary of the local computation to a central server. Central Server will be responsible for aggregating the data from all components, finding potential vulnerabilities in the combined global state and reporting the summary to the operator.

4 Timeline

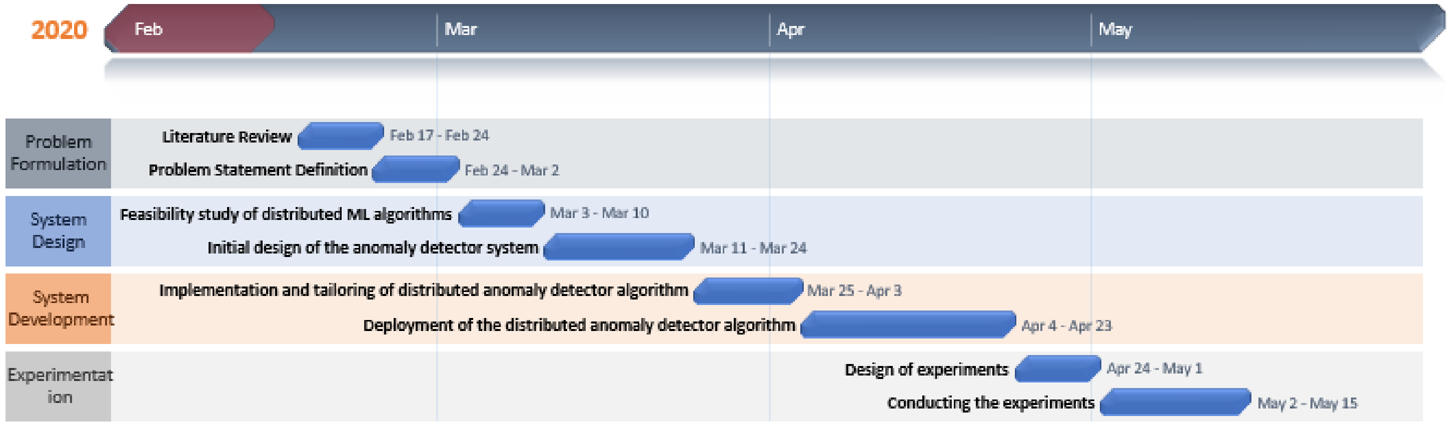

Figure 1: Timeline of the project

References

[1] Erricsson Mobility Report, June 2017, https://www.ericsson.com/49de56/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf. [Online; Accessed at 14/02/2020]

[2] Li, C. Y., Tu, G. H., Peng, C., Yuan, Z., Li, Y., Lu, S., Wang, X. (2015, October). Insecurity of voice solution volte in lte mobile networks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 316-327).

[3] Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., ... Kim, Y. (2015, October). Breaking and fixing volte: Exploiting hidden data channels and mis-implementations. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 328-339).

[4] Rupprecht, D., Kohls, K., Holz, T., Pöpper, C. (2019, May). Breaking LTE on layer two. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 1121-1136). IEEE.

[5] Van Den Broek, F., Verdult, R., de Ruiter, J. (2015, October). Defeating IMSI catchers. In Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (pp. 340-351).

[6] Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., Bertino, E. (2019, February). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In NDSS.

[7] Hussain, S., Chowdhury, O., Mehnaz, S., Bertino, E. (2018, February). LTEInspector: A systematic approach for adversarial testing of 4G LTE. In Network and Distributed Systems Security (NDSS) Symposium 2018.

[8] Hong, B., Bae, S., Kim, Y. (2018, February). GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In NDSS.

[9] Arapinis, M., Mancini, L. I., Ritter, E., Ryan, M. (2014, February). Privacy through Pseudonymity in Mobile Telephony Systems. In NDSS.

[10] Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J. P. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:1510.07563.