Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Cellular Threat Detection

Ανδρέας Ρουσιάς

Επιβλέπων Καθηγητής

Δρ. Αδαμαντίνη Περατικού

Μάιος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Cellular Threat Detection

Ανδρέας Ρουσιάς

Επιβλέπων Καθηγητής

Δρ. Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2022

Summary

Cellular Networks have become probably the most used types of networks, due to the explosion in the number of their users. Cellular devices nowadays can be found everywhere. The introduction and rise of the Internet of Things (IoT), further increases the need for cellular access. This high usage of cellular networks makes them a precious target for malicious entities.

The purpose of this thesis is to present ways that these malicious entities use to attack cellular networks, and thus compromise their users' security and privacy. Based on these attack vectors, possible detection methods are presented. The main objective, however, is to present and implement a detection method, namely a sensor-based one.

Throughout this thesis, the three most used cellular technologies of the past years, namely GSM (2G), UMTS (3G) and LTE (4G), and their main characteristics are described. After a brief presentation of these technologies, some of the known vulnerabilities and attacks that exploit them are described.

Considering these vulnerabilities and attacks, possible detection methods are presented. Subsequently, a complete detection method is proposed, using a cellular threat detection sensor (CTDsensor) that collects cellular logs, analyzes them and generated attack alerts when it detects a cell with an unusually high signal power. The alerts generated are then transmitted to a Security Operations Center, where they are stored, collectively analyzed, and displayed, providing a more complete overview of the cellular landscape.

Chapter 1

Introduction

In an era where the usage of computing devices is characterized by mobilization, cellular networks play a crucial role in sustaining the ever-growing digitization and interconnection of society. The number of cellular devices has risen drastically in the last ten years. According to [1], in 1993 there were around 34 million cellular subscriptions around the world, while in 2012, that number jumped to around 6.261 billion. In the time of this writing (2021-2022), the number of cellular subscriptions has jumped to more than 8.6 billion and has exceeded the number of the world's population.

The appearance and now advance of the Internet of Things, also played a crucial role in the increase of cellular usage. More everyday devices require connection to the Internet and a large number of them are located in remote areas and in non-fixed locations, thus requiring cellular access in order to operate. It is therefore clear that, cellular networks play an integral role in today's society, even if most people take them for granted.

It can be argued that the population's unlimited access to the Internet through cellular networks is the main factor for the evolution of modern society. With all of the above in mind, one can understand the high value of the information exchanged through mobile networks. Having such a large number of users, cellular networks pose one of the main targets for malicious entities that seek a high value "payout". By successfully attacking cellular networks, attackers can gain an eye in their users' activities and compromise their security and privacy.

Even more, in high value/high security areas, mobile devices are extremely vulnerable to attacks as they pose an even greater and more worthy target. Such areas can be anywhere, from government buildings, to airports, ports, and even military sites. It is therefore clear that, especially in those areas, measures should be taken to elevate their security.

Based on the above, some questions arise, regarding the security of cellular networks:

- What cellular networks are essentially and how do attackers act when trying to compromise them?
- What are the main vulnerabilities of cellular networks, and how do attackers exploit them?
- How do we prevent such attacks?

1.1 Scope

As the first step to increasing the security, detection is key. The main objective of this thesis is to present a method for detecting cellular threats, specifically in high security areas. Such a cellular threat detection method will be implemented for the three previous generations of cellular technologies, namely GSM, UMTS and LTE, as they are still the most prominent, with 5G being now on the rise. Most security aspects touch upon these generations.

During this thesis, the three generations of technologies will be described. Their architecture, components and basic procedures will be explained, in order to be able to more deeply understand what makes them vulnerable to attacks. Their most prominent vulnerabilities will then be described, following with the main ways attackers exploit them and attack cellular networks.

Based on the attack vectors that attackers use, several detection methods will be presented. Lastly, a sensor-based detection method will be implemented using one of these methods, with the goal of transmitting alerts of detection to a SOC. The main goal of

this thesis is therefore to provide and propose a detection solution that will give a security overview of the cellular landscape.

1.2 Basic Research Questions

- How are cellular networks structured and what components comprise them?
- What are the most important vulnerabilities of cellular networks and what are the main causes for the existence?
- How do attackers attack cellular networks and compromise their users' security and privacy? What attack vectors do they leverage?
- How can cellular threats be detected?

1.3 Importance of Research

The high security requirements of cellular communication, combined with the fact that not many actions have been taken to elevate their security, increases the need for a security solution. More research is needed into the security and privacy aspects of mobile networks, to come up with solutions that accomplish such purposes. A collective approach in the security of high-value areas, like the usage of a (multi)sensor-based detection method and a SOC, provides a high-level overview of the cellular security landscape and ensures that mobile users enjoy a threat-free environment.

Chapter 2

Methodology

The core purpose of this thesis is to provide a proof of concept for the detection of attacks in cellular networks based on the prominent vulnerabilities of the different generations of cellular technologies. Based on these vulnerabilities, as well as the ways that attackers exploit them, we derive the ways that attacks can be detected.

This thesis begins by researching the three most prominent cellular technologies of three different generations, namely GSM (2G), UMTS (3G) and LTE (4G). It should be noted that, these technologies are widely used in the European continent (among others) even today, after the 5G appearance. Analyzing the inter-workings, the vulnerabilities, and possible attacks on 5G networks is out of the scope of this thesis. Explaining the structure and functionality of these technologies is essential to understanding their usage and limitations, their vulnerabilities, and the ways that attackers exploit them in order to breach their and their users' security and privacy.

Following on, to understand the methods of detection more deeply (which is the main objective of this thesis), a list of common vulnerabilities and attacks on cellular networks and how they affect their operation is described. It is common practice among security researchers and practitioners, to first understand their adversaries' tactics and techniques to find solutions and implement security measures to detect, mitigate and stop attacks in their tracks.

Later on, research will be conducted on existing cellular attacks' detection methods, derived directly from the usual attacks against cellular networks and their users. This research will be useful as it will provide insights for the design of a detection solution that is tailored to the needs and goals of this thesis. More possible detection solutions will also be considered, based on the implementation plan. An implementation plan that will be largely based on a threat model. Thus, a threat model will be considered and determined.

The main goals of the implementation will be a detection solution that will be connected to a Security Operations Center (SOC) where alerts will be collected from several different sensors. This collective approach for the detection strives to monitor high risk and high value areas and alert on possible attacks. In order to generate alerts, a detection logic must be considered, and different metrics must be taken into account.

After implementing the attack detection solution, tests will be conducted, in order to determine whether alerts are generated on successful triggers and then, transmitted to the SOC. As transmission of any signals in a public area is forbidden, a test method will be determined, possibly using specific enclosed locations and a controlled environment. Lastly, some conclusions will be derived, and suggestions will be made for further upgrades and/or improvements. The basic structure of the methodology is described by the diagram of Figure 1.

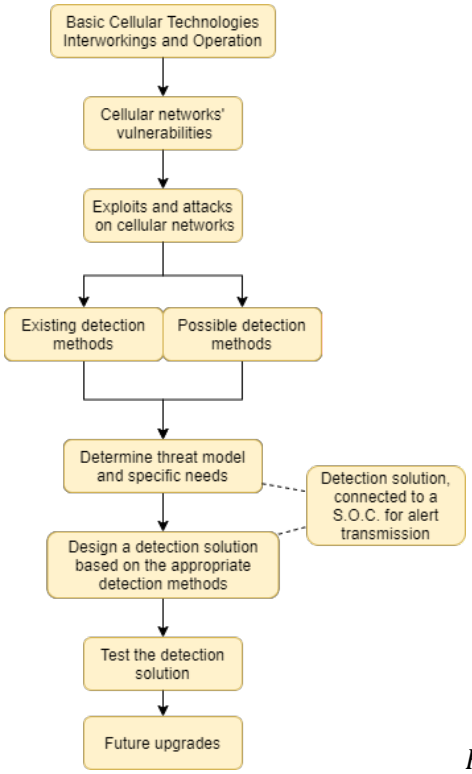

Figure 1: Abstract methodology diagram.