Summer Internship Report

Submitted

by

Chandrahas Maddineni – AP19110010536

Department of Computer Science and Engineering

SRM University-AP, Andhra Pradesh, India

July - 2021

DATA SHEET

Roll Number	:	AP19110010536
Name of the student	:	Chandrahas Maddineni
Branch & Section	:	CSE F
Batch	:	2019-2023
Type of internship	:	Project with Faculty
Company Name/Institute Name	:	Project with Faculty
Company/Institute Website	:	Project with Faculty
Start Date (MM/DD/YYYY)	:	02-06-2021
End Date (MM/DD/YYYY)	:	18-07-2021
Duration (No. of days)	:	47
Status of the internship	:	Completed
Name of internship mentor (SRM Faculty)	:	Dr. Shubham Gupta
Signature of the student	:	Chandrahas

ACKNOWLEDGEMENT

The internship opportunity I had with SRM Faculty: Dr. Shubham Gupta was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it.

Bearing in mind previous I am using this opportunity to express my deepest gratitude and special thanks to the Dr. Shubham Gupta who in spite of being extraordinarily busy with his duties, took time out to hear, guide and keep me on the correct path and allowing me to carry out our project and for taking part in useful decision & giving necessary advices and guidance.

I perceive as this opportunity as a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives. Hope to continue cooperation with all of you in the future,
Sincerely,

Name: Chandrahas Maddineni

Date: 18-07-2021

TABLE OF CONTENTS

I. INTRODUCTION

A cellular network or mobile network is a communication network where the link to and from end nodes is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver. We also use telecommunication network for sharing information via internet. A telecommunications network is a group of nodes interconnected by telecommunications links that are used to exchange messages between the nodes. Cellular networks are increasingly used for more than voice calls. Improved handsets and the networks' increased data transfer speeds have resulted in the development in a wide range of devices. Without this we cannot communicate with each other wirelessly [1].

1.1. 3G Network:

3G is the third generation of wireless mobile telecommunications technology. It is the upgrade for 2.5G GPRS (General Packet Radio Service) and 2.75G EDGE networks(Here EDGE means Enhanced Data Rates for GSM Evolution (sometimes also called EGPRS)), for faster data transfer.

1.1.1 Security architecture:

3G Network uses Universal Mobile Telecommunications System (UMTS) Architecture [1]. The 3G security architecture provides features such as authentication, confidentiality, integrity etc. Also, the WAP (Wireless Application Protocol) protocol makes use of network security layers such as TLS/WTLS/SSL to provide a secure path for HTTP communication.

1.1.2 Vulnerabilities:

In 3G Network due to vulnerabilities in the Signalling System 7 (SS7) protocol, hackers can potentially track a customer's every move, listen in on calls, intercept SMS messages, initiate fraud can even reduce the signal strength or completely strip them of service [2].

1.2 4G Network

4G is the fourth generation of broadband cellular network technology, succeeding 3G. A 4G system must provide capabilities defined by International Telecommunication Union (ITU) in International Mobile Telecommunications-Advanced (IMT-Advanced).

1.2.1 Security architecture:

4G uses the TCP/IP architecture as the network backbone with open interfaces, which makes it susceptible to various network security risks. The Long-term evolution (LTE) in the 4G system architecture is made up of an EPC (Evolved Packet Core) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). PKI (public key infrastructure) method of encryption is used for authentication and encryption of the data using digital certificates [3].

1.2.2 Vulnerabilities:

4G networks vulnerable to denial of service (DoS) attacks, subscriber tracking.[4] In this class of attacks, Once the device is on the fake tower, it's not connected to the real network, and the device is denied connectivity then the attacker can initiate up to three possible denials of service attacks on the target user equipment (UE). One of the attack is to force the target UE to use either 2G or 3G, even if there is 4G receptivity in the area. The aim of this form of attack is limitless. This kind of attack is to deny the target user equipment (UE) access to specific services, such as voice calls or internet access [5].

1.3 What is an IMSI Catcher?

IMSI Catchers act like false cell towers that trick the victim's device to connect to them. The communications (calls, text messages, Internet traffic, and more) are intercepted, then relayed to the target cell tower of the network carrier. To make matters worse, the victim is mostly unaware of what is happening. This type of hack is also known as a man-in-the-middle (MitM) attack [6].

1.3.1 **Types of Security Attacks by IMSI Catchers:**

There are four major types of security attacks done by IMSI Catcher. They are

1. **Communication Interception** –

   This is the most basic form of hacking performed today. The attackers simply "catch" the device's International Mobile Subscriber Identity (IMSI) in a classic case of digital identity theft. The next step is spoofing authentication, where the Stingray "convinces" the genuine mobile network that it's actually the targeted mobile phone for all communication purposes. This is done by the IMSI Catcher sending a Location Update Request to a legitimate cell tower and identifying itself with the stolen IMSI. Dealing with smartphone encryption security mechanisms is also not a big challenge due to the victim's phone "helping" with the requests.

2. **Location Tracking** –

   Often overlooked by security service providers, location tracking is becoming more and more common as it requires no cooperation from cell providers. For law enforcement authorities to track suspects or criminals they (usually) require a warrant and the cooperation of mobile service providers. IMSI Catchers can now be used to check for the presence of a victim or perpetrator in a specific area or even figure out their exact location without the need for operator cooperation.

3. **Denial of Service (DoS)** –

   Cell network denial of service is executed by connecting the device to the fake cell tower. Once the device is on the fake tower, it's not connected to the real network, and the device is denied connectivity. Only if the attacker chooses, then the device is connected to the network through the attacker's system (aka Man-in-the-Middle).

4. **Man in the Middle (MitM)** –

   A MitM attack consists of an actor intercepting communication between one device to another, for example an endpoint device (cell phone or tablet) communicating with a base station or AP.

1.4 How does this IMSI catcher work?

This cybercriminal activity is made possible due to a loophole in the GSM protocol. Mobile phones are constantly looking for the tower with the strongest signal to provide the best reception, which is usually the nearest one. It might, however, not be a genuine mobile provider tower [6].

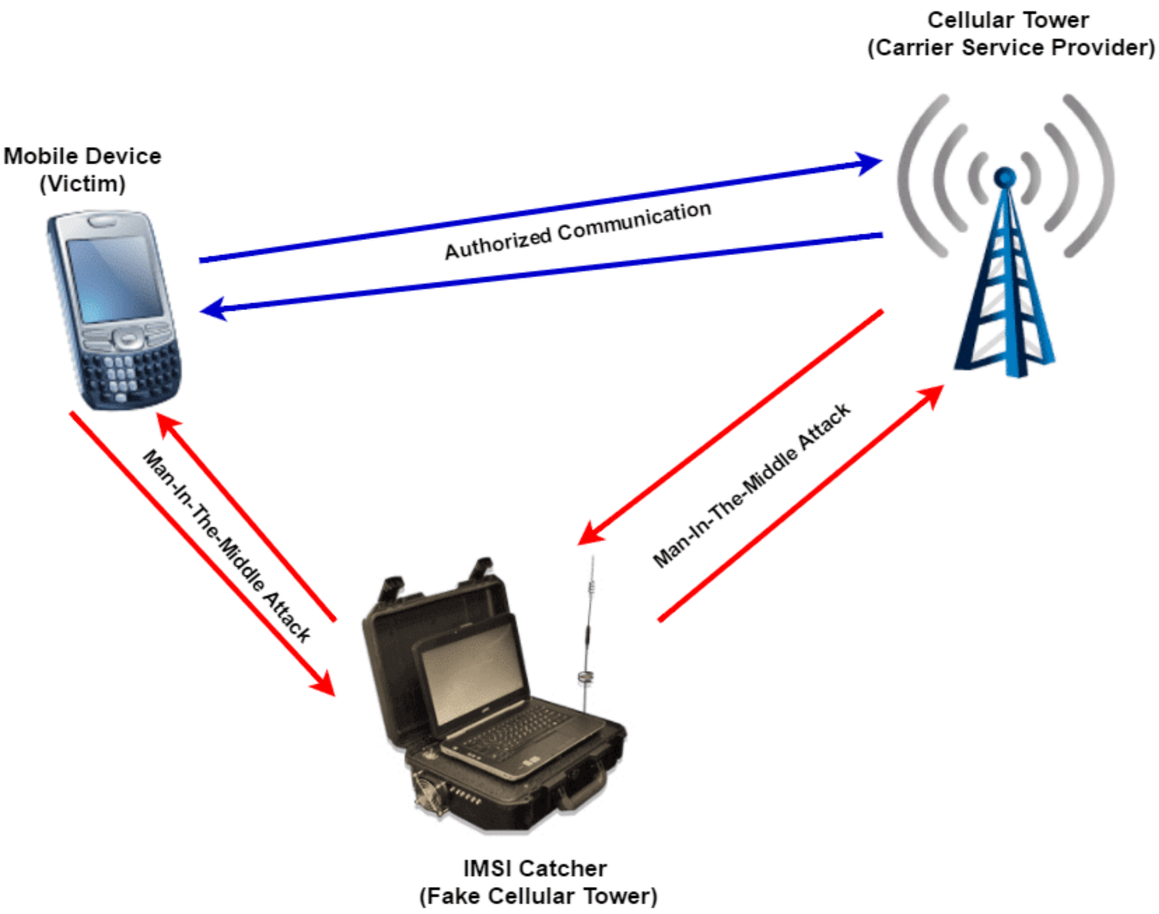

Figure 1 – Working of IMSI Catcher

When a device connects to a cell tower, it authenticates to it via its International Mobile Subscriber Identity (IMSI). IMSI is a unique identifier linked to your SIM card and is one of the pieces of data used to authenticate your device to the mobile network. The issue, however, is that the tower doesn’t have to authenticate back. This is why the IMSI Catcher is so effective. It simply pretends to be a cell tower near your phone, then seamlessly connects to it, and starts to harvest information. The simplistic nature of this mechanism is helping cybercriminals carry out their malicious acts with alarming ease. All they need is a laptop, some cheap hardware that is available on the net, and a few commands to initiate the hacking process in just a few minutes as shown in Figure in 1.

II. OBJECTIVE OF THE INTERNSHIP

The Objective of the Internship is to make an android app that can educate the people about the loopholes in network like 3G, 4G & 5G, ways to stop these attacks and to show the real-life demo of how an IMSI catcher work. We are planning to further develop this app, so that we can show the real-life demo of how an IMSI catcher work.

III. SKILLS ACQUIRED THROUGH THE INTERNSHIP

C language proficiency, Basic Android App Development, Cryptographic Protocols

IV. OVERVIEW OF THE PROJECT/WORK CARRIED OUT DURING INTERNSHIP

During this research we have researched about the loopholes in network like 3G, 4G & 5G, ways to stop these attacks and have gathered a lot of resources and made an android app. So that the people who installed the app can go through the resources that we have collected and understand the loopholes, different types of attacks and how to detect the IMSI Catchers. This app is only for the education purpose which contain multiple resources. We are planning to further develop this app, so that we can show the real-life demo of how an IMSI catcher work.

V. RESULTS/OUTPUT

Finally, we have made a simple basic Android App for the education purpose on loopholes in network like 3G, 4G & 5G and different types of attacks. By using this app people can learn how an IMSI catcher works, Different types of attacks, ways to find an IMSI Catcher & more.

VI. CONCLUSION

After referring to many research papers, articles and surveys done my many other researchers, I have come to a conclusion that there are some loopholes which cannot be corrected by the user side but can be corrected by the telecommunication authority with some effort. There are a lot of ways to identify fake cell tower (IMSI Catcher) but there are not any useful ways to avoid them. During this research we have made an android app for the education purpose about these IMSI Catchers. We are planning to further develop this app, so that we can show the real-life demo of how an IMSI catcher work.

VII. REFERENCES

1. Security In Wireless Cellular Networks. (2018). Www1.Cse.Wustl.Edu. https://www1.cse.wustl.edu/%7Ejain/cse574-06/ftp/cellular_security/#:%7E:text=2.3%203G%20%2D%20UMTS%20Architecture

2. Forrester, N. (2020, February 18). 2G and 3G networks are “open doors” for cyber-attacks. 2G and 3G Networks Are “open Doors” for Cyber Attacks. https://securitybrief.com.au/story/2g-and-3g-networks-are-open-doors-for-cyber-attacks#:%7E:text=Due%20to%20vulnerabilities%20in%20the,even%20strip%20them%20of%20service.&text=%E2%80%9CMessages%2C%20calls%20and%20your%20location,be%20tracked%20without%20your%20knowledge.

3. Distributed security architecture for authentication in 4G networks. (2016, October 1). IEEE Conference Publication, IEEE Xplore. https://ieeexplore.ieee.org/document/7887967/#:%7E:text=4G%20uses%20the%20TCP%2FIP,security%20risks%20in%204G%20network

4. Osborne, C. (2020, March 26). 4G networks vulnerable to denial-of-service attacks, subscriber tracking. ZDNet. https://www.zdnet.com/article/100-of-4g-networks-vulnerable-to-denial-of-service-attacks-researchers-claim/

5. Davis, B. R. (2020, June 22). 3 Models of Practical Attacks On 4G/LTE Devices - Brian Russel Davis. Medium. https://medium.com/@brianrusseldavis/3-models-of-practical-attacks-on-4g-lte-devices-9a7de16e2fe2

6. Top 7 IMSI Catcher Detection Solutions for 2020. First Point. (2021, May 19). https://www.firstpoint-mg.com/blog/top-7-imsi-catcher-detection-solutions-2020/