Wi-Fi-based IMSI Catcher

Bhanu Praharsha Rapelly¹, Shruti Bhargava Choubey²

Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, 501301, Telangana, India.

Abstract— The integration of Wi-Fi into smartphones and its ease of access has proven to be much use for its users on the global level. Such technology greatly influencing the world is generally well secured if not for the wildest minds trying to find some vulnerabilities in it. And thanks to them the loopholes are closed. The ban on IMSI catchers was a big blow to the attackers which made them investigate for a much wider network and low-cost alternative which is readily available – Wi-Fi. The properties like automatic Wi-Fi connections and Wi-Fi calling and its protocols are the reason attackers are exploiting this technology. Exploiting these vulnerabilities lead to man-in-the-middle (MITM) attacks.

Keywords—IMSI, IMSI catcher, MITM, vulnerabilities, Wi-Fi, Wi-Fi calling.

I. INTRODUCTION

IMSI or International Mobile Subscriber Identity is a unique identification number used to identify the subscriber of a particular cellular network. An IMSI catcher acts a fake base station which will route the data to a switching station. It acts as a middle man. The same can be implemented using a Wi-Fi. A rogue access point or a rouge base station is set up which performs the same operations as the Wi-Fi only that the user's data is exposed and can be stolen. The automatic Wi-Fi connection and Wi-Fi calling are based on EOP protocol. Because of the robust structuring of the lower layers of the communication model, it has become a burden to OS makers, mobile operators and trade groups to secure the loopholes. Evolution of the communication system in the coming years may include the ways to avoid being “stalked digitally” through software and hardware advances in technology.

II. IMSI

The international mobile subscriber identity or IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks [1]. An IMSI is usually presented as a 15-digit number but can be shorter. The first three-digit numbers are the MCC (mobile country code). The next three being the MNC (mobile network code). The remaining digits are the MSIN (mobile subscription identification number). An example is presented as a picture below.

![IMSI Example](image)

III. IMSI CATCHER

A sting-ray or an IMSI catcher is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users [2]. It essentially acts as a fake mobile base station between the user’s mobile phone and the original towers of the service provider. An IMSI catcher has an SDR (software defined radio) as its main component which enables the device to talk to the mobile handsets via cellular protocols.

An IMSI catcher masks itself as a base station and records the IMSI numbers of all the mobiles in the area as they try to connect to it. It forces the mobile to downgrade its connection to use no call encryption, making it easier to intercept and convert the data into audio. It is possible because there is no mutual authentication required for establishing a connection in lower generations like 2G. Because of the downgrade of its connections like 3G or LTE to 2G network services increases data consumption rate and puts a strain on the network. This causes jamming of the network service and lead to disruption of the service.

And because of the largeness in size of the data logs collected by the sting-ray, it becomes hard to search for the required and relevant data needed for the work to be done. It also requires a large amount of storage space to store the data collected. This can also be considered as one of the reasons attacks directed through Wi-Fi increased.
IV. PROTECTION AGAINST IMSI CATCHERS

Protecting oneself against this kind of attack need investment of time, money and thinking. Awareness about this kind of attack is a necessity and use of Wi-Fi platform solves it to some extent. The availability of special non-rooted mobile phones with advanced security features to protect from these attacks is helpful but costs a tad more money.

V. WI-FI BASED IMSI CATCHER

A Wi-Fi based IMSI catcher uses an open public Wi-Fi hotspot or a network service providers hotspot as a point of convergence of the data collection. This attack is target specified and can be applied to all mobile users within the range of the Wi-Fi hotspot. A Wi-Fi based IMSI catcher relies on the property – automatic Wi-Fi connection. The automatic Wi-Fi connection is a feature of the EAPOL (Extensible authentication protocol over LAN). The attacks are based on two EAPs:

A. EAP-SIM

EAP Subscriber Identity Module is used for authentication and session key distribution using the subscriber identity module (SIM) from the Global System for Mobile Communication (GSM) [3].

B. EAP-AKA

The EAP Authentication and Key Agreement protocol is a mechanism for authentication and session key distribution using the UMTS (Universal Mobile Telecommunications System) Subscriber Identity Module (USIM) [3]. The exchanges using this protocol are encrypted, but are not protected by a certificate, which means they are exposed to man-in-the-middle attacks that could recover the IMSI number [4].

VI. ROGUE ACCESS POINT

A Rogue Access Point is a wireless access point installed on a wired network without authorization form the network administrator [3].

Rogue access points with the same name as genuine devices are assumed to be a part of the network. Phones will automatically try to connect to it.

The attack work like this: the device tries to connect to the Wi-Fi network, and it is asked for its IMSI number so the wireless operator can check that the subscriber is authorized to access the service. The handset duly hands over the details [6]. But if the operator is not a mobile service provider the identity is compromised.

The IMSI is revealed during the handshake and during the early stages of the conversation, it is not encrypted [7].

VII. SOLUTION

OS makers and operators have acknowledged the problem, but there’s no easy way to fix it. There are EAP authentication methods that work over Transport Layer Security and are encrypted, but they need to be supported in both mobile OSes and operators’ systems. Deploying certificate-based infrastructure requires investments and is harder to maintain [8].

So far, the only company to take action is Apple. They have added “conservative” peer support for the Auto Wi-Fi authentication in iOS 10. In this mode, the device will only respond to requests for permanent identity when no pseudonym identity is available [8].

Other ways include using 4G LTE services for communications and manually connecting/disconnecting to/from Wi-Fi hotspots in a public area.

VIII. CONCLUSION

The way attackers using the vulnerabilities is evolving continuously. We cannot afford to fall behind. It is important to be aware of each of the attack we and our mobile devices area vulnerable to, and what steps we must take to defend against it. There are loopholes everywhere. It is just that we do not see them. Keeping an eye out for those loopholes is a good way to stop these attacks. Because any technology we use is not perfect, we must be able to support changes in it to make our lives secure.

REFERENCES