Invisible Dangers: To Understand the Security Posture of Wireless Networks Around Us


Lydia Fertil & Dr. Shuyuan Metcalfe
College of Communications and Information

Introduction

Wireless networks have become an important aspect of cyber infrastructure that impacts everyone's life. As users interact with wireless networks at home and work they have realized its efficiency. Thus, users are more inclined to join unsecured wireless networks on the go or while in a new location where they do not hold the information to join a secure wireless network.

Unfortunately, this has led to bad actors setting up rouge access points to steal online users' data. This is known as the **Evil Twin Attack** (**ETA**). An Evil Twin attack is when an attacker acquires the credentials of a legitimate access point to gain entry to a user's sensitive information by impersonating a legitimate access point. Wireless traffic and data traveling in the air are invisible; this invisible danger is not observable by the naked eye. The **goals** of the research are:

1) ***to conduct wireless network forensics*** and
2) ***to learn the behavioral differences among access points to identify rogue access points***.

Methods

Data was captured and compared between on campus and off campus traffic. The on-campus location was outside of the library and the off-campus location was an apartment complex.

- **Wireshark** was utilized to capture packets that contained traffic data with the aim of discovering network anomalies. The packets (.csv) were captured everyday at these locations for ten minutes, a timer was utilized during this process to ensure accuracy.
- **Excel** was used for a better analysis of the data. It was also used as a tool to clean the data. There were some inconsistencies throughout the data therefore they were erased to ensure accurate results. Despite the efficiency of Excel, the process of cleaning the data was tedious. Excel was also utilized to form the graphs related to the protocols.
- **Gephi** was also utilized as a graphs and networks visualizer. This system displayed all the data collected thus making it easier to identify the "bad data". After the packets were cleaned, Gephi was also used to visualize the network communication amongst the traffic data. This was done by downloading the Excel files (.xls) and saving them to a computer. The graphs were used for better analysis of the data.

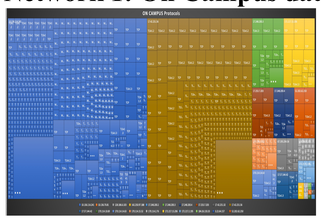
Discussion

The findings show that the traffic patterns between on-campus and off-campus are drastically different. Gephi reveals and visualizes the network diagrams for the off-campus environment is more complicated than the on-campus environment. Although a rogue access point was not detected, this can be seen as unfortunate for the study; it is however encouraging because the data samples are drawn from a realistic environment.

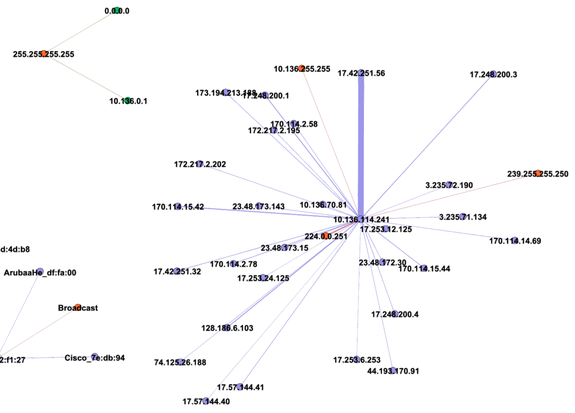
Based on the network 5-tuple information captured by Wireshark, the source and destination IP addresses and the protocols are essential to understand secure operational networks. We found a substantial number of unprotected hosts based on source and destination IP addresses. For instance, those hosts that utilize port 80 tend to be unprotected and those that utilize 443 are SSL-enabled secured traffic. We also found that DNS uses port 53. DNS is a protocol that is not encrypted and travels over the internet in plaintext. This prompts us to caution the possibility for a man-in-the-middle attack, which is that bad actors could intercept, and view packets transferred between the websites and the device.

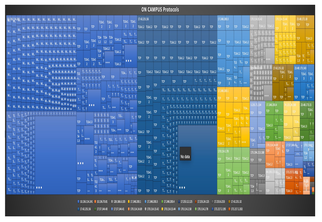
Analysis & Results

Network 1: On Campus data

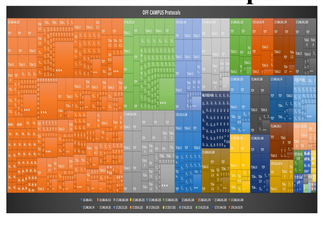


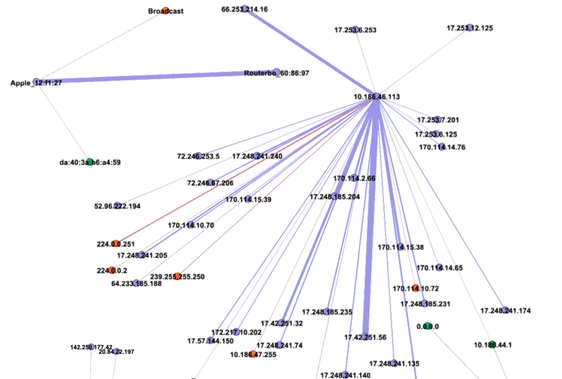
Wireless Network Visualization

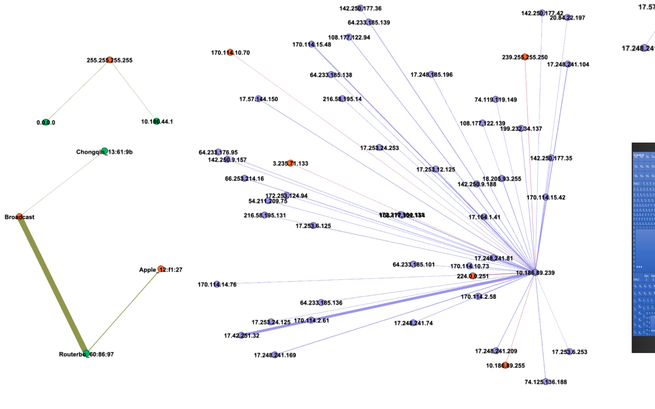


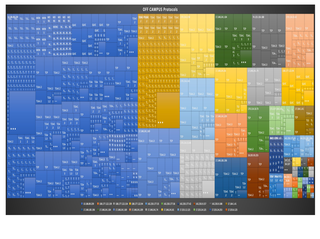


Network 2: Off Campus data









Limitations & Future Work

- As we have successfully achieved the goal of better understanding the Wireless Network, there is still work to be done. The reason that our current investigation did not find any Evil Twins may be caused by the limited research instruments, techniques, tools and methods adopted. The next steps will include a more in-depth literature review into advanced research work and articles. We anticipate that conducting a research experiment by setting up a rogue access point prototype. The Evil Twin research experiment will allow us to study and compare the different behavioral patterns between the legitimate vs. rogue access points in detail as well as understanding its movement.
- It's likely that more understanding of the wireless signal strengths and frequency can help identify and analyze the wireless environment. We will then be able to make more sense of the visual representations of the connections.
- The on-campus network as stated in the result is easier to comprehend. We can continue studying the off-campus environment and the role of the router within the wireless ecosystem.

Conclusions

The Evil Twin Attack is a serious threat to cyber security. The Evil Twin Attack consists of a bad actor mimicking a legitimate network. Today there is not a method that protects the general public from these attacks. The Evil Twin is not only dangerous due to its purpose of stealing personal information but the simple way of making it (smartphone). The Evil Twin Attack is not the only cybersecurity threat out there. The Man-in-the-middle (MITM) consist of a perpetrator eavesdropping between a user and an application. There are a plethora of other cyber security threat.

References

1. Asaduzzaman, M., Majib, M.S., & Rahman, M.M. (2020). Wi-Fi frame classification and feature selection analysis in detecting evil twin attack. In Proceedings of 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh.

2. Tchakounte, Franklin & Nakoe, Michael & Yenke, Blaise & Udagepola, Kalum. (2019). Recognizing illegitimate access points based on static features: A case study in a campus Wifi network. International Journal of Cyber-Security and Digital Forensics, 8(4), 279-291.

3. Benchikha, Nadia & Krim, Mohamed & Zeraoulia, Khaled & Benzaid, Chafika. (2016). IWNetFAF: An integrated wireless network forensic analysis framework. In Proceedings of 2016 Cybersecurity and Cyberforensics Conference (CCC).

Acknowledgements

I Would like to thank my research mentor Dr. Metcalfe for working with me on this project and exposing me to a new world of research and networks. In addition, I am thankful to The Undergraduate Research Opportunity Program for accepting me into this wonderful program at Florid State University. My Undergraduate Research mentors have guided me in this process and aided in any way they can.