Literature Review: Security of public Wi-Fi in New Zealand

Prepared by: Anastasiia Tiurina

School of Innovation, Design and Technology Whitireia

IT8x01 Research in IT

Supervisor: Dr. Marta Vos

Introduction

The matter of cyber security is a multifaceted question because it comprises technological, social and ethical aspects. The reason for this is that cyberspace has intertwined with other spheres of human life, and after the global pandemic – even more so (Veroni et al., 2022). The amount of data that is stored online has grown in recent years as well as its value. Sensitive personal data, credit cards, confidential information of organisations – all of that is like forbidden fruit to cyber criminals. Technologies are developing at a fast pace, and cyber attack methods mirror this development (Dutta et al., 2021). Hence, that brings up the question: how secure are the services and devices that we use every day?

The question of security triggered the creation of many institutions, like the Escal Institute of Advanced Technologies, that provide training and certification in the field of cyber security. One of the directions in cyber security system is Offensive Security (OffSec), the main field of expertise of the OffSec is finding vulnerabilities though penetration testing or vulnerability assessment and reporting the finding to the organisations, the owner of the faulty system, so that it can fix the vulnerability before someone could exploit it. But unfortunately the domain of the Internet has grown so vast that many vulnerabilities stay unnoticed and people or organisations fall victims to the perpetrators. Vulnerability can be found on different levels of the global web, even when people simply access the Internet. When user needs Internet connection it will not take a long time for them to find public Wi-Fi (wireless network of IEEE 802.11 standard). Wi-Fi networks a considered as a vital service because it is a key element in business and everyday life and work: employees and digital nomads work remotely or in public libraries and co-workings – and the amount of Wi-Fi hotspots keeps growing (Veroni et al., 2022). But is public Wi-Fi secure?

The underlying idea of wireless network is transmission of information going through the air as radio waves which is its key feature but also the main drawback. With the knowledge of what frequencies and channels of the frequency are in use and possession of proper equipment it is possible to peek at the transferring message. However, the security protocols of Wi-Fi have evolved over the years, but so have the attack methods. Hence, one of the objectives of this work is to look into research of the vulnerabilities of modern wireless networks of 802.11 IEEE standards as well as guidelines from agencies, like the National Institute of Standards and Technology (NIST), on defense recommendations against perpetrators. But not every public facility follows the guidelines and this is why it is worth question to look into and test public Wi-Fi hotspots for vulnerabilities. However, it raises the questions of boundaries of penetration test execution and ethics (Happe & Cito, 2023).

Public Wi-Fi safety is a crucial subject to investigate because it can provide useful intel on potential actions to take in order to localise and decrease the amount of cybercrime cases. Another possible benefit is raising the cyber security awareness of people who use public Wi-Fi. Cyber security awareness is often addressed separately in articles and user best-practice guides from institutions like the European Cybercrime Centre (EC3) or companies like Kaspersky or NordVPN. Another point of view that is worth exploration is the user experience and behaviour of people in regards to usage of public Wi-Fi, because apart from technologies, the human factor contributes greatly to overall security. Existence of refined encryption methods does not mean that a manager of a public facility will choose to buy a modern router over the one that is cheaper but does not support the latest security protocols. Additionally, a user of the network might expose their personal data if they are not cautious while connecting to an unsecured network. It may not be the case that people follow the recommendations for security which will enrich the overall public Wi-Fi security outlook. More than that, digital literacy can differ depending on a country (Herbert et al., 2023) – some countries are more digitised than others and the attitude towards cyber security varies. Thus, for example The Australian Signals Directorate developed an Information Security Manual (ISM), the National Institute of Standards and Technology in the USA created cyber security standards – organizations and individuals can reference these documents to establish defense against cyber attacks. In presented work the main focus will be the situation in New Zealand. New Zealand has undertaken a rapid strategy in digitisation and addressed the problem of cyber security as well.

1. Security testing

The research piece, conducted by Happe and Cito (2023) explores the subtleties of security testing. In regards to current work the most valuable information is about Penetration Testing and Vulnerability Assessment. The main objective of Vulnerability Assessment is overall evaluation and providing summary of vulnerabilities. On the other hand, Penetration Testing delves deeper into the target system. Vulnerability Assessment usually precedes Penetration Testing. The main authors' goal of the uncover the specifics of ethical hacking through qualitative research.

2. Question of ethics

In their research Formosa et al. (2021) cover the theme of ethics in security testing. The point out that the question of ethics often gets left out of the scope of standards. Therefore, they have analysed major security testing standards and compiled their own framework based on five principles: beneficence, non-maleficence, autonomy, justice, and explicability in a cyber security context. Each principle maps to one or more guidelines in existing standards. Their framework is adjusted to penetration testing domain, although there is still a gap in regards to the case when company or organisation fails to fix the reported vulnerability. The actions of the tester depend on the context (Formosa et al., 2021).

3. Public Wi-Fi and vulnerabilities

The evaluation of security level in contemporary Wi-Fi networks first requires the understanding of vulnerabilities. Wireless Local Area Networks (WLANs) are considered less protected because transmissions can be intercepted or altered with relative ease. In order to monitor the traffic on wired network the attacker needs to physically access the system. On the other hand, for WLAN it is sufficient to be within the range of transmission signal.

As Patra and Mukherjee (2021) state in their work, the main vulnerabilities that Wi-Fi suffers from are: weak or non-existent authentication, default configurations and non-existent or old encryption methods, such as Wired Equivalent Privacy (WEP). A perpetrator can exploit these vulnerabilities and perform and attack where they gain access to data they are not supposed to. These attacks can be passive and active. The researchers claim, that passive attacks are more difficult to detect. During passive attack the content of messages sent over the network is not altered and attacker monitors the network traffic. Active attacks include gaining unauthorised access, Man in the Middle attack (MITM), Session Hijacking, Replay attack and others. These attacks, on the other hand, involve changing the information that gets transmitted or sabotaging user’s connection.

3.1 Passwords

Moving on to the question of passwords – Veroni et al. (2022) defined the features of public Wi-Fi passwords and whether the leaked dataset of public Wi-Fi passwords can be used to seed a password dictionary to crack the password of web accounts. Unlike private Wi-Fi passwords, the public Wi-Fi password is meant to be shared, so people use those pass-phrases that are easy to pronounce. The authors examined the collection of passwords from mapping applications (Wi-Fi finders) data leaks and from the data they discovered that most used password phrases are sequences of ascending, descending or repetitive numbers or strings.

Veroni et al. came up to the conclusion that dataset of public Wi-Fi passwords overlaps with web accounts passwords dataset and, as a result, can be leveraged in the Dictionary Attack, which means that the domain of public Wi-Fi security expands to web security (Veroni et al., 2022). They also suggest that the high popularity of a password means that it has been reused. Additionally, some percent of these pass-phrases have a length of less than 8, which implies that Wi-Fi setup uses WEP encryption. WEP was broken in 2001 and its disadvantages are described in “Weaknesses in the Key Scheduling Algorithm of RC”. Veroni et al. rightfully added that it is obsolete, however, it appears that it still remains widely in use.

3.2 Encryption

Wireless encryption methods ensure the confidentiality of the information that goes through the network.

3.2.1 WEP and WPA

As mentioned earlier, *WEP* is an old encryption method and among wireless encryption protocols it is the weakest one. It uses the Rivest Cipher 4 (RC4) and provides two levels of encryption using 64-bit or 128-bit key, however, the first 24 bits of the key-stream are initialisation vector (IV) and it is always the same. Therefore, with enough packets collected and the computational power of a modern devices it is easy to decipher the key and get access everything going back and forth over the Wi-Fi (Alvarez et al., 2022).

3.2.2 WPA

According to Alvarez et al. (2022),to solve the problem with WEP the *Wi-Fi Protected Access* (*WPA*) protocol was created. The main advantage over *WEP* was adding *Temporal Key Integrity Protocol* (*TKIP*) – hash IV that is longer than in *WEP* and it gets generated for each packet. However, as Carballal et al. (2022) mention, *WPA* encryption method still uses the same cipher (RC4) and it suffers from same problems as *WEP*.

3.2.3 WPA2

In their work Alvarez et al. (2022) say that in WPA2 the RC4 cipher was replaced by Advanced Encryption Standard (AES) and TKIP gave way to Counter Mode with Cipher Block Chaining (CCMP). Carballal et al. (2022) add that there was another important novelty in WPA2 – before a user allowed to connect to the network they have to go through four-way *handshake*. In their research work Carballal et al. made an attempt to brute force passwords from *handshakes* gathered from hotspots in a small area of Coruña city in Spain. They used the available password dictionaries, like RockYou and China Software Developer Network (CSDN) datasets for Brute Force attack. What they discovered was that many establishments in the area used unsafe passwords and concluded that password restrictions are necessary when setting up the Wi-Fi network.

3.3 Default configurations

As a part of the research Veroni et al. (2022) conducted a survey revealing that 30% of respondents do not change default configuration at all. The Dodson et al. (2021) highlight it as poorly configured network. The default configurations are not safe to use because it is provided in the installation manual with the router, therefore, easily accessed by the attacker (Patra & Mukherjee, 2021). This intel is reinforced by the point Choi et al. (2022) made in their work about “Evil Twin” attack. Since users’ devices might have a setting of automatic connection to the known network, there is a chance that they unknowingly connect to a rouge Wi-Fi access point which has the same Service Set Identifier (SSID), which leads to personal data exposure. Hence, this makes the suggestion from Patra and Mukherfee (2021) to change the SSID, turning off SSID broadcasting and changing preset password as countermeasures and a method of hardening the network totally justified.

The best way to harden the Wi-Fi network is to use strong encryption protocols, which are provided in latest 802.11 IEEE standards (Patra & Mukherjee, 2021).

However, it is worth pointing out, that among all the precaution measures Patra and Mukherfee (2021, p. 4153) highlighted education and training of users as “the first step in wireless network security”. This implies that public Wi-Fi security comprises the user’s side. In other words, the confidentiality of user’s data depends on their behavioural patterns while connected to public Wi-Fi.

4. User’s behaviour

A user’s perspective is thoroughly analysed in the research conducted in the USA by Choi et al. (2022), and according to it, people are prone to risky behaviour — such as checking their bank account and email — while connected to public access points. Generally, the question of convenience comes before security and the study gives the details about the reasons people do that while taking into account internal and external components of this decision. The study is based on four major theories: technology threat avoidance, prospect theory, risk taking behaviour and self-determination theory (SDT). The authors address the question of why people would still engage in careless actions on public wireless networks even when they are aware that it is dangerous. As an empirical side of the research 1313 participants were given a survey, which provided useful data to test Choi et al.s’ hypotheses. First, they found out that *avoidance motivation* has a negative correlation with intent to use public Wi-Fi and safeguard effectiveness. Safeguard effectiveness here is perceived efficiency of safeguard measures in preventing IT threats. Secondly, safeguard costs has a positive correlation with *avoidance motivation*, however, self-efficacy does not strongly affect it. Following that, risk averting tendency diminishes if the experience of use of public AP is positive and they most likely would use it in future. Demographics did not have strong affect on the findings, but education increases the *risk averting propensity*. Researchers also found similarities in impulsive decision-making patterns between smoking or alcohol consumption and the actions users take while connected to public wireless networks. Empirical data gave an insight on internal and external motivations. For instance, a user might connect to public Wi-Fi to fulfill their entertainment needs (gaming, media content etc.) which is internal motivation, and external inducements could include completing urgent and practical tasks, like emailing or the use of online services (taxi, automated bureaucracy tools etc.). The researchers concluded that public facilities ought to warn users of possible threats which might decrease the tendency for risky behaviour.

Another piece of research from the USA regarding public Wi-Fi usage patterns was carried out by Maimon et al. (2022), which raised the question of Situational Awareness (SA). They refer to SA as mindfulness of setting or context and capability to recognise potential threats. The researchers state that SA is a factor that defines the user’s actions performed on the Internet and each individual has a different level of SA. They had three main hypotheses:

- The higher SA a person possesses has a positive correlation with a possibility of using public Wi-Fi.
- The level of SA has a positive correlation with the chance that they use self-protective behaviour while using public Wi-Fi.
- Having more place managers encourages people into using self-protective behaviour while connected to public Wi-Fi.

For the first two points the authors conducted a 12-month survey on the university campus and they ended up with 749 participants. The survey confirmed that situationally aware individuals tend to

use self-protective behaviour. The study showed that among 749 respondents, 23% replied that they use public Wi-Fi and half of them check their personal accounts.
The researchers also conducted a field study by installing their own private wireless network without authentication at 109 public places for 16 months. The goal of the field research was to test the third hypothesis. As a result, the experiment showed that in crowded places or in the presence of an employee or a manager people are more inclined to use safeguard methods like hiding the screen of their device. The researchers concluded that raising SA is crucial to increase the percent of people who cautiously approach the use of public Wi-Fi.

These research works approach the problem of behavioural study from different perspectives and confirms that, apart from technologically poor network setup (such as using routers that support old encryption protocol), careless behaviour can make it easier for an attacker to get sensitive data.

5. Cybersecurity in New Zealand

New Zealand government provides a range of online resources when it comes to online services. One of them is Digital.govt.nz and it contains standards and guidance about Digital Service Design, which built upon certain principles that online services are recommended to follow. One of the principles is integration of security and privacy proportionate to risk from the outset and endorses to consider security matter when designing the service (Digital.govt.nz, 2019). Digital.govt.nz also provides NZ Information Security Manual (NZISM), however, it does not uncover the details about the setup and, again, provides recommendations but not standards that facility should comply with. There is no resource that addresses the question of actually checking the standard, like, NIST has Technical Guide to Information Security Testing and Assessment.

On the other hand, New Zealand's Computer Emergency Response Team (NZ CERT), which is a part of the National Cyber Security Centre (NCSC), conducts their own research and quarterly reports on cyber security insights gathering data from people across New Zealand. Thus, in the latest report people show high percent of awareness of threats and cyber crime, for example, 75% of respondents were of credit card credentials theft, 6% of participants experienced it themselves. However, there is still a room for improvement in domain of behavioural habits, for example, only 38% of survey-takers use password manager and 58% change default configurations on devices (NZ CERT, 2022). NZ CERT has a variety of guides. Some of them are Mitigating denial-of-service attacks, Hardening RDP and Cloud-based identity providers and authentication. One of the guides that can be related to public Wi-Fi are Default credentials guide and guide on Legacy Systems – this information can help to increase literacy in the domain of cyber security.

Conclusion

The problem of cyber security is ongoing one due to increasing amount of confidential information stored online. It important to conceal and prevent this information from exploitation in order to protect the privacy of people that in belongs to.
Wi-Fi network provides convenient way of using the Internet due to its feature of transmitting signals through radio waves but this advantage makes Wi-Fi network susceptible to various cyber attacks. Investigation of public Wi-Fi networks will provide an insight how public places design their Wi-Fi hotspot and how the regulations on the country influence the public cyber security awareness and literacy. In contemporary world, where online world is integrated with physical, the cost of data exposure can be high. Therefore, several questions need to be answered:
How secure is public Wi-Fi in large cities across New Zealand?
What to test the security of public Wi-Fi?
What to ensure that security test is performed ethically?
How secure is the users' behaviour while they use public Wi-Fi?
What regulations on the question of public Wi-Fi does the government have?
How effective these regualtions?

Glossary

Advanced Encryption Standard (AES): symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Brute Force attack: attack method of accessing device by attempting multiple combinations of passwords.

Dictionary Attack: cyber attack where an attacker uses a list of words and phrases from a dictionary, which is usually a leaked dataset.

Evil Twin attack: cyber attack where a hacker creates a false Wi-Fi network that mimics the name and settings of a legitimate public Wi-Fi hotspot.

Hardening: the process of enhancing the security of the system.

Initialisation vector: starting point for a cryptographic process, it consists of pseudorandom sequence of characters added to an encryption key

Man in the Middle attack: cyber attack where an attacker secretly intercepts and relays messages between sender and receiver.

Network traffic: data moving across a network at a given point in time

Replay attack: The attacker monitors transmissions (passive attack) and retransmits messages posing as the legitimate user.

Rivest Cipher 4 (RC4): is a stream cipher with a symmetric key algorithm.

Session Hijacking: the exploitation of a valid computer session or session key to gain unauthorized access to the system.

Wi-Fi: subset of WLAN, wireless network of IEEE 802.11 standard.

Wireless Local Area Networks: a group of wireless networking devices within a limited geographic area.

Reference list

Alvarez, L. A., B. Blancaflor, E., Dionisio, N. M., Acuna, G. E., Funilas, J. R., & Odicta, J. M. (2022). Penetration Test on Home Network Environments: A Cybersecurity Case Study. *Proceedings of the 8th International Conference on Management of E-Commerce and e-Government*, 100–104. https://doi.org/10.1145/3483816.3483834

Carballal, A., Galego-Carro, J. P., Rodriguez-Fernandez, N., & Fernandez-Lozano, C. (2022). Wi-Fi Handshake: Analysis of password patterns in Wi-Fi networks. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.1185

Choi, H. S., Carpenter, D., & Ko, M. S. (2022). Risk Taking Behaviors Using Public Wi-Fi^{TM}. *Information Systems Frontiers*, *24*(3), 965–982. https://doi.org/10.1007/s10796-021-10119-7

Digital.govt.nz. (2019, November 13). *Digital Service Design Standard*. New Zealand Digital Government. https://www.digital.govt.nz/standards-and-guidance/digital-service-design-standard/

Dodson, D., Montgomery, D., Polk, T., Ranganathan, M., Souppaya, M., Johnson, S., Kadam, A., Pratt, C., Thakore, D., Walker, M., Lear, E., Weis, B., Barker, W. C., Coclin, D., Hojjati, A., Wilson, C., Jones, T., Baykal, A., Cohen, D., … Singh, J. (2021). *Securing small-business and home internet of things (IoT) devices: Mitigating network-based attacks using manufacturer usage description (MUD)* (NIST SP 1800-15; p. NIST SP 1800-15). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.1800-15

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2021). *Cyber Security: Issues and current trends*. Springer. http://ebookcentral.proquest.com/lib/weltec/detail.action?docID=6796414

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*, 102382. https://doi.org/10.1016/j.cose.2021.102382

Happe, A., & Cito, J. (2023). Understanding Hackers’ Work: An Empirical Study of Offensive Security Practitioners. *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 1669–1680. https://doi.org/10.1145/3611643.3613900

Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, A., Acar, Y., & Dürmuth, M. (2023). A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–23. https://doi.org/10.1145/3544548.3581410

Maimon, D., Jordan, H. C., Scott, J., & Perkins, R. C. (2022). Situational awareness and public Wi-Fi users’ self-protective behaviors. *Security Journal*, *35*(1), 154–174. https://doi.org/10.1057/s41284-020-00270-2

NZ CERT. (2022). *Cyber security behavioural research*. https://www.cert.govt.nz/insights-and-research/cyber-security-behavioural-research/

Patra, J. P., & Mukherjee, S. (2021). Wireless Network Security Threats and Best Method to Warn. *Turkish Journal of Computer and Mathematics Education*, *12*(12), 4147–4155.

Veroni, E., Ntantogian, C., & Xenakis, C. (2022a). A large-scale analysis of Wi-Fi passwords. *Journal of Information Security and Applications*, *67*, 103190. https://doi.org/10.1016/j.jisa.2022.103190