THE UNIVERSITY of EDINBURGH
Edinburgh Law School

POSTGRADUATE LAW COURSE
ASSESSMENT COVER SHEET

Instructions for students:

Please ensure you have read the formatting and submission guidance available in the Programme Handbook. Unless stated otherwise in the course guidebook, the deadline for submission is 2pm.

1. Please complete the grey shaded areas below.

2. This coversheet must be attached as the first page of your work. No further information is required. Page 2 thereafter, will be the first page of your assessment.

3. When you save and upload your work for submission, you must use the naming convention as laid out in the Programme Handbook. Exam Numbers ensure student anonymity when marking; UUNs and other personal identifiers cannot be used. Failure to follow the naming convention could mean your assessment is not accepted, and penalties may occur.

EXAM NUMBER:	B205697
COURSE CODE:	LAWS11396
QUESTION NUMBER:	n/a
WORD COUNT:	2484

Security implications for users when using public WiFi: A briefing paper for the general public.

1. Introduction

Public WiFi hotspots are becoming very popular across the globe, as many forms of public transportation such as buses, subways and trains offer users a free method to browse the internet during their commutes(Qin et al., 2020). Research shows 46% of participants do not wait more than a few minutes before connecting to a complementary WiFi network ordered many vendors such as; airports, hotels or even shopping centres. However 60% of these participants are unaware of the security risks associated with doing so (Lotfy et al., 2021). Cybercriminals can then use this to their advantage, to intercept, control and manipulate a user's network requests, using a variety of different methods. Therefore, there is a need to educate the general public on the security implications regarding these platforms and how users should deploy mitigation methods to safeguard their privacy. This paper aims to brief the general public on security implications for users when using public WiFi and present the argument that public WiFi should not be used without the use of appropriate mitigation methods, such as a 'Virtual Private Network'.

The structure of this paper is as follows: Section 1 introduces the paper topic to the user. Section 2 provides background knowledge on public WiFi regarding motivation for how the platform is typically used. Section 3 examines three types of attacks which can occur when using public WiFi. Section 4 explores the use of a Virtual Private Network which are used to provide the user with protection from malicious attackers. Section 5 concludes the ideas presented in this paper.

2. Background Research

2.1 Mobile Data vs Public WiFi

A survey undertaken by Norton, the industry leading anti-virus company, found that the reason 49% of users would connect to public WiFi is due to them being unable to get a connection when using their 3G/4G mobile data (Al Neyadi et al., 2020). Individuals may use public WiFi networks to avoid depleting their monthly mobile data allowance. Sombatruang et al. (2019) claims that mobile data preservation is one of the key reasons users may opt to make use public WiFi networks, particularly when their remaining allowance reached around 30%. This was surprising as mobile data can be substantially faster than public WiFi networks, but is understandable from a user's point of view. Most mobile operators follow a usage-based billing policy not allowing data to roll-over each month, therefore users may wish to converse their data usage to avoid additional costs. A recent research survey found that 38% of users feel their monthly data allowance is not enough, in relation to the amount of money they are paying (Ming et al., 2017).

2.2 Who hosts Public WiFi?

Public WiFi networks can be hosted by a variety of different vendors as a 2014 industry report indicates 50% of the worldwide commercial WiFi hotspots are owned businesses such as airports, restaurants and hotels (Gabriel, 2014). Suggestions have also been made for businesses to monetize their approach to offering free WiFi This could be done via either paying for advertisement-free WiFi at the venue or by allowing users access to free WiFi hotpots and generate revenue from mandatory advertisements, which they must periodically complete to stay online. (Yu et al., 2017)

2.3 Tasks Undertaken on Public WiFi

Users of public WiFi can connect to the network for a various of different purposes and the nature of these purposes can determine which security implications they may be exposing themselves to. Maimon et al. (2017) performed an analysis of internet packets observed on 24 different public WiFi locations and associated the tasks undertaken by users with social media usage, checking email accounts and accessing their personal cloud server. Additionally, 54% of packets identified were associated with banking, despite previous requests by governmental agencies to not use a public WiFi network for banking purposes This interesting finding directly conflicts with previously presented claims as a research survey undertaken by Goldsborough (2015) indicates that it is not likely for users to perform banking on a public WiFi network. Performing an analysis of the research methods used, indicates the approach taken by Maimon et al. (2017) to be more reputable as it is more recent and accurate. This is because the experiment was conducted based on live data collected across multiple public WiFi-networks in comparison to a simple user survey undertaken by Goldsborough (2015). The two-year gap between experiments however could suggest that users are becoming less concerned with performing sensitive tasks on public WiFi networks and are thus creating a bigger attack vector for cybercriminals.

2.4 Decision to Use Public WiFi

This paper presents the idea that human behavioural factors can influence if a user would decide to use public WiFi or not, since it could affect an individual's decision making. Klasnja et al. (2009) examined the impact trust could play in this decision process and claimed users trusted the security measures on their device would protect them from any

harm when using a public WiFi network. However, Sombatruang and Sasse et al. (2016) critiqued this claim and stated that no evidence was provided to justify it. Additionally, these authors also identified a research gap which states that no evidence exists at all, regarding the decision process made by users when considering joining a public WiFi network.

Chiang and Tang (2022) undertook an attempt to fill this gap and came to the conclusion that the driving factor behind a user's decision is fear, indicating the more frightful a user is of an attack occurring, the less likely they would be to join a public WiFi network. Although no elaboration were made on this by them, an examination of previous research by Klasnja et al. (2009), justified their claim. The fear of identity theft or financial damage was previously identified as security concern, which can influence a user's decision to use a WiFi network.

3. Security Concerns when using Public WiFi

3.1 Rouge WiFi Networks

Meng et al. (2019) presents claims that it can be dangerously simple to deploy a rouge WiFi network in a public space, as it can be performed by someone using their mobile as a hot spot. The network could be designed to look appealing such as containing the word 'free' to entice users into connecting and traffic from users who do choose to connect may then be visible to a malicious actor.

An 'Evil Twin Attack' is a common method used by attackers in order to trick a user into connecting to a malicious network by creating a rouge access point, which is easily achieved using a mobile hotspot, to mimic a trusted WiFi network (Burns et al., 2017). This could enable users to perceive it to be legitimate network. However, this would be configured so that it can eaves drop on any connected devices (Burns et al., 2017). Since it can be difficult for a standard individual to identify a malicious network from a trusted one, this could result in multiple connections to the rouge access point, exposing sensitive information to an attacker (Choi, Carpenter & Ko, 2021). Once connected to the malicious network, an attacker may re-direct an individual to a fake website, prompting them to enter their authentication details where they would be recorded and exploited. This form of attack may be extremely effective in busy areas such as airports, cafés or in areas and the attacker could use this wifi network as a forwarding point to perform other types of attacks.

An idea is presented here, that sensitive user information may be obtained from an individual's device as soon as they connect to a rouge access point, regardless of their internet activity. Könings et al. (2013) supports this hypothesis as an examination of connections on a semi-public university WiFi network revealed 59% of user's device names contained sensitive information such as either their first name, last name, or both.

3.2 Leakage of Data

In cases when malicious actors are not actively attempting to steal information, users can be unaware that their data is be leaked when using public WiFi networks and their network traffic may be able to be linked back to them. Understanding privacy leakage of public WiFi hotspots can have both technical and social impacts (Cheng et al., 2013). A technical impact could enable web developers to encrypt sensitive information, to mitigate the impact of

unauthorised access and a social impact could make people aware of the data leakage which occurs thus prompting then to use a secured connection. Cheng et al. (2013) examined the security implications data leakage can hold and found that two thirds of travelling users leak their private information when connected to public WiFi in an airport. This can occur as due to the open nature of public WiFi networks, network protocols can be examined, and transfers of information within these protocols may include the device name, associated email address and the MAC address. A MAC address is a globally unique identifier for a specific device, which is a critical part of communication with WiFi network (Martin et al., 2017).

Prevention may not be easy as if a device name or associated email address did not reveal any personal information, the MAC address this could be used. Once certain network activity has linked to a MAC address, the associated management frames for this MAC address could be explored (Cunche, 2014). Management frames are chunks of data which are necessary when connecting to a WiFi network and they are not protected by and additional security measures on public networks (Jiang et al., 2013). These may contain the history of WiFi networks a device has previously connected which could be used to infer private information on a user, thus linking them to their network activity undertaken on a public-WiFi hotspot.

3.3 Interception of Data

A user's data can be intercepted on a public WiFi network by an attacker who is on the same network by using a 'Man in the Middle Attack'. Within this type of attack there are two end points, which are the user and the server they are trying to connect to. The attack would then insert themselves in-between this communication channel to view and manipulate any data being sent between these two end points, thus monitoring all network communications. (Mallik, 2019). The objective of this kind of attack would be to obtain information from the user such as their login credentials or financial information without either party knowing until it is too late. Man in the Middle attacks can be very common on public WiFi networks allowing attackers to intercept any unencrypted communications, and with the growth of public WiFi hotspots as a marketing strategy by multiple businesses this problem must be mitigated (Nigam et al., 2022). There are many different variations of this form of attack, one of them include pushing malware to a user's system to monitor information held on user user's device and this malware once downloaded could stay on the user's device even once a user disconnects from the public WiFi network (Mallik, 2019).

4. Mitigation Strategies

4.1 Need for Updated Guidance

Although there currently multiple laws in place to protect users from hackers, as far as we are aware, currently only a small amount of legislation exists to protect users from the security implications regarding the use of public WiFi (Shahin, 2016). Despite the multiple security flaws associated with connecting to a public WiFi network, it is unlikely users will stop using this service especially in situations where mobile data coverage is not great. Sombatruang et al. (2019) suggests that policy makers should consider issuing alternative advice, such as; to encourage the use of a VPN amongst users. This could be substantially more beneficial than current suggestions of requesting users to use 3G/4G and to stay away from unknown hotspots as a precaution.

4.2 Use of a VPN

A 'Virtual Private Network' or otherwise called a VPN, is a connection that is routed over the internet on a public network, from the sender's private network to a server. VPNs are typically created to ensure secure communication over a network (Ezra et al., 2022).
As of May 2020, over 200 VPN apps are available on both the Apple App Store and the Google Play Store, however despite this a research study shows only 25% of users seem to have used a VPN. Additionally, 80% of users in the same study have admitted to making use of a public WiFi network for email and online banking, which indicates they may have been vulnerable to multiple forms of attacks when performing these transactions (Sombatruang et al., 2020).

Burkert et al. (2021) claims VPNs can be used to prevent sensitive data being revealed across a public WiFi network as it applies a layer of encryption to the communications between an individual and server. Academics have proven VPNs to be effective at providing protection against 'Man in The Middle' attacks (Kurniawan et al., 2019), therefore, the encryption provided by has can be deemed as sufficient to protect a user when browsing on public WiFi.

4.3 Contrasting View on VPNs

Despite multiple VPN platforms being available for a user and the ease of setup for these platforms using modern user interfaces, using a VPN may pose as a challenge to some individuals based on the actions they wish to perform on the internet. Viewing media content on the streaming platform Netflix for example, has been blocked while using a VPN for secure communication. This was done to avoid distributing content in countries where it the company is not licensed to do so (Markham, Stavrova & Schlüter, 2019). Although limitations like these could influence a user's decision to use a VPN, it should be noted that these limitations are not widely enforced. The use of modern VPNs rarely restricts a user's internet activity as security companies tend of find a way around them and the benefits which involve safeguarding a user's data can far outweigh the cons.

5. Conclusion

Public WiFi networks can be incredibly beneficial for users and is an effective selling point for businesses to attract customers. However due to the vast amount of security vulnerabilities within public WiFi network protocols, caution must be exercised by users who wish to connect to a hotspot. Users may not even be aware an attacker is intercepting their information, as attackers can target multiple individuals on this vulnerable public network by using rogue WiFi networks and ‘Man in the Middle’ attacks. The use of a VPN ensures secure communication, as it encrypts all network data between two parties using strong encryption algorithms, therefore even if an attacker attempted to intercept communications, they would be unable to decipher them. As the cost of VPNs are low and variety of choice is high, this paper recommends all users should make use of this technology, when connected to a public WiFi network to protect themselves from the unknown.

References

Burkert, C., McDougall, J.A., Federrath, H. & Fischer, M. (2021) Analysing Leakage during VPN Establishment in Public Wi-Fi Networks. In: *ICC 2021-IEEE International Conference on Communications*. 2021 IEEE. pp. 1–6.

Burns, A., Wu, L., Du, X. & Zhu, L. (2017) A novel traceroute-based detection scheme for wi-fi evil twin attacks. In: *GLOBECOM 2017-2017 IEEE Global Communications Conference*. 2017 IEEE. pp. 1–6.

Chiang, C.-Y. & Tang, X. (2022) Use public Wi-Fi? Fear arouse and avoidance behavior. *Journal of Computer Information Systems*. 62 (1), 73–81.

Choi, H.S., Carpenter, D. & Ko, M.S. (2021) Risk taking behaviors using public Wi-fi™. *Information Systems Frontiers*. 1–18.

Cunche, M. (2014) I know your MAC address: targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*. 10 (4), 219–227.

Ezra, P.J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R. & Damasevicius, R. (2022) Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics*. 309–319.

Gabriel, C. (2014) Carrier Wi-Fi: State of the market 2014. *Wireless Broadband Alliance, San Jose, CA, USA, Tech. Rep*.

Goldsborough, R. (2015) Staying safe when using WiFi. *Teacher Librarian*. 42 (4), 65.

Jiang, Z., Zhao, J., Li, X.-Y., Han, J. & Xi, W. (2013) Rejecting the attack: Source authentication for wi-fi management frames using csi information. In: *2013 Proceedings IEEE INFOCOM*. 2013 IEEE. pp. 2544–2552.

Könings, B., Bachmaier, C., Schaub, F. & Weber, M. (2013) Device names in the wild: Investigating privacy risks of zero configuration networking. In: *2013 IEEE 14th International Conference on Mobile Data Management*. 2013 IEEE. pp. 51–56.

Kurniawan, D.E., Arif, H., Nelmiawati, N., Tohari, A.H. & Fani, M. (2019) Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator. In: *Journal of Physics: Conference Series*. 2019 IOP Publishing. p. 12031.

Lotfy, A.Y., Zaki, A.M., Abd-El-Hafeez, T. & Mahmoud, T.M. (2021) Privacy Issues of Public Wi-Fi Networks. In: *The International Conference on Artificial Intelligence and Computer Vision*. 2021 Springer. pp. 656–665.

Maimon, D., Becker, M., Patil, S. & Katz, J. (2017) Self-Protective Behaviors Over Public WiFi Networks. In: *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*. 2017 pp. 69–76.

Mallik, A. (2019) Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*. 2 (2), 109–134.

Markham, A., Stavrova, S. & Schlüter, M. (2019) Netflix, imagined affordances, and the illusion of control. *T. Plothe and AM Buck, Netflix at the Nexus. Content, Practice, and Production in the Age of Streaming Television*. 29–46.

Martin, J., Mayberry, T., Donahue, C., Foppe, L., Brown, L., Riggins, C., Rye, E.C. & Brown, D. (2017) A Study of MAC Address Randomization in Mobile Devices and When it Fails. *Proc. Priv. Enhancing Technol.* 2017 (4), 365–383.

Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y. & Ruan, N. (2019) Revealing your mobile password via WiFi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*. 19 (2), 432–449.

Ming, Z., Xu, M., Wang, N., Gao, B. & Li, Q. (2017) Truthful auctions for user data allowance trading in mobile networks. In: *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. 2017 IEEE. pp. 1271–1280.

Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Mohammad, Q. & Alrabaee, S. (2020) Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux. In: *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*. 2020 IEEE. pp. 1–4.

Nigam, A., Sharma, S., Patel, R.K. & Agrawal, M. (2022) Man-In-The-Middle-Attack and Proposed Algorithm for Detection. In: *2022 International Mobile and Embedded Technology Conference (MECON)*. 2022 IEEE. pp. 83–88.

Shahin, E. (2016) Is WiFi worth it: the hidden dangers of public WiFi. *Cath. UJL & Tech*. 25, 205.

Sombatruang, N., Omiya, T., Miyamoto, D., Sasse, M.A., Kadobayashi, Y. & Baddeley, M. (2020) Attributes affecting user decision to adopt a Virtual Private Network (VPN) app. In: *International Conference on Information and Communications Security*. 2020 Springer. pp. 223–242.

Sombatruang, N., Onwuzurike, L., Sasse, M.A. & Baddeley, M. (2019) Factors influencing users to use unsecured wi-fi networks: evidence in the wild. In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 2019 pp. 203–213.

Sombatruang, N., Sasse, M.A. & Baddeley, M. (2016) Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions. In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. 2016 pp. 61–72.

Yu, H., Cheung, M.H., Gao, L. & Huang, J. (2017) Public Wi-Fi monetization via advertising. *IEEE/ACM Transactions on Networking*. 25 (4), 2110–2121.