Opening Our Wi-Fi Network to Guests

CS4203 Practical 1 Briefing Document

200002872 200018789 200036815 200007626 170027560

October 11, 2023

Due to customer and partner feedback, we as a company have decided to open our Wi-Fi network to guests. Here are the possible repercussions and what we are doing to prevent them, as well as how these changes will affect you.

1 Access to Internal Shared Resources

When considering opening up our Wi-Fi network to guests, we should acknowledge the prospect of exposing internal shared files and hardware resources. Permitting unauthorized access to sensitive corporate information could lead to conceivable scenarios where guests with bad intentions dig into our shared files, networked printing infrastructure, and assorted peripheral devices in our network infrastructure. The repercussions of these actions would be substantial, including possible data breaches and exploitation of hardware assets.

To ameliorate the inherent risks, the establishment of a separate, virtual guest network is a viable option, thereby isolating guests from critical internal resources and avoiding attacks.

2 Malware Propagation

A guest connection could provide malware (malicious software) access to our network, leading to stolen private data, or infection of other connected devices [2]. We can combat this by using a creating a Virtual Local Area Network within our network – a 'guest network'. All trusted internal devices will not be discoverable from the guest network, even to malware. Some routers cannot maintain the virtual network when they experience high levels of traffic [8]; if our router has this defect, we should consider deploying different routers to separate the business and guest networks. We should endeavour to keep guest network clean, as we may be open to legal suits for negligence against us if malware on our network damages a guest's device [3]. To avoid claims, we can include 'terms and conditions' for use, as well as deploying multi-factor authentication and anti-malware software on our guest network. We should also periodically shut down and deep-clean the guest network as a safety precaution.

3 ARP Spoofing

Successful ARP spoofing could lead to unauthorised access to private information such credentials, credit card details and any other confidential information. To mitigate the risk of guests being exposed to such threat, we could manually create a static ARP table - this is highly effective, as it ignores incoming claims from external devices, and thereby eliminates any direct methods for the attacker to claim a false identity. Additionally, we could enable the use of 'Dynamic ARP' inspection, which validates messages that are sent to ARP, and drops messages that are suspicious or malicious. Similarly, deploying a packet-filtering network-level firewall allows detection of imposter devices by flagging data packets that are repeatedly sent from the same address. Lastly, we could encrypt all network traffic within the Wi-Fi network. This will not prevent ARP spoofing, but will mitigate the risk of a data breach even if the attacker intercepts the communication, as they will not be able to understand the encrypted messages.

4 Denial of Service Attacks

The UK National Cyber Security Centre defines a Denial of Service attack as one which will "render a service inaccessible" [7]. Attackers can purchase month-long distributed DoS attack services for under 900 USD [10]. These attacks have the potential to disrupt our access to vital services within our local network. There are two main types of DoS attacks: bandwidth depletion, and resource depletion. While bandwidth depletion attacks focus mainly on disrupting the passageway through the network, resource depletion attacks target individual devices or services to consume processing power and render them unusable [4]. To mitigate the efficacy of bandwidth depletion attacks, we can use network access controls and firewalls to limit the bandwidth allocated to guests, and detect and discard suspicious traffic. Additionally, virtualization within our network already provides a barrier between guests and internal authenticated users, ensuring guests cannot see or access internal devices and services [9], and thereby preventing resource depletion attacks.

5 Illegal Activities

Our current obligations for dealing with illegal activities are mostly laid out in the Digital Economy Act 2010. The act's provisions apply if "a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner's copyright by means of the service" [1]. In such a case, we must be able to take action against whoever used our connection to break the law by preventing them further access from our network. We should also prevent access to any websites which are known to contain such illegal materials. The best way to achieve this would be to use a DNS filtering solution, which will block users of the network from accessing any websites blacklisted by the filter [5]. We can purchase a solution which will allow us to leverage an existing and continuously updating database of known malicious websites. We should also leverage content filtering [6] to flag and block certain phrases that might indicate illegal or undesirable content.

References

[1] Digital Economy Act 2010. https://www.legislation.gov.uk/ukpga/2010/24/section/3. Accessed on 10-10-2023.

[2] Most Common Malware. https://arcticwolf.com/resources/blog/8-types-of-malware/, May 2023. Accessed on 08-10-2023.

[3] WiFi Law 101: Legal Compliance and Your Guest WiFi Network. https://project-vision.co.uk/networks/wifi-law-101-legal-compliance-and-your-guest-wireless-network/, 2023. Accessed on 10-10-2023.

[4] C. Douligeris and A. Mitrokotsa. DDoS attacks and defense mechanisms: a classification. In *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795)*, pages 190–193, December 2003. URL: https://ieeexplore.ieee.org/abstract/document/1341092, doi:10.1109/ISSPIT.2003.1341092.

[5] Sead Fadilpašić. What is DNS filtering? https://www.techradar.com/features/what-is-dns-filtering, Apr 2022. Accessed on 10-10-2023.

[6] Peter Loshin and Andrew Zola. What is content filtering and how does it work? https://www.techtarget.com/searchsecurity/definition/content-filtering, Apr 2022. Accessed on 10-10-2023.

[7] NCSQ UK. Denial of Service (DoS) guidance, November 2020. URL: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection.

[8] Adar Ovadia, Rom Ogen, Yakov Mallah, Niv Gilboa, and Yossi Oren. Cross-Router covert channels. In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, Aug 2019. USENIX Association. URL: https://www.usenix.org/conference/woot19/presentation/ovadia.

[9] Aleksandr Ovcharov, Natalia Efanova, and Rui Pedro Lopes. Multi VLAN Visualization in Network Management. In Ana I. Pereira, Andrej Košir, Florbela P. Fernandes, Maria F. Pacheco, João P. Teixeira, and Rui P. Lopes, editors, *Optimization, Learning Algorithms and Applications*, volume 1754, pages 131–143. Springer International Publishing, Cham, 2022. URL: https://link.springer.com/10.1007/978-3-031-23236-7_10, doi:10.1007/978-3-031-23236-7_10.

[10] Statista Research Department. Dark web price of malware/DDoS services 2023, September 2023. URL: https://www.statista.com/statistics/1350155/selling-price-malware-ddos-attacks-dark-web/.