Network Traffic Monitoring Project

Daiwik Swaminathan, Brandon Howell, Wyatt Colburn
California Polytechnic State University, San Luis Obispo

ABSTRACT

This project explores the feasibility of monitoring a user's network traffic by tricking them into connecting to a rogue network/access point via an NFC-based attack. We discuss the security implications, methodologies for data capture, and potential countermeasures. Our findings highlight the ease of exploiting unsecured networks and the importance of user awareness in preventing such attacks. Additionally, we explore countermeasures and discuss the limitations of our approach in real-world scenarios.

1 INTRODUCTION

Untrusted Wi-Fi connections are highly vulnerable to man-in-the-middle (MITM) attacks. Generally, users avoid such risks by not connecting to suspicious networks. However, this project investigates a scenario where users unknowingly connect to a malicious network via NFC-based Wi-Fi onboarding, making them vulnerable without explicit intent. By leveraging an NFC tag, we can automatically prompt a target's device to join our rogue Wi-Fi network. Our goal is to demonstrate this attack vector, analyze its implications, and propose mitigations.

We hypothesize that an attacker can easily convince a target to connect to an untrusted network using NFC technology, leveraging automatic connection prompts as a social engineering attack.

2 RELATED WORK

Previous research on rogue networks and MITM attacks [3] has shown that unsuspecting users can be easily tricked into connecting to malicious networks. Studies have also explored techniques such as Evil Twin attacks, DNS spoofing, and traffic analysis as effective mechanisms for data interception. NFC-based attacks, however, remain relatively unexplored in this domain, making our work novel in demonstrating its feasibility for practical exploitation.

Prior studies have highlighted the security risks associated with automatic network onboarding mechanisms. Work on Evil Twin attacks [2] demonstrates how users can be deceived into connecting to rogue networks. Similarly, studies on Wi-Fi Pineapple devices show how attackers can intercept and manipulate network traffic [5]. However, little research has been done on leveraging NFC for onboarding attacks, making this study a unique contribution.

3 METHODOLOGY

Our attack setup consisted of the following key components:

- A MikroTik router running RouterOS to create and manage the rogue Wi-Fi network.
- NFC tags programmed to contain Wi-Fi connection details.
- Targeted Android devices, which automatically prompt users to connect to the rogue network upon detecting the NFC tag.
- Network logging and analysis tools to capture and profile traffic from connected devices.

The attack was carried out as follows:

(1) The attacker approaches a target in a public space and subtly places the NFC tag near their Android device.
(2) The target's phone detects the NFC tag and prompts them to connect to our network (e.g., we mimicked "eduroam", which is the campus network).
(3) If the user clicks 'Connect,' their traffic is routed through our malicious network.
(4) Using RouterOS logs, we analyze the victim's browsing activity.

To maintain seamless internet access and reduce suspicion, our malicious network piggybacks off a legitimate internet connection via Ethernet. Additionally, we experimented with redirecting users via DNS spoofing [4], though HTTPS protections limited its effectiveness.

4 RESULTS AND DISCUSSION

Our testing revealed the following insights:

- We successfully tricked Android users into connecting to our rogue Wi-Fi network using NFC-based onboarding.
- Network logs provided insight into users' online activity, including visited websites (e.g., Reddit, Disney, ChatGPT).
- Sometimes websites did not consistently appear in the logs and some even never showed up in the logs. We unfortunately did not have too much time to investigate why this was happening but did have suspicions it might have to do with load balancing and content-delivery network behaviors.
- By forcing our router to act as a DNS provider, we were able to redirect domain requests (e.g., making calpoly.edu resolve to Yahoo.com), though this was limited by SSL/TLS warnings.
- Android devices automatically prompted users to connect, demonstrating the risk of automatic network onboarding. In contrast, we were unable to perform this attack on Apple devices, as they do not automatically connect to unknown NFC tags.
- We did also observe that even with intentionally connecting to our rogue network, Apple devices issues several warnings indicating the suspicious nature of our network.

These results highlight the real-world feasibility of this attack and the importance of user awareness in preventing accidental connections to untrusted networks. However, limitations exist, such

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

as the need for close physical proximity to the target and the increasing adoption of HTTPS, which reduces the effectiveness of simple traffic monitoring. Further, this attack was only possible with Android devices and not Apple devices.

5 LESSONS LEARNED

Throughout this project, we encountered several challenges and key takeaways:

- NFC-based attacks are highly effective but require close physical proximity.
- Some websites implement security measures that obscure their traffic in logs, limiting the effectiveness of simple traffic monitoring.
- DNS spoofing is limited in effectiveness due to HTTPS and certificate authority validation.
- Future work could include QR code-based Wi-Fi onboarding (which affects iPhones), more advanced traffic profiling, and further exploration of phishing techniques using collected browsing data.

6 FUTURE WORK

Other Connection Methods

Apple does not allow its users to connect to WiFi networks through NFC tags. Therefore, we were interested in other ways we could connect individuals to a hidden nefarious network. One possibility was QR codes. Brandon (on Android) was able to scan the NFC tag, connect to it, and then generate a QR code. When Wyatt scanned the QR code the iPhone was prompted to connect to a hidden network. Both Apple and Android OS only show the SSID (which can be named identical to a real network, such as eduroam).

Setting up a QR code in a coffee shop would be an easy way to piggyback on the existing network (safe) and social engineer people into logging your identical named nefarious network.

Profiling

Another attack vector was when, with the ability to see the traffic of an individual device, we can create profiles of users. Creating a script that captures the time spent on a website, the types of websites, or even the security risks of that website would be helpful to an attacker. If someone frequently visits a site with a known vulnerability, that could perhaps be used to attack them. Alternatively, if you were to log an entire company's router traffic, you could make note of any user that visits compromised websites and give them an integrity value. Then attacks those users with lowest scores; this would be another way to profile a possible victim.

Spoofing

With the ability to create hidden networks that have the same name as real networks, we have the opportunity to create spoof attacks. Often, logging into a network will ask users for information. For instance, when logging into eduroam you asked for your Cal Poly Login. Since we can redirect traffic, we could create specific pop-ups depending on what network we are impersonating and steal vital information.

SpearFishing

Similarly to profiling, with the ability to log user web traffic, we can phish target avenues. For instance, if a target is often on job-listing sites such as Indeed or Linkedin, a spear fished attack with an email of a job listing would surely be effective.

7 RECOMMENDATIONS

To protect against such attacks, users should:

- Avoid clicking "Connect" when an unexpected Wi-Fi connection prompt appears.
- Disable NFC when not in use to prevent unintended connections.
- Advocate for Android to improve transparency in NFC-based Wi-Fi onboarding.
- Use VPNs to encrypt traffic, mitigating the impact of network-based eavesdropping. [1]

Additionally, developers and manufacturers should implement security measures such as requiring explicit user confirmation before connecting to NFC-based networks and enforcing stricter authentication for onboarding mechanisms.

8 PIVOT STAGE

The initially intent was to create a secure WiFi network which used near field communication (NFC) tags to authenticate devices onto a network. Imagine a WiFi network at home has a super complicated (therefore secure) password. Rather than having to say the password to a guest, they would scan a NFC tag. In addition, the goal was to develop a raspberry pi to act as a central controller, facilitating interaction between the NFC tags and router. In case the password was compromised, the central controller would change the password and reprogram the NFC, thus reducing the pain of changing the passwords on all your devices. The central controller is also responsible for validating that the NFC tags are on the approved tag list to avoid NFC cloning.

There were three main security benefits to this system.

- 1) Enhanced access control by incorporating a physical element of a NFC tag.
- 2) By authorizing through a NFC tag, the password to the network can be much more advanced which would be more resilient to brute force attacks.
- 3) Centralized management: the raspberry pi would monitor the NFC tags, suspend access if the user went to a compromised website, and update the password if necessary.

However, iPhones do not support using NFC to connect to WiFi network, which serverly limited the accessibility of our system. In addition, our router already had an OS called MikroTik which allowed us to provide control over our network. Therefore, we decided to pivot to the project described above.

REFERENCES

[1] Homam El-Taj and Lamar Miralam. 2024. Network sniffing and its consequences: a comprehensive survey. *International Journal of Computer Science and Information Security (IJCSIS)* 22, 3 (2024).

[2] Harold Gonzales, Kevin Bauer, Janne Lindqvist, Damon McCoy, and Douglas Sicker. 2010. Practical Defenses for Evil Twin Attacks in 802.11. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. 1–6. https://doi.org/10.1109/GLOCOM.2010.5684213

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

[4] U Steinhoff, A Wiesmaier, and R Araújo. 2006. The state of the art in DNS spoofing. In *Proc. 4th Intl. Conf. Applied Cryptography and Network Security (ACNS)*. Citeseer.

[5] Gent Thaqi. 2024. Creating Labs for Ethical Hacking Course Based on WiFi Pineapple and USB Rubber Ducky. (2024).