

Enhancing Public Wi-Fi Security Through Digital Certificate Authentication

MSc Research Project
Master of Science in Cyber Security

Niall Coughlan
Student ID: 21121214

School of Computing
National College of Ireland

Supervisor: Raza Ul Mustafa

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name:Niall Coughlan.....

Student ID:21121214.....

Programme:MSCCYBETOP..... **Year:**2023.....

Module:Research Project.....

Supervisor:Raza Ul Mustafa.....


Submission Due Date:14th August 2023.....

Project Title:Enhancing Public Wi-Fi Security Through Digital Certificate Authentication.....

Word Count:8055..... **Page Count:**.....20.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

Date: 17/09/2023.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Public Wi-Fi Security Through Digital Certificate Authentication

Niall Coughlan
21121214

Abstract

The proliferation of devices allowing access to the internet has created a corollary need for network access at a wide variety of locations. There is an expectation that many businesses, such as cafés and hotels, will provide Wi-Fi to their customers. This has led to the availability of public Wi-Fi networks to cater to these customers. However, the security provided by these networks is often lacking, and users may not realise the risks to which they are exposing themselves when connecting to public networks, with the potential for their data to be compromised. This research project examined the risks posed to users of public Wi-Fi networks and proposes a method of authenticating users to public Wi-Fi, which provides greater protection to users than other commonly used methods. This method was subjected to penetration testing, using techniques and tools which are most likely to be used during the course of real-world attacks. These tests were also performed against other Wi-Fi security methods, to provide a comparison that demonstrates both the lack of attention given to securing public Wi-Fi networks, and the possibility of defending these weaknesses.

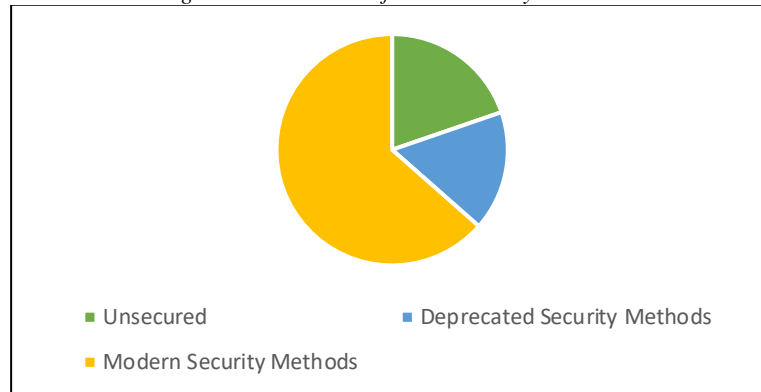
1 Introduction

The 21st century has seen the arrival of personal, portable, internet-connected devices, such as laptops, tables and smartphones. These devices have allowed people access to the internet beyond their home and office, unrestricted by wired connections. But as they require wireless networking, they have also created a need for public Wi-Fi networks. This has provided some businesses (such as cafes, restaurants, hotels, etc.) an opportunity of attracting customers, with over 70% of people saying they are more inclined to patronise establishments which provide Wi-Fi to customers (Sonola, 2022). Even governments have begun investing in wireless infrastructure, with large cities such as New York and Seoul spending money on projects to increase the availability of Wi-Fi to their citizens (Choi et al, 2021). With this level of eagerness for public Wi-Fi, it is expected that businesses and other providers will continue to deliver it as a free service.

However, these networks also provide a new vector by which malicious actors may attempt to steal from people. Email, banking, and other sensitive communications can all be conducted through Wi-Fi networks, and the wireless nature of these networks means any data transferred through them is theoretically available to an attacker. Although it is possible to implement security measures to prevent attackers from obtaining data that has been transmitted through a Wi-Fi network, studies have shown that over one-third of networks use outdated security measures that are prone to exploitation (Schepers, Ranganathann, and Vanhoef, 2021) or do not provide any security measures (Noman, Noman, and Al-Maatouk, 2020). Figure 1

shows the results of a survey conducted by Noman, Noman, and Al-Maatouk, (2020), demonstrating the incidence of weak Wi-Fi security. As 48% of people admit to accessing sensitive data through public Wi-Fi networks (Maimon et al, 2021), this presents attackers with an attractive potential for theft.

Figure 1. Prevalence of Wi-Fi Security Methods



The purpose of this research project is to examine the possibility of securing public Wi-Fi networks using digital certificate authentication, to reduce the risk that people using public Wi-Fi networks will have their information compromised. This will be achieved through the following stages:

1. Examining current state-of-the-art solutions utilised in public Wi-Fi authentication, and the security issues that they present, and also methods of testing the security of Wi-Fi networks
2. Developing a solution for Wi-Fi authentication using digital certificates, while allowing for user registration upon initial network connection
3. Testing the proposed solution against other public Wi-Fi security methods, using testing techniques identified in step 1
4. Determining the efficacy of the proposed solution in comparison to contemporary security methods.

In the context of this research, a public Wi-Fi network is a wireless network which is open to any member of the public. This assumes that the network itself can have no prior knowledge of the devices which connect to it. Digital certificate authentication should be a method which uses shared certificates to allow the following:

1. The Wi-Fi network to authenticate a connecting device
2. The connecting device to authenticate the Wi-Fi network

This would allow the network to identify which devices are connected, and to prevent a user from unintentionally connecting to a spoofed Wi-Fi network. This research is important to identify a method of Wi-Fi authentication that can reduce the possibility of unaware users being compromised when connecting to public Wi-Fi. As 70% of people of people admit to using unsecured Wi-Fi networks when they are available¹, a secure public Wi-Fi network will reduce the vectors via which an attacker may potentially compromise users.

¹ <https://hbr.org/2017/05/why-you-really-need-to-stop-using-public-wi-fi>

2 Related Work

This research project began by investigating existing research that has already been conducted on the topic of Wi-Fi security, with a focus on the security of public Wi-Fi networks (though not an exclusive focus, as methods of Wi-Fi security evaluation were relevant to both public and private networks). The papers examined were selected from literature repositories (Google Scholar and IEEE), and were chosen based on their discussion of one of the following four areas related to Wi-Fi security:

1. Discussions of current Wi-Fi security standards and methods
2. Security issues prevalent within Wi-Fi security
3. Methods of assessing the security of Wi-Fi networks
4. Possible improvements to Wi-Fi security methods

These assisted in identifying the risks that are particularly prevalent in public Wi-Fi networks, and the security features which must be provided to ensure that they are sufficiently protected. This guided in the development of the solution examined as part of this project. In addition, papers were selected based on their recency, as only papers published since 2017 were selected. This ensured that any discussion was relevant to contemporary Wi-Fi security issues.

2.1 Current standards in public Wi-Fi

As was examined by Noman, Noman, and Al-Maatouk (2020), Wi-Fi networks are predominantly protect access via three methods:

1. Wired Equivalent Privacy
2. Wi-Fi Protected Access
3. Unprotected

The first wireless security method to protect Wi-Fi networks from unwanted intrusion and exploitation, Wired Equivalent Privacy (WEP) was introduced in 1997 to encrypt traffic transmitted between an access point and a connecting client device (Duc et al, 2021). Utilising either a 64-bit or 128-bit RC4 cipher, a pre-shared key is combined with an initialisation vector to generate an RC4 key. When a client attempts to connect to the network, they encrypt their authentication request with RC4 key, which is then decrypted by the access point to ensure the correct key is in use. Once this is confirmed, the key is then used to encrypt all traffic between the client and the access point. However, even at it's creation WEP was known to be insecure (Moissinac et al, 2021), so new methods were already being developed.

WEP was superseded in 2003 by Wi-Fi Protected Access (WPA). Since it became available, WPA has gone through three iterations: WPA, released in 2003; WPA2, released in 2004; and WPA3, released in 2018 (Moissinac et al, 2021). Authentication to WPA protected networks can be used either via personal or enterprise methods. Personal involves the use a pre-shared key known to both the client and access point. Enterprise involves the use of an external authentication server to identify clients. However, due to requirement of an external authenticator, and the need to have existing knowledge of the devices which are expected to

connect to it, Enterprise authentication is less suited to public Wi-Fi networks where devices are not known prior to authentication (Moissinac et al, 2021).

Another method, discussed by Wahyudi, Luthfi, and Efendi (2019), is Captive Portal authentication. This forces a connecting user to a registration page, where they must input some details to allow internet access through the network. Once the user has registered, their devices MAC address is added to a whitelist of devices, following which MAC address filtering is used to allow access through the access point and to the internet. The inclusion of Captive Portal authentication highlights a deficiency in previous surveys of Wi-Fi security methods, such as Schepers, Ranganathann, and Vanhoef (2021) and Noman, Noman, and Al-Maatouk (2020). Both of these surveys identified Wi-Fi security methods through scanning, which only detects if encryption is used to protect the network. Since Captive Portal does not use encryption to authenticate clients to its network, it will appear as unsecured. This prevents an accurate assessment of its prevalence as a Wi-Fi security method.

Finally, further security methods which can protect user information in Wi-Fi networks are discussed by Ali et al (2019) and Sahu (2022). These include the use of HTTPS websites, and personal VPNs. Both of these methods are similar, as they provide a form encryption that is separate from the data link layer (as used by the above protocols), thus providing encryption on the users device which is in addition to the Wi-Fi network. However, both of these methods are beyond the control of a Wi-Fi network administrator. Thus, any such administrator who wants to protect users of their network cannot rely on their implementation.

2.2 Issues with public Wi-Fi security

The wireless nature of Wi-Fi networks necessitates the transmission of data over the air. While this increases the usability of such networks (by not requiring a wired connection), it also makes this transmission open to malicious users in the same vicinity. As just under 50% of users admit to using public Wi-Fi networks to access sensitive applications (Maimon et al, 2021), this leaves users open to eavesdropping attacks. In such attacks, an attacker passively listens to a Wi-Fi network to attempt to capture valuable information such as usernames and passwords. Wahyudi, Luthfi, and Efendi discuss how this attack can be accomplished using the traffic sniffing tool Wireshark (2019). Although their test was completed with foreknowledge of the pre-shared key used to protect the network, this is a risk that is particularly pronounced with public Wi-Fi networks, where the key can be made freely available, or sometimes where a key is not used. This highlights eavesdropping as a danger that is very relevant to public Wi-Fi. Further, as mentioned by Zou et al, even in cases where businesses attempt to keep the key private, many Wi-Fi networks use security methods which are trivial to bypass (2016).

Such exploitation methods that are applicable to public Wi-Fi networks generally involve password cracking. These weaknesses are found in protocols that use pre-shared keys, such as WEP and WPA, with older, deprecated protocols being more susceptible to these attacks. WEP, being the oldest Wi-Fi security protocol, was known to be insecure even at its inception, (Schepers, Ranganathann, and Vanhoef, 2021). Its use of an initialisation vector in the key generation, intended to vary the key and prevent its repetition, but the vector used is too small

(24 bits), which results in its reuse, thus leaving WEP open to brute-force attacks (Alhamry and Alomary, 2022). Once the key is obtained, WEP is then open to eavesdropping attacks. WPA, and its later iterations, provided a more difficult key to crack, but even these are possible to exploit using traditional password cracking techniques, such as dictionary attacks (Abo-Soliman and Azer, 2021) or brute-forcing (Radivilova and Hassan, 2017). It should be noted, that unlike WEP, the security of WPA personal networks increases with the complexity of the pre-shared key used to protect it (Alhamry and Alomary, 2022). However, while this can be advantageous in networks where the pre-shared key can be kept secret (i.e., a private network used only by a few users), the open nature of public Wi-Fi necessitates that the key be made available for public use. Thus, the increased security of later iterations of pre-shared key based secure networks do not avoid the problem of ensuring malicious users cannot intercept the traffic of legitimate users.

While eavesdropping traffic on a Wi-Fi network allows an attacker to view traffic transmitted through the network, a more active attack that can be performed, to which public Wi-Fi networks are particularly vulnerable, is a Man-in-the-Middle attack, such as Evil Twin (Bartoli et al, 2018). This involves an attacker deploying their own access point, replicating the settings of an existing public Wi-Fi network, in an attempt to trick devices into connecting to it. Once a target device has connected to the malicious access point, an attacker can forward the target onto their own servers, allowing them to steal user credentials. For example, an attacker can clone a banking website and direct the user to their page instead of the legitimate one, allowing them to steal the user's password to their bank. This method of exploitation presents itself even in WPA Enterprise environments, whereby an attacker could gain network credentials (Radivilova and Hassan, 2017).

Finally, a risk that should not be forgotten during the creation of any solution to protect public Wi-Fi networks is the possibility of misconfiguration within that network. Lugovic, Mrcic, and Korona examined the configuration of public Wi-Fi access points, finding that 59% had kept their default configuration (2019). Similarly, Bartoli et al, find that even in Wi-Fi networks that are using ostensibly secure protocols (in this case, WPA2 Enterprise), misconfiguration issues can lead to attackers exploiting a network and its users (2018). For example, configuring the network profile to not force the client to authenticate the access point, leaving the client open to an Evil Twin attack. Though these examples are not directly related to public Wi-Fi security protocols, they demonstrate the importance of ensuring that any protocol is configured correctly to ensure its security is correctly applied.

All of these weaknesses illustrate the weaknesses that exist within current Wi-Fi security protocols. Public Wi-Fi networks, in particular, are more prone to using insecure methods of authentication. Although the existing research shows that no method is completely free of risk, there is a lack of methods available to public Wi-Fi networks that would increase their security, making them comparable to the methods available to enterprise Wi-Fi solutions.

2.3 Assessing Wi-Fi Security

While it is useful for this research to identify the various security issues that are present in the security methods of Wi-Fi networks, it is also important to critically assess these issues so that the relative strength of each security method can be determined. This will allow the comparison of this solution against existing methods. Various authors have discussed systems for measuring security of Wi-Fi networks, with the most common feature being the importance of penetration testing in such assessments. These authors also align in the steps that these tests should take.

Both Lu and Yu (2021) and Fikriyadi, Ritzkal, and Prayosa (2020) discuss how any test should begin with an identification of the objective of the tests. Fikriyadi, Ritzkal, and Prayosa identify gaining access to the network as the primary goal of any penetration test. While this may be suitable for an enterprise network, where this would allow access to further devices on the network, such as sensitive file shares, it is not as useful for a public network, where access is likely to be allowed without exploitation. This is similar to the method of Astrida, Saputra, and Assaafi, who identify network access as the primary goal, and who's tests focus on cracking the pre-shared key of the Wi-Fi network (2022). Conversely, Lu and Yu identify further opportunities when attacking a Wi-Fi network, such as the capture of user data on that network (2021). Their method involves using open-source tools, such as Wireshark, to listen on the network and attempt to capture user traffic. Their method then assigns a pass-fail mark to each network, depending on whether such an attack would be successful or not. While this is a useful indicator of security, it is also possible that a penetration test conducted by a more experienced tester could succeed in exploitation where another may not. This is important to note for any assessment, as the lack of exploitation during one test only indicates that it is more complex to access, not that it is inaccessible.

While the above research highlights the importance of penetration testing in security assessments, the ability to rank the results of a penetration test is also required to identify security methods by their effectiveness. This ability is discussed by Abdullah and Singh, who identify metrics which could be used in a measurement of security (2022). The metric which appears most relevant to an assessment of public Wi-Fi security, in particular the ability of those networks to protect user data, is the time taken for a successful attack. In their discussion, the longer the time taken for a successful attack, the less likely that the target will be exploited. This aligns with the research of Ramos et al, who concur that the longer the time taken for exploitation, the more secure a system is (2017). From this, a method of penetration testing can be established to identify the objective of a test (i.e., to exploit that which the security method is designed to protect) and rank the results of each security method according to the time taken for a successful attack.

2.4 Possible solutions to public Wi-Fi security issues

As has been discussed in prior research above, there are many issues present in Wi-Fi networks, which can be exacerbated in public networks. Their open nature means that a malicious user could legitimately access the network without requiring any exploitation

techniques. Legitimate users would then be at risk due to sharing the network with such malicious users, rendering their private data vulnerable to compromise. To avoid leaving users at risk in this manner, some authors have investigated potential security solutions that could be implemented in public Wi-Fi networks.

Hoseini, Hartog, and Bouhafis propose a method of configuring wireless networks that replicates Physical Layer Security (2023). In their proposal, wireless networks could be configured to transfer the connections of legitimate users between multiple access points. By moving users between access points, the network would decrease an attacker's ability to capture traffic, as some access points may be out of their range. While the idea of using the physical attributes of a wireless network is unique, it encounters two problems. The first is the requirement for multiple access points to be deployed, which may provide too high a cost for some businesses to implement. The second issue is that there is no guarantee that a user will not be located directly beside an attacker, giving the attacker access to the same access points as the user, and allowing them to capture all traffic.

Another method which has been researched is to extend the implementation of WPA2 Enterprise authentication, using 802.1x certificates, to public Wi-Fi networks. This has been examined by both Marques, Zuquete, and Barraca (2019), and Moissinac et al (2021). In such systems, the network is configured to use certificates located on the connecting client to authenticate the client, and then encrypt traffic between the client and the access point. However, a problem that has prevented this from being applied to public Wi-Fi networks is the management of these certificates, and the difficulty of getting them onto devices (Khasawneh et al, 2014). Marques, Zuquete, and Barraca suggest that a combination of captive portal and WPA2 Enterprise could be used, with users first authenticating against the portal, after which their certificate is accepted by the Wi-Fi network for authentication. However, this does not avoid the problem discussed by Khasawneh et al, as users must still possess a client authentication certificate prior to their connection to the network. As public Wi-Fi networks can be used by users attempting to get internet access at short notice, it is not realistic to assume they will already possess the necessary certificate, rendering them unable to connect. Similarly, Moissinac et al suggest that users would already possess such a certificate when they attempt to connect, encountering the same issue (2021). However, while these methods would not be useful for a network which wishes to ensure that all potential users can connect, the possibility of using WPA2 Enterprise authentication for a public Wi-Fi network is one that should be further explored, due to the improved security it possesses over pre-shared key authentication. Also, as discussed by Song et al, these solutions can be prone to misconfiguration, which render them ineffective against certain threats (2022). This highlights the importance of testing the deployment of all solutions, to ensure misconfiguration is avoided.

Other solutions which were discussed involve the use of endpoint based protective measures, which can encrypt a user's traffic before it traverses the Wi-Fi network. Sahu recommends the adoption of VPN's on end user devices (2022). This creates a private tunnel from the user's device to a virtual network. Ali et al. advise that users should only use HTTPS web applications, as the traffic will be forced to encrypt by the web application itself (2019).

Both of these methods will encrypt traffic on the end user's device, thus rendering it encrypted as it traverses the public Wi-Fi network, reducing the possibility of an attacker being able to compromise it. However, both of these methods rely on configurations that are outside the control of the public Wi-Fi network administrator, and thus they cannot be relied upon when deploying a public network. This renders them unsuitable as solution in this scenario.

In conclusion, the papers examined demonstrate that the current state-of-the-art for public Wi-Fi security (namely, the preponderance of networks using either no authentication or pre-shared key authentication methods) are not sufficient to protect the traffic of network users. This arises from the nature of these networks, whereby access must be granted to all users who request it, thus allowing malicious users to share a network with legitimate users. The solution proposed by this research project will provide a method that authenticates users via individual certificates, which can be obtained upon initial connection to the network. This would allow a public Wi-Fi network to permit all users to connect to it, while still ensuring that users cannot compromise the traffic of other users.

3 Research Methodology

As the objective of this research is to identify a method of securing public Wi-Fi networks that provides greater protection for the users of those networks, the research approach is based around the level of security provided to users by various methods. The following assumptions were made about the Wi-Fi network, to assist with creating the parameters of the test:

1. The network must be accessible by anyone who wishes to use it, including attackers. Any pre-shared key cannot be hidden.
2. The only connections on the network are other users (i.e., no servers, or information related to the business providing the Wi-Fi). Thus, the network is only concerned with protecting these users.
3. No endpoint based security methods were to be used during testing (e.g., VPN, HTTPS). These are outside the scope of a network administrator to configure and cannot be relied upon, thus they could not be used during testing.
4. It must be possible to connect to the network by a first time user with no prior knowledge of the network.

To provide a comparative assessment of the efficacy of a digital certificate approach to public Wi-Fi security, four other methods of security were chosen to be assessed: Unsecured; WEP, pre-shared key; WPA2 pre-shared key; Captive Portal. These methods were chosen based on their incidence in real-world Wi-Fi networks (Noman, Noman, and Al-Maatouk, 2020).

Prior research highlighted that the greatest risk to a user of a Wi-Fi network is the possible capture of their internet traffic, either through passive eavesdropping while connected to a network, or through intentional capture via man-in-the-middle attacks. This led to the following questions, around which the evaluation method was devised:

1. Can an attacker connected to the Wi-Fi network capture the traffic of another user in plaintext?
2. Can an attacker, duplicating the Wi-Fi network, force another user to connect to them?

For a secure Wi-Fi network, the answer to these questions would be no. Identifying the answer to these could only be achieved through penetration testing. This led to the creation of the following test methods:

Table 1. Penetration test cases

	Test Case	Purpose	Techniques
1	Attempt to capture the traffic of users connected to a Wi-Fi network	Determine the ability of a Wi-Fi network to maintain the confidentiality of user data	While connected to a Wi-Fi network, listen for traffic from other users. Attempt to identify useful information from that network (i.e., usernames, passwords, bank details). The following tools were used during this test: - Wireshark - Aircrack-ng suite
2	Attempt to force users to connect to a duplicate Wi-Fi network	Determine the resistance of a Wi-Fi network to man-in-the-middle attacks	Create a Wi-Fi network which replicates the legitimate test network, Attempt to force users to connect to this network. The following tools were used during this test: - Hostapd - Aircrack-ng suite

While these tests can identify if a network is susceptible to a specific attack, it is limited in only allowing a binary answer to each test case (i.e., whether an attack of each type would be successful). As penetration tests are only able to capture a fraction of the techniques which could be used, this answer can't be extrapolated to say that the security method will always prevent such an attack, only that they can prevent an attack in the limited circumstances which were tested. By themselves, these tests cannot provide a means of identifying the relative efficacy of each security method. To provide this, a timing and complexity aspect was added to each test as a quantitative metric, whereby each test was timed and ranked by complexity of access. Complexity was determined by the amount of different tools and techniques which were required to achieve exploitation. Those tests which took longer, and were more complex, to complete were determined to be more secure. This criteria is supported by Abdullah and Singh, who discuss how the likelihood of an attack succeeding decreases as the time and complexity of the attack increases (2022). From this, the each public Wi-Fi security method was ranked according to the time and complexity taken for each test case to complete, with the quickest, least complex, tests highlighting the least secure methods, and the longest tests highlighting the most secure.

4 Design Specification

As stated above, the purpose of this research project is to identify a method of securing public Wi-Fi networks. This means that the method must possess three qualities:

1. **Accessibility:** All users who wish to connect to the network must be able to do so. Users cannot be known to the network prior to connection.
2. **Security:** As with other forms of cybersecurity, any security implementation for a public Wi-Fi network should attempt to provide confidentiality, integrity, and authenticity. Users who connect to the network must not have their data accessed by other users of that network, and it must not be possible for malicious users to modify that data.

3. **Verifiability:** It must be possible for users of a network to verify that the network to which they are connecting is legitimate, and not a malicious network masquerading as a real one.

The network must also assume that it is the only provider of security to devices on the network (i.e., no endpoint based security methods are in use). The design of the solution devised for this research aims to incorporate these features into a Wi-Fi authentication method.

5 Implementation

The implementation of this proposed solution is based on 802.1x certification for wireless networks (commonly found in WPA Enterprise networks). This was chosen based on its ability to provide end-to-end encryption between the client device and the access point, thus satisfying the criteria of providing security to users sharing a network with unmanaged devices. By removing the need for pre-shared keys, it also removes a possible attack vector, as there is no key which may be disclosed by human error. Within this method, there are four objects, with different attributes and functions that contribute to the method:

Table 2. System objects

	Attributes	Functions
Certificate Authority	<ul style="list-style-type: none"> • Root Certificate 	<ul style="list-style-type: none"> • Signs server and client certificates for RADIUS Servers and end users, respectively
End User	<ul style="list-style-type: none"> • Root certificate in certificate store • 802.1x client certificate signed by root CA 	<ul style="list-style-type: none"> • Connects to Wi-Fi network • Provides client certificate for authentication • Encrypts traffic between self and access point, using client certificate • Checks validity of server certificate
Access Point	<ul style="list-style-type: none"> • SSID 	<ul style="list-style-type: none"> • Provides Wi-Fi SSID • Receives end user connection request • Forwards request to RADIUS server • Accepts/reject network access based on results of authentication request • Encrypts traffic between each end user and self, using client certificate
RADIUS Server	<ul style="list-style-type: none"> • Root certificate in certificate store • 802.1x server certificate signed by root CA 	<ul style="list-style-type: none"> • Receives authentication request from access point • Checks validity of client certificate • Accepts/rejects authentication request

While this method allows for authentication of users with 802.1x certificates, it does not yet provide a means of distributing the root and client certificates to users of a public network. To facilitate this, a second access point and a web server are added to the environment, which allow users to register with the Wi-Fi network, after which they are provided with an executable file that installs a unique 802.1x client certificate, the root certificate, and configures a Wi-Fi profile on the users machine which automatically connects them to the primary Wi-Fi. This profile is also configured to only trust server certificates signed by the root CA, preventing an attacker from tricking a device into connecting to a replicated Wi-Fi network.

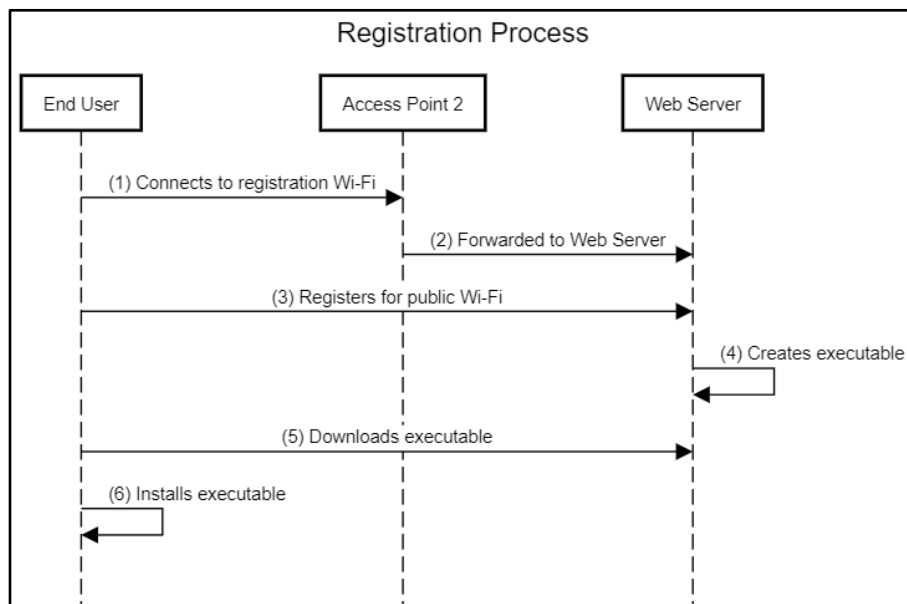
Table 3. Additional objects

	Attributes	Functions
--	------------	-----------

Access Point 2	<ul style="list-style-type: none"> • SSID 	<ul style="list-style-type: none"> • Allows users to connect and forwards them to web server • No other access is allowed
Web Server	<ul style="list-style-type: none"> • Registration application 	<ul style="list-style-type: none"> • Allows users to register • Creates executable for user which: <ul style="list-style-type: none"> ○ Installs unique 802.1x client certificate ○ Installs root certificate ○ Configures public Wi-Fi profile ○ Connects to public Wi-Fi

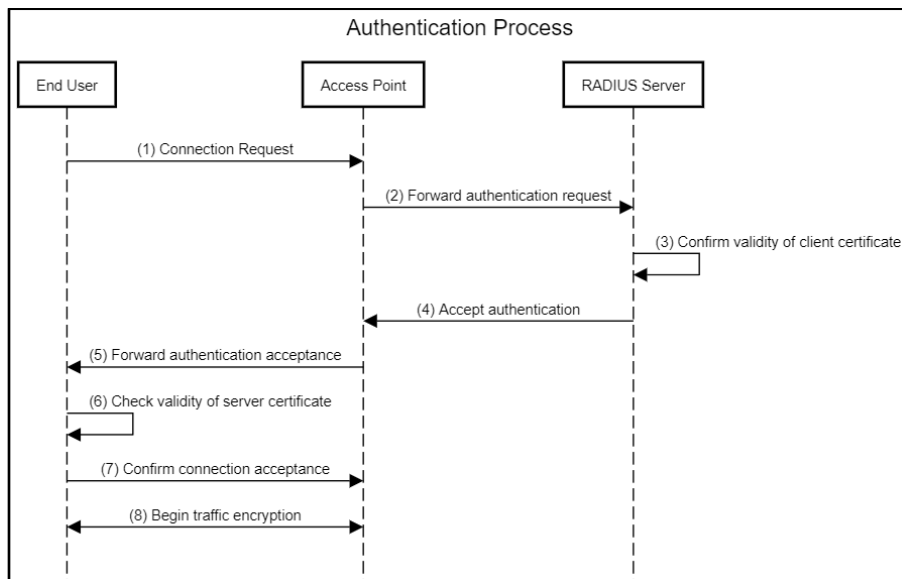
Once all the above objects exist in a network, the system will be able to register and authenticate users, without having prior knowledge of the users or their devices. The sequence for this will begin with the user registration process:

Figure 2. Registration process sequence diagram



Once this completes, the user will automatically attempt to connect to the public Wi-Fi network:

Figure 3. Authentication process sequence diagram



This solution was created using the following tools

Table 4. Tools used

Object	Device	Tools	Notes
Certificate Authority	Ubuntu 20.04	OpenSSL	Creation of root CA Creation of server CA
End User	Windows 10	N/A	N/A
Access Point	Zyxel D2000 Modem	N/A	Hosting of public Wi-Fi
Access Point 2	Ubuntu 20.04	Hostapd	Hosting of registration Wi-Fi
RADIUS Server	Ubuntu 20.04	FreeRadius 3.0	Authentication of users to public Wi-Fi
Web Server	Windows 11	Node.js + Express	Registration Application
		OpenSSL	Signing of client certificates
		WinRAR	Compiling of executable

This application is configured to only work with Windows devices. Porting to other devices was not completed during this project.

6 Evaluation

Evaluation of the proposed solution was determined by its security impact in comparison to existing methods of public Wi-Fi authentication. The methods chosen for comparison were based on their prevalence of use. The tests chosen were selected based on the existing research which identified them as possible attack points for public Wi-Fi networks. Other attacks were discounted from evaluation, as they were deemed to be irrelevant, or unapplicable to public Wi-Fi networks. For example, password cracking attacks were not examined, as public Wi-Fi networks are assumed to provide this password to all users, rendering it unnecessary for an attack to attempt its exploitation. Similarly, device-to-device exploitation on the network was not tested, as this involves security configuration on the target device itself, not the network. The following attack types were chosen for evaluation:

1. **Network eavesdropping:** An attacker attempts to intercept traffic on the network
2. **Evil Twin:** An attacker attempts to intercept the connection of a user on the network, by using a malicious access point

6.1 Case Study 1 – Network Eavesdropping

An attacking device (Linux Mint 21.1 with ASUS036NHA wireless adapter) was configured in monitor mode using the Aircrack-ng suite of tools. A target access point and connected device (Zyxel D2000 Modem and Windows 10 laptop) was configured to use five Wi-Fi authentication methods:

1. Unsecured
2. WEP-PSK
3. WPA2-PSK
4. Captive Portal

5. Digital Certificate Authentication

For each authentication method, the target device connected to a test HTTP application, while the attacking device attempted to intercept and read this traffic. Each method was timed, and the number of tools/techniques required was used to identify the complexity. Testing began by setting up the attacking device in monitoring mode, and identifying the target network, using Airodump-ng, as can be seen in figure 4.

Figure 4. Airodump-ng identifying Unsecure Wi-Fi network

```
File Edit View Search Terminal Help
CH 1 ][ Elapsed: 12 s ][ 2023-08-06 14:56

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
-----
54:83:3A:71:C6:9C -59 16         0  0  11 130  OPN                RePro-WiFi-NA
54:83:3A:71:C6:9C -59 39         2  0  6 195  WPA2 CCMP PSK                RePro-WiFi-NA
54:83:3A:71:C6:9C -59 14         4  0  11 130  WPA2 CCMP PSK                RePro-WiFi-NA
54:83:3A:71:C6:9C -59 24         0  0  6 360  WPA2 CCMP PSK                RePro-WiFi-NA
54:83:3A:71:C6:9C -59 35         1  0  6 360  WPA2 CCMP PSK                RePro-WiFi-NA
54:83:3A:71:C6:9C -59 3         3  0  1 130  WPA2 CCMP PSK                RePro-WiFi-NA

BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
-----
(not associated) 54:83:3A:71:C6:9C -49 0 - 1  0      2
(not associated) 54:83:3A:71:C6:9C -90 0 - 1  0      2
(not associated) 54:83:3A:71:C6:9C -53 0 - 1  7      5
(not associated) 54:83:3A:71:C6:9C -77 0 - 1  27     7
```

This identifies the SSID for the network (ESSID), the MAC address for the access point (BSSID), the channel on which it is broadcasting, and the encryption type. With this information, Airodump-ng is then used to listen exclusively on this network for target devices, shown figure 5. Airodump-ng was allowed to run for five minutes on each Wi-Fi network, while the target device accessed a HTTP application on the network.

Figure 5. Airodump-ng identifying clients on WEP Wi-Fi network

```
File Edit View Search Terminal Help
CH 1 ][ Elapsed: 3 mins ][ 2023-08-06 16:23

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
-----
54:83:3A:71:C6:9C -45 1      1883    3706  2  1  54e WEP WEP  OPN RePro-WiFi-WEP

BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
-----
54:83:3A:71:C6:9C E8:DE:27:39:C2:80 -42 54e-54e 1      4073                RePro-WiFi-WEP
```

This provided the baseline method for this case study. The setup time and five minute collection time did not count towards the ranking time. Once this was completed, the resulting capture was opened in Wireshark to inspect the targets traffic. Any network keys had already been added to Wireshark to perform decryption. The results for each method are discussed below.

6.1.1 Unsecured

On the unsecure Wi-Fi network, he targets traffic was immediately readable in Wireshark. No further tools or techniques were required. Upon viewing the HTTP traffic between the target and the test application was visible, from which it was possible to extract the session key, as seen in figure 6. This provided the following results:

Table 5. Unsecured Wi-Fi results

Unsecured Network	
Time taken	Complexity
0 seconds: - No extra time beyond the baseline setup required to read user data	0: - Only the baseline tools and techniques required to read user data

Figure 6. Cookie visible in Unsecured capture

```

> Frame 2346: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits)
> IEEE 802.11 QoS Data, Flags: ....R..T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.0.79, Dst: 192.168.0.40
> Transmission Control Protocol, Src Port: 63020, Dst Port: 80, Seq: 2208, Ack: 216461, Len: 474
  Hypertext Transfer Protocol
    GET /favicon.ico HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /favicon.ico
      Request Version: HTTP/1.1
      Host: 192.168.0.40\r\n
      Connection: keep-alive\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36\r\n
      Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
      Referer: http://192.168.0.40/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      Cookie: connect.sid=s%3ATCc0K817kkDdDgCaX9ke9Mrjedezi10.Ki0qeZ0LIvnd3XfI7KP%2FyQS2XuR%2Fq61IXCw%smymq2nw\r\n
      Cookie pair: connect.sid=s%3ATCc0K817kkDdDgCaX9ke9Mrjedezi10.Ki0qeZ0LIvnd3XfI7KP%2FyQS2XuR%2Fq61IXCw%smymq2nw\r\n
      [Full request URI: http://192.168.0.40/favicon.ico]
      [HTTP request 2/2]
  
```

6.1.2 Captive Portal

Captive portal networks behave similar to Unsecured networks, in that no encryption occurs between the client and the access point. The only security measure is MAC address filtering, which is used to restrict access through the access point to the internet. Thus, the results were the same as for the Unsecured Wi-Fi network, whereby the captured traffic was immediately visible in Wireshark, with no modification required, allowing for visibility on HTTP traffic which traversed the network.

Table 6. Captive Portal Wi-Fi results

Unsecured Network	
Time taken	Complexity
0 seconds: - No extra time beyond the baseline setup required to read user data	0: - Only the baseline tools and techniques required to read user data

6.1.3 WEP-PSK

Unlike the previous networks, when the traffic capture was opened in Wireshark, it was not immediately readable, as seen in figure 7. Since the traffic was encrypted using the WEP pre-shared key, this was required to decrypt it. This was possible using Wireshark’s in-built decryption feature, which used the known key to decrypt the traffic. Following this, the targets traffic was made readable, resulting in the capture of the users session key, and also their input to a login form. This gave access to the username and password which the target had input to that form, seen in figure 8.

Table 7. WEP Wi-Fi results

Unsecured Network

Time taken	Complexity
0 seconds: - No extra time required beyond the baseline setup, as keys had already been added to Wireshark	1: - Required use of Wireshark's decryption

Figure 7. Encrypted WEP traffic

1 0.000000	ZyxelCom_71:c6:9c	Broadcast	802.11	143	Beacon frame, SN=3979, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
2 2.395888	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4003, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
3 2.396007		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
4 2.397501	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4004, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
5 2.397617		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
6 2.402537	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4005, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
7 2.402568		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
8 2.426786	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4006, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
9 2.426818		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
10 2.428356	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4007, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
11 2.428391		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
12 2.429989	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4008, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
13 2.430022		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
14 2.731888	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4012, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
15 2.731921		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
16 2.733718	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4013, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"
17 2.733771		ZyxelCom_71:c6:9c (-	802.11	10	Acknowledgement, Flags=.....
18 2.735032	ZyxelCom_71:c6:9c	Tp-LinkT_39:c2:80	802.11	127	Probe Response, SN=4014, FN=0, Flags=....., BI=100, SSID="RePro-WiFi-WEP"

Figure 8. Username and password detected in Wireshark

```
> Cookie: connect.sid=s%3Axh2-pkpHbvGPw4mIdYhLCqtHAKUWznw2.v2as7V6Mrjww0Pic88FobEU%2BrAoktRg1z7eKhumYErAr\n
\n
[Full request URI: http://192.168.0.40/users/login]
[HTTP request 2/4]
[Prev request in frame: 5303]
[Response in frame: 5425]
[Next request in frame: 5431]
File Data: 29 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "admin"
> Form item: "password" = "admin"
```

6.1.4 WPA2-PSK

As with the WEP encrypted network, viewing the traffic capture from the WPA2 protected network is Wireshark will only display encrypted 802.11 packets between the target device and the access point. Inputting the pre-shared key for the network into Wireshark also does not decrypt the traffic, as WPA2s security mechanisms create an encryption key at the start of the connection process, using a 4-way EAPOL handshake. Since the target had already connected prior to monitoring, this 4-way handshake was not captured. To force this, a deauthentication attack was conducted against the target device, using Aireplay-ng. This forced the target to deauthenticate from the WPA2 Wi-Fi network and reauthenticate. The reauthentication allowed the attacker to capture the 4-way handshake. However, this required multiple attempts, as each step of the 4-way handshake is required for decryption (see figure 9), and not all steps were captured at each attempt. Once a complete handshake was detected, Wireshark was again used, at which point all traffic following the handshake was readable, including HTTP traffic to the test application, which again revealed the users session cookie.

Table 8. WPA2 Wi-Fi results

Unsecure Network	
Time taken	Complexity
15 minutes: - Four attempts of monitoring the target network required	3: - Required use of Aireplay-ng to force reauthentication

to capture full EAPOL handshake	<ul style="list-style-type: none"> - Required multiple use of Airodump-ng packet captures - Required use of Wireshark's decryption
---------------------------------	--

Figure 9. 4-Way EAPOL Handshake

No.	Time	Source	Destination	Protocol	Length	Info
52	7.512898	ZyxeCom_71:c6:9c	Tp-LinkT_39:c2:80	EAPOL	133	Key (Message 1 of 4)
54	7.514765	Tp-LinkT_39:c2:80	ZyxeCom_71:c6:9c	EAPOL	155	Key (Message 2 of 4)
56	7.517761	ZyxeCom_71:c6:9c	Tp-LinkT_39:c2:80	EAPOL	189	Key (Message 3 of 4)
58	7.519474	Tp-LinkT_39:c2:80	ZyxeCom_71:c6:9c	EAPOL	133	Key (Message 4 of 4)

6.1.5 Digital Certificate Authentication

As with WEP and WPA2 Wi-Fi networks, captured traffic from the Digital Certificate authentication network is encrypted when initially viewed. However, since there is no key shared to the user (as the network uses 802.1x certificates instead of a pre-shared key), there is no key which can be added to Wireshark for decryption. Instead the key is shared between the access point and the client through EAP-TLS, following which the 4-way EAPOL handshake occurs, which can be seen in figure 10. This prevents an attacker from decrypting the traffic through Wireshark, and reduces the risk for the client that their traffic can be made visible to others.

However, it must be noted that the failure of this test to successfully exploit the network means that it is not possible to exploit it. This only demonstrates that common Wi-Fi penetration test techniques are unsuccessful against this network. Other methods may be available which do allow target devices to be compromised. As these were not discussed in relevant literature, they were not attempted here.

Table 9. Digital Certificate Authentication Wi-Fi results

Unsecure Network	
Time taken	Complexity
N/A: - Unable to compromise network through eavesdropping	N/A: - Unable to compromise network through eavesdropping

Figure 10. Captured certificate and EAPOL handshakes

TLSv1.2	1002	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
TLSv1.2	1321	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2	101	Change Cipher Spec, Encrypted Handshake Message
EAP	44	Response, TLS EAP (EAP-TLS)
EAP	44	Success
EAPOL	133	Key (Message 1 of 4)
EAPOL	155	Key (Message 2 of 4)
EAPOL	189	Key (Message 3 of 4)
EAPOL	133	Key (Message 4 of 4)

6.1.6 Results

From the tests performed, it is possible to rate various security methods according to their resistance to eavesdropping attacks. It can be seen that digital signature authentication performs

better against known penetration attacks in preventing attackers from eavesdropping clients attached to it. This does not mean that Digital Certificate Authentication will always prevent such attacks, only that it is more resistant to known attack types than existing methods of public Wi-Fi security.

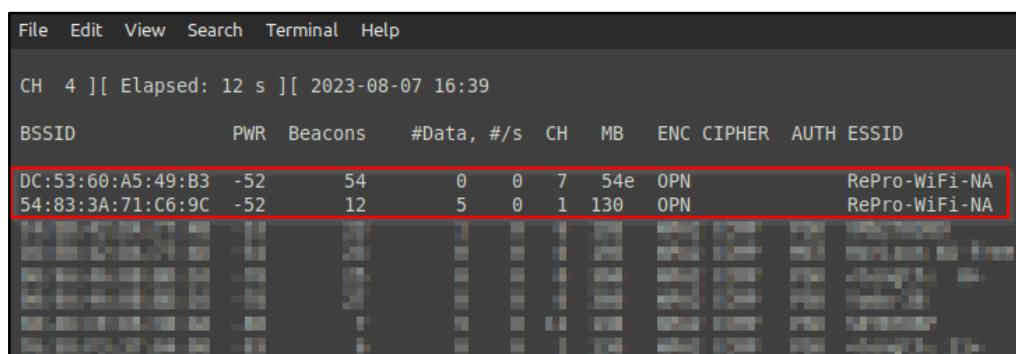
Tables 10. Results of Network Eavesdropping test

Authentication Method	Time take to exploit	Complexity required to exploit
Unsecured	0 seconds	0
Captive Portal	0 seconds	0
WEP-PSK	0 seconds	1
WPA2-PSK	15 minutes	3
Digital Certificate Authentication	Exploit unsuccessful	Exploit unsuccessful

6.2 Case Study 2 – Evil Twin

The initial setup for this test involved an attacking device (Linux 21.1) with Hostapd installed. Hostapd was configured to replicate each of the target networks, using the same authentication methods. As this is replicating a public Wi-Fi network, it is assumed that an attacker would be aware of the authentication method and any pre-shared keys required to access it. Once this was configured and the attacking device was in range of a target client, the attacker sent out deauthentication requests to the target client, using Aireplay-ng, to try and force it to connect to the attacker. The test was completed once a client had connected to the attacking device and began using it for internet access. Once this occurred, Wireshark was used to inspect the targets traffic.

Figure 11. Legitimate network and malicious duplicate



For each comparison network (Unsecured, Captive Portal, WEP-PSK, and WPA2-PSK), once the malicious duplicate network was configured using the SSID of the target network, and pre-shared key if applicable, it was possible to trick the target device into connecting once the deauthentication requests were sent. The target device then immediately attempted to reconnect to the Wi-Fi network, connecting instead to the malicious network thinking it was the legitimate one. All traffic passing through the malicious network was then visible, regardless of the authentication method used. This indicates the vulnerability of public Wi-Fi networks to Evil Twin attacks, as attackers will have free access to all information required to successfully replicate the network (SSID and pre-shared key), without incurring any issues from a target device.

Extra steps were required when attempting to create a duplicate of the Digital Certificate Authentication method, as this uses a RADIUS server for authentication. It was then necessary

to deploy another instance of FreeRadius on the attacking device, and configuring it to authenticate clients via certificate. This also required the capture of the certificate from the TLS handshake, seen in figure 10, to create a new root CA using the same parameters as those found in the legitimate network. This was done to better replicate the server certificate. Once the RADIUS server was deployed and Hostapd configured to forward authentication requests, Aireplay-ng was used again to deauthenticate the target device. However, while the deauthentication was successful and the target attempted to connect to the malicious network, the connection failed (see figure 12). When investigated on the target device, it could be seen that the failure occurred due to the target rejecting the certificate from the malicious network, as seen in figure 13. Because the network configures a profile for each user specifying the certificate which can be trusted, it was not possible for an attacker to replicate it by copying the parameters from the original certificate. Similar to the eavesdropping test, this does not indicate that the Digital Certificate Authentication method of public Wi-Fi security will resist exploitation, only that it performs better against common attack types.

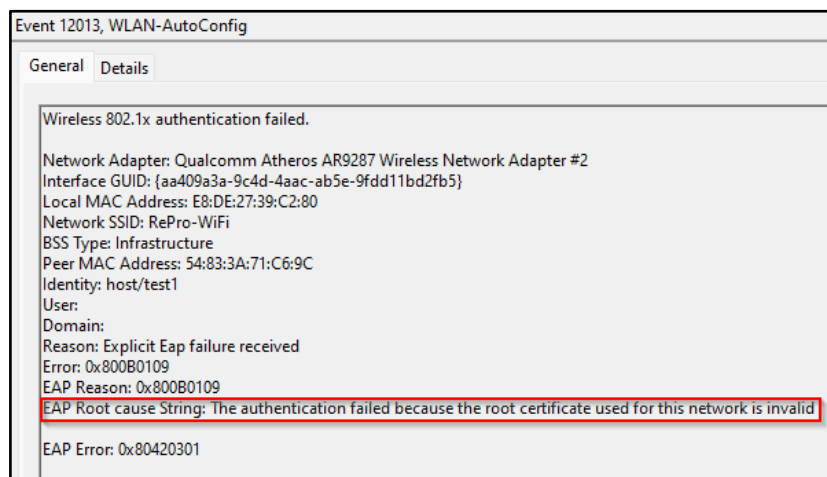
Figure 12. Hostapd authentication failure

```

File Edit View Search Terminal Help
niall@mintbox:~$ sudo hostapd /home/niall/RP/hostapd dca.conf
hotspot1: RADIUS Authentication server 192.168.0.72:1812
hotspot1: interface state UNINITIALIZED->ENABLED
hotspot1: AP-ENABLED
hotspot1: STA e8:de:27:39:c2:80 IEEE 802.11: authenticated
hotspot1: STA e8:de:27:39:c2:80 IEEE 802.11: associated (aid 1)
hotspot1: CTRL-EVENT-EAP-STARTED e8:de:27:39:c2:80
hotspot1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
hotspot1: CTRL-EVENT-EAP-FAILURE2 e8:de:27:39:c2:80
hotspot1: STA e8:de:27:39:c2:80 IEEE 802.1X: authentication failed - EAP type: 1
3 (TLS)
hotspot1: STA e8:de:27:39:c2:80 IEEE 802.11: deauthenticated due to local death
request
^Chotspot1: interface state ENABLED->DISABLED
hotspot1: AP-DISABLED
hotspot1: CTRL-EVENT-TERMINATING

```

Figure 13. Client rejection of malicious network



As with eavesdropping attacks, each method was ranked according to the time and complexity required to successfully exploit it. The initial setup of Hostapd with the SSID and pre-shared key of the network were not counted. It can be seen from these results that the

Digital Certificate Authentication method performed better than common public Wi-Fi security methods when an Evil Twin attack was performed each network.

Table 11. Evil Twin attack results

Security Method	Time taken to exploit	Complexity of exploit
Unsecured/ Captive Portal/ WEP-PSK/ WPA2-PSK	5 seconds: <ul style="list-style-type: none"> - Target connected to malicious network once deauthentication attack sent. 	1: <ul style="list-style-type: none"> - Required deauthentication attack from Aireplay-ng to force target to connect
Digital Certificate Authentication	N/A: <ul style="list-style-type: none"> - Unable to compromise network via Evil Twin attack 	N/A: <ul style="list-style-type: none"> - Unable to compromise network via Evil Twin attack

6.3 Discussion

From the tests conducted above, it is possible to compare the security of the proposed public Wi-Fi authentication solution against the most commonly used authentication solutions. The results in table 12 show the relative efficacy of each solution at protecting against attacks which are likely to be conducted against public networks (5 being the most secure, and 1 being the least). As could be assumed, unsecured networks provide no protection for users. Traffic is clearly visible to anyone monitoring traffic on that network. This is also the case with Captive Portal, whose method of authentication only prevents internet access, but no defence for other users of the network. Pre-shared key methods do at least encrypt traffic between the user and access point, but as the sharing of keys is inherent in the concept of a public Wi-Fi network, it is trivial for an attacker to bypass this and decrypt the traffic of other users. When an Evil Twin attack was conducted against these networks, all common solutions failed to be effective, as none provide a means for users of the network to verify the identity of the access point.

Rating	Security Method	Results
5	Digital Certificate Authentication	<ul style="list-style-type: none"> - Per-client certificate based encryption provides users with an individually encrypted tunnel, preventing other users from reading traffic. Lack of pre-shared key means attacker have no access to encryption keys - Certificates allow clients to verify identity of Wi-Fi network, reducing risk of an Evil Twin attack
4	WPA2-PSK	<ul style="list-style-type: none"> - Traffic is encrypted using WPA2 algorithms, but availability of key renders it easy to decrypt. Requirement of an attacker to capture EAPOL handshakes is a slight improvement over WEP - No means of allowing users to verify identity of access point
3	WEP-PSK	<ul style="list-style-type: none"> - Traffic is encrypted using WEP algorithms, but availability of key means all traffic will be at risk of decryption by malicious users - No means of allowing users to verify identity of access point
1	Captive Portal	<ul style="list-style-type: none"> - No encryption between user and access point. Traffic is clearly readable anyone monitoring network - No means of allowing users to verify identity of access point
1	Unsecured	<ul style="list-style-type: none"> - No encryption between user and access point. Traffic is clearly readable anyone monitoring network - No means of allowing users to verify identity of access point

This suggests the solution proposed as part of this project, the application of Digital Certificate Authentication for public Wi-Fi networks, performs better under the sample penetration tests. This does not indicate that the solution has no vulnerability to such attacks,

as there are many methods by which they could be achieved that were not possible to cover as part of this project. Instead, it demonstrates that it can reduce the risk of a successful attack when conducted with well known methods, when compared with other solutions currently available for public Wi-Fi protection.

7 Conclusion and Future Work

The purpose of this research project was to identify the security issues which are present in public Wi-Fi networks, and propose a method of securing such networks against those weaknesses. The difficulty with securing public Wi-Fi networks is the lack of focus given to the dangers they present to users, with the ability for attackers to intercept traffic across those networks. Solutions to this have been created, but are only ever applied to private networks and WLANs. This is because of the perceived difficulty in managing access for unmanaged devices. However, this project has shown that it is possible to provide better authentication solutions for public Wi-Fi networks, thereby granting users of these networks a product on which their data is at less risk of being compromised. The research conducted to compare the security impact of this solution against other methods of public Wi-Fi security was limited, in that it merely provides a sample of penetration tests which could be conducted against Wi-Fi networks. Further research would be able to produce a more in-depth assessment of Wi-Fi security. However, while existing research indicates that penetration tests are currently the most effective means of assessing the security of a Wi-Fi network, they are not as suitable for collecting measurable data, as the scope and variation required for each attack prevents standardised comparison between different security methods. More time could be given simply to identifying a more effective means of measuring Wi-Fi security.

Finally, the solution created for this project could be improved with more time. Primarily, a next step would be to allow it to extend its capabilities to devices beyond Windows. It is likely that smartphones would provide a significant proportion of users of public Wi-Fi networks, so the solution's extension to Android and iOS devices would be useful. The registration Wi-Fi network could also be integrated into the access network, reducing the need for a second access point. It may also be possible to combine each aspect of the network into a single device, allowing network administrators to deploy public Wi-Fi networks without requiring the configuration and management of backend servers. This would produce a more compact solution, and potentially allow for commercial viability. The main outcome from this research, though, is to underscore the significant weaknesses present in current public Wi-Fi solutions, and the danger they pose to users. While cybersecurity requires a multi-layered approach, Wi-Fi networks present an obvious vector for attackers, and more attention could be paid to securing such networks.

Link to Video Presentation

https://youtu.be/wiA2feT_KO4

References

- Abdullah and Singh, J., (2022), April. Security Metrics and Applications for the Information and Communications Technology Industry. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 480-486). IEEE.
- Abo-Soliman, M.A. and Azer, M.A., (2017), December. A study in WPA2 enterprise recent attacks. In *2017 13th International Computer Engineering Conference (ICENCO)* (pp. 323-330). IEEE.
- Alhamry, M. and Alomary, A., (2022), October. Exploring Wi-Fi WPA2-PSK protocol weaknesses. In *2022 International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 190-195). IEEE.
- Ali, S., Osman, T., Mannan, M. and Youssef, A., (2019). On privacy risks of public wifi captive portals. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14* (pp. 80-98). Springer International Publishing.
- Astrida, D.N., Saputra, A.R. and Assaufi, A.I., (2022). Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sinkron: jurnal dan penelitian teknik informatika*, 7(1), pp.147-154.
- Bartoli, A., Medvet, E., De Lorenzo, A. and Tarlao, F., (2018), August. (in) secure configuration practices of wpa2 enterprise supplicants. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1-6).
- Choi, H.S., Carpenter, D. and Ko, M.S., (2021). Risk taking behaviors using public Wi-Fi™. *Information Systems Frontiers*, pp.1-18.
- Duc, H.B., Pocarovsky, S., Orgon, M. and Koppl, M., (2021). Penetration Testing of WiFi Networks Secured by WEP and WPA/WPA2 Protocols. In *Informatics and Cybernetics in Intelligent Systems: Proceedings of 10th Computer Science On-line Conference 2021, Vol. 3* (pp. 571-585). Springer International Publishing.
- Fikriyadi, F., Ritzkal, R. and Prakosa, B.A., (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, 4(3), pp.1658-1662.
- Hoseini, S.A., den Hartog, F. and Bouhaf, F., (2023), January. Realizing Physical Layer Security with common off-the-shelf WiFi equipment. In *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)* (pp. 935-936). IEEE.
- Khasawneh, M., Kajman, I., Alkhudaidy, R. and Althubayani, A., (2014). A survey on Wi-Fi protocols: WPA and WPA2. In *Recent Trends in Computer Networks and Distributed Systems Security: Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings 2* (pp. 496-511). Springer Berlin Heidelberg.
- Lu, H.J. and Yu, Y., (2021). Research on WiFi penetration testing with Kali Linux. *Complexity*, 2021, pp.1-8.
- Lugovic, S., Mrcic, L. and Korona, L.Z., (2019). Public WiFi security network protocol practices in tourist destination. In *Pervasive Systems, Algorithms and Networks: 16th International Symposium, I-SPAN 2019, Naples, Italy, September 16-20, 2019, Proceedings 16* (pp. 321-332). Springer International Publishing.
- Maimon, D., Howell, C.J., Jacques, S. and Perkins, R.C., (2020). Situational awareness and public Wi-Fi users' self-protective behaviors. *Security Journal*, pp.1-21.

- Marques, N., Zúquete, A. and Barraca, J.P., (2019). Integration of the Captive Portal paradigm with the 802.1 X architecture. *arXiv preprint arXiv:1908.09927*.
- Moissinac, K., Ramos, D., Rendon, G. and Elleithy, A., (2021), January. Wireless encryption and WPA2 weaknesses. In *2021 IEEE 11th Annual computing and communication workshop and conference (CCWC)* (pp. 1007-1015). IEEE.
- Noman, H.A., Noman, S.A. and Al-Maatouk, Q., (2019). Wireless Security In Malaysia: A Survey Paper. *Journal Of Critical Reviews*, 7(4), p.2020.
- Radivilova, T. and Hassan, H.A., (2017), September. Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise. In *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)* (pp. 1-4). IEEE.
- Ramos, A., Lazar, M., Holanda Filho, R. and Rodrigues, J.J., (2017). Model-based quantitative network security metrics: A survey. *IEEE Communications Surveys & Tutorials*, 19(4), pp.2704-2734.
- Sahu, T.C. (2022) ‘Security and Privacy of Public WiFi’, *International Journal of Research Publication and Reviews*, 3(11), pp. 918–925.
- Schepers, D., Ranganathan, A. and Vanhoef, M., (2021), June. Let numbers tell the tale: measuring security trends in wi-fi networks and best practices. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 100-105).
- Song, L., Wang, Q., Jia, S., Lin, J., Lu, L. and Fu, Y., (2022), December. You Cannot Fully Trust Your Device: An Empirical Study of Client-Side Certificate Validation in WPA2-Enterprise Networks. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 266-273). IEEE.
- Sonola, F., (2022), Hidden Cyber Security Risks: Why you Should Exercise Caution When Using Public Wi-Fi, *Research Gate*
- Wahyudi, E., Luthfi, E.T., Efendi, M.M. and Mataram, S.T.M.I.K., (2019). Wireless penetration testing method to analyze WPA2-PSK system security and captive portal. *Jurnal Explore STMIK Mataram*, 9(1).
- Zou, Y., Zhu, J., Wang, X. and Hanzo, L., (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), pp.1727-1765.