Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

RESEARCH ARTICLE

An Exploration of Cyber-Security in Free Public Wi-Fi Networks

Markos Markou* | Andriani Piki

[1] Dept. Business Computing, P.A. College, Larnaca, Cyprus

Correspondence
*Markos Markou, Corner Faneromenis & Kalvou str., 6307, Larnaca, Cyprus. Email: m.markou@faculty.pacollege.ac.cy

Abstract

Information security is considered both an evolving field and a key concern in the modern mobile society. This research explores the vulnerabilities of public, free Wi-Fi hotspots, how their security can be compromised, and the perceptions of end-users, network administrators/owners and information security experts on cyber-security. Primary data was gathered through interviews with these three groups of stakeholders. An experimental test was also set up in a controlled environment to perform penetration testing. The goal of the experimental test was two-fold: to verify whether it is indeed practically possible to exploit the vulnerabilities of public Wi-Fi networks and to assess the level of difficulty for achieving this. The gathered insights were critically evaluated against the literature towards exploring the state of cyber-security in Cyprus. The findings from the thematic analysis of the interviews reaffirm what the literature suggests with regards to users' and owners' lack of awareness and technical skills. Additionally, convenience and cost were cited as major factors explaining why strict security measures are not deployed by small businesses. Coupled with these findings, the experimental test revealed the ease and speed with which public Wi-Fi networks can be compromised.

KEYWORDS:
case study, Cyber-security, infromation security awareness

1 | INTRODUCTION

The Internet has become a mission critical constituent for companies of all sizes in every industry, mainly due to the unique features which render the Web a successful commercial medium[1]. Many individuals also rely greatly on the Internet and the use of Web services for performing professional, social, and personal activities[2]. However, the prevalence of insecure, open, Wi-Fi networks in public venues increases the possibility of being hacked. "As a result, users transmitting sensitive data, like authentication credentials, over such networks, risk having their data intercepted and exposed."[3, p. 205]. Behind the evident advantages of communications networks to businesses and consumers alike, there is the prevailing presence of attackers attempting to infringe users' privacy. Given the frequency and variety of existing cyber-attacks, as well as the threat of new and more destructive future attacks, network security has become a central topic in the field of computer networking[2]. Consequently, there is a genuine need to investigate the latest technological advancements as well as the vulnerabilities in the field of network security and how hackers can exploit them; to explore the potential impact these vulnerabilities may have on users and administrators/owners of public, free Wi-Fi networks; as well as get insights on the state of cyber-security awareness, specifically in Cyprus. In the context of our study the terms administrator and owner are used interchangeably as in most cases the owner of the small business was also the administrator of the Wi-Fi hotspot.

The inspiration behind the current study was the recurrent observation that individuals of all ages and educational levels spontaneously connect to free Wi-Fi networks available at various public venues including cafeterias, restaurants, universities, bus stops, and hotel lobbies, amongst others. Given the rising number of available free Wi-Fi hotspots, performing research in the field of cyber-security was presented as an appealing and significant opportunity. The main aim of the study is to conduct exploratory research on cyber-security in the context of Cyprus focusing on the use of free, public Wi-Fi networks. At the outset, a review of relevant literature is presented on the broader field of information security, cyber-security and hacking. The literature survey is followed by employing a hybrid methodological framework for gathering and analysing data from experts, owners, and users of free public Wi-Fi networks in Cyprus, combined with hands-on experience gained through an experimental test. The proposed methodological approach constitutes an element of originality as it successfully fuses qualitative, interpretivistic exploration with experimental testing. This study attempts to fill the gap that exists with regards to conducting qualitative research in computing-related fields[4]. Subsequently, the analysis of the data gathered is presented along with a thorough discussion of the key findings in relation to existing literature. Finally, the social/pedagogical, and business-oriented implications stemming from this study are outlined. The importance of this study lies in its attempt to make decision makers, owners, business managers and individuals that either use or administer public hotspots more aware of the dangers involved.

2 | LITERATURE REVIEW

The terms cyber-security, information security, and Internet or network security are often used interchangeably. Network security is a continuously evolving computing field concerned with "how the bad guys can attack computer networks and about how [...] experts in computer networking, can defend networks against those attacks, or better yet, design new architectures that are immune to such attacks in the first place"[2, pp. 81–82]. Historically, the evolution of Information and Communication Technologies (ICTs) and Information Systems (ISs) has always been accompanied by even more advanced infringing mechanisms implemented by black hat hackers – the 'bad guys'. Their target is to gain unauthorised access to Internet-connected devices (including desktop and laptop computers, tablets and smartphones), hence violating users' privacy and rendering inoperable the

Internet services on which users depend[2]. In recent years, information and network security has been established as a highly paid, respected, technical profession as a result of the increasing concerns of individual users and businesses with respect to their private data when using the Internet. Given that "there are many facets to security"[2, p. 698], both users and owners need to take the necessary precautions; the former by becoming more knowledgeable, and the latter by realising what it takes to identify their company's potential security vulnerabilities, before these vulnerabilities are discovered and exploited.

A gap identified in the available literature in the field of cyber-security is the lack of empirical and theoretical studies performed in the context of Cyprus. In particular, there is insufficient information in the literature about the level of awareness of Cypriot users and administrators with regards to security issues making it difficult to extract an informed conclusion. Hence, it is apparent that hacking and cyber-security constitute an interesting field that needs to be further researched. Delving into this field involves initially exploring what constitutes a secure network, understanding what makes a computer network vulnerable by identifying the most prevalent types of attacks plausible today, considering how to secure networks from potential attacks, as well as investigating common procedures followed by hackers to perform these attacks. The following paragraphs explore these aspects through the available literature.

2.1 | Properties of a Secure Network

A secure network is one which supports safe, protected communication between Internet-connected users. Principally, any form of network communication needs to satisfy the following four desirable properties in order to be considered secure: confidentiality, message integrity, end-point authentication, and operational security[2]. The principle of confidentiality is satisfied if the contents of the message transmitted through a network are understandable only by the sender and intended receiver. Due to the potential presence of eavesdroppers, securing confidentiality requires that the message be encrypted so that an intercepted message cannot be understood by an interceptor[2]. Numerous cryptographic and encryption techniques exist for encrypting and decrypting data[5,2].

Achieving message integrity involves ensuring that when two users communicate the content of their message is not altered either maliciously or accidentally, while in transit through numerous routers, switches, and other networking devices. Various techniques are built into reliable transport and data link protocols to provide such message integrity[2,6]. Additionally, the process of end-point authentication is necessary so that both the sender and the receiver are able to confirm each other's identity and that they are indeed who or what they claim to be[2]. Routing protocol authentication mechanisms can be used in order to confirm or verify the identity of the users/devices[7,6].

Finally, in addition to finding ways to secure Internet-based communications and defend a network, it is essential to ensure that the network is accessible by and available to legitimate users, and that it operates properly in the first place. A vast majority of businesses, organisations and institutions today – both in Cyprus and internationally – offer Wi-Fi networks to their customers

TABLE 1 Common attacks and countermeasures

Type of attack	Countermeasures
Man-in-the-Middle	Strong encryption between client and server, static ARP table, enterprise grade firewall.
Packet sniffing	Encryption.
DNS redirection	Use of firewall.
Pharming/Phishing	Being vigilant while online. Avoid sharing sensitive information (passwords, e-banking accounts, PIN numbers, etc.) on dubious websites. URL filtering. Use of anti-phishing tools.
Malware	Antivirus and anti-spam software, firewall, IDS, disable Adobe Flash and JavaScript in browsers, ensure good internet practices.
Session hijacking	Use only SSL encrypted webpages.
Denial of Service	Enterprise grade router, other specialised hardware or software, IDS, IPS.
IP spoofing	Properly configured router and firewall.

and employees which can be potentially compromised. Hence, operational security is of pivotal importance. Attackers may attempt to deposit worms into the network, obtain corporate secrets, infringe internal network configurations, and launch Denial of Service (DoS) attacks. Various operational network devices, such as firewalls and Intrusion Detection Systems (IDS) can be used to mitigate attacks against an organisation's network.

2.2 | Types of Attacks and Countermeasures

Computer networks in general and wireless networks in particular are susceptible to a wide range of network attacks. Some of the most prevalent and damaging classes of attacks include the Man-in-the-Middle (MitM) attack, packet sniffing, Domain Name System (DNS) redirection, phishing and pharming, malware infections, session hijacking, DoS attacks, and IP spoofing. Table 1 summarises these types of attacks and outlines some common practices either network owners or end-users can employ to counteract these attacks. Additional countermeasures have also been proposed in the literature including the recognition of authorised wireless NICs on a network through spectral analysis during active scanning[8]. However, methods such as this assume a controlled network environment like those deployed in enterprises, and therefore cannot be applied in public free Wi-Fi networks like the ones considered in our study.

The common denominator in most network attacks is known as MitM attack[9]. During a MitM attack, users are tricked into thinking that there is direct and safe communication between the legitimate receiver and sender devices when in fact, all communication passes through the hacker's device. As a consequence, the communication can be scrutinised by the hacker. Prior to showing how a MitM attack can be performed, it is necessary to explain how communication between two devices occurs on an Ethernet network. All devices on a network have two addresses; one permanent, hardware address assigned by the manufacturer (called a MAC address) and an address assigned by the network (called an IP address). Both addresses are necessary for the

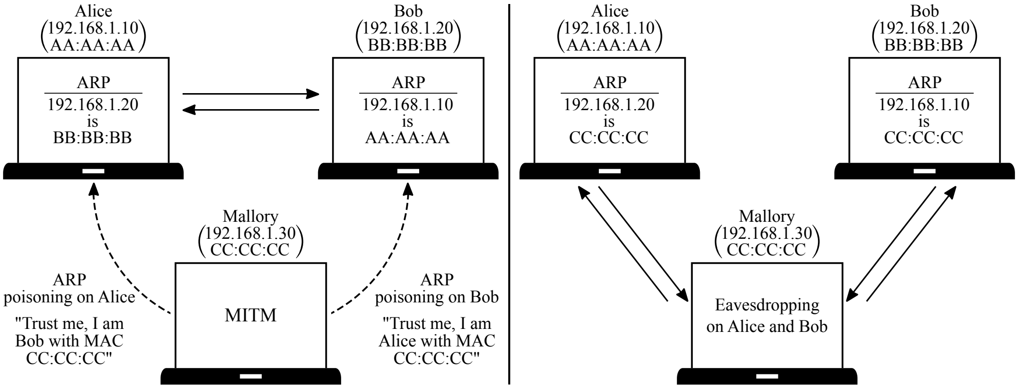

FIGURE 1 Man-in-the-Middle attack (MAC addresses are simplified for illustration purposes).

devices to communicate. When the sender (device D_1) wants to communicate with the receiver (device D_2), the sender must first translate the IP address of the receiver to the corresponding MAC address. However, this information is initially unknown so the sender asks all devices on the network ‘who owns x.x.x.x IP address?’ and accepts the response as being accurate. Furthermore, once a response arrives, it is saved for future reference in a local database called Address Resolution Protocol (ARP) table[2, pp. 491–494].

A MitM attack exploits the inherent weaknesses of this protocol. Figure 1 illustrates how a typical MitM attack is launched. Alice (IP: `192.168.1.10`, MAC: `AA:AA:AA`) wants to communicate with her friend Bob (IP: `192.168.1.20`, MAC: `BB:BB:BB`). Alice knows Bob’s IP address, and initiates the communication. However, Bob’s MAC address is also required for the actual transfer of data. Consequently, her device consults its ARP table, determines that Bob’s MAC address is `BB:BB:BB` and the data transfer begins. On the other end, Bob accepts the incoming connection from Alice and, after consulting the ARP table establishes an outgoing connection with Alice’s device. Mallory (IP: `192.168.1.30`, MAC: `CC:CC:CC`) is an attacker initiating a MitM routine. First, Mallory performs ARP poisoning on Alice’s device, essentially tricking Alice into thinking that Mallory’s MAC address corresponds to Bob’s IP address. Following that, Mallory plays the same trick on Bob’s device. Now, when both Alice and Bob consult their ARP tables before establishing a connection with each other, their device will erroneously report Mallory’s MAC address as their respective recipient, thus placing Mallory in the middle of their communication.

Once attackers succeed in performing the MitM routine, open source and freely available tools (e.g. Ettercap, sslstrip, driftnet, urlsnarf) can be employed to steal security credentials[10]; monitor users’ actions on the network; redirect web traffic; or perform a combination of these. ‘Ettercap’ is an easily obtainable software, featuring a point-and-click interface that automates the MitM attack and does not require any special training or knowledge to use. The benefits of performing this type of attack by hackers are numerous, including intercepting private communications, transforming secure communications to insecure and redirecting traffic from legitimate devices to illegitimate ones. In addition to automating the MitM attack, ‘Ettercap’ can also be used to extract username and password combinations from unencrypted connections such as those made to FTP or telnet servers.

Even though it is considered common knowledge that unencrypted communication is vulnerable to various types of attacks and encrypted is totally safe, in reality encrypted connections are not immune to a MitM attack either[3]. Specifically, secure SSL connections can be rendered insecure by simply replacing the HTTPS protocol with its insecure counterpart, the HTTP protocol[9,10]. The open source software ‘sslstrip’ can be employed to easily perform this[9]. Victims of ‘sslstrip’ may suspect that something is wrong if they happen to notice that the web address in their browser was changed from an HTTPS connection to an HTTP (e.g. http://secure.com instead of https://secure.com). URL filtering can be used as a countermeasure by filtering and constraining the URLs that a user can visit[11]. In addition to ‘Ettercap’ and ‘sslstrip’, tools like ‘driftnet’ can be used to collect any or all images victims view in their browsers, while ‘urlsnarf’ can be used to save all web addresses that victims have visited and to monitor the actions and behaviour of the targeted devices.

Although safeguarding a network against MitM attacks is not trivial, it can be achieved by using specialised, expensive enterprise grade firewalls that prevent ARP poisoning. A cheaper alternative is to disable the use of dynamic ARP tables and rely instead on statically mapping the IP to MAC address of all devices on the network manually. This solution, however, becomes impractical with large networks or when unknown devices need to connect to the network temporarily. Unfortunately, this is exactly the case in public Wi-Fi networks, like the ones considered in our study. Finally, it should be noted that the use of strong encryption, and making sure that the encryption protocol is in place (i.e. HTTPS connections are used), can prevent the attacker from gaining any meaningful information from the communicating parties, even if a MitM attack might have been successful. Another means of detecting eavesdroppers on a network is the use of ‘honeypots’ and ‘honeytokens’ enticing potential attackers to access decoy servers and documents[3].

Following the successful implementation of the MitM attack, an eavesdropper can also monitor users’ communication through packet sniffing[9,10]. Packet sniffing entails intercepting and copying all packets of data sent between two communicating devices before forwarding these packets to their legitimate destination. When enough packets have been intercepted, an eavesdropper can reconstruct the communication messages, either in full or in part, and gain access to potentially confidential or private information. This type of attack is particularly common in the types of networks considered in this study. The most common countermeasure to packet sniffing is to encrypt the communication through state-of-the-art encryption protocols such as AES (Advanced Encryption Standard). However, encryption is not usually employed when connecting to free Wi-Fi networks.

An even more potentially dangerous situation called DNS redirection may manifest itself on unprotected networks. DNS is the system that links the numerical IP address of services such as websites to easy-to-remember names. For example, DNS is used to link the fictional website with IP: `10.221.67.194` to the name ‘trust-banking.com’. This is achieved by maintaining an internal database with numbers-to-name pairs. When a user requests a name, DNS translates that name to the corresponding IP address. Through DNS redirection, also known as DNS poisoning or hijacking, an attacker taints this internal database and links a valid name to an IP address belonging to a hacked website[10]. Consequently, when users visit ‘trust-banking.com’ they are either directed to a website that may be loaded with malicious software (malware) such as viruses or worms that can inflict serious damage to the visitor, or to websites that resemble the legitimate destination but are under the control of the hacker and as such can be used for pharming or phishing attacks. Aleroud and Zhou[12] give a detailed taxonomy of phishing techniques and possible countermeasures including the use of anti-phishing tools, machine learning, information retrieval, increasing human awareness, etc. With regards to DNS poisoning in general, using a properly configured firewall solution and following good Internet practices can help minimise the danger. An expertly configured firewall would restrict modifications to the DNS database and, by being vigilant when visiting websites (e.g. by ensuring that the websites use properly signed SSL certificates), can help mitigate the effects of these types of attacks. As an additional precaution against malware, using up-to-date antivirus and anti-spam software, and disabling Adobe Flash and JavaScript in browsers is considered common practice.

Another easy-to-execute attack, that uses MitM as a staging ground is the so-called session hijacking. Browsers often issue cookies to users that contain their session information. This is done to allow easy subsequent access to Internet resources (e.g. by logging into a Gmail account, access is granted to all related services). Hackers can exploit this by intercepting these cookies and using them to their own ends (i.e. to log into users' accounts). A possible countermeasure is for the websites to encrypt these cookies. Unfortunately, this is beyond the control of the end-user and websites often neglect to do so[3].

DoS is one of the oldest and most devastating types of network attacks[13]. Essentially, the attacker attempts to flood a host (e.g. web server, application server, database server, etc.) with so many requests for services that the server is overwhelmed in its attempt to comply. As a result, requested services are denied or become unavailable to legitimate users[13]. DoS attacks may take several forms but they are usually mitigated using enterprise grade routers, capable of packet inspection, and with specialised Intruder Detection Systems (IDS) and Intruder Prevention Systems (IPS). These systems can be considered as a sort of flood-gates sitting at the router boundaries of a network, performing deep analysis of incoming traffic and report (in the case of an IDS) or even prevent (in the case of an IPS) malicious data packets from entering the network[2]. Since DoS attacks usually occur from outside the network (i.e. Internet) and not from within the local network, it was considered as beyond the scope of the current study and was excluded from the experimental penetration testing. Nevertheless, unless specialised hardware is used, all computer networks, including the ones considered in this study, are susceptible to DoS attacks.

IP spoofing is one of the ways hackers employ to masquerade their IP address as one that rightfully belongs to the network under attack. It allows hackers to inject packets into the Internet with a false source address[2] making them appear as someone that other users can trust. This is usually done to hide their presence and to gain unauthorised access to systems that differentiate legitimate users from unauthorised ones using their IP address. Similar to DoS attacks, this is usually performed from beyond a network's boundary to gain access to the local network and can be prevented through the proper configuration of routers and firewalls. IP spoofing was also excluded from the experimental testing.

Another popular means of attacking network users in recent years is the social engineering attack. Instead of the hacker trying to guess or fake credentials (username and password), the authorised users of the system are tricked into relinquishing theirs. A popular technique used by skilled social engineers is to call unsuspecting users and impersonate network technicians, IT department employees or telephone company employees and simply tell the victim that there is some sort of problem with their accounts and ask that they change their password to some specific phrase or reveal their current password. This form of attack is in fact the safest for the hacker as it is carried out swiftly and without leaving any entries in servers' logs for security specialists to trace. If social engineering is not possible or desirable, a MitM attack can be employed instead. In case none of the above is a viable option for the attacker, trying to guess the username/password combination might be the last resort. Tools like 'John The Ripper' are freely available tools that try to intelligently guess passwords[14]. This, however, requires time and, if not performed offline, leaves traces in servers' logs that might enable system administrators to track the attacker's movements. To minimise the possibility of brute forcing passwords, specialised hardware-dependent schemes, such as the one proposed by Gutierrez et al.[15] can be employed to hinder attackers from recovering hashed passwords stored on servers.

It becomes obvious from the discussion thus far that if someone wants to attack a network there are manifold means to do so. Nevertheless, information security researchers continuously explore new ways to counteract network attacks including the use of Artificial Intelligence to detect infected devices (known as bots), used in Distributed Denial of Service (DDoS) attacks[16]. In an extensive survey on security for mobile devices, LaPolla et al.[17] provides a detailed classification of various detection principles including machine learning, signature matching, run-time policy enforcement and integrity verification, amongst others.

3 | RESEARCH METHODOLOGY

A mixed-methods methodology was employed to empirically explore cyber-security in the context of small businesses in Cyprus offering Wi-Fi hotspots as an additional free service to their customers. This research combines an interpretivistic study with the experimental approach. To contextualise the discussion on cyber-security in relevance to Cyprus, and depict the perceptions of key stakeholders, a set of interviews was performed, analysed and interpreted while being compared and contrasted with the studied literature. Findings stemming from this exploration subsequently informed the design and setup of the experimental test (which was performed in a controlled setting) aiming to empirically and critically assess the insights gathered both through the interviews and by surveying existing literature.

Primary data was gathered through semi-structured interviews conducted with two experts in the field of information security, nine network administrators/owners, and fifteen users of public, free Wi-Fi hotspots. The experts interviewed are security administrators of networks and systems infrastructure at two different banks (public companies) in Cyprus. Their main responsibilities include, but are not limited to, the administration and implementation of the internal and external firewall perimeter of the bank's infrastructure, active directory policies, mail communication, troubleshooting and network configuration, managing the access levels and rights of network users, and overall security. Out of the nine administrators interviewed only one was a qualified network professional employed by the company while the remaining eight were the owners of the small business offering the free Wi-Fi hotspot as a service. This reflects the typical case in small businesses, in Cyprus. Coincidently, one of the eight owners has a background in computer science and hence is also qualified to properly setup a secure Wi-Fi network. Finally, the users interviewed were randomly selected and the sample included male and female users, in different age groups and of varying educational levels. The aim of conducting interviews with these three groups of informants was to determine their perceptions and get a deeper insight on the level of awareness in terms of cyber-security. The use of prompting questions during the interviews helped to delve into the specifics of recurrent or prominent topics. The three set of interviews were recorded and fully transcribed before being qualitatively analysed[18,19] and interpreted, in order to extract the key findings and their practical implications.

In addition to the interpretivistic approach taken to analyse the interview data, an experimental test was performed to ascertain that compromising public Wi-Fi networks, often without leaving a trace, is indeed a relatively straightforward task. An open Wi-Fi network was established in a controlled environment and this was subsequently attacked using tools that are freely and widely available. The goal of experimental testing was two-fold: first, to investigate whether it is indeed practically possible for a hacker to harm users connected to a public Wi-Fi network; and secondly, to find out how complicated or straightforward it is for the hacker to attack users in a public place. The experimental tests have been captured on video for detailed analysis.

Synthesising the insights gathered from established literature with primary data gathered through interviews and experimental testing shed light on key issues related to cyber-security in the context of Cyprus. The methodological approach employed constitutes an element of originality as it successfully fuses interpretivistic exploration with network penetration testing in an experimental setup. Essentially, the study emphasises the value of exploratory research combining current knowledge with empirical findings gained through experiments and interviews, rather than solely statistically analysing perceptions based on quantitative data, as it is often the case.

4 | DATA ANALYSIS AND INTERPRETATION OF RESEARCH FINDINGS

4.1 | Analysis and Interpretation of Interviews

Qualitative data was gathered using interviews from three groups of informants. Experts (n=2), administrators of public hotspots (n=9) and users of public hotspots (n=15) were interviewed using a semi-structured interviewing approach. Following transcription of the interviews, qualitative data analysis was performed[18] to identify key themes and prominent issues in an attempt to confirm and/or critically evaluate what has been suggested in the literature. The overarching theme in all interviews was to investigate the level of awareness with regards to cyber-security of public Wi-Fi networks in Cyprus. In the discussion of the main findings presented below, verbatim quotes[20] are used for two main reasons; firstly, in an attempt to portray a more meaningful and rich account of the informants' perceptions, and secondly, in order to substantiate the researchers' interpretations.

4.1.1 | Insights from Information Security Experts

Analysing the interview data gathered from experts, a prominent finding was their observation regarding the evident lack of awareness of both administrators/owners and users in relation to how safe Wi-Fi networks are and their underlying vulnerabilities. Referring to end-users, experts reported that regardless of their age group users often appear to be naive and ignorant with regards to security issues. Many users seem to consider a password-protected Wi-Fi connection as secure, which is definitely not the case, especially since this password is provided to all customers at the cafeteria or restaurant. In reality, as one of the experts explicates, open, public, free Wi-Fi networks *"are not really safe. I think they are as safe as your browsing habits are. They are unsafe because everyone has access to them, not because they are open [...]. Even if they have a password, if someone has access to them and you are in the same network they can sniff your traffic, they can get packets and analyse them, and then use them maliciously"* (Excerpt, Expert B). Therefore, being safe does not depend on whether the network is password-protected, as many users tend to think. Rather, *"it depends on what you are doing, because if you are visiting an HTTPS site that has SSL certificate and the traffic is encrypted you are sort of OK. If you are visiting an HTTP site then everything is open and anyone on the same network can view that and intercept that and manipulate that"* (Excerpt, Expert B).

Despite the largely unsuspected population, one of the experts explains that a pattern frequently observed in Cyprus in recent years is that *"younger people know and they warn their parents"* (Excerpt, Expert B) about the potential risks when browsing the Web or using e-banking services. The other expert also suggests that the *"younger generation is more aware of cyber-security nowadays. But again, due to our nature most of the time we do not take into consideration the risks when connecting to such vulnerable networks such as public Wi-Fi, open Wi-Fi hotspots"* (Excerpt, Expert A). This illustrates that human nature, and the need to socialise online, often override common sense for securing their devices and personal data. The experts also report that, increasingly, employers in Cyprus make an effort to reduce the level of ignorance by training and educating their employees. *"People in specific areas such as banks, auditing firms, telecommunication companies and the government have started getting educated around the term 'cyber-attacks' and how they can get protected from them"* (Excerpt, Expert A). Business-wise, these efforts are mainly motivated by the recognition that any security threat can negatively affect a firm's reputation. *"People are more aware lately and companies are paying attention [not only] because they have regulatory requirements, they have legal requirements, they have all those ISOs"* with which they need to comply, but also because if the company does not carefully consider security issues *"and they get hacked, then it's all over the Internet, they cannot hide it, and it is really bad about their* *reputation. So companies are actually afraid of the bad reputation and they are taking notice"* (Excerpt, Expert B). Even though users may be cautious of security issues in their workplace networks, they do not seem to take into consideration the underlying risks when connecting to public networks.

Referring to the recent phishing attacks which involved two of the major banks in Cyprus, the experts also emphasise the role of broadcasting and social media in informing and increasing the level of awareness. In these attacks, customers received an SMS informing them that their bank account has been locked and that they need to visit the bank's website to restore it. Basically, the individuals behind these attacks attempted to trick customers into providing their username and password and as a result, their accounts were susceptible to fraud. The experts emphasise that broadcasting and social media can help in sharing these situations and raising awareness. They also advise that end-users in Cyprus ought to become better informed about cyber-security and cyber-attacks as the latter are becoming increasingly more common in Cyprus and, as a result, *"more people are getting affected"* (Excerpt, Expert B).

According to the experts interviewed, a high degree of ignorance is also attributed to administrators/owners of Wi-Fi hotspots. Although the ways to protect against simple threats are well known, very few public hotspots (only one in our study) provide a safe networking environment. The interviewed experts suggested that small businesses in the service industry like cafeterias, bars, restaurants, hair salons, etc. are not concerned with the security of their hotspots due to three main reasons: lack of awareness of the frequency and ease with which wireless networks can be compromised; lack of technical skills and knowledge regarding maintenance and proper administration of hardware and software needed to secure the network; and finally, cost. This observation is corroborated by the findings of Osborn and Simpson[21] in their recent study of common networking architectures employed by SMEs in the UK. As one of the information specialists explains, most administrators simply obtain a router from an Internet Service Provider (ISP) (e.g. the widely used Thomson router), and plug it in without re-configuring it or changing the default password. As a result, their network is at risk since *"those routers have very specific algorithms of computing the key you have to enter in order to access the Wi-Fi. There is an application that cracks that and you can download it on your phone and you can just walk around and get into [public] Wi-Fi. Nobody changes the password, nobody changes the SSID, because people just don't know"* (Excerpt, Expert B). Another commonly observed attitude from administrators/owners is that they simply ignorantly restart the affected devices/routers when unknown issues occur, failing both to investigate the potential causes and to take measures towards protecting their network and its users from cyber-attacks. This illustrates that in many cases they lack the awareness, competence and skills to take further action. As one of the experts explains *"they simply provide open free hotspots for their customers. I don't think they bother to secure it anyway. They mostly just restart it when they have an issue, that's as much they [...] do with it"* (Excerpt, Expert B). Nevertheless, securing a network infrastructure *"depends on how you configure it, because if it's just there and it's not properly configured and it's not getting updated, you are doing nothing"* (Excerpt, Expert B).

Coupled with the lack of awareness and technical skills on behalf of administrators/owners, cost appears to be a reason why security measures are not taken seriously by most small businesses in Cyprus. *"The problem with open Wi-Fi is that administrators can barely take any good countermeasures to protect their clients as it would need a huge investment"* (Excerpt, Expert A). The high cost is attributed to the fact that specialised hardware and software licensing as well as expert technical knowledge and on-going maintenance is high for small companies such as the ones considered in this study. *"We are talking about a huge investment as most of the solutions are based on user licenses and concurrent sessions. That is why I consider that for small business like cafes, bars, restaurants such investment is prohibitive. It's a huge investment in terms of initial cost and on-going maintenance. To build a secure environment needs proper administration and daily maintenance that increase the overall cost"* (Excerpt, Expert A). Hence, although necessary, cyber-security may be considered as a luxury. This is a classic case of owners not being willing to invest money in technology that will not result in direct monetary returns[22,21], as Wi-Fi is generally provided as a free service to customers.

When asked about the ease, frequency, and severity of hacking attacks today, specifically in Cyprus, the experts explained that hackers can harm unsuspected users connected to public, free Wi-Fi networks, in a variety of ways, and at a remarkable ease. The following excerpt from one of the experts interviewed provides a rich depiction of the current situation in the field of cyber-security: *"It's really (with an emphasis) easy to make an attack today! You have what we call Script kiddies, so a fourteen year old, who knows nothing about... (pauses for a moment and thinks) ...who probably knows more than most of us (laughs and continues) [...] a fourteen year old that knows nothing about security or the basics on hacking [...] can find online scripts and programs like Kali Linux [and] use them to attack someone. Also [...] if you organise crime or if you have money and you want to spend it to attack someone you can actually buy a Botnet, you can pay people that have control of thousands of computers and you can use their computers. You have this little software on them that's running on the background and it's just waiting for a command from your server. If you have a hundred or thousands of computers and in one moment you send them a command saying 'ping this target' and all of them start pinging that target, at some point their Internet lines will fill up and then you have a Denial of Service attack because they cannot use their Internet and [...] the server just crashes. So, we have scripts, we have organised crime and even governments do that. Anyone can do it these days. Another recent example is when a group of hackers managed to hack a software used by the government and the police and released all emails online and were selling this for a huge (with an emphasis) amount of money to [...] criminal organisations, even to the Cyprus' Information Department or the secret services [...]. So it comes in many different forms"* (Excerpt, Expert B).

Moreover, hackers may implement DoS attacks hence denying the legitimate users access to the network. *"Most wireless networks [...] use the default passwords for the routers [...] so for example, if you see a Linksys wireless and you connect to it and its open, chances are the username and password for the router are 'admin/admin' or 'admin/empty password'. So you have admin access to the router and then you can change its password, you can shut it down, you can do whatever you want. So that's* *a Denial of Service attack"* (Excerpt, Expert B). Another form of attack is manipulating and redirecting traffic through DNS poisoning. *"If you have access to the router you can manipulate the DNS records, so if you visit Facebook I can manipulate that and make you visit [...] a malicious website. Then I can use the website for a phishing attack where I can have a log-in prompt. You can enter a username and password and I can use them to infect your computer. So [this malicious website] may have a virus loaded and once you visit it you just get infected. So it can be used in different ways"* (Excerpt, Expert B). Hackers can gain access to usernames and passwords of users' accounts (e.g. e-banking, email, online utility bills, etc.) through pharming, phishing or packet sniffing. They can also redirect traffic through DNS poisoning, and generally monitor users' actions or compromise users' devices through the MitM attack. The latter is used as a mediating phase for achieving the outcomes stated above.

The information gathered from experts with regards to hacking and cyber-attacks not only reconfirms what the literature suggests as the most widely reported types of attacks which hackers may exercise, but also emphasises the complexity and high degree of interrelationship between the various types of attacks. Still, the experts agree that the main threat the users of public Wi-Fi hotspots may face is raised by other users on the same hotspot. This implies that a casual user on a laptop, without necessarily having advanced hacking skills (e.g. a script kiddie), poses the most common threat on a shared network. *"Public Wi-Fi networks are not nearly as safe as you think. Even if they have a password, you're sharing a network with tons of other people, which means your data is at risk. Just because most wireless routers have a firewall to protect you from the Internet it doesn't mean you're protected from others connected to the same network. It's remarkably easy to steal someone's username and password, or see what they're doing just by being on the same network. Therefore, I consider that open and in general public Wi-Fi [networks] are not safe at all"* (Excerpt, Expert A).

Additionally, the information security specialists provided some recommendations and countermeasures for administrators and users of public hotpots to safeguard their networks and devices, respectively, from hackers. For administrators, the experts recommended a number of countermeasures, including using Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS), providing VPN connection over open Wi-Fi, using advanced firewall, URL filtering, threat emulation, and wireless client isolation amongst other. Special emphasis was also placed on the technicalities of the wireless network infrastructure suggesting that *"an administrator could consider building a secure topology by protecting the Wi-Fi network from threats with a multi-layered security approach. There are multiple vendors that can provide an overall solution that can protect with different technologies [including] firewalls (both hardware and software or [combined] appliances based on vendor), different options for a multi-layer security environment [...], switches, wireless access points and wireless controllers"* (Excerpt, Expert A). Therefore, we can infer that it is the administrators'/owners' responsibility to invest in appropriately securing their network infrastructure, by allocating this task to knowledgeable individuals or companies, in case they do not have the skills and expertise to properly administer the network themselves.

For users, the suggested countermeasures range from trivial measures, such as turning the Wi-Fi connection off when not in use, to more meticulous ones such as using an updated antivirus software and having firewall enabled, being vigilant of phishing websites, using VPN connection over Wi-Fi, preferably using their provider's 3G or 4G mobile network if available, rather than connecting to the public free Wi-Fi network, and visiting only secure HTTPS sites and checking the site's certificate. Nevertheless, valid certificates, counter to popular belief, do not always ensure security since certificate agencies (CAs) might be compromised resulting in rogue (i.e. valid yet untrustworthy) certificates being issued. However,[23] suggest a neural-network based approach for detecting rogue certificates from trusted CAs.

Essentially, as Aleroud and Zhou[12] suggest, one of the most important countermeasures against cyber-security attacks entails educating human users, increasing user awareness and involving users in identifying common types of attacks. As one of the experts advises, *"the effort should also be concentrated on educating people to take necessary precautions when using public open Wi-Fi, at least when they are performing specific operations [such as] Internet banking transactions and connecting to corporate resources"* (Excerpt, Expert A).

With regards to penetration testing, both experts strongly agree that it constitutes a very important part in the auditing process for securing computer networks. *"There are different types of penetration testing and it's definitely necessary (with an emphasis); it's 100% necessary. You cannot go without that, you have to have it and you have to fix the problems that the penetration testing finds because they are the most common problems. So, what a hacker does is actually penetration testing. They find your vulnerabilities and then they exploit them (laughs). So you have to beat them to it"* (Excerpt, Expert B). Therefore, penetration testing must be performed to *"reveal vulnerabilities on the system and take the necessary actions to mitigate these vulnerabilities [...]. Depending on the system we perform an initial vulnerability assessment to reveal any exploitation that can be performed on our systems. Then we perform a hardening on the operating system and our applications"* (Excerpt, Expert A). When the networking infrastructure is critical to the business model, such as e-commerce, e-banking, e-government, even more advanced measures need to be considered. In these cases, professional services are employed performing more exhaustive penetration tests to secure the networking perimeter.

The interviews with security exerts confirmed what has been found in the studied literature with regards to the procedures performed by hackers and the various stages that penetration testing involves (i.e. scope/goal definition, information gathering, vulnerability detection, information analysis and planning, attack and penetration/privilege escalation, result analysis and reporting, and clean-up) and these were considered in a subsequent phase in our study while designing our experimental test.

4.1.2 | Insights from Network Administrators

For triangulation purposes, in addition to the rich information gathered from the security experts, data was also collected from nine administrators of free Wi-Fi hotspots. The aim for performing these interviews was to explore the current practices in the context of small businesses in Cyprus. Seven out of nine administrators interviewed, admitted that they lack the necessary technical knowledge to setup and maintain a secure Wi-Fi network and that they depend on their ISPs to provide these services. When the same owners were asked about the security mode of their Wi-Fi hotspot (e.g. Open, WEP, WPA or WPA2) they stated that they were not familiar with the concept of Wi-Fi security modes and that they used the default security mode that their ISP had pre-configured. This however does not ensure a secure configuration as some ISPs in Cyprus still employ the insecure WEP mode in order to maintain backwards compatibility with older devices. There are primarily two security concerns stemming from having public Wi-Fi hotspots setup by non-experts following the ISPs' instructions. The first security issue involves the hardware provided by the ISP. Essential security features such as an IDS, an IPS, and a stateful firewall are not build into typical all-in-one ISP-provided routers (which also act as Ethernet switches and Wi-Fi access points). These routers are meant to be used in a trusted environment, such as a home and not in a public setting where user separation is critical. To compound this problem, a second security issue relates to the Wi-Fi network architecture. Osborn and Simpson[21] discuss alternative network architectures including the use of the ISP/SOHO (Small Office Home Office) router acting as the Wi-Fi hotspot and the use of a second user-owned and user-controlled SOHO router for enhanced security. In the second case, the owner is allowed to implement additional security measures and "to avoid the ISP having total freedom to reset any perimeter security configurations"[21]. Nevertheless, the first setup was used in eight of the small businesses included in our study while only one used the second architecture. The typical small business network architecture is illustrated in Figure 2. Convenience, trust in the ISPs' expertise and the lack of concern over security issues due to the fact that Wi-Fi is offered as a free service were quoted as the main reasons explaining why the first architecture was preferred by eight out of nine businesses.

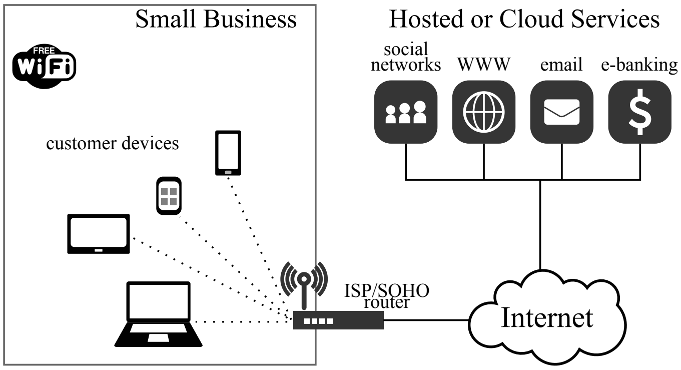

FIGURE 2 Typical small business network architecture (adapted from[21, p. 30])

Only one of the hotspots investigated was open. Interestingly, this was the network administered by the qualified networking professional. In his interview, he stated that despite his warnings, the owner of the hotspot insisted on having an open Wi-Fi network for ease of use. Nevertheless, he employed specialised hardware (i.e enterprise grade access points) to ensure that users are limited to using the Internet and cannot intercept other users' communications. This additional cost protects against most of the attacks investigated in our study but some attacks (e.g. phishing) are still possible. For the remaining eight networks which were password-protected, their administrators incorrectly assumed that they are secure. However, sharing passwords freely with customers or displaying them on walls nullifies their usefulness and relegates the networks' protection to the same level as open public Wi-Fi networks. Six administrators admitted that they have never changed their password and it has been the same since they first installed their network while two administrators changed the password only once. When asked whether any of their customers ever experienced a security threat or attack while being connected to their network, all nine responded negatively. However, apparently even if an attack did occur, neither the administrators nor the users would be in position to recognise the cause or source of the attack. These facts demonstrate the overall lack of awareness and technical skills alike with regards to network security issues.

4.1.3 | Insights from Wi-Fi Hotspot Users

An emergent theme from the analysis of the interviews with end-users was the overall lack of awareness of the specific dangers of using shared networks and the means of protecting their devices from being compromised. Most users (13 out of 15) admitted that connecting to Wi-Fi networks is the first thing they do when such networks are available. The two remaining users (who have an IT-related background) explained that they are conscious of the dangers inherent in shared public Wi-Fi networks and they generally prefer using their 3G/4G connection. Yet, they might still connect to a public Wi-Fi hotspot depending on the urgency (in one of the cases urgency was defined as children begging for Youtube videos!). They explained that when they connect, they do so for a limited amount of time, only if the venue is not crowded, and they never access or provide sensitive/personal information. They also disconnect from the network as soon as they have performed the necessary tasks. This illuminates the fact that emotional aspects – in addition to cognitive aspects, prior knowledge, and perceptions – may also affect the behavior of a user when it comes to making certain decisions regarding privacy and security. The findings from interviewing end-users indicate that a multifaceted relationship exists among users' privacy concerns, their affective responses, and their coping behaviours in the context of privacy threats[24].

Another interesting finding was the fact that despite attributing high value to their personal information (e.g. personal photographs, date of birth, usernames and passwords, etc.) all fifteen respondents would connect (under certain circumstances) to a free public Wi-Fi network. Kokolakis[25] refers to this discrepancy between the value users assign to their privacy information and their actual behaviour as the 'privacy paradox phenomenon'. He suggests that "users actively share personal information despite their concerns, because they do not only consider risk but also the expected benefit"[25, p. 125]. Individuals will connect to potentially insecure networks and may be willing to reveal personal information for relatively small rewards, often just for accessing social networks[25]. Overall, the insights provided by analysing the interview data from users, administrators, and information security specialists confirmed what has been suggested in the studied literature.

4.2 | Description and Outcomes of Experimental Test

A pre-eminent approach towards understanding the process of compromising a freely accessible network, and what this process entails, is to actually perform a penetration testing on one. Therefore, in our attempt to further explore the possible harm that hackers can cause to the users of public, free Wi-Fi hotspots in Cyprus an experimental test was set up. Expert opinion was sought with regards to the practicalities and legal and ethical aspects involved in performing such a test. The experts explained that *"it's illegal and you may get in trouble for it"* and advised that we keep in mind the following: *"First of all, do not harm and if you are doing it on someone else's Wi-Fi hotspot make sure you get permission. And even if you get permission make sure you don't do something bad to their wireless or some others users"* (Excerpt, Expert B). They also recommend that *"You should be ethical and not harm anyone. It is not a good idea to crack an existing Wi-Fi at a cafeteria; it is most preferable to setup your own Wi-Fi"* (Excerpt, Expert A). In addition to their suggestions and expert advice, both specialists provided detailed, practical guidelines and information about how exactly to perform the penetration test, what software and hardware is needed (e.g. router, modem, laptops of other mobile devices such as smartphones and tablets, Kali Linux with Virtual machine, Ettercap, Wireshark, etc.), where to find it, and how to set the experiment up.

The experimental test took place in a lab using a controlled Wi-Fi hotspot. This decision is also in agreement with what Ramachandran[26] suggests in his book. Consequently, for ethical as well as practical reasons, the hacking session was performed in a controlled environment instead of a venue sponsoring a free Wi-Fi connection. The explicit purpose of the experiment was primarily to verify what has been argued by the interviewees and also what has been put forward in current literature. Achieving this goal involved addressing two research objectives: firstly, investigating whether it is indeed practically possible for a hacker to harm users connected to a public Wi-Fi network, revealing the vulnerabilities in a network and the ways a hacker may wish to exploit them to attack users; and secondly, exploring how complicated or straightforward it is for a hacker to attack users in a public network.

Experienced hackers typically follow a set of predefined steps to successfully carry out an attack on a computer network. Although no single official methodology exists for carrying out cyber-attacks, these steps are so commonly used that they can be perceived as being part of a hacking method. Each stage in this method depends on the successful completion of the previous stages. Moreover, these stages cannot be performed concurrently bur rather in a sequence, one after the other. A typical hacking attack commences with (i) information gathering of the targeted network (also called 'footprint analysis' or 'reconnaissance') and continues with (ii) detecting vulnerable devices on the network (called 'enumeration'). Following the enumeration stage, (iii) penetration is performed on the vulnerable devices. Once a device has been successfully compromised, the hacker seeks to (iv) gain access to sensitive (private or security) information or gain higher level access on the network (called 'privilege escalation'). This can be achieved by carefully reading any documentation, emails, correspondence, log files, error reports etc. on the compromised system that may contain useful information that will allow the attacker to either gain access or to guess

TABLE 2 Hacking goals and tools used in the experimental test.

Hacking goal	Attack used	Tools used	Results/implications
Password Sniffing	MitM, Packet Sniffing	Arpspoof, IPTables, Ettercap, sslstrip	Steal usernames and passwords from eBay, PayPal, MS Outlook, commercial LMS, Facebook, and e-banking accounts
Image and URL Monitoring	MitM, Packet Sniffing	Arpspoof, IPTables, Ettercap, Urlsnarf, Driftnet	View images and URLs visited. Extract browsing actions and behaviour
DNS Redirection and Website cloning	MitM, Phishing	Social Engineering Toolkit (SET)	Steal usernames and passwords from commercial LMS and e-banking accounts

super user credentials. Once super-user credentials have been obtained, the attacker has full control of the compromised system and can then mount an attack on the next target in the network. Finally, the hacker may (v) install software (called 'backdoors') on the compromised device that would ensure easy future access to the system and (vi) cleans any trace that the attack took place.

Although the hacking method itself appears to be simple, each stage requires a great deal of skill and patience by the attacker, especially to penetrate high security systems. Expert level knowledge of networking hardware and programming is required when the target is well protected. However, the multitude of freely available tools, such as the ones presented in this section, greatly simplifies the task of attacking relatively unprotected systems such as the ones found in most small to medium sized businesses in Cyprus. The procedure presented in this section was replicated during the experimental penetration testing that was performed in this study.

Specifically in our experimental test we carried out the first four stages (i-iv) to achieve three of the most common hacking goals. These goals are: (a) *password sniffing* (i.e. stealing username and password combinations); (b) *image and URL monitoring* (i.e. monitoring user actions on the network, including the websites visited, the servers connected, the databases used etc.); and (c) *DNS redirection and website cloning* (i.e. redirecting traffic from legitimate websites to nefarious hacking sites containing viruses or to cloned websites that appear legitimate but in fact may be used for stealing personal information, also known as phishing). These hacking goals are listed in Table 2 along with the attacks and tools used to achieve them and the results and implications involved.

Common commercial hardware (router, wireless access point) were used to create the Wi-Fi network for the purposes of the experiment. The network was set up in a manner identical to the networks as identified in the interviews (see Figure 2). The hardware devices used in the experiment are listed in Table 3 and shown in Figure 3. The attacker/experimenter used freely available hardware and software to perform the penetration testing. Before initiating the experiment, Kali Linux 2 was installed on a laptop computer designated as 'hacker's computer' (Kali virtual machine), which was equipped with an Intellinet RT73 USB Wireless Network Interface Card (NIC). The Wi-Fi hotspot was set up by connecting the ISP's wireless router with a modem and setting the security mode to 'open' to simulate venues that promote open Wi-Fi or easily obtainable passwords. The four victim devices (a laptop computer running Windows 10, two smartphones and a tablet computer) used as recipients of the attacks were purposefully chosen to represent the diversity of the devices on a public Wi-Fi network such as the ones considered in the study.

TABLE 3 Hardware employed in the experimental test

#	Hardware device	Description/Purpose
1	Modem	A modem was used to access the Internet. This was a common modem supplied by the ISP.
2	Wireless Router and Access Point	This device was used to connect the local area network with the Internet and give access to all devices connected on the access point to the network resources. A wireless LAN was created using this device similar to the networks run by most public places.
3	Laptop (Hacker)	This laptop running the freely available operating system Kali Linux served as the attacker's vehicle for performing the penetration testing. The laptop was running tools used by the hacker to perform the attacks. All software used on this laptop was either open source or free to use.
4	Wireless Network Interface Card (NIC)	The hacker's laptop was equipped with an Intellinet RT73 USB Wireless LAN card. This is a cheap (under $20) wireless NIC that allows the hacker to use it for reading data in the network that was not meant for it (this is commonly called a promiscuous mode).
5	Laptop (Victim 1)	A laptop running Windows 10 served as the victim's personal computer.
6	Tablet (Victim 2)	A tablet with the Android operating system served as the second victim.
7	Smartphone (Victim 3)	A smartphone with the Android operating system was designated as victim number three.
8	Smartphone (Victim 4)	An additional smartphone running Android was used as the fourth victim.

Once the test environment was set up and the devices were connected to the wireless network, the experimenter began to systematically attempt to achieve the three stated hacking objectives. Sun Tzu, states that "victorious warriors win first and then go to war"[27]. Executing cyber-attacks is not unlike mounting military campaigns. In this respect, thorough reconnaissance of the target is paramount for the successful outcome of the attack. Hackers spend up to three times longer analysing the targeted network than in any other phase of the attack. During reconnaissance, the hacker gathers information on the devices connected to the network, including the type of the device (router, server, personal computer, mobile device, etc.), the IP address of each device, the operating system each device uses, applications that run on the network, and what ports, services and domains are active on the servers. This information gives valuable insight to the attacker providing possible attack vectors. Additionally, hackers identify security measures that the network may be employing and devise ways to circumvent them[14].

According to[28], network reconnaissance can be performed through the successive use of three types of scans; namely 'network scan', 'port scan', and 'vulnerability scan'. During the 'network scan' phase, the targeted network is scanned for active devices, called hosts, along with their IP addresses. These hosts can then be assessed and classified as either potential targets or network security devices (e.g. firewalls). Once the devices on the network have been identified, the 'port scan' phase commences through

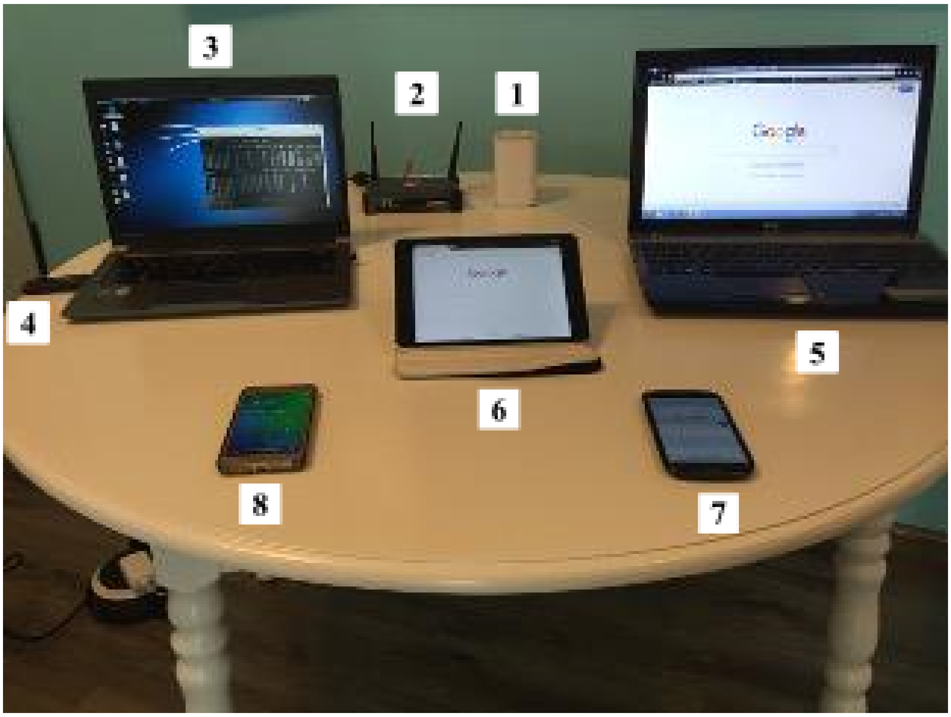

FIGURE 3 Experimental setup. Photo credit: Maria Mammous

which all open TCP/IP and UDP ports are listed. This scan lists potential services that may be active on the hosts identified in the 'network scan' phase. Finally, the hacker performs a 'vulnerability scan' on the services identified in the 'port scan' phase targeting services that, in conjunction with the operating system in use, are known to be vulnerable. Typical network analysis software that can be employed during this initial phase includes the well-known 'nmap' and 'Sam Spade' tools. 'Nmap' and 'Sam Spade' are general purpose tools that together can be used to scan a large number of devices in a single session and perform ping sweeps, port scans, service identification, operating system detection, reverse DNS searches, traceroutes, whois and network lookups, etc.[14,29]. In our test, the 'nmap' tool was used to identify active hosts (potential targets) on the network and the designated Wi-Fi router/access point. Specifically, 'nmap' successfully identified all devices listed in Table 3. Since we were dealing with a small network, no other tool was required and a full map of the network was drawn within five minutes of initiating the attack. Finally, no warning that an attack was underway was send to the users of the network.

Once a map of the network is acquired, the attacker moves onto the 'enumeration stage'. During this phase, the hacker examines each identified potential target (hosts and services) closely, trying to determine the operating system protocols in use (e.g. IP, IPX, NetBIOS, etc.)[29] and services such as e-mail, file servers, remote access service, secure shell, virtual private computing and virtual private network, database applications etc.[14,29]. Specifically, the hacker tries to identify the type of service and, more importantly, the version of the software listening on each TCP port. Additionally, information such as user names, user groups, last logon dates, and password change dates can be discovered. The information combined with knowing the specific version of the services running on the server, allows the attacker to search online vulnerability databases for possible attack vectors and formulate a 'battle plan'. There is a plethora of freely available tools that hackers can employ to successfully carry out this phase in the hacking method. To name just a few, 'netcat' can be used to grab ftp and telnet banners along with the services' version, 'Epdump' and 'Rpcdump' can be used to find out information about remote procedure calls (RPC) on Windows servers, 'Zenmap' can be employed to enumerate the operating system of the server and 'DumpSec' can be used to extract user and group names as well as file and share permissions directly from windows servers[29].

The probability of a successful cyber-attack is directly proportional to the amount of time spent and the quality of analysis performed during the enumeration stage. Spending more time during the enumeration stage, leads to more information obtained with regards to the network and its resources and, consequently, to more vulnerabilities discovered that would allow the attacker to gain unauthorised access to the computing resources. In fact, attackers who have thoroughly and systematically performed the enumeration stage have already won half the battle. All that is left is for the attacker to gain access to the system. In our experimental test, the 'Zenmap' tool was used to compliment the results of the previous stage. Specifically, the analysis showed that no server was connected to the network and that the operating system of the connected devices was a mixture of Windows 10 (fully patched) and Android. This allowed the hacker to identify the potential target (Windows 10 laptop) and avoid, in the initial attack, the android smartphones. This information proved invaluable in the subsequent stages of the hacking effort. Specifically, the hacker intuited that since no server is active on the network, there will be no vulnerable services to exploit and that the easiest attack vector available was a phishing attack.

Up to this point, we managed to construct a blueprint of the network and identify potential targets in that network. Essentially, a passive attack was carried out with no damage caused to the victims. From this point onwards, all attacks we performed were actively aiming to gain unauthorised access to systems with the explicit purpose to steal personal and security information, a primary objective of most hackers. This can be achieved through several means, with the most popular in recent years being the social engineering attack. If social engineering is not possible or desirable, a MitM attack can be employed instead.

Based on the information gathered in the reconnaissance and enumeration stages, to achieve our stated objectives, it was decided to perform a MitM attack and monitor the communication of the targeted device (Windows 10 laptop) with the router. To achieve this, ARP poisoning was used to trick the victim's laptop into sending all communication to the hacker's device (Kali Linux 2 virtual machine), thus completing a MitM attack. Routing tools (e.g. 'arpspoof' and 'IPTables') were employed to redirect traffic to the experimenter's laptop (designated as hacker's device).

To perform password sniffing, the 'Ettercap' software was subsequently used to filter the incoming communication and extract username and password combinations that the victim used while browsing the Internet. At this point, the victim device had no indication that it was under attack and that personal information was stolen. Once we were successful in stealing personal information from unencrypted websites, the victim was instructed to connect to SSL secured websites. The 'sslstrip' tool[9] was used to strip the HTTPS protocol from the communication and replace it with the insecure HTTP protocol. Normally, the victim will receive a warning suggesting that the presented website uses an invalid certificate (i.e. the website is not guaranteed to be secure). If the victim chooses to ignore the message and proceed anyway, then the hacker will be able to monitor, capture and reveal security information to the hacker, even though the websites appear to be using a secure connection. In our test, the information revealed included accounts from eBay, PayPal, Microsoft Outlook, Facebook, a commercial LMS (Learning Management System), as well as e-banking credentials from two banks in Cyprus.

For the image and URL monitoring test the same initial procedure described above was used to accomplish the MitM attack and packet sniffing. The tool 'urlsnarf' was successfully used to list all URLs that the victim has visited during the experiment. Furthermore, the experimenter utilised 'Driftnet' to download and copy all images and videos that the victim viewed while browsing the Web. In one of the tests, the victim connected to a Cyprus news website and the experimenter was able to see all images and media on the site with small delays of 15 to 20 seconds. The implication for this is that the hacker gains more intimate knowledge of the victim's habits and browsing behaviour hence making it easier to perform better-targeted future attacks.

DNS redirection and website cloning was achieved using the 'Social Engineering Toolkit (SET)' available in Kali Linux 2. This tool allowed the experimenter to clone the LMS website of a higher education institution in Cyprus. This readily available software is capable of copying legitimate websites down to the smallest detail, making them indistinguishable from the original. Subsequently, DNS poisoning was used to redirect traffic from the legitimate website to the local cloned one. Once victims landed on the hacked website, any credentials entered on the login screen were automatically saved and presented to the hacker. This type of attack was also successfully carried out using the website of one of the largest banks in Cyprus. The end result of the combination of DNS redirection and website cloning was a hard to detect and avoid phishing attack.

Following the successful attack on the Windows 10 laptop, the same hacking procedure was also used to attack the three Android devices, listed in Table 3, reaffirming the effectiveness of all attacks. The only device that warned the user that an attack was in progress was one of the smartphones which was equipped with a security application called CM security, informing its user of the potential danger and security threats.

Overall, the experience from the experimental test aligns perfectly with what was found in the literature and also with what was suggested by the interviewed experts. The attacks carried out in our experiments are merely a small subset of what is possible with a basic laptop computer and a $20 USB Wireless LAN card. It must be pointed out that no special knowledge or programming skills are required beyond basic understanding of computer networking and how communication devices work. The experimenter/hacker, armed only with basic networking knowledge, an online guide and tools that are freely available was able to successfully and effectively carry out an array of attacks with the explicit aim of causing as much harm as possible on a shared wireless network. Specifically, the experimenter was able to monitor other users on the network and record their browsing habits, including the images and videos that the users have downloaded. Furthermore, personal, sensitive information such as passwords and credit card numbers were readily pulled from the air as unsuspecting users went about their normal routine.

Even supposedly-secure websites were no match for our hacking prowess. Information was stolen even from SSL encrypted websites (albeit with a little more effort and a pinch of luck) simply because users dismissed the browser's obscure warning that their connection might not be secure. The social engineering attack carried through cloning existing sites was easy to execute. Similarly, DNS manipulation on devices that use commonly misconfigured firewalls was successfully executed and an instant phishing attack was launched that was difficult for casual users to recognise and avoid.

In addition to the ease with which all attacks were executed, the time required to perform the hacking attacks was negligible. Each attack that was launched during the experimental test lasted from a few seconds to a few minutes and left little or no trace on the network. Essentially, there was nothing to link the attack back to the hacker, nothing to notify the administrator that something was afoul, and nothing to warn the users that their most sensitive information was made public. Finally, in the experimental test, no tedious, lengthy brute forcing of passwords or WPA/WPA2 password cracking was required since the main premise of this experimental test was that the Wi-Fi password was readily available to customers or no password was used at all, a commonality in most venues offering free wireless networks, as in the case of the nine public venues considered in our study.

5 | DISCUSSION OF RESEARCH FINDINGS

The findings resulting from analysing the interview data as well as the outcomes of the experimental test highlight a set of social/pedagogical and business-oriented implications. From a social/pedagogical point of view, the findings have implications with regards to user awareness. The need for educating the public, through the media and other means, on the potential dangers that lie in wait when connecting on insecure Wi-Fi networks, has become prevalent. Even in cases where the pre-installed security software warns users of the potential dangers (i.e. in the case of HTTPS websites) a common tactic followed by users is to ignore the security messages and (either consciously or subconsciously) opt to "proceed anyway". As a result, a hacker can gain access to their passwords or other personal information, and compromise their devices. This observation calls for drastic measures in increase awareness with regards to cyber-security and cyber-attacks. A practical countermeasure extracted from this observation is that users should ensure they enter their credentials only to secure, HTTPS sites which use official digital certificates, and most importantly, be vigilant for any security warnings. With regards to administrators/owners, possible security countermeasures include: installing a stateful firewall so that it blocks attempts to DNS redirection; using URL filtering[11] to constrain their customers' access to known insecure sites, installing an additional user-owned and user-controlled router[21]; and using anti-phishing tools[12], amongst others. The results also draw attention to the need for properly trained technicians to set up and manage secure networks. Therefore, from a business-oriented point of view, owners of small businesses need to consider the investment in network security infrastructure as part of their overall marketing and branding strategy rather than as a superfluous cost.

An interesting, yet expected, outcome of the experimental test was the effectiveness in stealing user passwords and usernames from the websites of two banks which use strong encryption. Due to the user potential impulsiveness and lack of awareness, a phishing attack was possible even on the SSL-encrypted bank websites. Therefore, it is suggested that users should refrain from accessing sensitive personal information over public, Wi-Fi networks. Additionally, various security applications are available (e.g. antivirus or security suits) for protecting devices from being attacked.

Overall, our findings support what the literature suggests with regards to cyber-security and the practices employed by small businesses related to security configurations and architectures. Although a relatively small sample was used for the exploration of cyber-security in free public Wi-Fi hotspots, it was still possible to extract emerging themes. Future research should include longitudinal and comparative studies in an attempt to identify ways to better inform and educate users of public Wi-Fi networks and the owners that administer such networks. Another potential route to further this research is to explore the research questions addressed in this study in relation to other European countries. Further research in the field will raise the level of awareness with regards to the effects of cyber-security and hacking – in the context of Cyprus and beyond.

6 | CONCLUSION

An exploration of cyber-security was performed in the context of public, free Wi-Fi networks offered by small businesses in Cyprus with the aim to explore plausible vulnerabilities, how network security can be compromised, and the perceptions of end-users, network administrators/owners and information security experts on cyber-security. An experimental test was also set up in a controlled environment to explore whether it is indeed possible to exploit the vulnerabilities of public Wi-Fi networks and to assess the level of difficulty for achieving this. The methodological approach employed constitutes an element of originality as it successfully fuses interpretivistic exploration with network penetration testing in an experimental setup. Essentially, the study emphasises the value of exploratory research combining current knowledge with empirical data gained through experiments and interviews. The interviews were instrumental in generating an understanding of the current state of cyber-security – specifically in the context of small businesses in Cyprus – from three different perspectives, those of users, administrators/owners, and information security professionals. At its core, this research findings are grounded on the observation that most administrators/owners of public Wi-Fi networks in Cyprus, as well as the users of these networks, are unaware of the fact that these networks can be easily compromised by even novice attackers, and that to attack such systems is, in fact, a trivial task. The results therefore highlight the need for educating the public of the potential dangers that lie in wait when connecting to insecure Wi-Fi hotspots, and the need for Wi-Fi networks to be set up and managed by security experts. Finally, owners of small businesses need to consider the investment in network security infrastructure as part of their overall marketing/branding strategy rather than as a superfluous cost. The social/pedagogical and business implications stemming from this study are extracted and discussed. The importance of this research lies in its attempt to make individuals in Cyprus that use, provide, and/or administer public Wi-Fi hotspots more aware of the security dangers involved. Raising awareness becomes increasingly more critical given the ubiquity of mobile devices.

ACKNOWLEDGMENTS

We would like to acknowledge the contribution of Ms. Maria Mammous in data gathering and for conducting the experimental test.

Conflict of interest

The authors declare no potential conflict of interests.

References

1. Laudon KC, Laudon JP. *Management Information Systems: Managing the Digital Firm*. Pearson . 2014.
2. Kurose JF, Ross KW. *Computer Networking: A Top-Down Approach*. Pearson. (International Edition). 6 ed. 2013.
3. Chakravarty S, Portokalidis G, Polychronakis M, Keromytis AD. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security* 2015; 14(3): 205–220.
4. Twinning P, Heller RS, Nussbaum M, Tsai CC. Some guidance on conducting and reporting qualitative studies. *Computers & Education* 2017.
5. Dent AW. A survey of certificateless encryption schemes and security models. *International Journal of Information Security* 2008; 7(5): 349–377.
6. Peterson LL, Davie BS. *Computer networks: a systems approach*. Elsevier. 5 ed. 2012.
7. Wilkins S. Routing Protocol Authentication Concepts and Configuration. *Cisco Press* 2011.
8. Corbett CL, Beyah RA, Copeland JA. Passive classification of wireless NICs during active scanning. *International Journal of Information Security* 2008; 7(5): 335–348.
9. Marlinspike M. New Tricks For Defeating SSL in Practice. In: BlackHat USA. ; 2009.
10. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR. Security issues in cloud environments: a survey. *International Journal of Information Security* 2014; 13(2): 113–170.

11. Rajesh K. Why is URL Filtering required and how it is accomplished. [Online]; 2013.

12. Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: a survey. *Computers & Security* 2017.

13. Anagnostopoulos M, Kambourakis G, Kopanos P, Louloudakis G, Gritzalis S. DNS amplification attack revisited. *Computers & Security* 2013; 39: 475–485.

14. Schultze E. Thinking like a hacker. [online]; 2002.

15. Gutierrez CN, Almeshekah MH, Spafford EH, Atallah MJ, Avery J. Inhibiting and Detecting Offline Password Cracking Using ErsatzPasswords. *ACM Trans. Priv. Secur.* 2016; 19(3): 9:1–9:30. doi: 10.1145/2996457

16. Feizollah A, Anuar NB, Salleh R, Amalina F, Ma'arof RR, Shamshirband S. A study of machine learning classifiers for anomaly-based mobile botnet detection. *Malaysian Journal of Computer Science* 2014; 26(4).

17. La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices. *IEEE communications surveys & tutorials* 2013; 15(1): 446–471.

18. Miles MB, Huberman AM. *Qualitative data analysis: An expanded sourcebook*. Sage . 1994.

19. Rogers Y, Preece J, Sharp H. *Interaction Design: Beyond Human-computer Interaction*. Wiley. 4 ed. 2015.

20. Hammersley M, Atkinson P. *Ethnography: Principles in practice*. Routledge. 3 ed. 2007.

21. Osborn E, Simpson A. On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security* 2017; 70: 27–50.

22. Austin RD, Nolan RL, O'Donnell S. IT Priorities, Prioritizing Among a Portfolio of Projects. In: Harvard Business School Publishing Corporation. USA. 2009.

23. Dong Z, Kane K, Camp LJ. Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks. *ACM Trans. Priv. Secur.* 2016; 19(2): 5:1–5:31. doi: 10.1145/2975591

24. Jung Y, Park J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management* 2018; 43: 15 – 24. doi: https://doi.org/10.1016/j.ijinfomgt.2018.05.007

25. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 2017; 64: 122–134.

26. Ramachandran V. *Backtrack 5 Wireless Penetration Testing: Beginner's Guide*. Packt Publishing Ltd . 2011.

27. Tzu S. *The art of war*. CreateSpace Independent Publishing Platform . 2016.

28. Sharan R. Hacking Techniques - Scanning Networks and Countermeasures. [Blog]; 2010.

29. Beaver K. *Hacking for dummies*. John Wiley & Sons. 4 ed. 2013.

How to cite this article: M. Markou, and A. Piki (2020), An Exploration of Cyber-Security in Free Public Wi-Fi Networks, *Engineering Reports*, .