SACRAMENTO STATE
COLLEGE OF ENGINEERING & COMPUTER SCIENCE

Comprehensive Overview of Mobile Security

Anthony Chavez, Mario Palacios
Professor Jun Dai
California State University, Sacramento
6000 J St, Sacramento, CA 95819

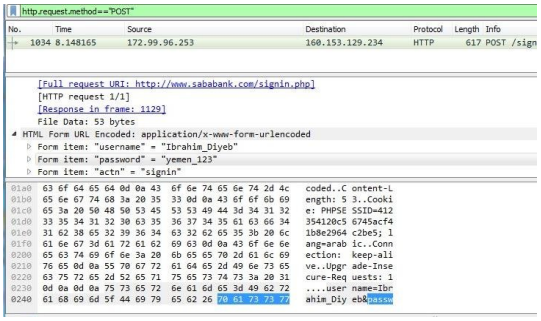
Abstract — In today's society, just about any product in the Internet of Things ecosystem is hackable. With several consumers and businesses utilizing such products, cyber security is becoming more prevalent and necessary to mitigate the various vulnerabilities becoming available to cyber attackers. Our project focuses on these Mobile Security vulnerabilities and the countermeasures to be taken.

1. Unsecure WiFi

1.1. Introduction

Today, most public areas such as airports, coffee shops, and hotels provide some form of free, public Wi-Fi. According to one study, 78 percent of people around the world actively look for Public Wi-Fi sources and 72 percent of those have complete confidence in connection without any regard to security.[1] However, these types of connections can allow hackers to easily monitor unsuspecting, connected users' activity and capture sensitive information like login credentials for a user's bank account. Packet

1.2. Incident / Possible Scenario



Wireshark Filtering Showing Amy's Username and Password in plain text [2]

For example, Amy walks into a local Starbucks to get a cup of coffee and begins browsing the Internet on her laptop. Meanwhile, a hacker who has been pretending to be studying is passively sniffing the coffee shop's network. Since the network lacks any form of data encryption, all of Amy's data packets are being transmitted in plain text. Amy remembers that it's payday and decides to check her banking account. Upon entering in her login credentials, she has already compromised her banking account's integrity now that the hacker can gain access to her account using the login information captured from the unencrypted data packets.

1.3. Countermeasures

Although public Wi-Fi isn't secure, there are several countermeasures one can use to secure their traffic on such connections.

First, a user can use a Virtual Private Network (VPN) when connected to public Wi-Fi. A VPN will make you more anonymous online and encrypt your network traffic. Some great examples of trusted VPN service providers are ExpressVPN and SurfShark. However, steer clear of free VPN service providers as they generally contain malware, track your online activity and sell it for profit, bombard you with ads, and slow your internet speeds. [3]

Another option is to use SSL connections when browsing the Internet. A user can configure his/her browser settings to HTTPS-Only Mode to upgrade all connections to HTTPS if the site supports HTTPS. If a user's browser does not already have such a built-in setting, there are some browser extensions such as HTTPS Everywhere that accomplish the same goal.

Additionally, turning off file sharing, "Network Discovery" settings, and having any trusted anti-virus software can stop attackers in their tracks. File sharing could allow attackers to gain unwanted access to a user's public folders. "Network Discovery" allows attacker's scanners to detect your devices and become a potential target. Anti-virus software not only offers malware detection through system scans, but also provides real-time protection when browsing the web and downloading files.

2. Phishing

2.1. Introduction

Phishing is when a cyber criminal impersonates an individual or organization in hopes of gaining the trust of an unsuspecting user. There are several phishing techniques that hackers can use, one of them being Smishing (SMS Phishing). Smishing is when an attacker sends text messages to several phone numbers at a time with a link to some fraudulent website. Another form of phishing is Vishing (Voice Phishing) which is when a criminal calls a target and attempts to get sensitive information by posing as an organization representative for the victim's bank or insurance.

2.2. Incident / Possible Scenario

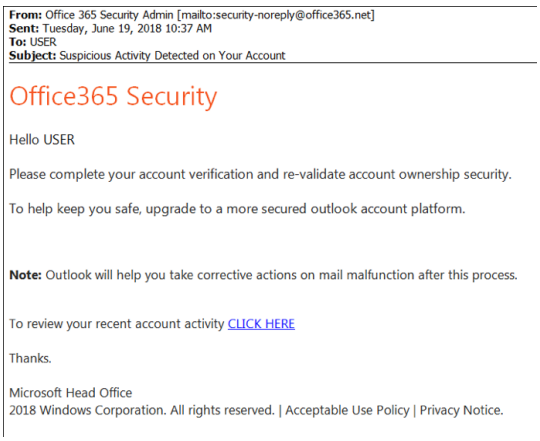
Back in 2014, Ryan Collins leaked hundreds of nude photographs of celebrities like Jennifer Lawrence, Ariana Grande, and Kate

Upton from their iCloud accounts. Collins pretended to be an employee at Apple and sent phishing emails asking the celebrities to reset their password. Thinking the emails were legit, the celebrities willingly entered their password. Upon receiving the login credentials, Collins then was able to obtain the photos from the celebrities accounts. [4]

2.3. Countermeasures

In order to avoid becoming a victim of a phishing attack, there are several red flags to look for when receiving messages through an email, SMS, and phone call.

Starting with email and SMS phishing attacks, a user must pay close attention to who the message is from, the subject matter, hyperlinks, and attachments.


From: Office 365 Security Admin [mailto:security-noreply@office365.net]
Sent: Tuesday, June 19, 2018 10:37 AM
To: USER
Subject: Suspicious Activity Detected on Your Account

Office365 Security

Hello USER

Please complete your account verification and re-validate account ownership security.

To help keep you safe, upgrade to a more secured outlook account platform.

Note: Outlook will help you take corrective actions on mail malfunction after this process.

To review your recent account activity CLICK HERE

Thanks.

Microsoft Head Office
2018 Windows Corporation. All rights reserved. | Acceptable Use Policy | Privacy Notice.

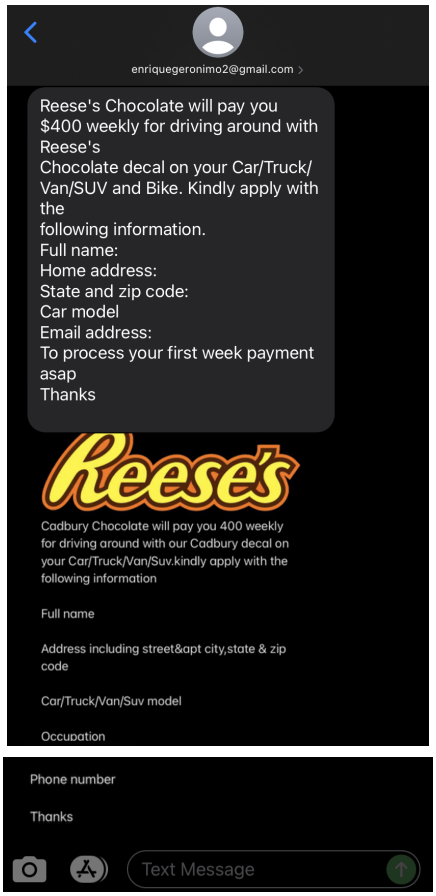
Phishing Email with Fraudulent Hyperlink [5]

Referring to the image above, a user must determine if the sender is trustworthy. Some questions to think about are, "Do I recognize this email address or phone number?", "Is the email address from a suspicious domain (such as office365protectionservices)?", or "Does anyone I know recognize the sender's email address or phone number?"

Based on the image above, a user must read the content of the message carefully. Most of the time, scammers carelessly misspell words or have poor grammar and they will try to give a sense of urgency to avoid a negative consequence or to obtain a prize by providing a hyperlink or attachment to click.

Most fraudulent emails will be filtered out by a properly configured firewall and mailbox filters. Additionally, employees should be given training courses to become familiar with such attacks to ensure the integrity and confidentiality of the network's resources and user information.

As for phone call scams, the same red flags apply. However, the best course of action is to not answer the phone call if you do not recognize the phone number. If a user does answer the call, do not ask or answer any questions and hang up immediately. Even answering with a simple 'Yes' response can jeopardize accounts in the user's name.



Smishing Text Message Received by Anthony

3. Cryptojacking

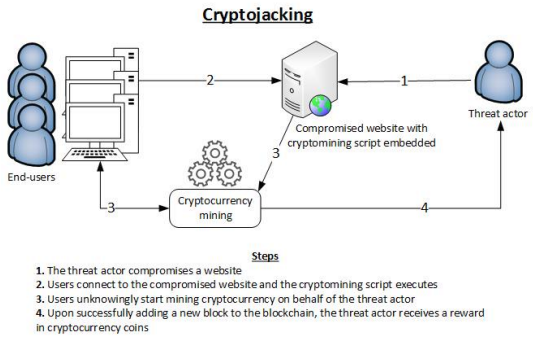
3.1. Introduction

According to The European Agency for Cybersecurity (ENISA), cryptomining is the process by which cryptocurrency transactions are verified and added to a public ledger, known as the blockchain … [and] by which new cryptocurrency coins are released." [6] In the past, cryptomining used to be only possible through using specialized mining software, so an adversary would need to install such software

onto a victim's system through using trojan horses or phishing techniques. However, with the introduction of Coinhive, which allows website owners to embed this code into their website, has visitors mine cryptocurrency, and generates revenue without placing ads on the site.

On the other hand, adversaries have leveraged this new technology through cryptojacking, "[t]he technique of hijacking browsers for mining cryptocurrency (without user consent)." [6] Even legitimate sites are guilty of cryptojacking if they do not ask visitors for their consent or allow them to opt-out of using their browser to mine. Although Coinhive was shut down back in 2019, several alternatives such as Minr, Crypto-Loot, and CoinImp still remain.

Crypto miners do not steal data or modify any users' data, instead, the system and network resources are at risk. Users may experience slower system and network performance since crytpomining is highly CPU and GPU intensive. For the average user, this wouldn't seem any more than a nuisance. However, for larger corporations with hundreds of systems on a network, this could lead to a major headache for the employees, especially the IT department.

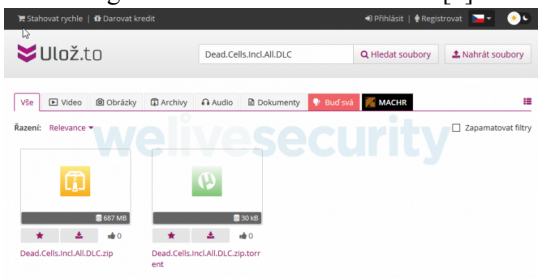


Cryptojacking In Action[6]

3.2. Incident / Possible Scenario

There are several kinds of cryptojacking malware, but some of them come with extra features like stealing cryptocurrency wallet addresses. For example, KryptoCibule has been a triple threat since December 2018. KryptoCibule is capable of exploiting the CPU and GPU of infected computers to mine for Moneero and Ethereum, monitoring the user's clipboard for a cryptocurrency wallet address, and scraping drives on the infected computer for content such as passwords and private keys. [7]

According to ESET's research, KryptoCibule has primarily been distributed through malicious torrents posing as pirated software and video games on uloz.to; a popular file sharing site in Czechia and Slovakia. [8]



One of the malicious torrents on uloz.to [8]

To avoid detection, KryptoCibule has two ways of hiding it's background processes. First, the malicious installer will not deploy it's cryptomining code if the system is running any security products by Avast, AVG, and ESET. This still leaves the system exposed to the malware's clipboard monitoring, drive scraping, and Remote Access Trojan (RAT) which allows adversaries to utilize a backdoor to install additional malicious code. [8] Second, KryptoCibule's cryptomining code monitors the system's battery level and user's inactivity time to determine resource utilization for mining. There are three cases on which the mining code operates. First, cryptomining will not occur if the system's battery level is below 10%. [7] Since cryptomining is resource intensive, the battery will drain rather quickly and this could easily draw the user's attention. Second, between 10% and 30%, only CPU mining will occur and GPU mining will be suspended. [7] Since CPU mining isn't as intensive as GPU mining, the battery life of the system would not drop quickly enough to draw attention. Third, both GPU and CPU mining will run without limits when the battery level is 30% or more and the user has been inactive for the past three minutes. [7]

3.3. Countermeasures

The most obvious countermeasure to consider is to be extremely cautious when torrenting files. Most users should refrain from torrenting if they do not understand the risks of torrenting or lack proper preparation to protect their system. Therefore, a user must do plenty of research to gain a general understanding of how torrenting works, the risks associated with torrenting, and how to prevent any unwanted harm to their system.

Some other precautions to consider when torrenting are to have a reputable antivirus

software and Virtual Private Network (VPN) installed on the system used for torrenting. Antivirus software will thwart most malicious installers from executing and the VPN will help keep your identity safe.

As for preventing cryptojacking while browsing the Internet, installing a reputable ad blocker can help prevent the cryptomining code from executing when visiting sites that have embedded cryptominers. Additionally, having IT monitor the network for suspicious traffic and investigating any reports of slow or overheating systems in the IT ticket system will help mitigate cryptojacking threats.

4. Jailbreaking and Rooting Phones

4.1. Introduction

Jailbreaking is the process of removing software restrictions set in place by a device's manufacturer. [9] Primarily, jailbreaking is done on iPhones and any other Apple devices. On the other hand, Rooting is the process of gaining root access to an android device or any device running a Linux operating system. [9] Some benefits of jailbreaking and rooting a device are allowing the user to install tweaked apps, customize the appearance of the interface, and remove bloatware. However, some risks of jailbreaking and rooting include third-party app vendors distributing malware, devices are unable to receive software updates, and losing access to some app services such as banking and social media.

4.2. Incident / Possible Scenario

Back in late 2015, 250,000 Apple accounts were hijacked by KeyRaider, a malware that only infects jailbroken iOS devices. The malware is able to leverage Cydia, a jailbreak exclusive app store that allows users to download tweaked apps and custom themes. Once the malware infects a device, iTunes traffic such as passwords, usernames, the device's GUID can be intercepted. Furthermore, the hackers were reported making in-app purchases without paying using the stolen user credentials in the official Apple app store. [10]

In addition, the hackers could gain access to a user's iCloud account and obtain contact lists, photos, emails, iMessage logs, and sell users accounts to spammers to use for premium SMS. [10]

4.3. Countermeasures

There are four ways to detect if an iOS device is jailbroken. First, the Cydia package manager can only be installed on jailbroken devices and is responsible for installing unauthorized iOS binaries. Second, changes in file permissions and system partitions can be signs of jailbreaking. Third, some system APIs can be leveraged by jailbreak detectors by calling functions such as system(). [11] Here are some examples of the expected outputs for a non-jailbroken and jailbroken device:

System( )	Jailbroken
0	no
1	yes

Fork( )	Jailbroken
Failure	no
Success	yes

_dyld_image_name(...)	Jailbroken
-	no
'MobileSubstrate'	yes

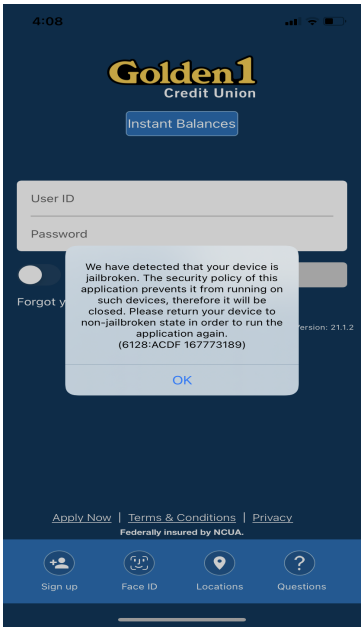
System API function calls and outputs [11]

Fourth, a jailbreak detector could try verifying an incorrect code signature. [11] It is known that a non-jailbroken device will report a bad signature error, but a jailbroken device will always validate.

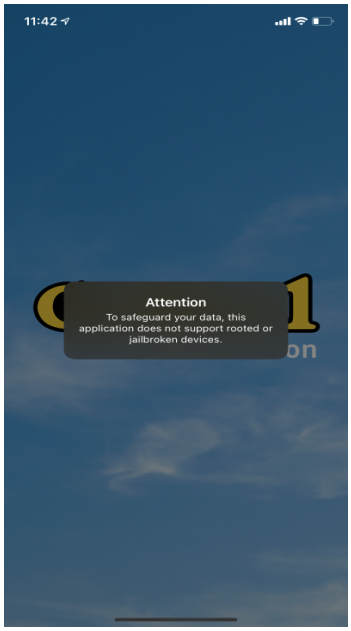
As for Android devices, the same root detection techniques for iOS devices will work. Unlike iOS, Android has an official root detection package called SafetyNet. This package uses billions of devices that are play-enabled to gather information from various sources and use this data to detect rooted devices. Some signs of a rooted Android device include the presence of several

packages, build tags not containing "standard" values, and changed permissions.

One countermeasure that has been put in place by most app developers is restricting any jailbroken or rooted device from accessing their app's services. For example, banking apps like Golden 1 Credit Union will not allow a user to log into their account. On Anthony's rooted device, the banking system will display the following error message upon opening the app:



Golden 1 Credit Union (old interface)



Golden 1 Credit Union (new interface)

5. Broken Cryptography

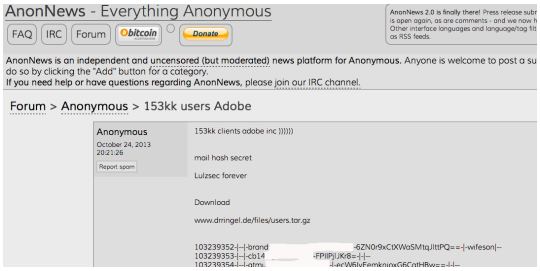
5.1. Introduction

Broken Cryptography involves exploiting weak encryption algorithms or even flaws within the encryption process. As an attacker they take advantage of this but first they must successfully return encrypted code/sensitive data back from its original form. This can be done by decryption of data via physical access to the device/network traffic capture or by malicious apps on a device with access to the encrypted data [12].

5.2. Incident / Possible Scenario

The following scenarios can result in such an attack being done; reliance upon built-in code encryption process, poor key management processes, creation and use of custom encryption protocols, and lastly use of insecure and/or deprecated algorithms. Overall this type of attack can have major impact on businesses such as; privacy violations, information theft, code theft, intellectual property theft, or even reputational damage [12].

On October 4, 2013, Adobe's poorly designed cryptography led to the data breaching of 153 million Adobe accounts. Nearly 3 million encrypted customer credit card records, along with login data for an undetermined number of user accounts [13]. All this was done by attackers that got a hold of Adobe Photoshop source code. During this course a file was uploaded to a website which was a tar file containing about three gigabytes of usernames and hashed passwords.



Post of Tar File Containing Username and Passwords [14]

5.3. Countermeasures

As stated in the previous section of possible scenarios that can lead to attacks, if the opposite is done then it can be sufficient enough to prevent attackers from exploiting Broken Cryptography. If as a developer try not to use algorithms that have

known weakness or try to develop new/custom encryption algorithms.

A strong algorithm that has been successful in creating strong encryptions is called RSA. It works on a block cipher concept that converts plain text into ciphertext and the same goes for the receiver side [18]. It creates a public and private key, where if the public key is used to decrypt something it will need the private key as well.

Having a private key is a good concept/idea, however this is just the beginning of having good encryption. Maintaining a strong key management is also essential. There should be a strong implementation of creating strong private keys, good key rotation, established control access to keys, and proper disposal of keys.

6. Data Leakage

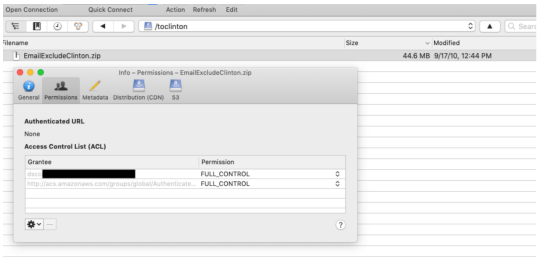
6.1. Introduction

Not to get confused with a Data Breach, a Data Leakage does not require a cyber attack but usually comes from poor data security practices or accidents by an individual. Cyber criminals look for Personal Identifiable Information (PII) or even Protected Health Information (PHI). Some common ways that Data Leaks are exploited are by social engineering, doxxing, surveillance/intelligence, and disruption [15]. One thing to keep in mind that can cause Data Leaks is poor application security and cybersecurity measures in the data custody chain.

6.2. Incident / Possible Scenario

Healthcare, finance, and politics are the areas that most personal data is being collected and used. In one case involving the Democratic Senatorial Campaign Committee (DSCC) approximately over 6 million email addresses were exposed due to a misconfiguration in an Amazon S3 Storage Bucket. The comma separated list containing email addresses from universities, government agencies, email providers, and military, was uploaded in 2010 by a DSCC employee [16].

Then in 2019 it was discovered by researchers, the bucket was available to globally authenticated AWS users, which is one of two public groups available in the S3 permissions. Upon further examination it was found that one of the users tied to the storage bucket worked for the DSCC. In this case the storage bucket was set to "FULL_CONTROL" meaning anyone can download/modify the contents or even change the permissions to the storage bucket, which could've led to a complete loss of data. [16].



Screenshot of S3 Storage Bucket Permissions [16]

6.3. Countermeasures

As saving data onto cloud storage becomes more available to people, the amount of data being moved is growing exponentially [15]. The scenario seen in the previous section will become more common. That is why it is important to check cloud storage configurations. Continuous validations will minimize the risk of data leakage. Along with checking the configurations one can even automate process controls which ensures that cloud storage is always secured [15].

Having third party vendors can also lead to a data leakage. Where these third party vendors might not take cybersecurity as seriously as the company hiring them. As a company one can send out questionnaires or risk assessments to assess the state of security being upheld at these third party vendors.

7. Hardware Trojans

7.1. Introduction

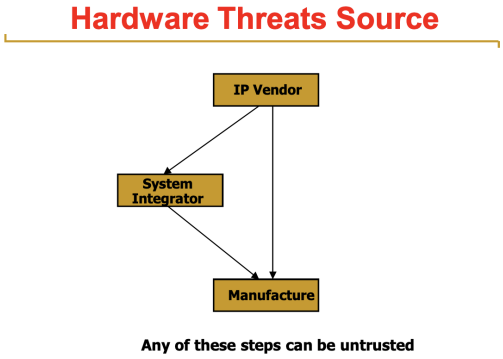
A malicious addition or modification to existing circuit elements; that can change functionality, reduce reliability, and leak valuable information from a device [12]. Two types of Hardware Trojans are Back Door; where an attacker can disable, blowup, send wrong processing data, and impact circuit information on a chip. The other is Time Bomb that can cause major reliability issues and has the advantage of not being detected because it does not impact the functionality of the circuit [12].

In the Trojan classification there are three major types; physical, activation, and action. Physical Trojans take advantage of their type, size, distribution, and structure. Trojans that are activated can be done so externally via antenna/receiver or accessing data and internally via condition or having it always running. While action Trojans exploit hardware by modifying

function, specification, or manipulate the information being transmitted [12].

7.2. Incident / Possible Scenario

Hardware threats pray on the trust of one another and there are three scenarios in which untrust can lead to a Hardware Trojan attack. The first one area of untrust can be with the IP (Intellectual Property) Vendor with the System Integrator and Manufacturer. Where the IP vendor can install Trojans in the IP before sending it to either.



Hardware Possible Scenarios [12]

The next is with the System Integrator that can be a victim or even an attacker. It could face an attack from the IP Vendor as stated before or even pass on the attack from IP Vendor and pass it to the Manufacture who could be the one to trigger the attack or be the intended victim.

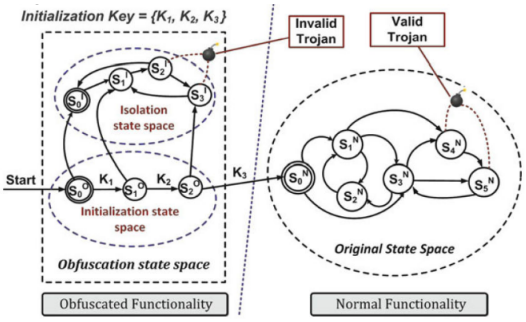
7.3. Countermeasures

Even when there is trust amongst all parties in the creation of devices there needs to be a way to check if IP will contain a Trojan. It can start at a pre-synthesis level where a formal verification is conducted that checks the property, model, and equivalence; a coverage analysis can also be done that goes over the coverage of code and functionality.

In this approach the formal verification will ensure the IP is exactly the same as it is specified and nothing more or less. Every requirement is defined as listed in testbenches and has been checked. While the coverage analysis will look at every line of code to understand what states can be reached in the Finite State Machine diagrams and check each signal in gate-level. While this seems like a fine countermeasure, it ensures only that it will carry out the desired function only and does not focus on detection [12].

There are two approaches one can take when trying to detect Hardware Trojans, a non-destructive or a destructive. When going the destructive path it can be time consuming and expensive. An engineer would have to reverse engineer the IP by extracting it layer-by-layer using a Scanning Electron Microscope; this will identify transistors/gates and routing elements [12]. The non-destructive approach focuses more on run-time monitoring, to try to exploit pre-existing redundancies in a circuit by comparing results and selecting trusted parts to avoid infected parts on a circuit [12]. Another non-destructive way is to try and detect Trojans throughout the test duration by doing either a logic-testing or side-channel analysis.

Lastly another way to deter attackers from inserting Trojans inside the design is by designing obfuscation. The idea behind this is to transform the design to another one but still keeping the functionality equivalent to its original state [12]. This will make it much more difficult for attackers to obtain complete understanding of the internal logic and reverse engineering.



Design of Obfuscation [12]

References

[1] finjanmobile, “The Dangers of Using Unsecured Wi-Fi: How Bad is it, Really?,” *Finjan Mobile*, 01-Aug-2018. [Online]. Available: https://www.finjanmobile.com/the-dangers-of-using-unsecured-wi-fi/. [Accessed: 15-Oct-2021].

[2] Thiyeb, Ibrahim & Saif, Anwar & Al-Shaibany,Nagi. (2018). Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study. International Journal of Computer Network and Information Security. 10. 12-22. 10.5815/ijcnis.2018.07.02.

[3] Levavi-Eilat, S., 2021. *Are VPNs Safe? Some Aren't (And It's Not Only the Free Ones)*. [online] vpnMentor. Available at: <https://www.vpnmentor.com/blog/free-vpns-are-not-safe-to-use/> [Accessed 15 October 2021].

[4] Cook, J., 2016. The US government says it has found the man behind the massive iCloud celebrity photos hack. *Insider*, [online] Available at: <https://www.businessinsider.com/ryan-collins-allegedly-naked-photographs-celebrity-icloud-2016-3> [Accessed 18 October 2021].

[5] Center for Internet Security. 2021. *A Short Guide for Spotting Phishing Attempts*. [online] Available at: <https://www.cisecurity.org/blog/a-short-guide-for-spotting-phishing-attempts/> [Accessed 18 October 2021].

[6] Enisa.europa.eu. 2017. *Cryptojacking - Cryptomining in the browser*. [online] Available at: <https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser> [Accessed 23 October 2021].

[7] Cluley, G., 2020. Newly-discovered KryptoCibule malware has been stealing and mining cryptocurrency since 2018. [Blog] *Tripwire*, Available at: <https://www.tripwire.com/state-of-security/featured/kryptocibule-malware-stealing-mining-cryptocurrency/> [Accessed 23 October 2021].

[8] Faou, M. and Côté Cyr, A., 2020. *KryptoCibule: The multitasking multicurrency cryptostealer | WeLiveSecurity*.[online] WeLiveSecurity. Available at: <https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/> [Accessed 23 October 2021].

[9] Hoffman, C., 2017. What's the Difference Between Jailbreaking, Rooting, and Unlocking?. [Blog] *How-To Geek*, Available at: <https://www.howtogeek.com/135663/htg-explains-whats-the-difference-between-jailbreaking-rooting-and-unlocking/> [Accessed 21 October 2021].

[10] Salmi, D., 2015. Apple jailbroken phones hit with malware. [Blog] *Avast*, Available at: <https://blog.avast.com/2015/09/02/apple-jailbroken-phones-hit-with-malware/> [Accessed 22 October 2021].

[11] Rupp, M., 2020. *Application Hardening for Mobile Banking Apps: Root and Jailbreak Detection*. [online] Cryptomathic.com. Available at: <https://www.cryptomathic.com/news-events/blog/application-hardening-for-mobile-banking-apps-root-and-jailbreak-detection> [Accessed 22 October 2021].

[12] Mohammad Tehranipoor Modified / updated by Siavash Bayat-Sarmadi *Hardware Trojans,* [*Lecture*] Available at: http://ce.sharif.edu/courses/92-93/2/ce843-1/resources/root/Slides/04-Hardware%20Trojan.pdf [Accessed 5 December 2021]

[13] Harshit Agarwal, 2015, *Understanding OWASP Top 10 Mobile: Broken Cryptography* [*Blog*] Available at: https://www.appknox.com/blog/understanding-owasp-top-10-mobile-broken-cryptography [Accessed 30 November 2021]

[14] Brian Krebs, 2013 *Adobe Breach Impacted At Least 38 Million Users* [*Blog*] Available at: https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ [Accessed 30 November 2021]

[15] Abi Tyas Tunggal, 2021, *What is a Data Leak? Stop Giving Cybercriminals Free Access* [*Post*] Available at: https://www.upguard.com/blog/data-leak [Accessed 30 November 2021]

[16] UpGuard Team, 2019, *Political History: How A Democratic Organization Leaked Six Million Email Addresses* [*Post*]

Available at: https://www.upguard.com/breaches/data-leak-dscc-six-million-email-addresses [Accessed 2 December 2021]

[17] Chris Northwood, *Cryptography, Attacks and Countermeasures* [*Notes*] Available at: https://www.pling.org.uk/cs/cry.html [Accessed 6 December 2021]

[18] IntelliPaat, 2021, *What is Cryptography?* [*Article*] Available at: https://intellipaat.com/blog/what-is-cryptography/#7 [Accessed6 December 2021]