BISM3205 Assignment 1

Daniel Ciccotosto-Camp

S45857278

Question 1 solns:

a) The first question deciphers to:

CONGRATULATIONSYOUHAVECOMPLETEDTHEFIRSTQUESTIONSUCESSFULLY

b)

The Enigma machine uses a polyalphabetic *substitution cipher*, which is a type of cipher that replaces each letter in the plaintext with a different plaintext letter based on a series of substitution alphabets. The enigma machine introduces complexity into its polyalphabetic substitution using moveable rotors (I to VIII) which each internally had unique mappings of the English alphabet. When deciphering text, each keystroke caused the rightmost rotor to rotate one step so that subsequent text it would not be enciphered with the same ciphertext letter (piotte13, 2016).

Further complexity was added to the enigma machine with a plugboard, which allowed pairs of letters to be swapped before going through the moveable elements of the enigma. These components combined made the Enigma's encryption extremely complex and difficult to break without knowledge of the machine's configuration settings.

c) The deciphered message from 1a), using the setting outlined in the task description, now becomes:

HJGCPHSIIELUKQTGGLXRCSHPCOQRQJEZDTINSGOOPRLIASQYSWXULGDISAH

Question 2:

a)

Phishing is a type of cyber-attack where attackers attempt to trick individuals into divulging personal or confidential information such as passwords or credit card details. This attack vector often involves deceptive emails, messages, or websites that appear legitimate but are crafted to manipulate the victim into sharing their sensitive data.

The term "phishing" was coined in the mid-1990s when cybercriminals used these tactics to impersonate AOL (America Online) staffers and message victims to reveal their passwords and credit card information. (Gillin, 2024)

b) What is spear phishing?

Spear phishing is a specialised and targeted phishing attack aimed at specific individuals within an organisation. Like phishing, cybercriminals craft personalised messages to deceive their victims into revealing sensitive information (including passwords or administrative access), which is especially valuable due to the extensive access and power the individual may provide within the company (Kosinski, 2024).

c) What is clone phishing?

Clone phishing is a phishing attack where an attacker replicates a legitimate email or message with a cloned message, replacing the contents with malicious links or malware under the guise as the original attachments. The cloned message is sent to the victim under the guise of it being a resend or update, to deceive them into engaging with harmful content (Eemeli, 2024).

d) What is whaling?

Whaling is a type of phishing attack that specifically targets high-profile individuals within an organisation, such as executives or senior managers. These type of phishing attacks use personalised messages to deceive high-target individuals into revealing sensitive information or authorising fraudulent transactions (mimecast, 2024).

e) What is vishing?

Vishing, or ‘voice phishing’, is a type of phishing attack where attackers use phone calls or voice messages to deceive individuals into providing sensitive information, such as passwords, credit card numbers, or personal details. The attacker often impersonates a legitimate entity, such as a bank or government agency, to gain the victim's trust and trick them into revealing confidential information (kasperkey, 2024).

f) What is Pharming?

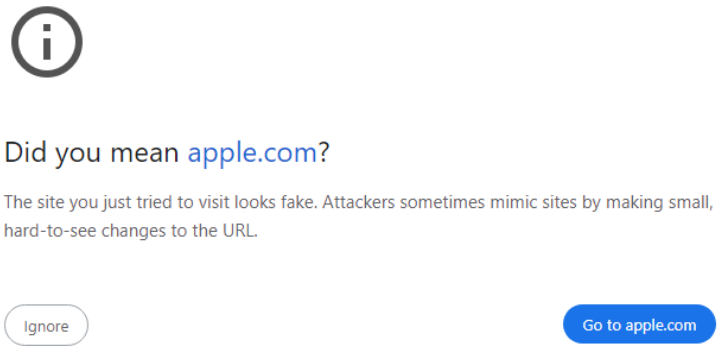
Pharming is a type of cyber attack where an attacker redirects a website's traffic to a fraudulent website without the user's knowledge. This is typically done by exploiting vulnerabilities in the DNS (Domain Name System) or compromising the user's device. The goal is to trick users into entering sensitive information, such as login credentials or financial details on the fake website, which looks almost identical to the legitimate one (Malwarebytes, 2024).

g) Homoglyph Attack

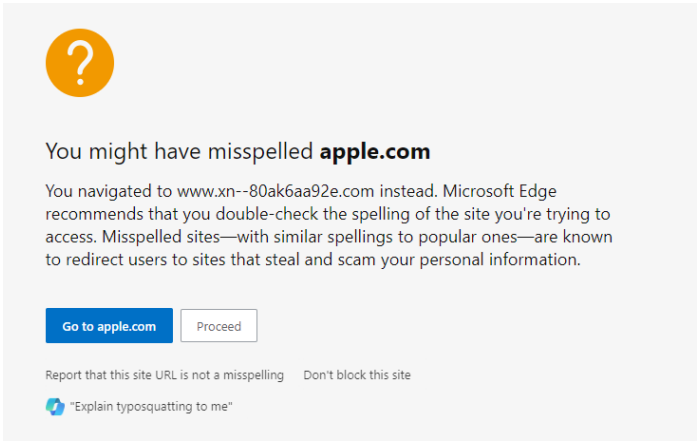
This type of attack is called a Homoglyph Attack. It works by using characters from different character sets that visually resemble standard characters but are actually different. In this case, the URL uses a character that looks almost identical to the standard letter ‘a’ but is actually a different Unicode character. When users click on the link, they may think they are visiting a legitimate site, such as "apple.com," but they are actually being directed to a malicious website that could be used for phishing or other types of cyber attacks. This kind of deception exploits the similarity between characters to trick users into visiting harmful websites (OCD Tech, 2023).

The following browsers display warnings on a potential homoglyph attack.

Chrome:



Edge:



h) Preventative measures – Phishing attacks

1. Security Awareness and training: Educate employees to identify telltale signs of phishing scams in emails, attachments and letters. Courses such as Phriendly Phishing – security awareness training can be provided to employees as both training and simulated phishing to improve their responses (Phriendly Phishing, 2024).

2. Implement Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring multiple forms of verification for accessing sensitive systems and data. This makes it harder for attackers to gain unauthorised access, even if they have obtained user credentials (Coates, 2024).
3. Use Spam Filters or Secure Email Gateways to Block Deceptive Emails: Employ email filtering and anti-phishing software, such as spam filters or secure email gateways, to monitor and block phishing emails before they reach employees' inboxes. These tools help identify and prevent unwanted or fraudulent content from reaching staff (Office of then Victorian Information Commissioner, 2024).
4. Establish Clear Reporting Mechanisms and Report Phishing Attempts: Create straightforward procedures for employees to report suspected phishing attempts, allowing IT teams to respond quickly and prevent widespread harm. Encourage reporting to relevant authorities. Australian-based organisations, can report their scams to the national anti-scam centre *Scamwatch* (Australian Signals Directorate, 2024).

i)

A 10Mbps (Megabits per second) digital communication device can send:

$$10(\text{Mbps}) \cdot 10^6 = 10{,}000{,}000 \text{ bits}$$

Assuming no latency, jitter and packet loss, all the bits sent could be '1's in a digital signal, thus the most '1' bits sent over a 10Mbps communication link is 10 million ($10{,}000{,}000$).

j)

The MD5 hash has known vulnerabilities, including its susceptibility to collision attacks (where two different inputs can produce the same hash value) and preimage attacks (finding an input that hashes to a specific hash value). Because of known vulnerabilities, MD5 is no longer considered secure for protecting valuable data. In contrast, SHA-256, part of the SHA-2 family, addresses many of these issues by offering stronger security, better collision resistance, and a longer hash length.

Mathematic comparison of brute-force time:

MD5 generates a 129-bit has, leading to 2^{128} possible hashes.

Assuming an attacker can compute 10^{12} hashes per second:

$$\text{Time (seconds)} = \frac{2^{128}}{10^{12}} \approx \frac{3.4 \times 10^{38}}{10^{12}} = 3.4 \times 10^{26} \text{ seconds}$$

However, due to MD5's known weaknesses, effective attacks could drastically reduce this time.

Compared to the SHA256 Hash, which generates a 256-bit hash:

$$\text{Time (seconds)} = \frac{2^{256}}{10^{12}} \approx \frac{1.16 \times 10^{77}}{10^{12}} = 1.17 \times 10^{65} \text{ seconds}$$

Given these significant differences in security and the time required to brute-force, it would be better to use SHA-256 rather than MD5 to hash your valuable data before backing it up to prevent unauthorised access.

Question 3

1. Identifying the Appropriate Notices

The AFP have express authority to issue either a TAR or TAN, but issuing a **TAN** in this case seems most appropriate. Securechat may be reluctant to respond to a TAR, and since SecureChat is already an established encrypted messaging app, they likely have existing capabilities that the AFP could compel them to use. A TCN might be considered if SecureChat is reluctant or their current capabilities are insufficient but this would require the authority of the Attorney-General.

2. Legal and Procedural Requirements

Legal Authority and considerations**:** The AFP must have an existing legal authority, such as a warrant, before issuing a TAN. The decision maker (a senior official in the organisation) must be satisfied that the request of requirement is reasonable and proportionate, and that compliance is practicable and technically feasible. Before exercising their authority to issue a TAN, the decision make must consider whether the notice is the minimally invasive form of industry assistance as to not introduce vulnerabilities into the organisations' systems.

Systemic Weaknesses**:** The AFP must ensure that their requests do not force SecureChat to implement systemic weaknesses or vulnerabilities in their systems. The AFP must work closely with SecureChat to find a solution that meets the investigation's needs without compromising overall security.

3. Impact on Stakeholders

Impact on SecureChat**:** Assisting law enforcement could tarnish SecureChat's reputation if users perceive that their privacy is compromised. Cooperating with the AFP under the TOLA Act could position SecureChat as a responsible company that supports lawful investigations, improving their reputation with users who value security and collaboration with law enforcement.

Impact on Users: Users may lose trust in SecureChat if they believe the platform can no longer guarantee privacy of their communications. This could lead to financial implications and loss in market share.

Broader Societal Implications: While the TOLA Act aims to aid law enforcement, it raises concerns about overreach and the potential for abuse. If mismanaged, the Act could undermine public trust in encrypted communications, leading to broader societal concerns about privacy and civil liberties.

Question 4

Asset valuation by:	Daniel Ciccotosto-Camp											
Asset	**Attack**	**Impact to revenue**	**Probability**	**Weight**	**Impact to public image**	**Probability**	**Weight**	**Asset value**	**Likelihood**	**Current controls effectiveness**	**Certain of assumptions**	**Relative Risk**
Oracle SQL Database	Insider Abuse	High	80%	75	Moderate	65%	25	76.25	10%	70%	80%	3.81
UNIX transaction server	malware	Very high	100%	75	High	80%	25	55	20%	50%	90%	**6.60**

Quantitative and qualitative risk data points	
Very high	100%
High	80%
Moderate	65%
Medium	50%
Low	35%
Very Low	20%

Weighted Factor Analysis	
Information Asset	Criterion Weight
Impact to Revenue	75
Impact to Public Image	25
Weighted Score	100

References

Australian Signals Directorate. (2024, August 25). *Scams are a common way that cybercriminals compromise accounts*. Retrieved from Australian Government: https://www.cyber.gov.au/learn-basics/explore-basics/recognise-and-report-scams

Coates, S. (2024, July 10). *5 ways to prevent a phishing attack in Microsoft 365*. Retrieved from Intelogy: https://www.intelogy.co.uk/blog/5-ways-to-protect-against-a-phishing-attack-in-microsoft-365/

Eemeli. (2024, April 11). *Clone Phishing: Here's What You Need to Know To Protect Your Organization*. Retrieved from HoxHunt: https://hoxhunt.com/blog/clone-phishing#:~:text=Clone%20phishing%20is%20a%20type,trick%20you%20or%20your%20employees.

Gillin, P. (2024, August 25). *The history of Phishing*. Retrieved from Verizon Business: https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/#:~:text=The%20first%20phish,passwords%20and%20hijack%20their%20accounts.

kasperkey. (2024, August 25). *What Is Vishing?* Retrieved from kasperkey: https://www.kaspersky.com/resource-center/definitions/vishing

Kosinski, M. (2024, June 6). *What is spear Phishing*. Retrieved from IBM: https://www.ibm.com/topics/spear-phishing#:~:text=Spear%20phishing%20is%20a%20type,sending%20money%20to%20an%20attacker.

Malwarebytes. (2024, August 2024). *What is pharming?* Retrieved from Malwarebytes: https://www.malwarebytes.com/pharming?srsltid=AfmBOoo_1jy5JHf-nLpoxSzsjMV4EVqlYi2PeIhVmbZi0-I9dSCrA0yI

mimecast. (2024, August 25). *What is a whaling phishing attack?* Retrieved from mimecast: https://www.mimecast.com/content/whaling-phishing-attacks/#:~:text=A%20whaling%20attack%20is%20a,transfer%20to%20a%20fraudulent%20account.

OCD Tech. (2023, March 3). *What is a Homoglyph Attack?* Retrieved from OCDTech: https://ocd-tech.com/2023/03/03/homoglyph-attack/

Office of then Victorian Information Commissioner. (2024, August 25). *Phishing Attacks and How to Protect Against Them*. Retrieved from Office of then Victorian Information Commissioner: https://ovic.vic.gov.au/privacy/resources-for-organisations/phishing-attacks-and-how-to-protect-against-them/

Phriendly Phishing. (2024, August 25). *Phishing simulation & cyber security awareness training*. Retrieved from Phriendly Phishing: https://www.phriendlyphishing.com/

piotte13. (2016, Janurary 1). *Enigma Machine*. Retrieved from Enigma Mechanics: https://piotte13.github.io/enigma-cipher/