Case Study (CLO 2.1, CLO 3.)
All-in-one-app

Rimas Nawi Alshehri

Raghad Mohamad Alshsatri

University of Jeddah - College of Computer Science and Engineering

CCCY-112: Computing Ethics

Dr. Maha Al-aslani

26/11/2021

Student name	ID Number	Section	Tasks
Raghad Mohammed Alshatri	**2113093**	**A2**	• **Point(1,2)** • **Document Format** • **Check the overview**
Rimas Nawi Alshehri	**2110240**	**A2**	• **Point(3,4)** • **Overview** • **Cover page**
Both students			• **Point(5)** • **Reference page**

overview:

Our “All-in-one-app” study case is about "Tawakkalna" application, which started as the pandemic of COVID-19 raised to the world. This application became a necessity in any Saudi citizen’s/resident’s phone, since it is obligatory in universities, malls, restaurants, airports, and even hospitals. This application consists of almost all the identifications a Saudi citizen/resident must have from (ID-digital card, driving license, Qiyas grades, digital passport, etc).

This application can be more beneficial for Saudi citizens more than it already is.

In this study case, our case is that we have so many applications in our phones that damages or minimizes our phones’ storage, so we would like to consider new improvements/additions on the application’s services in a way that offers us advantages as follows:

•A transportation system linked to the General Directorate of Ministry of Interior.

•An automatic appointment scheduling system linked to Ministry of Health

•A flight booking system linked to Saudi Airlines

1. communication channel is secure for secure communication of the data

communications channels :

It is the medium through which two entities communicate by exchanging data. such as email or social media channels. But when we talk about secure communication, it is important to focus on:

- Virtual Private Network (VPN): This, in turn, protects and encrypts data from the third party so that it is difficult for the other user to access and decrypt this data. We used a VPN because it is useful for the application in terms of securing user privacy and ensuring that private user data does not eavesdrop. Virtual Private Network (VPN) is highly preferred to create a secure medium. It provides the security of the "Tawakkalna" application.[1]
- Encryption: The process of scrambling data or messages so that only authorized parties can read them. We used encryption to improve data security, but appropriate encryption technologies must be used. the multiple encryption strategy provides acceptable security. To improve the security of confidential data, numerous encryption techniques are recommended for use in Secure communication channels. This technology improves data security by preventing unauthorized users from accessing any information that belongs to the users.[2]

Firewalls: A system that stands as a guard between the application's internal network and the Internet. In terms of security, firewalls provide a number of services to networks. They enable virtual private networks (VPNs) and traffic filtering that does not comply with the network's stated security policy. The reason for using a firewall is to provide a secure communication system with better processing performance.[3]

- Intrusion Detection System (IDS): This is the most important communication channel. (IDS) is a device that monitors the system and sends a report when an unsafe movement occurs or a strange target. So, the reason for choosing this security service is to prevent users' penetration and protect the infrastructure of the application.[4]

2. User authentication is secure enough to stop unauthorized login attempts

Authentication is the process of confirming a user's identity. When a user login into a computer system, user authentication is the process of verifying that user's identity. The fundamental goal of authentication is to allow authorized users access to the computer while denying unauthorized users access. Authentication technology checks if a user's credentials match those in a database of authorized users or in a data authentication server to offer access control for systems.

- **Authentication in the network layer:** Users attempting to access the Tawakkalna network must be authenticated using one of the three methods listed below: [5]
  - Passwords: The most popular and often used authentication method is password verification. A password is should only be known by the user. The system administrator assigns each user a valid username and password. All usernames and passwords are saved in the system. When a user logs in, the stored login name and password are compared to the user's username and password. If the contents are the same, the user is granted access to the system. In addition, it will be used one-time passwords provide additional security along with normal authentication. There are some password policies for the Tawakkalna app:
    - A password should have at least 10 characters.
    - It should not include any personal information about the user. such as the user's true name.
    - A password should include all characters, including uppercase and lowercase letters, digits, and symbols.
    - A password should be changed every 120 days to maintain network security.
  - Biometrics: This authentication method depends on the biological characteristics on the basis of which users are differentiated, which are:
    - Fingerprint.
    - Face ID.
    - Retina scan.
    - Voice pattern sample.

- **Authentication in the application layer:** In the Tawakkalna app, multifactor authentication is required: [6]
  - A password is something that you know.
  - Verification code sent to the user's mobile number is something that you have.
  - User biometrics is something that you are.

we used multifactor authentication to provide more security and ensure that the right user is accessing the application.

- **Authentication in the end-user layer:** Educate end users about these ways to protect devices from unauthorized access:
  - Update the application first Powell.
  - Turn on the firewall on the user's device.
  - Not using public Wi-Fi.
  - When discarding old devices, make sure all data is erased.

3. Privacy of users is not compromised

The concept of user privacy can be addressed as securing/not sharing personal information of users of an application without permission, such as a user's: address, location, identification, or financial income. Applications in general must only collect the data needed to serve the users of an application.

We can avoid compromising a users' privacy in "Tawakkalna "especially after considering adding extra personal information and identifications such as (location Setting a well-planned security policy that insists on mitigating cross-site script vulnerabilities, where it defines the security requirements for an application, as well as setting and delineating what is acceptable for employees working for it.

- Setting periodic security audits for the system that regularly checks up on the application's own set policies and the actions of the application regarding those policies, are they effective? Are the policies being followed? Does the system need new/improved policies?[13]
- Owning an original disaster recovery plan made for the application itself, in which it has a main cantered goal for the action that should be taken at the time of security damage, as well as the members/teams and their obligated roles when they are needed.[13]
- Usage of firewalls &the implementation of encryption which will allow only authorized users to access, move, or carry data. Serving as a guard between an organization's system and internal network. And guarantees that data ca be revealed to those who know the encryption key, otherwise no data shown.[13]
- Providing an Instruction detection system which is a system that monitors system resources and activity and sends alerts when it detects a breach of network security when it detects network traffic attempting to circumvent security measures. And this will allow users' information to be under protection. [13]

4. All-in-one-app follows the relevant CITC (Communications and Information Technology Commission) and Saudi NCA (National Cybersecurity Authority) policies

CITC policies/Laws followed in the application:

- **The Telecommunications Act**, this act stipulates the provision of the minimum level of telecommunications services with adequate quality and affordable prices to all users. This act stipulates the following:
  - Offer affordable telecommunications services that are advanced and adequ ate
  - To assure that the public can access telecommunications equipment, networks, and services at affordable rates.
  - secure reasonable and interference-free usage of regularities
  - protect the public interest and the client interest just as keep up with the secrecy and security of media communications data.

This act will allow users to access the application without any hardships or complex policies regarding the normal usage of an application, it is free where all citizen/residents can download and use as any other basic necessary application.[9]

- **Anti-Cyber Crime Law of 1428H/2007**

Cybercrime can be portrayed as bad behaviour executed by using a PC or the web. Many exercises may be considered a cybercrime, including obtaining unapproved access through the web to someone else's information or Mastercard data, supporting manipulator affiliations, or criticizing someone. The Saudi Anti-Cyber Crime Law sets out all cybercrimes and their connected disciplines. This law considers the following cybercrimes: hacking someone's account on social media, identity thefting, threatening the privacy of a person by taking pictures or recording videos without permission using phones, and publishing private information/personal data of a person.

All those laws are prior related to the building of the additions on the application, since it's precisely used as a legal identification in the Kingdom of Saudi Arabia everywhere. And any violation regarding the mentioned cybercrimes will lead to legal lawsuits, fines, or prison terms.[7]

Saudi NCA policies/protocols followed in the application are:

- **Traffic Light Protocol (TLP)**

This protocol is used not only in Saudi, but also globally. It states the colours of traffic lights (red, amber, green, white).

Red – Personal, Confidential and for Intended Recipient Only:
Red states that receivers have no right in sharing any of the red information outside of the actual receiver's circle whether it was inside or outside the organization.

Amber – Restricted Sharing: Sharing information classified in amber is permitted with intended recipients inside the organization, as well as with recipients who need to act on the shared information.

Green – Sharing within the Same Community: It is allowed for the recipient to share information classified in green with other recipients inside or outside the organization

if they are in the same sector. However, it isn't permitted to publish or exchange this information publicly.
White - No Restrictions: No restrictions in white traffic light. [8]

- **One of the cryptographic protocols: Transport Layer Security (TLS)**

A privacy-preserving protocol ensuring the security of communications between applications on the Internet and their users.
The TLS protocol allows each client to establish a temporary private conversation with the server.

Those two protocols from the Saudi NCA will work with the application's additions serving as protection and security strengthening in terms of personal data sharing and personal data protection of users of the application.[8]

5. **Relevant intellectual property rights are not violated**

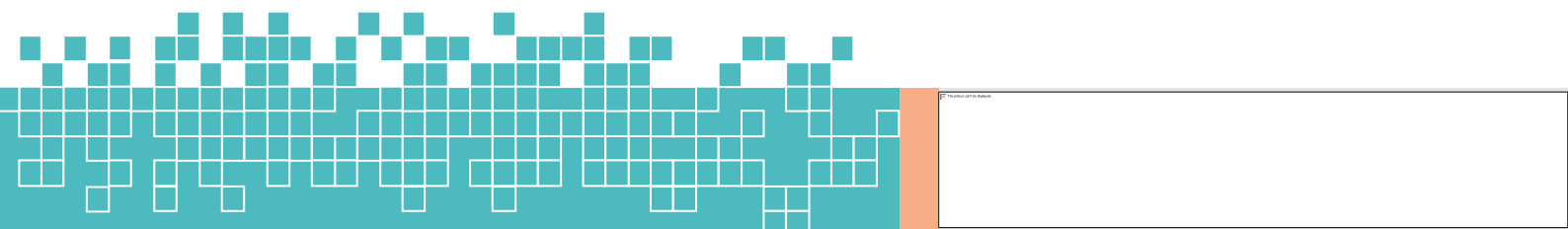
This application and the developments it will encounter follows the regulations and laws of the intellectual property such as:

Trademarks: which is a symbol, brand logo, phrase, sound, or term that allows a customer to tell one company's products from from another's. As long as a mark is in use, it can be renewed indefinitely. "Tawakkalna"our all in one app has its own original name and logo in the market.[12]

Copyright: which is a type of intellectual property that grants its owner the exclusive right to copy and spread an original content for a set period of time, usually for a fee or can be an original expression of an idea and the original expression of this idea is protected by copyright, but not the concept itself. In other words, "Tawakkalna" has its own original ideas and services but it does not mean that another application with another name cannot provide the same services one day.[12]

Patent: which is a sort of intellectual property that grants the owner the legal right to prevent others from creating, using, or selling an invention for a set amount of time. In order to enforce his rights, the patent holder must sue the person who infringes on the patent. Because it has the right to exclude others and prohibit others from exploiting the invention, the patent is the best way to implement "Tawakkalna" A patent is a restricted property right issued by the government to innovators in exchange for their permission to disclose details about their creations to the general public. The patent is valid for a duration of 20 years.[10]

Trade secrets: which is a sort of intellectual property that consists of a set of information that has economic value. In contrast to a patent, the owner makes an effort to keep the information private. Owners of trade secrets want to keep their secrets safe from prying eyes. Employees frequently sign agreements not to reveal the employer's own information, with substantial financial penalties applied if the agreement is broken. Because the "Tawakkalna" application has a high governmental commercial value, trade secrets are required to protect the confidentiality of the application's data and those of its users.[11]



References

[1] Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies (pp. 1-5).

[2] Gupta, H., & Sharma, V. K. (2011). Role of multiple encryption in secure electronic transaction. International Journal of Network Security & Its Applications, 3(6), 89.

[3] Dubrawsky, I. (2003). Firewall evolution-deep packet inspection. Security Focus, 29, 21

[4] Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). International Journal of Scientific and Engineering Research, 2(1), 1-4.

[5] GeeksforGeeks. 2021. *Authentication in Computer Network - GeeksforGeeks*. [online] Available at: <https://www.geeksforgeeks.org/authentication-in-computer-network/> [Accessed 30 November 2021].

[6] Azad, T., 2021. *Understanding XenApp Security*. [online] ScienceDirect. Available at: <https://www.sciencedirect.com/topics/computer-science/authentication-factor> [Accessed 30 November 2021].

[7] Mcit.gov.sa. 2007. *Anti-Cyber Crime Law*. [online] Available at: <https://www.mcit.gov.sa/sites/default/files/prints/la_004_e_anti-cyber_crime_law.pdf> [Accessed 24 November 2021].

[8] National Cybersecurity Authority. 2020. *National Cryptographic Standards*. [online] Available at: <https://www.nca.gov.sa/files/ncs_en.pdf> [Accessed 24 November 2021].

[9] CITC. 2021. Public Consultation Document on the Proposed Regulation for Cloud Computing. [online] Available at: <http://www.citc.gov.sa/en/new/publicConsultation/Documents/143703_en.pdf#search=cyber%20security> [Accessed 24 November 2021].

[10] Wipo.int. 2021. *Patents*. [online] Available at: <https://www.wipo.int/patents/en/index.html> [Accessed 30 November 2021].

[11] Wipo.int. 2021. *Trade secrets*. [online] Available at: <https://www.wipo.int/tradesecrets/en/index.html> [Accessed 30 November 2021].

[12] SaudiLegal. n.d. *SaudiLegal*. [online] Available at: <https://www.saudilegal.com/> [Accessed 2 December 2021].

[13] Simsim, M. T. (2011). Internet usage and user preferences in Saudi Arabia. *Journal of King Saud University-Engineering Sciences*, *23*(2), 101-107.