Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 2
Software design document

Group Members: Ryustem Shaban (rs223fx),
Faruk Yildirim (fy222av),
Ibrahim Groshar (ig222je)
Henry Shafer (hs223nr)

1. Introduction

Loco news has been breached too many times. The media company has various holes in their information security that will be filled with the implementation of this SDD. This plan includes new login security, policy changes, mobile device security restrictions, and solutions to physical security at Loco. In addition, the system will integrate smoothly, and only cause minute inconveniences, for exponentially better information security.

1.1 Purpose of the Software Design Document (SDD)

The purpose of this SDD is to provide information security for Loco news. Loco as a media company relies on its information security, not only for its employees but to stay successful and keep any exclusive information to themselves. However, Loco has countless security issues that pose a threat to its employees and their exclusivity. By following the plans laid out in this SDD Loco will be able to minimize security risks while remaining efficient.

1.2 Scope

This SDD will make use of external and original systems to secure Loco news. The following are the systems to be implemented.

Authentication
A new authentication process will be implemented. The new authentication system will be tokenized to allow for fully secure logins. The login will also time you out after a set number of failed attempts. Finally, if a logged-in user is inactive for too long it will log them out to prevent information theft from unattended devices.

Clearance System
Currently Loco gives full access to all its employees; this is a problem. Employees do not need access to everything. Implementing a clearance system for Loco will limit the risks of information leaks/attacks by making it harder to get access to more sensitive information.

External Device Security

1. *Printers:*
   One of the main dependencies as a magazine organization of Loco News are the printers. The information on these external devices can be stolen like any other device since these devices are with memory as well. Printers will ask for login credentials without the token and either authorized personnel or automatically expired information will be cleared from the printers after every 30 days. Printers should be kept up to date and checks for malware should be made for these devices.
2. *WPA WI-FI router:*
   Should be upgraded to WPA2, additional equipment will be implemented such as MAC filtering to restrict connections only to registered to the network devices. WPA2 will have an ordinary password with AES (Advanced encryption standard) encryption and MAC filter [1]
3. *WI-FI extenders:*
   These extenders will be replaced with powerline adapters which are much securer and will eliminate the fact of forgetting to update the extenders which is a human factor. Powerline adapters will help to achieve better protection, enough for the company and at the same time budget friendly [2].

Laptops and Computers

Laptops and computers have multiple operating systems which can confuse the users, bring out compatibility problems and difficulties for the IT department in case of required system maintenance or repairing processes of any of the devices. We believe it will be much simpler and budget-friendly if the company migrates 26 of the computers to Windows and leaves 2 Mac PCs as well. Many will say that Windows is more vulnerable, but this is not why Windows is more attractive to hackers, this is because globally Windows users are far more than the Mac computers and when hackers do create a virus, they will create it for the majority. If users are careful and follow the regulations and suggestions, security levels will be high enough to stop the hackers. The reason for choosing Windows was, mainly because more companies do support Windows OSs, they are more budget-friendly, simpler to use, and cheaper to repair again. Instead of going for Mac which are less attractive for the hackers just because minorities do use them and nothing else, we believe buying tokens with the money left tokens can be set up which will far exceed the security the Mac does provide. The two Macs on the other side will be kept in case a cooperative company does use Macs where utf-8 won't work, and data will need to be exchanged.

Hire-N-Fire

It is vital for Loco to use more thorough agreements when hiring and firing employees to ensure information is not leaked during or after employment. In addition, thorough background checks should be conducted when hiring, to ensure the new hire will be reliable, useful, and trustworthy.

Network Security

Network security will be one of the main components of the new system since users will need to access the system inside and outside from various not trustable WI-FI providers. To ensure a secure network connection, on-site connections will be made with WPA2 WI-FI encrypted with a password and MAC IP registrar. The MAC register will allow only registered devices to connect, and this will prevent personal devices such as phones and so on from connecting to the work network. For these devices, special "GUEST" connections will be ensured. Additionally, Network Firewall (Cisco ASA) [3]*Instead of wireless WI-FI extenders, powerline adapters will be used to prevent any possible vulnerabilities and to avoid the possibility of forgetting to keep extenders up to date. Away from the building, VPN will be used.*

New Policy

Loco news doesn't use any of its employees aside from the CTO to maintain information security. This SDD describes how Loco will utilize more employees for information security to prevent corruption and take some of the work of the CTO.

2. System Overview

This system will minimize security risks to Loco News by implementing a variety of security strategies. Loco news is currently plagued with security issues and their previous failures will be used as guidelines for our solutions. The new system will include tokenized password protection, VPN usage, HTTPS connections, antiviruses, MAC registrations to the WI-FI, clearance system, employee security policies, logout countdown, collaborative responsibilities, system logs, and physical security measures for the server room such as vented server rack. These strategies will be implemented primarily by the CEO and the new CTO, however, security is not their job, therefore additional employees will be utilized for the implementation of this SSD.

2.1 General Overview

This system will be designed around the existing issues regarding Loco News information security, with the intent to fix them. Our solution will be organized into two groups, network and physical. The network security programs include security programs installed on every work device, Wi-Fi security, log reading, and a secure authentication process. The physical aspects include securing the servers, implementing new security policies, and adding new hiring and firing policies. After complete implementation of our system, Loco News will have a smooth, and secure workflow.

2.2 Assumptions

Proper implementation of an outstanding authentication program that has no sufficient problems with tokenized devices is the main concern of the system. The main drawback of the security application is that almost all security systems will depend on the software which is going to be implemented in the overall system. Acquiring a tokenized authorization device and the processes that come a long way may cause frustration on users since it is a multifactor authentication system.

2.3 Constraints

2.3.1 Budget

Although the system is secure, it is not perfect and will always have room for improvement. With a greater budget, we could have moved the server room to somewhere more secure. We also could have hired more employees to work under the new CTO.

2.3.2 Human Error

Our proposed system does not rely solely on machines, because of this human error is a factor. Each employee will be held accountable for their mistakes with regards to information security, but this will not eliminate human error, because of this we have included provisions to combat this.

2.3.3 Ease Of Use

This security plan, although thorough, is not impenetrable. However, adding more security would only cause problems with worker efficiency and login difficulties.

2.3.4 Tokens

The authentication process to access the software will be made assisted with a tokenized device, however, to make something better we always need to compromise something, and in that case, the compromise will be the expenses that will be used to get a device for each worker, another disadvantage of the tokens is that it can be confusing for users that are not so interested onto the technology and this can cause minor problems for the Admin such as often bans from the system after failed attempts and delays on the workplace. Last, but not least in case of lost token purchasing new token and delay of work again can occur, which can be a major drawback for the company, so it is highly recommended for the company to make additions to the current policy of the organization regarding these risks.

2.4 Risks

Describe any risks associated with the system design and proposed mitigation strategies. For instance, what types of risks would be mitigated?

Design risks include the likelihood that the information systems are insufficiently protected against certain types of damage.

This means that the security design has vulnerabilities to cover. We tried minimizing the vulnerabilities and balancing the overall instabilities to produce the most stable and attractive system design for Loco News.

Physical risks:

1. Environmental:

While the system is mostly based on software security additions, there are some hidden risks out there. Environmental risks are only a part of these. In cases such as fire or flood, the company should have a fire alarm with water sprinklers, all the workers should be taught about the exit plans in case of emergency. Under such circumstances, the data will be the last thing workers will think about. To prevent loss of critical data all the data should be kept in cold storage away from the site and separately in cloud storage as well and should be updated once a month. What we mean by updating is not only uploading the new documents it is also modifying and deleting expired data if necessary.

2. Thievery controls

In case of theft in the workplace, the doors will be locked with card scanners which will be only on a minority of the personnel. All the external windows will be locked, there will be CCTV implemented, and if some of the devices are being stolen Microsoft does have built-in trackers. In the worst-case scenario, the thief will be able to get the device, but not the information inside it without the token,

and Admin will be able to delete the account of that user who was using the laptop. One drawback of this will be that getting the device back won't be 100 percent.

Technical vulnerabilities:

1. *Mac filtering*

   There is a possibility to duplicate the workers' Mac address which can cause harm. For that sake users should consider keeping the workplace information at the workplace and not letting know the outsiders that there is a Mac filtering on point. Even though it is possible to duplicate Mac address user will still need to get worker account credentials which will be much effort just to connect to work Wi-Fi so the hacker would look for other area where it is possible to find a hole to get in (There is always one).

2. *SQL injections*

   This is a simple human fault which even till today cause big harm to the companies and organizations. To avoid this user should make sure that:

   a) *Stop writing dynamic queries*

   b) *Prevent user supplied input which contains malicious SQL from affecting the logic of executed query*

3. *VPN*

   User can forget to open VPN while connecting to unknown network. Even in that case HTTP Strict Transport Security (HSTS) that is built on the software can filter the secure web pages until some extend, however, this does not guarantee security. The best countermeasure in that case would be warning the user with pop-up before entering or accessing confidential information.

3. System Design

While implementing the system, software designers should keep in mind that this will be Multipurpose Software that will provide a secure and easy-to-use work environment on SQL databases [4]. *The application will start asking for user credentials and in case of wrong credentials, the system will give 2 minutes for a new trial, with 4 max tries. After logging in successfully to the system user will have multiple built-in choices such as:*

Browse - will give an opportunity to the user to check for information under a safe working environment and save addresses for later access

Write – This will be a system module to create or modify data (photos, videos, .docx, text files)

Cloud upload – Specified module to upload a document with a built-in malware scanner

User communications – Office 365 team is being used on this module

Settings – Ability for users to check bookmarks, change passwords, and log out from the system manually

Additionally, a system logout counter will need to be implemented in case of a user abandons the software unattended. The counter will request the user to provide login information once more after 5 minutes of inactivity. Check Figure 1 for visual information

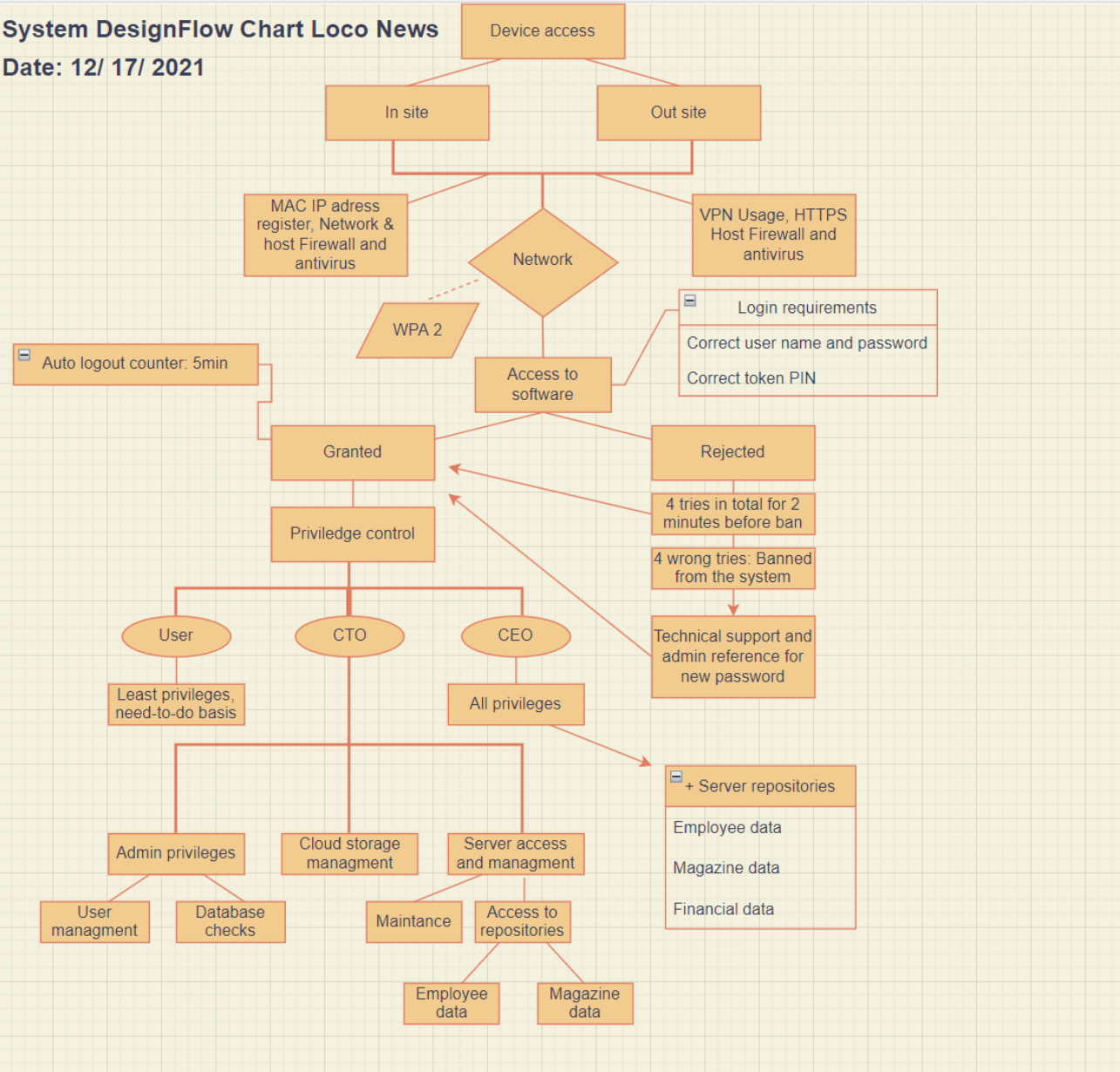

Figure 1

Software design flow chart

3.1 Software Design

The software is mainly focused on Windows, but while designing the software designers can build up Mac versions as well, however, in our case Microsoft as host is the first requirement for the system to run. A random 6-digit PIN generator token will be necessary for multiple authentication processes besides the user login and password. This token will need to have many built-in applications such as sending each login detail to the SQL database and to be stored in case of suspicious actions or catastrophe, where this information can be analyzed and can be of great help for the recovery from the flaw. Additionally, the token will need to connect to the network directly through the software login (Software will act as a hotspot for the token, however, the token won't be affected by the VPN

getting location information and forwarding it to the database. As mentioned, SQL databases will be used to store information through the software, with SQL database Varchar (500) will be used to store favorite or important bookmarks [5]. *Another major aspect of the system will be Office 365 Even though office 365 doesn't have a good editor program (simple, but limited programs) it does cover most of the necessary aspects for office work and overall, it is one of the best options. One more reason to choose Office 365 was its built-in malware checker before uploading to one drive which will save the CTO a lot of time checking all the files before uploading and human factors should be considered as well. Since most of the needs of the company will be in the online environment, not much physical space will be used. The software will be installed on each device. Further information on Figure 2*

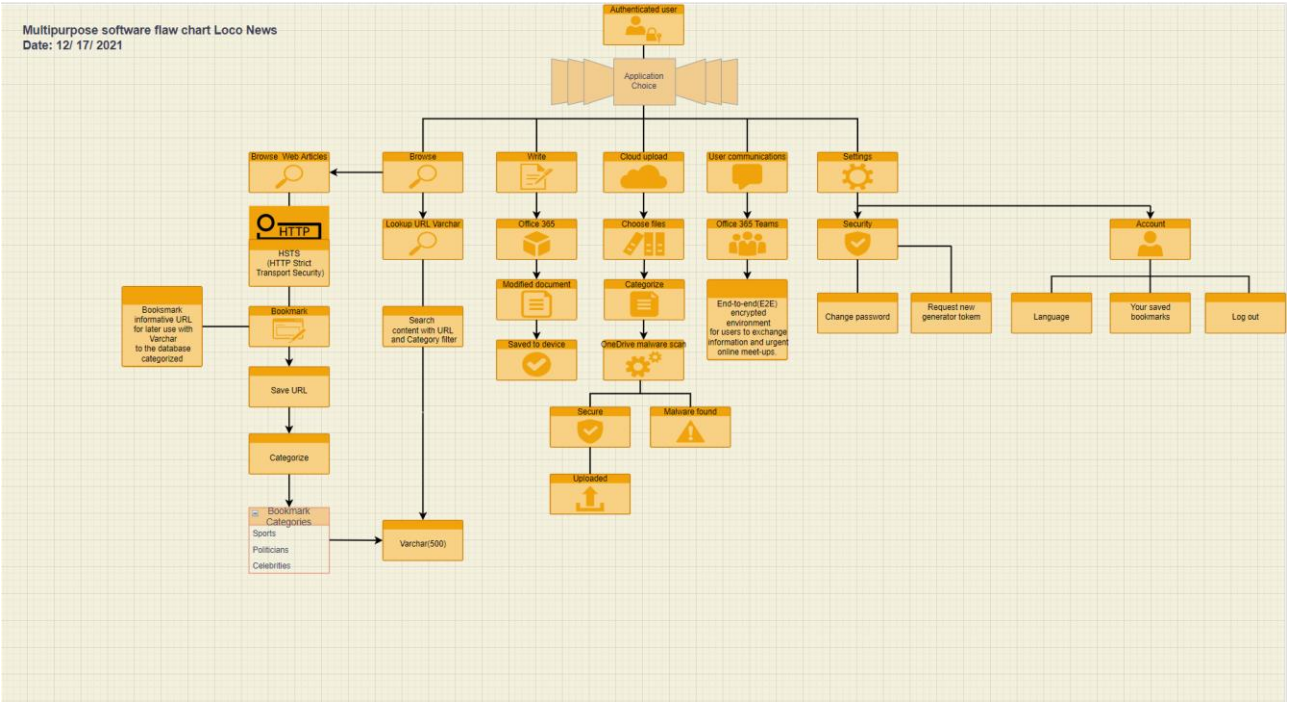

Figure 2

Multipurpose software

3.2 Security Software Design

Before requesting access if the user was on site the WI-FI network will be accessible with a simple WPA2 password and MAC recognition to restrict users from connecting to the main database with their own phones and other private devices. For these devices ``GUEST'' WI-FI will be used. Additionally, for in-site connections Network firewall (Cisco ASA) will be considered apart from the host Firewall also. However, if the user is out of the site, the user will need to open a VPN to ensure a secure connection. When a secure connection is ensured, the user will head to the software. Software security will be ensured by 2-Factor authentication. When access is requested, the system will ask for user login credentials (UserID and Password) when a user enters these, then the system directly will ask for a 6-digit PIN generated by a tokenized device. One thing to mention here is that even if the user adds wrong credentials the system will request the 6 digits, but 6 digits will be generated uniquely for each user with their credentials and since there won't be users with such

credentials in case of the wrong password nothing will happen for 30 seconds given time range, this will prevent the potential intruder to try multiple passwords and spam the system. The user can try a 6-digit combination also, however, 4 wrong tries will be the maximum amount of possible tries for a given time limit and if the user can't authenticate himself, he will need to get technical support and request a new password from the Admin. All this information and tries will be saved and redirected to the database with an expiry date of 1 month. Since all this information will be string and coordinations it won't consume much memory space. Once the user authenticates himself, the system will give him privileges regarding his user credentials and implement access control policies. Most users will have only the general privileges such as modifying and creating their own documents, searching for information, uploading some information to the database, etc. CTO will have almost all the privileges only without the ability to access the financial server repository without requesting access from the CEO. The CEO himself will be fully privileged. After privileges are checked and boundaries are set, a secure work environment will be ensured. When the user is done working, the user will save the data to the database or if the document modification is done to the cloud storage as well and log out. For visual description please check Figure 3.

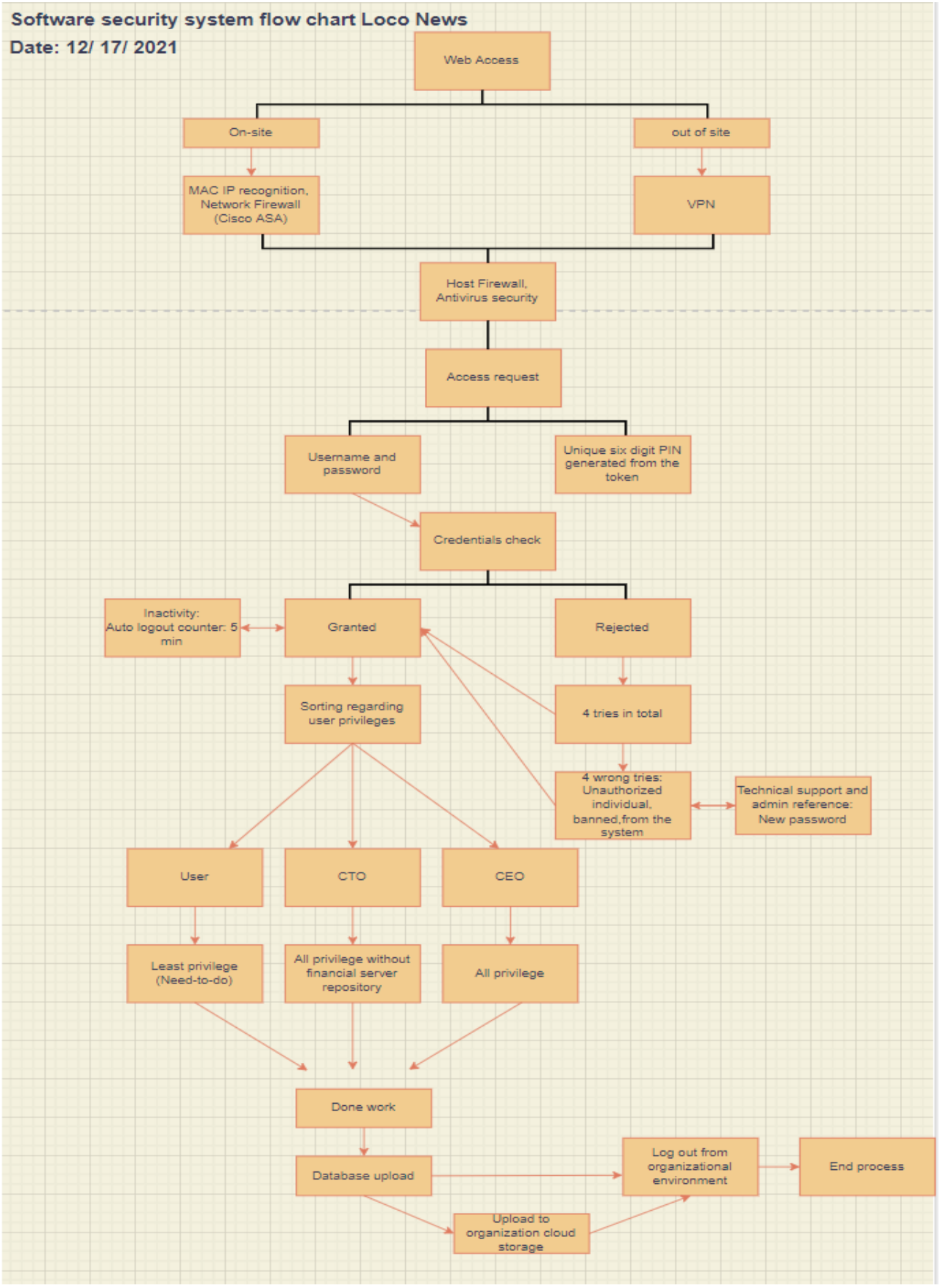

Figure 3

Software security flow chart

4. Use Case Scenarios

In this section will be explained a set of use case scenarios that the user will need to do while using the system.

1. Connect to network

1.1 On-site connections for work devices

Open the WI-FI settings, type in the WI-FI password, if requesting the device's MAC address was registered the device will be connected to the network, if not please contact the IT department to get registered.

a. ***FOR THE IT DEPARTMENT***

i. ***How to find user MAC:***

To Find the MAC address, right-click on the start button and select Command Prompt from the menu. Type in "ipconfig/ all" and press Enter. Your network configurations will be displayed. Scroll down to your network adapter and look at the values next to "Physical Address", which is the MAC address

ii. ***How to register MAC address to MAC filter:***

I. *Go to gateway settings.*
II. *Enter the Modem Access Code found on the side of your gateway*
III. *Select Home Network > MAC filtering*
IV. *From the MAC filtering type "dropdown", select Enabled*
V. *In MAC filter entry select: Your device's MAC addresses*
VI. *Select "Add"*
VII. *Select "Save"*

1.2 Connections for personal devices

Choose the network named "Loco News- GUEST" ; this network is specified for workers' personal devices. The password is the same as the main network.

1.3 Connections away from the site

i. Establish connection to the WI-FI network

ii. Go to the search icon right next to the Windows icon located on the left bottom corner

iii. Type "NordVPN"

iv. Log in to your account assured by the Loco News
v. Click the Quick Connect button which will automatically choose the most suitable network for you.

vi. enjoy secure internet connection

2.. Logging to the software using the token generator

1. *Open the software*

2. *Input your userID and password and tap Enter*
3. *6 Digit code will be sent to your token generator*
4. *Input the 6-digit combination*
5. *You're logged in.*

In case of lost token device or misfortune, the user will have 4 tries in total, if a typo was made by the user, try one more time steps stated above, however, if the case is lost token or forgotten password it is recommended for the user to reach out the Admin and request a new password or being granted to one-time login to the system without the token with the reference of the Admin.

3. *How to save and access saved URLs on SQL*

1. *Bookmarking URL address*
    a. *Open the "Browse" section and choose "Browse web articles" on your application and type in keywords or web addresses to access the keyword related contents on the World Wide Web or go directly to the webpage*
    b. *Once the webpage is found, go to the "Bookmark" button to save the URL for later use.*
    c. *Users will see a dropdown menu to categorize the content such as:*
        i. *Politics*
        ii. *Celebrities*
        iii. *Sports*

        Etc.

    d. *Fill out the details.*
    e. *Click the "Save" button*
2. *Opening a bookmarked URL*

    Go to the "Browse" section after being logged in and choose "Lookup for saved URLs ", fill in the full article name or keywords plus the category it belongs to from the dropdown menu. Full article names and saved details about each article will be visible. For ease of use if the user knows the date the article was published and/or any other details such as Author's name can go to "More filters" and input additional information.

3. *Removing bookmarked URL address*

    Since users will be able to store their own collection of filtered bookmarks from the general work environment bookmarked URLs users should:

    a. *Go to accounts*
    b. *Open "Your saved bookmarks"*
    c. *Click "Remove"*

NOTE: The bookmark will be deleted only from the user's own account database, but not from the SQL entirely.

4. Changing the user password or requesting a new token generator device

The users may need to change the password or request a new token generator device if the previous device is already not working correctly or there are technical problems with the device that limits the user's availability.

1. *Changing password*
    a. *Go to "Settings"*
    b. *Go to "Change password"*
    c. *Enter the old password and 6-digit PIN*
    d. *Enter a new password and confirm the new password.*
2. *Requesting a new tokenized device*
    a. *Enter user password*
    b. *Enter the device's authentication number written right next to the battery*
    c. *Clarify why a new device was requested.*

The request will be taken by the admin and the new device will be signed to the name of the user that made the request.

If the device is lost, the user will need to register a phone number with the Database with the assistance of the admin and the phone will be used for further authentication processes until a new token generator is ensured. The user will get the 6-digit number sent to the user's email address.

5. Logging out

1. *Choose "Settings" from the sections*
2. *Go to "Account"*
3. *Click "Log out"*

Bibliography

[1] R. D. Sari, . S. and A. P. Utama, "A Review of IP and MAC Address Filtering in Wireless Network Security," Department of Informatics, Politeknik Poliprofesi Medan, Medan, Indonesia, Medan, 2017.

[2] B. Smith, "Internet Access Guide," 21 02 2021. [Online]. Available: https://internet-access-guide.com/are-powerline-adapters-safe/. [Accessed 19 12 2021].

[3] "Cisco," [Online]. Available: https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html. [Accessed 19 12 2021].

[4] "NTC Hosting," [Online]. Available: https://www.ntchosting.com/encyclopedia/databases/structured-query-language/. [Accessed 19 12 2021].

[5] G. Majahan, "SQL varchar data type deep dive," 29 05 2019. [Online]. Available: https://www.sqlshack.com/sql-varchar-data-type-deep-dive/. [Accessed 19 12 2021].