Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 3

Software design document

Group Members: Henok Rezene, Philomina Ejegi, Melat Getachew, Gowthami Rallapalli

Table of Contents

1. Introduction

As requested, our security team has investigated security related issues within the existing system of the company, and we have found potential security vulnerabilities which could be a threat to your company. This document assesses and resolves suspected security vulnerabilities within your IT infrastructure and system. It is designed to assist your company in developing a comprehensive set of security controls to support the implementation of a risk-based, cost-effective information security program. The newly proposed system eliminates possible security vulnerabilities and protects the business from Cross-Site Scripting attacks, SQL Injection attacks and Privileges Escalation attacks and other threats.

1.1 Purpose

The purpose of this document is to enable Loco News management to migrate from operating locally to operating at a national level successfully in a more secure way. This document will itemise the existing systems with recommendations on how they can be improved to match the company's new status and also enlist a number of new systems that will be beneficial to the management and its infrastructure. It will also serve as a guide to the developers as they produce a new application to support Loco News business processes**.**

1.2 Scope

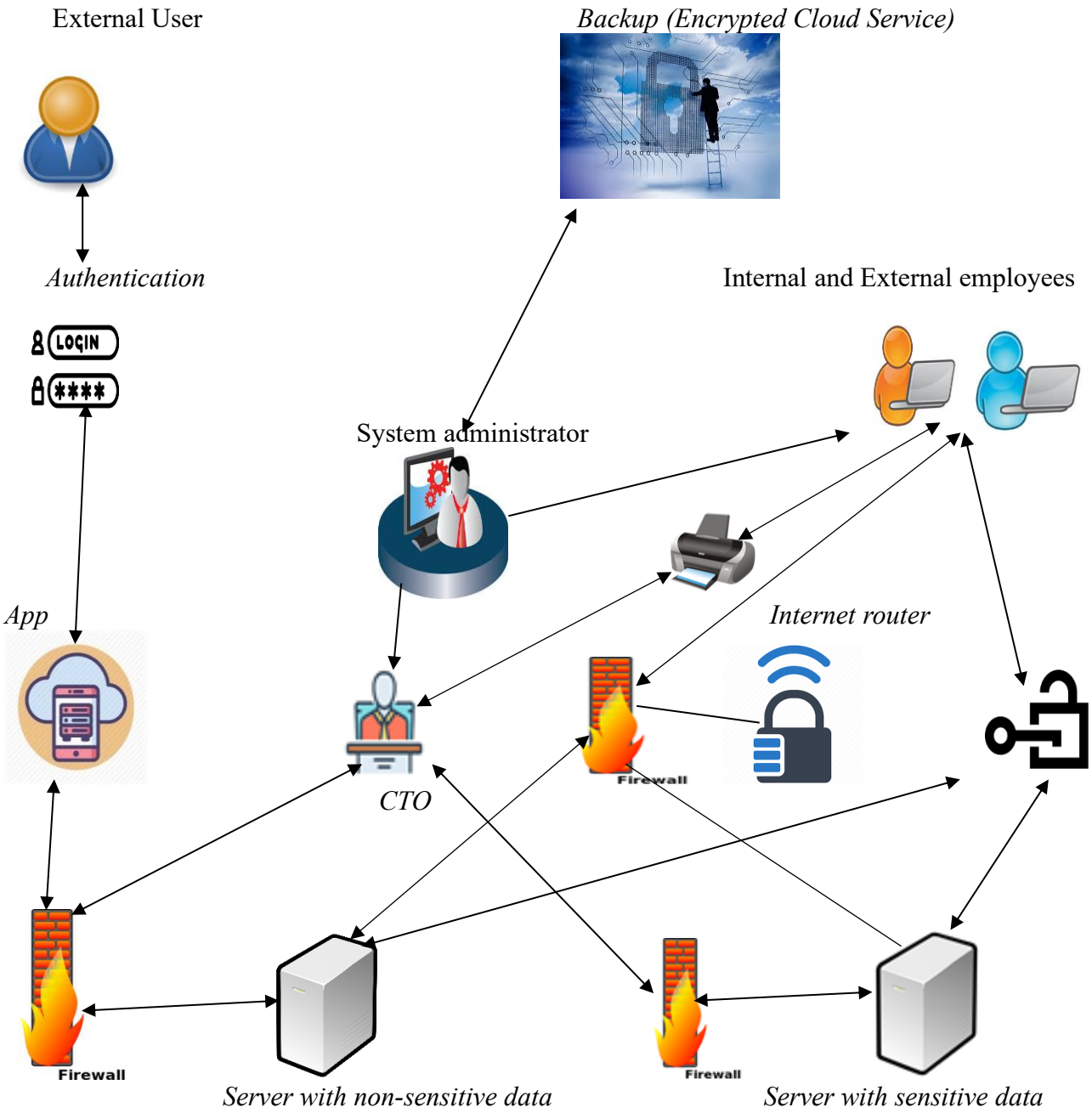
This document produces an application with a number of security requirements and specifications. The newly produced application needs to fulfill both the functional and non functional requirements. The system must fulfill the desired functionality, reliability, response time and storage requirements. To meet the desired requirements, an application needs to function in a fully hardened operating system, encrypting and hashing sensitive data and traffic, implementing access control and firewalls. The application should authenticate users, implement proper logging and auditing activity. The new application should ensure proper input validation to prevent Cross-Site Scripting attacks and SQL Injection attacks and strong authorization control to prevent Privileges Escalation attacks. Moreover, the application should authenticate the users and ensure a strong configuration management is applied. The application will be hosted on a cloud based service.

The system would provide a number of benefits for the organization ranging from economic revenue to reliable and trustworthy information. The objectives of the newly built system is to support the organization's business processes, helping with tracking the source of incoming information, the quality of different sources, type of information, cost associated with it and a number of other

functions. This new system will help the organization to broaden their source of network information and deliver a number of services to the clients.

2. System Overview

2.1 General overview



2.2 Assumptions

Since the system is running primarily on windows server and everybody uses windows operating system, we assume that there could be more malware attacks because Windows is more prone to such attacks. User accounts in Ubuntu have fewer system-wide permissions by default than in Windows.

Python 3.8 is being used to develop this system as it provides good flexibility of system design. The company can depend on a cloud-based server.

2.3 Constraints

The new application is constrained by the different Operating systems the organization is using because using different operating systems can create a compatibility problem. With different operating systems in play, common softwares running across multiple devices may not be compatible which can create a problem both for the software and the overall system. Backing up the data on a cloud based service can be another constraint since the data is managed by a third party.

The Internet connection is also a constraint for the application. Because the application is hosted on a cloud based server and there should be an Internet connection inorder for the application to work.

2.4 Risks

Running a heterogeneous system, will increase the risk of errors or inadvertent data security breaches caused by the diverse systems and components. It will also increase the overall complexity of the network since there could be a compatibility problem. This can lead to data inaccuracy

Some of the risks are relevant to software failures or software system functionalities. When the software developers compromise and add unnecessary features to the software, the software might reduce functionality and exhibit schedule overruns. There could be a security risk for the system if the external employees are exposed to hacking or lose their devices. Another security risk is that if the employees are downloading unsecured softwares/applications on their private devices using the company's Internet connection. Currently the company is using a WPA router which is a less secure version of the WPA family. There could be a risk of server overload. System crash is another risk which can affect the system.

3. System Design

3.1 Software design

A number of softwares and hardware components are required to support the system. The softwares that can support the system include different operating systems like Windows OP, Mac OSX Mavericks and UNIX, device drivers, different programming languages like python and java, and relational DB (SQL), software frameworks, anti malware softwares, scripting languages like HTML, CSS, and Javascript.

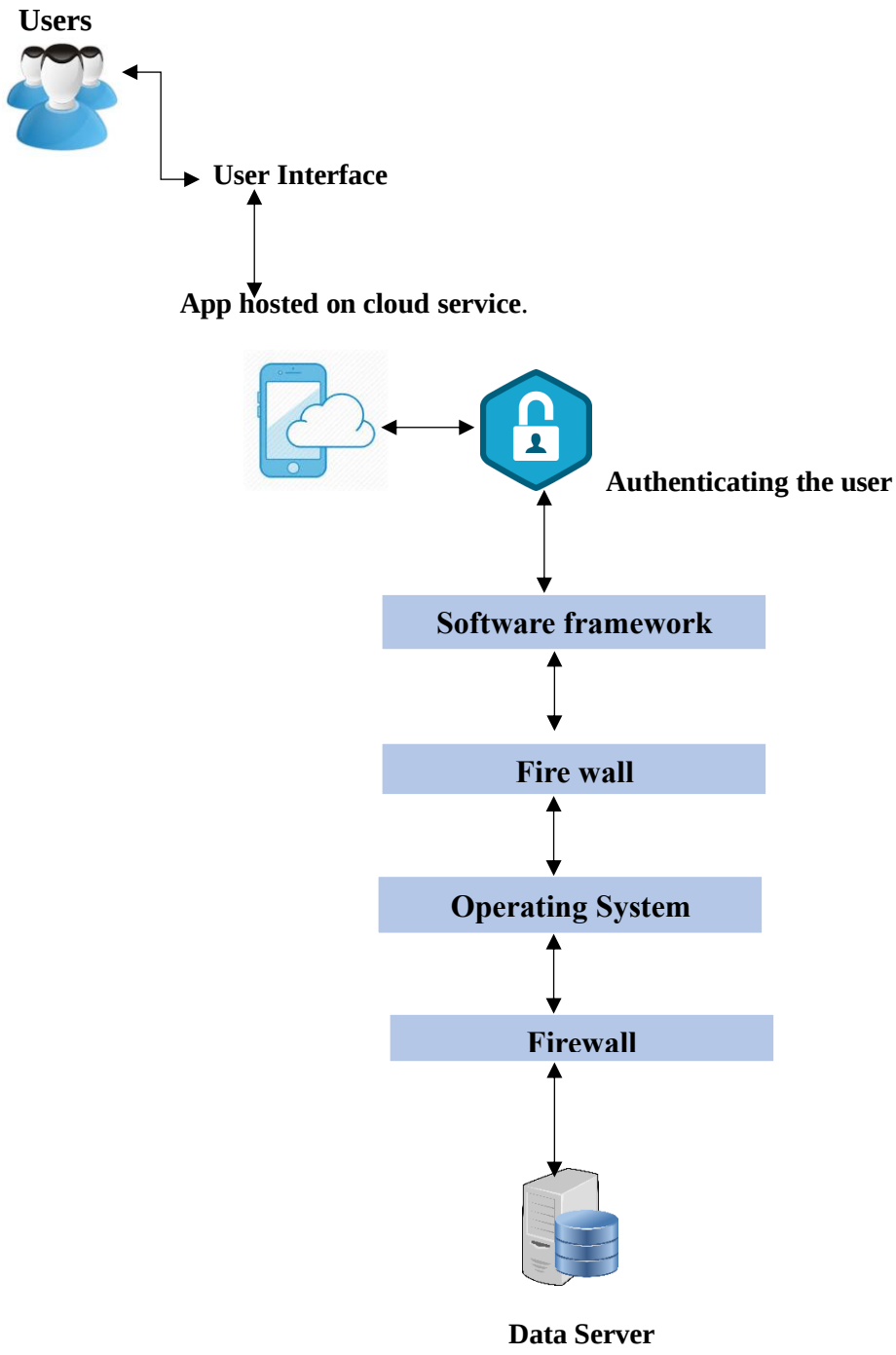
The operating system is responsible for functioning of all hardware parts and their interoperability to carry out tasks successfully. The system also requires hardware components that support the different software components. Hardware components that required could be enough memory, CPU Intel, and hardware drivers, minimum 16 GB RAM, virtual and physical servers, more than 1 TB HHP drive.

The different operating systems are located on both the servers and the employees' devices and the device drivers should be placed between the operating system and the hardwares to enable a proper communication between the operating system and the hardwares.

The database should be stored on the servers, and the anti-malware softwares can be installed on the whole system.

On what follows, the design of the software is presented.

Figure 2. Software Design



3.2 Security Software design

An operating system is a software which performs all the basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers [1]. And your company (Loco news) utilizes multiple operating

systems which needs administrative overhead and an IT department to configure, maintain and support the different operating systems.

Currently, the server is in the basement and the basement is shared with another company (a law firm) which is not secure. The server should be in a room properly secured so that only those who are authorized can access, and all access should be monitored and logged. Physical security equipments such as doors with electronic locks, biometric or security card access controls and CCTV cameras are required for a secure environment. In case, if something goes wrong with the server, there should be a backup on a cloud-based server which should be encrypted.

Since the new application will be hosted on a cloud-based server, users globally can easily access through the internet.

Security must be ensured through following the four basic software design principles: confidentiality, integrity, availability, and authenticity. Furthermore, the design must adhere to the following guidelines:

- The design must be consistent with the security policy of the company.
- The software must employ layers of abstraction to hide internal details from the user.
- It must segregate mechanisms and privileges.
- It must satisfy the principle of least privilege [2], *i.e.*, every module must be able to access only the information that is required for the legitimate execution of the given task.
- A double authorization may be provided at the root level, where any change of information would require approval both at the root level and at the node level. However, to avoid undue delays, the possibility to alter information at the node level before forwarding it to root must not be controlled at the root level.
- The software must not be vulnerable to malware attacks.

Security controls that mitigate the risks:

- Two-factor authentication
- Encrypting data on cloud-based server.
- Device encryption to prevent unauthorized access.
- Remote wipe for employees leaving the company as well as hacked, lost, or stolen devices.
- Using identity management software
- Manually configuring firewall settings and installing antivirus and anti-malware softwares.
- Training and educating employees about possible and potential security risks.
- The cloud storage for the data should be properly configured.
- WPA2 version router with proper encryption key should be used to protect from breaches.
- There should be a Service Level Agreement (SLA) with the third party who is holding our data to make them legally responsible for data breaches.

- We can provide a redundant server that will re-route information to another server that will help to balance the workload.
- We are suggesting 2 hours backup in case of a system crash.
- If application crashes, we suggest an automatic fall over server.
- There should be a proper system audit.

4. Use case scenarios

Use case gives a virtualized functional requirements of a system that will be translated into design choices and development priorities. It helps to identify internal and external factors that may influence the system and should be taken into consideration. It specifies how the system interacts with the actors (users) and provides a good high level analysis from outside the system [3].

Loco News Magazine Use case scenarios:

This Use case scenario is designed to meet the expansion and security requirements of Loco News. It typically depicts how the clients, staff and management would experience the functionality of the system. It describes the tasks they carry out, what information they see and how they interact with the system. Furthermore, it shows a description of how the system will in turn carry out the specified processes to fulfill the stated requests.

Loco News Magazine Use Case Diagram:

This diagram contains both the external entities (also known as "actors") that will be using the system and the discrete use cases that the users will be carrying out.

This use case diagram graphically shows the interactions among the entities of Loco News Magazine System. It represents the technicality used in the system analysis to identify, clarify and organize the system requirements of Loco News Magazine .

The main actors are The Loco News Magazine System, Administrator, Employees (Staff) and Clients, who perform different kinds of Use Cases such as:

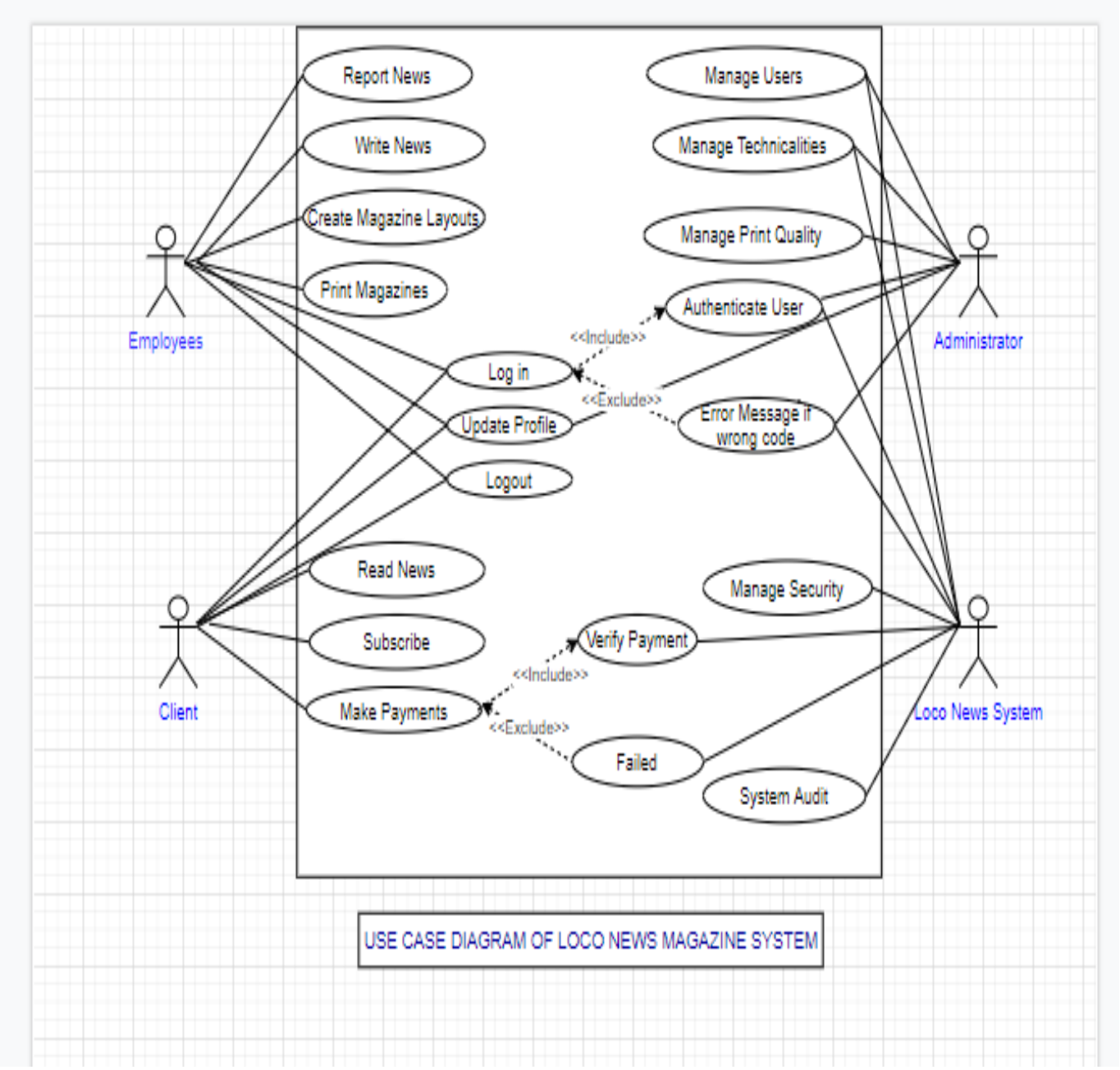
System Entity: Its Use Cases are Manage Users, Manage Technicalities, Authenticate users, Manage Security, Manage Payment and System Audit.

Administrator Entity: Manage Users, Manage Technicalities, Control Authentication, Manage Print quality,

Employees Entity: Report News, Write News, Create Magazine Layout, Print Magazines, etc.

Clients Entity: Read News, Subscribe, Make Payments [4].

Figure 3. Use Case Scenario Diagram



References

[1] "Operating System Overview", [2021-01-01], url: [https://www.tutorialspoint.com/operating_system/os_overview.htm]

[2] J. H. Seltzer and M. D. Schroeder, "The protection of information in computer systems," in *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, doi: 10.1109/PROC.1975.9939.

[3] "Use case and Scenarios", [2021-01-03], url: [https://www.inflectra.com/ideas/topic/use-cases.aspx]

[4] "Use case Diagram", [2021-01-04],url:
[https://www.freeprojectz.com/use-case/news-portal-system-use-case-diagram]