Linnéuniversitetet
Kalmar Växjö

# 1DV700 - Program Security
# Assignment 3
# Program Security

*Author:* Adam RASHDAN, Kalid DIRIYE, & Rashed QAZIZADA
*Supervisor*: Ola FLYGT
*Semester*: VT-21
*Discipline*: Computer Security
*Course code*: 1DV700

Linnéuniversitetet
Kalmar Växjö


## Abstract

The significant limitation or problem in the security of software is that the developers have very limited or no knowledge about the architecture of security. But, even if the developers know about the Even if a developer has good knowledge of the weaknesses in the software, he may not have a good understanding of how to take care of such weaknesses. It is also well-known fact that most of the issues, which make the software vulnerable, arise during the development of the software. On this document we are going to discuss about the software security of the Loco-news company.



## Keywords

Computer security, passwords

Linnéuniversitetet
Kalmar Växjö

# Contents

# 1 Introduction

In this document the details of the software are discussed which is going to be used for the security of a new agency. The news agency is based in Sweden and named LOCO News. The agency prints weekly magazines and sells them locally within the city. The company has grown well, during past two years, and not only in terms of their resources, but also, they have expanded their coverage areas.

With the increase in resources and coverage, it is very much required that the company might also improve their infrastructure and management. While the company did not upgrade much in these areas. To make the office more secured and structured, the company need to improve several areas. In this document, the need to new software and IT systems is highlighted, which will be helpful to create a more secured environment for the employees.

The company has a good understanding that with new advancements, how an important is it to make the IT department secure. The company is also familiar with how the data can be made secure, and how it helps to provide a comfortable environment for the employees. During an interview with an official of the company, he admitted that the they have several security issues which can be lethal for the company's software security. He also emphasized that the company wants that the new system may also work in future amendments and expansions. Considering the concerns of the company's officials, this document provides a system architecture which remove the vulnerabilities within the system.

# 2 Framework/System outline

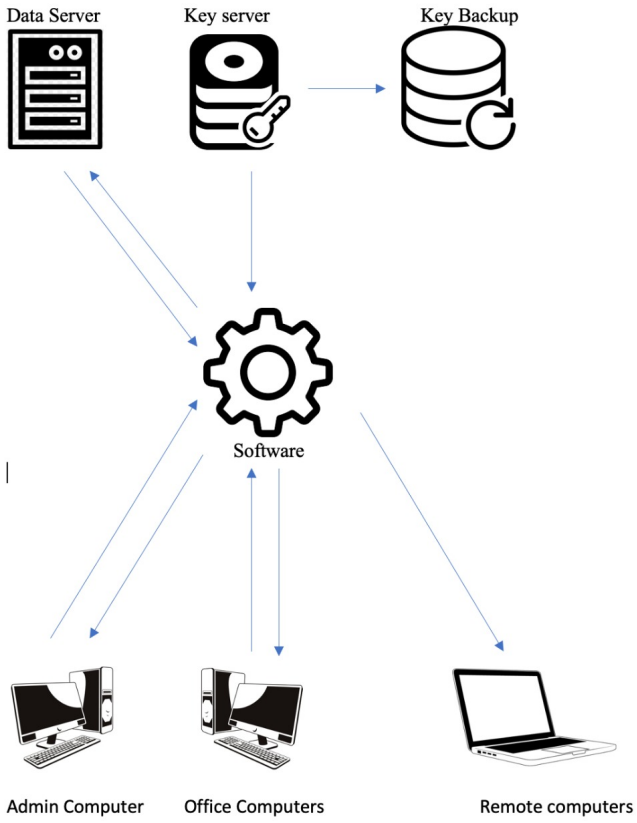
There are various sources to collect the information from, it is better to use the acquired information/data in presence of a specified system. This data is inspected by different origins, for the authenticity of the data, expenditure for collecting the data etc. To make this happen, the software is connected to the servers. The data is collected in the form of information which may include, origin, expenditure etc. The information, which is collected from various sources,

is stored in the database. The workers can alter this data when required.

The other important feature would be securing the data properly. As the data is present on the server side, it required that the data is backed up regularly on the cloud. Cloud would be password protected, and only accessible by authorized personnel. If there is any emergency, like loss of data on server, the cloud can be used to backup the system to its last location.

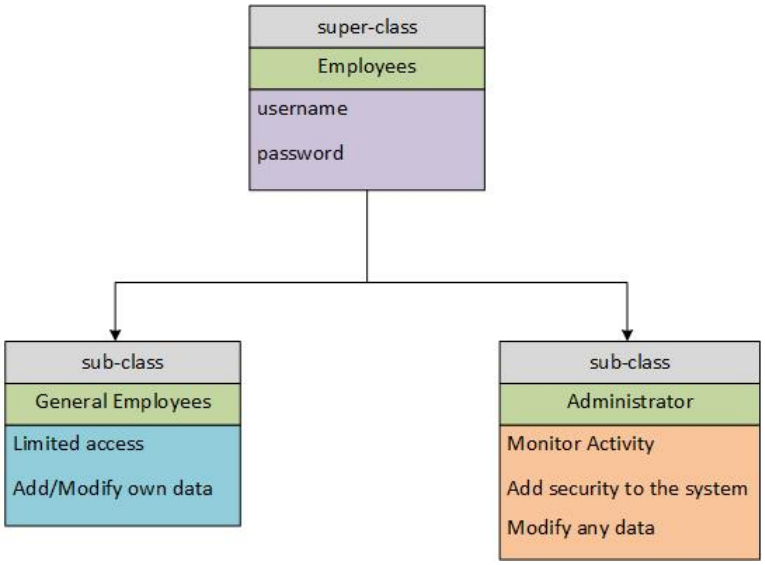
# 3 Framework Description and Architecture

The system requires a few features. For each worker, the system has an interim account. All the interim accounts are protected with an interim password, and the password is required to be changed once a user logs in for the first time. The worker, then, can access the data which it is authorized to. The worker can access the prohibited data only if the organization allows them to. The system has different tools which are, add, remove and organize the data. The worker can abandon the data only if he is authorized to. After some programmed time, the system logs out automatically.




The administrator shall have a special section, to allow him to manage different activities within the system. His accessibility includes various actions that can be performed on the users like, administering the accounts and data [1]. Authentication of two levels would be required by the controller before he accesses any of the functions. The worker might alter the data, as per the data orientation. Which infers, the system secures the very important data as in, source files or the worker's identification etc. This specific set of information would be accessible to the authorized personnel only. The precautionary measures are taken as to guarantee the security of possible confidential possessions. All the workers are required to use the programming languages which are approved. Like JAVA [2]. The other language which can be used is IDE IntelliJ [3]. All the employees who are using the languages are required to keep all the software and language tools up to date. In the following figure, the connection and use of software is described, like how it is connected to other users and machines [4].

In the diagram below, an example of class diagram is shown. In this diagram, a relation




and roles of administrators and employees is shown. The general employees and administrator come from same super-class, Employees, as all lie under this super-class. Considering both type of employees is coming from one super-class, it is not necessary that both will have same features. Like a general employee and administrator require username and password to login to their systems. But general employees can only add data related to their own work, while the administrators have access to all the data, and also have access to monitor and read the data of any employee [5].

As the super-class has an upper level so the access of methods from super-class will be available to regular employees. But the regular employee can have more methods other than the super-class methods, which could be: (a) permission to change the account's password, (b) if the employee have permission to get access to sensitive data, and (c) is the data, which is related to a specific employee, sensitive. If the comparison is made between a regular and admin class, the admin has access to more methods than a regular employee. Which is because admin has to manage all the accounts. He can add a new user as employee, he can set passwords for the employees, he can block an account and delete its data, if required and asked by CTO or CEO. The admin also have access to permissions which are assigned to regular employees. After having permission by CEO/CTO, the admin can provide access, to any employee, to the sensitive data.

# 4 Restrictions

The project has a few restrictions, which are listed here.

- There are instances of employees' system access without their permission, and the data is stolen, if the employees leave their logged-in or they forget to lock the systems, when they are away. The system automatically logs out the PC/system in a specific time frame. Finite attempts to log in are provided as in to stop intruders playing with the system.
- The codes within the software can decide where the data is going to be stored. So that it is the responsibility of our software to control the execution of the code and to decide where the location of data transfer.
- It is important to save the encryption key to a safer place and obviously this place cannot be the database. The key is used to encrypt information placed in the database and make it secure.
- The encryption key life cycle is important. It is required to apply a standard life cycle where generation of the key, its distribution and the usage of the key is to be decided. The other important factor is the deletion of the key, when it is no more required. As mentioned earlier that the encryption key and password cannot be stored in a database, so it could be stored in a memory. But the memory has to be reset to zero, when the usage of password or encryption key is completed.
- If Downloading information from online sources is a greater risk of being attacked by any hacker, as hacker can intrude through any file which is downloaded. It is important to apply restrictions on the usage of internet, like which websites are allowed, and what type of documents can be downloaded from internet. When a file is downloaded from internet, it should be scanned from using an approved antivirus software.
- There are times when the data is under inference attack. So, it is required to overcome such attacks. Whenever an employee received an information, he needs to analyze the

information carefully and decide if the received information is of a sensitive nature and needs protection.

# 5 Client's Guide / Activity Instructions

- To encrypt any data, it is required to create an encryption key which is to be managed and stored as per the policy mentioned above. And to access the system and login in a system, it is required to use a password with these guidelines: (a) the password must be at least 16 characters, (b) it must include special characters, numeric values, lowercase letters, uppercase letters. To make the password more secure, every employee must update its password after every six months. All the employees must be restricted to not use the old password, in future.

- If a user attempts to login and the attempt is failed, then the failed attempt must be registered and recorded. In this way it will be possible for the software to keep track of all the failed attempts and their causes. This will also help in deciding if there are any attempt of unauthenticated access to the system.

- Inference attacks are very dangerous, as one can find sensitive information from a non-sensitive data. Like name of a person, its social security number, and his address etc. So, the employees must take care of inference attacks.

- The integrity of information is very important. So, the organization should place an access control policy which may protect the information. The software must have a control over the process of giving access to employees for the data. All the employees must have a limited access to the information which is only meant for them. It may also have features where the software takes care of extra security of the data, in case of failure attempts to access the data. Only those employees, which have special permissions from CEO, will have access to the important information.

- All the top ranked employees need to have special access rights to get control over sensitive information. This could be, a temporary password which has limited life and also

another authentication which could be RFID, Face Recognition etc.

- It is important to invest in software like anti-viruses. It will provide additional support to the security and will help to detect if there is any malware attack from outside or within the organization.
- Security of SQL database is also important as it contains important information. An attacker can inject queries by interfering with SQL queries from company's software, this is known as injection attacks. Such attacks need to be taken care of with proper software.
- Employees should be restricted to upload type of data to the database. Only allowed file types should be uploaded to the database. There should also be a limitation of the size of file as well. This will save the bandwidth and also keep the limit for the information stored in the database.
- When a file is uploaded in the system/database, employees should not have a direct access to the file. Every employee must get proper authentication before access to the files.
- As mentioned earlier, all the data that is coming from internet needs to go through the anti-virus software. The anti-virus must scan and verify the health of the file downloaded from internet. This will help in reducing the attacks from internet sources and company's information will be secured.
- All the software which are used in the company should be updated on regular basis. The operating system needs to be up to date so that it might have the knowledge of the modern attacks and how to tackle them. If the systems have updating issues, the error log must only be shared with the concerned company and not anyone else.
- Besides the updating of the company's software, it is important that the company regularly monitors the information about who is accessing the company's resources and keeps a track of the information.

# 6 Client's Point of view

Depending on the nature of operation, several scenarios may rise. A few of them are discusses in this section.

- **Employee's accounts:** All the employees are offered their own PCs so that the secrecy of all the work on a specific employee must be intact. Each worker has access to the data which is required by him/her.
- **Deciding the Information Quality:** In the new agency, different pedigree provides different data figures. A worker gets specific data when it is acquired. A worker decides about the quality of information. Let us explain this in support of an example. Let us assume that there are two sources of information about some legitimate news and the first source provides data less authentic than the second one. These sources are required to be stored in a way that they are sorted with respect to their authenticity value.
- **Information's Sensitivity:** Confidential terms in a certain document would be categorized in a way that only authorized personnel can see the terms for example, name, address of the person sending the news. All these terms would be encrypted.
- **Security of sensitive information:** Those workers who have authorization to access the confidential data would also pass a protection key in order to access the data. Unauthorized personals may not even process the protection key.
- **Entering the details of any information:** Its obligatory to list the items as to which the new user can easily understand and use the data.

# References

[1] N. Lord, "What is data encryption? definition, best practices more." [Online]. Available: https://digitalguardian.com/blog/what-data-encryption [Kontrollerad: 05.01.2021]

[2] R. W. Sebesta, *Concepts of programming languages*. Pearson Education, Inc, 2012.

[3] E. Toporov, "Security update for intellij-based ides v2016.1 and older versions." [Online]. Available: https://blog.jetbrains.com/blog/2016/05/11/security-update-for-intellij-based-ides-v2016-1-and-older-versions/ [Kontrollerad: 05.01.2021]

[4] V. Paradigm, "Uml class diagram tutorial." [Online]. Available: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/uml-class-diagram-tutorial/ [Kontrollerad: 06.01.2021]

[5] M. Brambilla and P. Fraternali, *Interaction flow modeling language: Model-driven UI engineering of web and mobile apps with IFML*. Morgan Kaufmann, 2014.