A logo with a blue and white design

Description automatically generated with medium confidence

Academy of Economic Studies, Bucarest

Information Security Masters

An analysis of IT systems in financial institutions

dissertation

Coordonator Graduate

Prof. Univ. Dr. Cristian-Eugen CIUREA Cristian-Mihail DUMITRESCU

Bucharest 2024

Declaration regarding the originality of the content and assumption of responsibility

Through my pressence, I declare that the presented results in my work are my own results except for the case where I make a refferance to other authors. I confirm the fact that any material use from different sources (magazines, books and websites) are as clearly as possible referenced in the dissertation and are indicated in the bibliografic references.

Contents

[**Chapter 1 - Introduction** 1](#_Toc156336231)

[**Chapter 2 – The general structure of a financial institution’s IT system** 2](#_Toc156336232)

[Chapter 2.1 – Structure of the critical internal systems 2](#_Toc156336233)

[Chapter 2.2 – Ways most clients of a financial institustion interact with it 2](#_Toc156336234)

[Chapter 2.3 – Ways most employees of a financial institustion interact with it 2](#_Toc156336235)

[**Chapter 3 – Types of possible attacks** 3](#_Toc156336236)

[Chapter 3.1 – Third-party software and hardware security problems 3](#_Toc156336237)

[Chapter 3.2 – API problems 3](#_Toc156336238)

[**Chapter 4 – Prevention and mitigation of attacks** 4](#_Toc156336239)

[Chapter 4.1 – Prevention and mitigation of third-party software and hardware security problems 4](#_Toc156336240)

[Chapter 4.2 – Prevention and mitigation of API problems 4](#_Toc156336241)

[**Chapter 5 – Conclusiton** 5](#_Toc156336242)

[**Bibliography** 6](#_Toc156336243)

[**Anexa 1 – Figure list** 7](#_Toc156336244)

[**Anex 2 – Acronim list** 8](#_Toc156336245)

# **Chapter 1 - Introduction**

As the title suggests, in this piece of writing I will discuss, with examples, the possible security problems that may arise when designing, configuring and using software in a financial institution.

Firstly, I want to discuss the definition of a financial institution in the context of this paper.The United Stated Government through the Financial Crimes Enforcement Network [1] defines a financial institution as any person (as in individual, business, partnership, trust or estate) doing business in one or more of the following capacities:

1. Bank
2. Broker or dealer in securities
3. Money services business
4. Telegraphy company
5. Casino
6. Card club
7. A person subject to supervision by any state or federal bank supervisory authority

For the context of this paper, I will be refering to financial institution as a business that has the capacity of a bank, broker or dealer in securities or money services business.

The structure of the dissertation goes as following: presenting the general structure of a financial institustion - I will use the perspective of a bank -, exposing the possible weak points of the structure from an IT prespective and presenting possible fixes for those problems. The text will be accompanied by example projects posted in the following repository : ”<https://github.com/lieautman/Dissertation>”, which will showcase the aforementioned weak points and fixes.

# **Chapter 2 – The general structure of a financial institution’s IT system**

In this opening chapter, I would like to discuss the structure of the financial institution that I will be analysing from a secirity perspective. I will be taking on a top-down perspective, from the design of the systems to the outward facing capilaries.

## Chapter 2.1 – Structure of the critical internal systems

In this subchapter, I will be describing the internal structure of the critical internal systems of a financial institution, mostly Databases and Networks.

Databases are a critical piece of any infrastructure. For financial institutions, reputation plays a big role in their business. Thus, client data must always be kept safe.

A good rule is for any organization to have backups online and offline, as well as onsite and offsite. Since we are dealing with a financial organization such as a bank, we can assume that most data stored is of high value to the institution. Such data shall always be as protected as possible. Keeping backups will lead to an easier recovery in case of emergency. They also allow for minimization of risk.

When deciding on what database to use for any organization, there are a few questions we need to ask ourselves: what kind of database do we want? – structured or unstructured, SQL or non-SQL; what is the expected support for such a database? – making a contract with the creators of the database or just using a very popular database that will not be out of support soon; and what are the particular advantages of using a certain database? – some databases allow faster writes or faster reads, other databases allow greater data security through versioning and many other features.

Here we can also talk about cloud databases which can help with the security but have two inherent disadvantages: the data has to travel through an unsecure tunnel, the internet which has its own solutions such as VPN’s and the data is now in the possession of a third party that may or may not be trusted.

-- (here I can link with the idea of the app) – In the app created for this paper, I have used a local SQL database, thus minimizing the risks associated, but the risk can also be insured or accepted.

Networks and their management are another key component to any organization. Having proper security on any level of the iso/osi model [2] is of upmost importance. Although most software is not assuming a high level of security within the same organization when communicating, a multitude of security issues can lead to an incident.

When dealing with sensitive data, not only the access points, but the mode of transfer must also be secure. A secure network is not only maintained and guarded physically; it also must be maintained logically.

When discussing physical security, we can talk about maintaining proper procedures for entering restricted areas and maintaining the equipment.

On the other hand, logical security of a network has many components. There are passive security solutions such as honeypots and canaries. There are active security solutions such as intrusion detection systems.

There can also be layers of security, in the form of DeMilitarized Zones, DMZ [3], with ever-more restrictive firewall rules. And Virtual LAN [4] solutions that will lead to a more secure network.

With this subchapter, we can start painting a more holistic picture of an organization. We can now assume that an organization has databases that connect to software through networks and that these must be secure.

## Chapter 2.2 – Ways most clients of a financial institustion interact with it

As the title suggests, this subchapter will take on the task of presenting the ways in which clients can interact with the IT systems of financial institutions.

There are three main systems that are interfacing with the client of a financial institution. There is proprietary hardware facing the client, such as atms and pos-es, there is proprietary software such as websites of said financial institution and there are third party software and hardware facing the client such as network equipment in a subsidiary.

--talk about hardware facing clients such as atms – the atms and pos-es have failsafes and are monitored (atms are atached to a subsidiary with security personnel nearby, and pos-es should have self destruct and monitoring measures to ensure safety.)

--talk about websites facing clients

--talk about networks facing clients (such as wifi in subsidiaries)

## Chapter 2.3 – Ways most employees of a financial institustion interact with it

Altohw IBM X-Force Threat Intelligence Index 2024 [5] at page 9 say the phishing attacks have come down, it is a reflection of the continued adoption of phishing mitigation techniques. In 2016, the same research said that almoust 60% of the attacks come from within a company.

* Reread this

To mitigate this kind of problems, there have to exist protocols and training

--protocols and training in relation to this

--talk about following protocols and training

--talk about data safety through training

--talk about accont safety through training

---make callbacks to ISO and network for dummies + audit

# **Chapter 3 – Types of possible attacks**

Within the structure described above, there can be a big number of attacks. In this chapter, I will be emphasizing some of the most prevelent. According to OWASP Top 10 API Security Risks – 2023 [5], the most problematic vulnerabilities are:

1. Broken Object Level Authorisation
2. Broken Authentification
3. Broken Object Property Level Authorisation
4. Unrestricted Resource Consumption
5. Broken Function Level Authorisation
6. Unrestricted Access to Sensitive Business Flows
7. Server Side Request Forgery
8. Security Misconfiguration
9. Improper Inventory Management
10. Unsafe Consumption of APIs

Besides all of the above mentioned problems when writing a software APIs, there exist a lot more misconfiguration and mismanagement problems when using third-party software and hardware.

## Chapter 3.1 – Third-party software and hardware security problems

Firstly, I would like to discuss about possible problems with third-party software and hardware.

--add database security here

## Chapter 3.2 – API problems

Asdasda

# **Chapter 4 – Prevention and mitigation of attacks**

-- Description of this chapter

## Chapter 4.1 – Prevention and mitigation of third-party software and hardware security problems

According to the Plan-Do-Check-Act principle, any component must go through cycles of planning changes, implementing them, checking for issues (being security or otherwise) and acting to minimise the issues.

-- Risk avoidance

--database security

## Chapter 4.2 – Prevention and mitigation of API problems

-- Add API Prevention and Mitigation

# **Chapter 5 – Conclusiton**

-- Add conclusion

# **Bibliography**

|  |  |
| --- | --- |
| [1] | USA Gov, "financial-institution-definition," 01 01 2024. [Online]. Available: https://www.fincen.gov/financial-institution-definition. [Accessed 1 1 2024]. |
| [2] | International Organization for Standardization, ISO/IEC 7498-1:1994, Geneva: International Organization for Standardization, 1994. |
| [3] | Department of Homeland Security USA, „Archive of "Control System Security DMZ",” Department of Homeland Security USA, 9 May 2020. [Interactiv]. Available: https://web.archive.org/web/20200609134629/https://www.us-cert.gov/ics/Control\_System\_Security\_DMZ-Definition.html. [Accesat 2 February 2024]. |
| [4] | IEEE, „802.1Q-1998 - IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks,” IEEE, 1 1 1998. [Interactiv]. Available: https://ieeexplore.ieee.org/document/753056. [Accesat 24 2 2024]. |
| [5] | I. S. P. S. Erez Yallon, „OWASP API Security Top 10,” 2023. [Interactiv]. Available: https://owasp.org/API-Security/editions/2023/en/0x11-t10/. [Accesat 13 01 2024]. |

# **Anexa 1 – Figure list**

asdasd

# **Anex 2 – Acronym list**

|  |  |
| --- | --- |
| *API* | Application Programming Interface |
| *DB* | Data Base |
| *TCP* | Transmission Control Protocol |
| *LAN* | Local Area Network |
| *SQL* | Structured Query Language (databse type/language) |
| *VPN* | Virtual Private Network |