




Remote document access with ransomware protection

Network and Computer Security

Alameda

Grupo 46

Image	Name	Student Number
	Guilherme Nunes	89450
	Pedro Maximino	89524
	Larissa Tomaz	92506

1 Problem

The fact that there is so much data in document systems makes them targets for malicious people. That's why, in recent years, there has been an increasing number of ransomware attacks on these systems. In this type of attack the attacker manages to breach the system and encrypt the user's files. Once completed, they request a ransom (usually a cryptocurrency like BitCoin) to provide the decryption key and allow the user or company to recover their files. Therefore, the system must ensure data confidentiality, that third parties can't modify files illegally (i.e the users can read/write only if they have permission to do that) and reduce that impact of a ransomware attack.

1.1 Solution Requirements

- **R1:** The system must guarantee the confidentiality and integrity of the files;
- **R2:** The system must authenticate users;
- **R3:** The system must guarantee that viewers can only read the file;
- **R4:** The system must guarantee that editors can read or write the file;
- **R5:** The system must ensure that only the owner of the file can give privileges to another registered user;
- **R6:** The system must verify that users have the permissions they claim according the given file;
- **R7:** The system must be able to recover if any ransomware attack happen;
- **R8:** The system must guarantee the confidentiality and integrity of communications;
- **R9:** The user cannot repudiate their actions.

1.2 Trust assumptions

- Primary Server: **Fully Trusted** - the server is reliable in allowing only authorized users to access the files.
- Users: **Untrusted** - as we cannot control our users level of awareness against malicious threats in their own private systems.
- Database: **Fully Trusted** - as we assume that the database is kept securely and the system administrator, who has access, is fully trustworthy.
- Backup Server: **Partially Trusted** - as we assume that there is always

one machine alive, but we cannot fully guarantee that the ransomware won't propagate to the backup server.

- Cloud Server: **Partially Trusted** - since it is kept by another service and isolated from the system network, but we cannot guarantee that the data won't be shared with third parties.

2 Proposed Solution

2.1 Overview

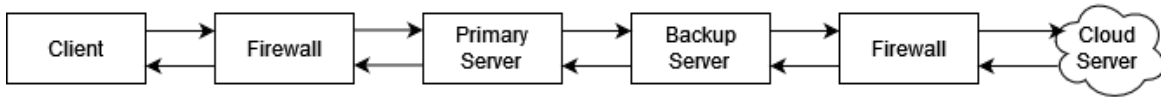


Figure 1: Solution Diagram

We propose a solution that combines the necessary security standards, in order to prevent or reduce the damage caused by ransomware attacks, including illegal file modifications and unauthorized access:

- Regular file backups with versions, to prevent the need to pay the ransom or have services affected due to files being encrypted;
- An authorization system, that allows a person to assign permissions for a specific user and validates whether a certain user has the permission to view and/or edit a specific file.
- A system that detect illegal modifications, by an attacker;
- A way to share files on the public network in a secure fashion.

2.2 Deployment

We will make use of two servers, connected in the same network: Primary Server and Backups Server. The first one will host the files and handle all requests that come from the clients and pass through the Firewall. The latter one will be used to host regular backups of the system. Furthermore, we will also make use of a remote cloud server, so that we are able to store backups safely, in case an attack takes place.

2.3 Secure Channel(s) to Configure

The components of the system (clients and server) can communicate with each other using a set of secure channels to be configured, shown below. Con-

nections between any clients and the Primary Server always pass through a Firewall as shown later on:

1. **Client ↔ Primary Server:** This channel will be used for the client to send requests to the server and for the server to reply to such requests, always using TLS and passing through the Firewall;
2. **Primary Server ↔ Backups Server:** This channel will be used to send backups to the Backups Server and to send older saved versions of specific files requested by the Primary Server, always through TLS;
3. **Backups Server → Cloud Remote Server:** This channel will be used for the Backups Server to upload Backups to a remote cloud server, in order to make sure there are backups that are not connected to the main network. TLS will also be used to ensure the channel remains secure.

2.4 Secure Protocol(s) to Develop

We present a diagram of our project, below:

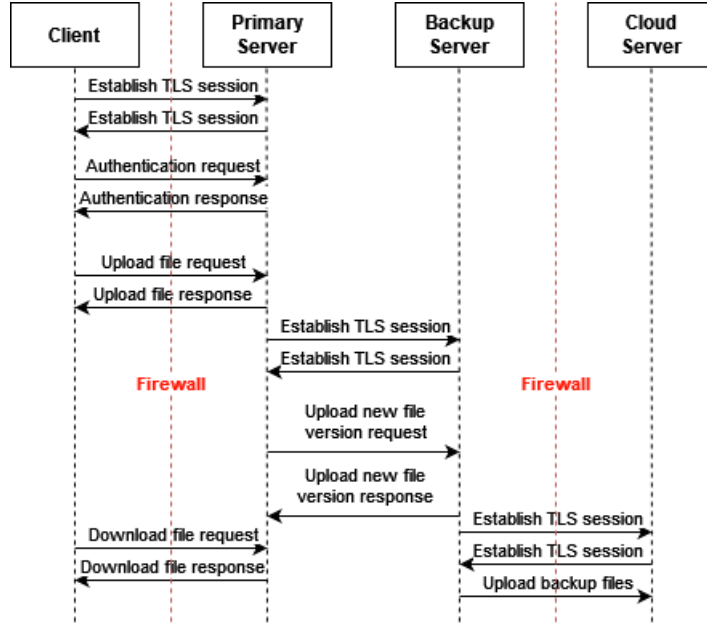


Figure 2: Sequence Diagram

3 Considered Technologies

We will use Java with Grpc to the communication between the system

and the clients (GRPC has a TLS option) and PostgreSQL for the database. Furthermore, we will use AES-256 algorithm to encrypt the files on the server and SHA-2 to compute the file digests, for integrity purposes. We will take advantage of the Java Crypto library for that.

4 Plan

4.1 Milestones

- **Basic Version:** Implement a basic version of the authentication and authorization (rbac) systems that checks whether a certain user has permission to edit/view specific files and allows people to assign permissions to users.
- **Intermediate Version:** Implement secure channels to communicate between clients and servers (using TLS). Furthermore, encrypt system files in order to prevent unauthorized access to them.
- **Advanced Version:** Enhance the authorization system, in order for it to detect unauthorized file modifications and to verify a person's identity. In addition to this, implement a backups strategy, so that files are backed up regularly.

4.2 Effort Commitments

	Basic Version	Intermediate Version	Advanced Version
Names	07/01 - 14/01	14/01 - 21/01	21/01 - 28/01
Guilherme Nunes	Server Implementation Database Implementation	Secure Channels File Encryption	Backup System Hash verification
Pedro Maximino	Client Implementation Authentication	Secure Channels File Encryption	Backup System Hash verification
Larissa Tomaz	Server Implementation Authorizations	Secure Channels File Encryption	Backup System Hash verification

5 References

- [1] André Zúquete. *Segurança em redes informáticas*. FCA, 5 edition.
- [2] Grpc Authentication, Sep 2021. <https://grpc.io/docs/guides/auth>
- [3] Nextcloud. How nextcloud helps protect against ransomware. <https://nextcloud.com/blog/how-nextcloud-helps-protect-against-ransomware/>