Instituto Superior Técnico

Network and Computer Security

Group 10 - Taguspark

Medical Test Records

Sara Machado
86923

Rafael Figueiredo
90770

Ricardo Grade
90774

1. Problem

The system goal is to manage hospital's patient's sensitive information.

The system users are the hospital Employees, according with their role they need to access specific information about its patients. It is necessary to ensure that Employees without permissions do not access privileged information. There are 10 different roles: Doctors, Nurses, Clinical Assistants, Patient Services Assistants, Porters, Ward Clerks, Laboratory Technician, Regular Employee, Partner Lab and Hospital's Manager.

Medical tests can be performed inside a Hospital Lab or in a Partner Lab. In the last case the test results need to be sent back in a secure way, such as it cannot be intercepted, modified, or stole. Moreover, it is necessary to store them with the guarantee that it can be verified its authenticity.

The system has different modes, the *Normal* and the *Pandemic* mode where the user's access levels are modified accordingly. This mode may only be changed by the Hospital's Manager. Regarding *Pandemic* mode, it is required that Employees help each other, due to the overload of patients, for this reason the information that Clinical Assistants, Patient Services Assistants and Porters have access to will be shared among them.

1.1. Requirements

- Secure Keys distribution among all system stakeholders.
- System communication channels need to ensure Freshness, Confidentiality, Integrity, Authenticity.
- Each employee may have different access controls based on its role and system's mode.
- Each medical test result has to be stored along with its emitter laboratory signature and Timestamp.

1.2. Trust Assumptions

- Hospital Server and Policy Authoring are always available.
- Stakeholders will not flood the system.
- Stakeholders have knowledge of Certificate's Authority (CA) Key Certificate.
- Stakeholders Key Certificate setup is made in a secure environment.
- Hospital Server and Partner Labs clocks are synchronized with each other.
- Hospital Server already has Hospital Manager's credentials stored in its Database.
- All requests that pass the Freshness, Confidentiality, Integrity, Authenticity tests are valid.

2. Proposed Solution

2.1. Overview

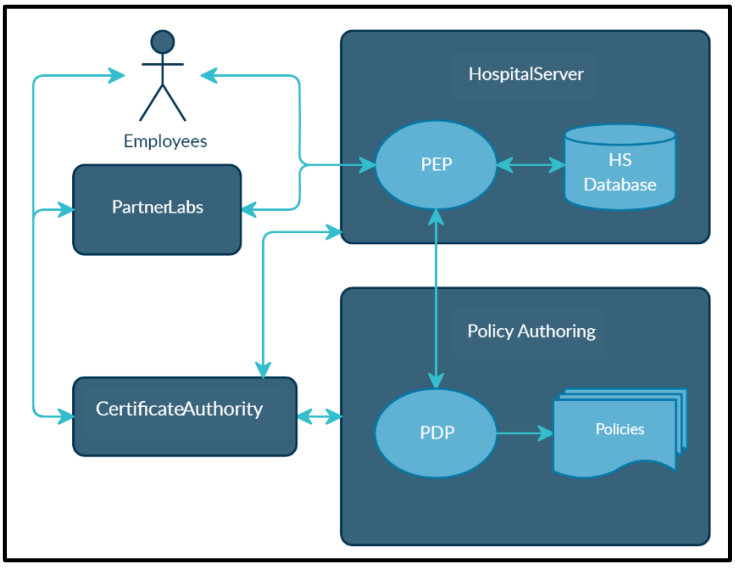

Figure 1: System Diagram

The system is composed by two clients of the Hospital Server which are the Employees and the Partner Labs. They are able to establish secure connections in order to make their requests. On the other hand, the Hospital Server is also a client of the Policy Authoring which makes access control decisions based on its policies.

2.2. Deployment

2.2.1. Certificate Authority

The Certificate Authority provides to all stakeholders except the Employees a Key Certificate, by signing their Certificate Signing Request (CSR), necessary for them to establish secure connections with each other.

2.2.2. Employees

The Employees have different roles according with their jobs inside the hospital. They are only able to read the patients' specific information needed in order to perform their jobs. Some also have write access on patients' records. In order for them to access these records they can establish a secure connection and authenticate themselves with the Hospital Server.

The following table describes the employee's permissions in *Regular Mode*:

Record	Action	Role
Test Result	Write	Lab Technician, Partner Lab and Hospital Manager
Test Result	Read, Authenticity Check	Doctor, Nurse, Lab Technician and Hospital Manager
Housekeeping	Read, Write	Doctor, Nurse, Clinical Assistant and Hospital Manager
Diet	Read, Write	Doctor, Nurse, Patient Services Assistant and Hospital Manager
Transport	Read, Write	Doctor, Nurse, Porter and Hospital Manager
Reception	Read, Write	Doctor, Nurse, Ward Clerk and Hospital Manager
Prescription	Read	Doctor, Nurse and Hospital Manager
Prescription	Write	Doctor and Hospital Manager
Patient Details	Read	Every Role
Patient Details	Write	Ward Clerk and Hospital Manager
Credentials	Write	Hospital Manager

Obs: The Employee's permissions in *Pandemic Mode* are described in the Problem section.

2.2.3. Partner Labs

The Partner Labs perform medical tests to patients, its results are sent through a secure connection to the Hospital Server to be kept along with its laboratory emitter signature and Timestamp in the patient's records.

2.2.4. Hospital Server

The Hospital Server has a Database with the user's usernames, passwords Hash and Salt, patients' records and Partner Labs certificates. Hospital Server is in charge of performing user's authentication for them to be able to access records, due to their different access controls it is necessary to enforce policies to validate its requests. This enforcement is performed by the Policy Enforcement Point (PEP) establishing a secure connection to the Policy Decision Point (PDP).

2.2.5. Policy Authoring

The Policy Authoring is composed by the Policy Decision Point (PDP), the Policy Administration Policy (PAP) and the Policy Information Point (PIP), therefore it contains the assignment of roles to the Employees ensuring that only the ones with permission are allowed to access the patients' records. PDP is the entering point of the Policy Authoring receiving requests made by PEP at the Hospital Server in order to accept or deny the Employees' requests. To make this decision PDP evaluates the policies provided by PAP, for doing so it may reach PIP to access to the employee's role.

2.3. Secure Channels

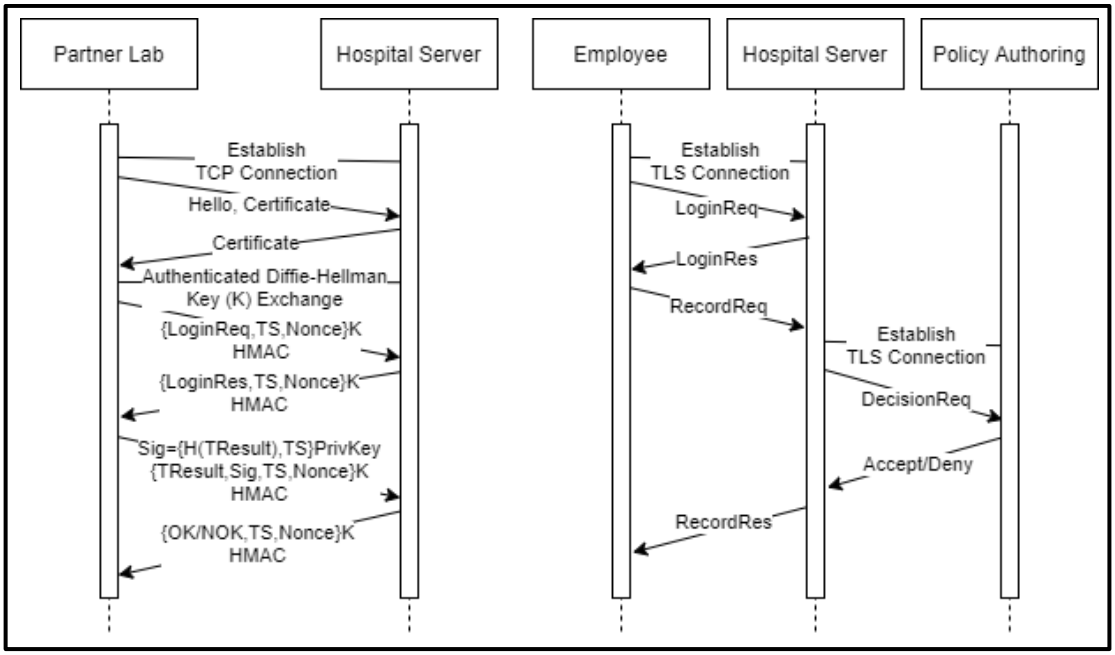

Figure 2: Communication Diagram

There are two different communication channels in the system. A custom one is implemented between the Partner Labs and the Hospital Server, as well as a TLS based one between the Hospital Server and the Employees or the Policy Authoring.

2.4. Secure Protocols

Regarding Key Distribution on the Custom Security Protocol, it is used the Diffie Hellman algorithm.

A Custom Security Protocol is used whenever a Partner Lab needs to establish a secure connection to the Hospital Server. Primarily a TCP connection is established. Following this its Certificates are exchanged in order to authenticate the handshake, then the Diffie Hellman algorithm is used to exchange a secret key (K). This K is used to encrypt all messages within the current session from now on. The messages contain a payload, a Timestamp (TS) and Nonce. A Hash of this elements and K (HMAC) is sent along with all messages.

Whenever a valid login request is sent to the Hospital Server, it sends back an access token, allowing the stakeholder in question to continue to perform its desired requests.

Whenever a Partner Lab needs to send results of medical tests performed to hospital patients or wants to read patients' information, it establishes a custom secure connection with the Hospital Server and logs in.

After the authentication, the Hospital Server associates the Partner Lab certificate to its credentials, in order to allow the Employees to verify the authenticity of the received test results without the need of contacting the emitter Partner Lab.

Whenever an employee desires to access patients records, it establishes a TLS connection with the Hospital Server to ensure that the communication is secure. Once it is established, the employee logs in and requests the desired records.

All requests related to patients and their records made to Hospital Server, need to be validated in order to assure that the user has permissions to do so. This is done by the Hospital Server enforcement point requesting, using a TLS connection, the Policy Authoring to decide, which will accept or deny requests based on the resource that will be accessed, the action that will be performed, the role of the requester and the system's current mode. Given its response the Hospital Server will either perform the operation or not.

The security properties granted by the system are Freshness, Confidentiality, Integrity and Authentication.

The system is designed in Java and using XACML as a policy language.

3. Results

On the Final Version of this system, it was achieved the fully implementation of the Employees, Partner Labs, Hospital Server, and Policy Authoring. All of them are communicating using secure channels:

- TLS, between Employees and Hospital Servers, and Hospital Server and Policy Authoring.
- Custom Security Protocol, between Partner Labs and Hospital Server.

Strongs:

- In all messages (Including Exceptions thrown) exchanged through the system nodes are guaranteed its Freshness, Confidentiality, Integrity and Authenticity.
- On the Custom Security Protocol, it is used Diffie-Hellman in order to establish an agreement on what Secret Key will be used within the current Session. This provides perfect forward secrecy. It is better to not encrypt messages with the same Secret Key across several sessions because it could give attackers time and hints to figure the Key out. Also, Asymmetric Keys are heavy in terms of computation. Certificates are exchange prior to Diffie-Hellman in order to authenticate this Handshake granting protection against Man in the Middle Attacks.
- Access controls are implemented. This will make the Hospital Server decline all unauthorized requests made by an Employee or Partner Lab. This is achieved by Hospital Server using its PEP to contact the Policy Authoring which uses PDP and its Policies to decide whether the request should be performed or not.
- Policies are written in XACML using RBAC access control model. This provides the desired flexibility and scalability to system access control. It was chosen the RBAC model because it provides more efficiency to the PDP evaluation by analysing less rules than it would in the case ABAC model was implemented instead.

Weaknesses:

- Message Fields are encrypted separately for the sake of simplicity without losing any security. It may increase the overhead of the message's encryption, but it provides simplicity to the Field retrieval of the encrypted messages.
- There is no revocation service of certificates available in the system, and the requirement of new certificates must be made manually.

3.1. Work Distribution

Weeks/Names	Sara Machado	Rafael Figueiredo	Ricardo Grade
1	Employee and CA Implementation	Hospital DB Configuration and CA Implementation	Hospital Server and CA Implementation
2	TLS Connection Implementation	TLS Connection Implementation	TLS Connection Implementation
3	PDP	Definition of Policies	PEP
4	Custom Security Protocol Implementation (Partner Lab)	Custom Security Protocol Implementation (Hospital Server) and DH Crypto Implementation	Custom Security Protocol Implementation (Hospital Server) and Partner Lab Implementation

4. References

- Java: JDK 11
- Maven: Apache Maven
- Grpc: io.grpc
- Protobuf: com.google.protobuf
- TLS: io.grpc.netty
- XACML: Authzforce
- Cryptographic Algorithms: javax.crypto
- PostgreSQLJDBC: java.sql
- Keys Management: java.security