System Description and Risk Analysis

Thomas Knell Danny Schweizer Samuel Hitz

November 21, 2013

Contents

1 System Characterization

1.1 System Overview

The company iMovies needs to exchange information via email confidentially. In order to achieve this, we implemented a certificate authority (CA) to provide employees with digital certificates which subsequently can be used for secure communication.
The core functionality of the CA is found on a server, which we will call the core server. It has the functionality to issue and revoke certificates and maintains a list of all issued and revoked certificate as well as a backup for each private key and issued certificate in case of data loss on the side of the employee (further called client). A database where the user information of the clients is stored is also maintained by the core server.
Additionally, the core server serves a web site, which acts as an interface for clients and CA administrators to the core functionality. A client of the system can use this web interface via a browser to issue or revoke a certificate based on his user information and to change said information in the database. In order to authenticate himself, he needs to enter his username and password. For CA administrators an admin web interface is provided, which shows the total number of issued and revoked certificates as well as the current serial number to be used for the next certificate the CA will issue. CA administrators authenticate themselves to the server using digital certificates. System administrators can access the core server remotely to perform configuration and maintenance tasks.
There is a second server running which serves as a firewall between the client machines and the core server. The firewall has an interface to the intranet of iMovies where the clients are located as well as an interface to the core server which runs in a different network. This allows the system administrators to tightly control the access to the core server and thus expose a very limited attack surface to possible attackers. Additionally a second firewall is installed on the core server itself. This further increases security by acting as a second line of defenses against an intruder.

1.2 System Functionality

1.2.1 Certificate Issuing Process

The user logs in via web form by entering his username and password. The provided information is verified by consulting the information stored in the database. If the verification is successful a new session is created by generating a new cookie storing session information. The authenticated client can then see his current user information stored in the database, i.e. his name, email address and the number of active/revoked certificates. The client can change this information and his password at any time. The username and a temporary password is created by the company's Human Resource department (not part of this analysis) at the time of employment. In contrast to the password, the username cannot be changed by the client, mainly due to administrative reasons.
If the client chooses to edit his name, he can do so by entering the new first and/or last name and providing his password. If the correct password was entered, the new name is stored in the database.
If the client chooses to edit his email address, he can do so by entering the

new email address and providing his password. The string entered for the new email address is verified to indeed represent an email address and if the correct password was entered, the change is stored in the database.
If the client chooses to edit his password, he can do by providing the old password and the new password (twice, to prevent typing errors). If the old password is correct and the two new passwords match, the change is stored in the database.
If the client chooses to edit his certificates, a list of all his active and revoked certificates is displayed in addition to giving him the option to generate and download a new certificate based on the user information (name and email) stored in the database. To do so, the user has to enter his password which is also used to encrypt the new certificate, including the corresponding private key, in PKCS#12 format. The private key is backed up immediately after a user has requested the new certificate. This is to ensure that encrypted data is still accessible even in the case of loss of an employee's certificate or private key, or even the employee himself.
Having to enter the password before each action serves two purposes, one is to authenticate the client again and therefore preventing someone else altering his data even if the session is still valid. Additionally an attacker doing a cross-site request forgery needs to know/guess the password correctly to be successful. The session is terminated if the user logs out or closes the browser, thereby invalidating the cookie stored in the client's browser.

1.2.2 Certificate Revocation Process

The affected user authenticates himself to the web application, either certificate-based over SSL/TLS (if the user still holds the certificate and the corresponding private key) or the user uses his username and password stored in the database. If the user authenticated himself with a valid certificate, a list of all his active/revoked certificates is displayed in addition to giving the user the possibility to revoke all of his affected certificates. If the user authenticates himself with username and password the same functionality is offered after choosing to edit his certificates (described in section 1.2.1).
After revoking a certificate, a new certificate revocation list is generated and published on the web server. The possibility to revoke certificates without providing username and password was implemented to compensate for the missing password recovery feature. Even if the user forgets his password and realizes that one or many of his certificates were compromised, he can quickly react by login in with one of his certificates and then revoke the affected certificates.
To prevent attackers from easily generating cross-site request forgeries (as the user does not have to enter his password), a random token is generated and stored at the start of the session. The token is passed along in the request to revoke the certificate and has to match the token stored in the session for the request to be accepted.

1.2.3 CA Administration Interface

Using a dedicated web interface, CA administrators can consult the CA's current state. The interface provides the following information:

1. Number of issued certificates

2. Number of revoked certificates

3. Current serial number.

CA administrators authenticate themselves with their digital certificate. To differentiate between administrators and normal users, the CA uses two different keys to sign the certificates.

1.2.4 System Administration and Maintenance

To maintain the system administrators can remotely connect to the core server using `SSH`. Access and error logs of Apache are automatically backed up daily using `logrotate`. A custom script backs up the whole CA as well as important logs to `/home/sysadmin/backup` periodically.

1.3 Components and Subsystems

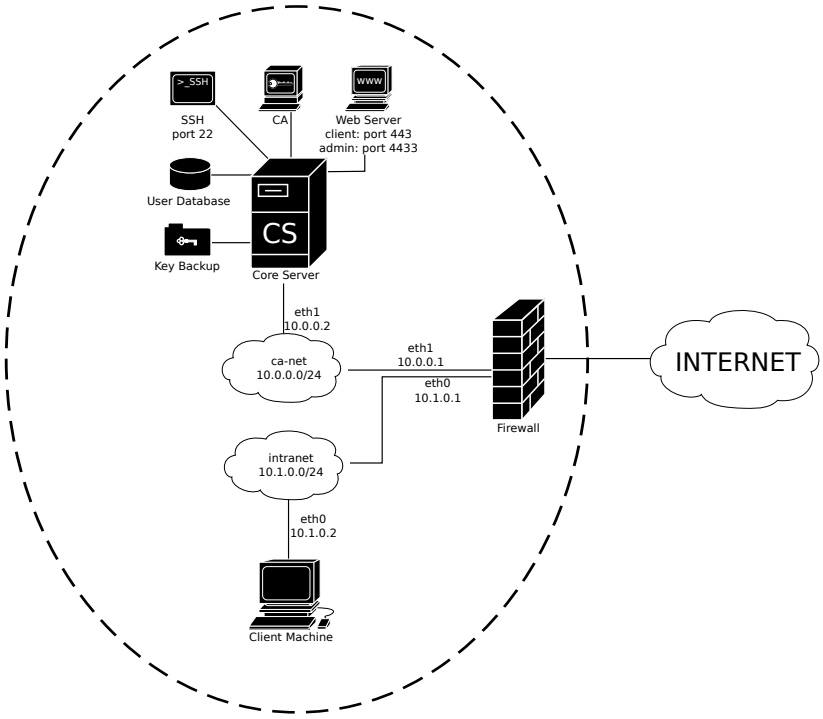

Figure 1: Network diagram

The system's relevant technical and network components are depicted in Fig. 1.

1.3.1 Core Server

The core server is an Ubuntu server providing the core functionality of the system. It hosts the certificate authority as well as the web interface to access and

maintain the CA. This server is connected to the firewall system by an internal network called `ca-net` and has the IP address `10.0.0.2` statically assigned. The `ca-net` is a class C subnet in the IP range `10.0.0.0/24`. Below all the components running on the core server are listed.

Certificate Authority The core functionality of the server is the CA itself. The CA is implemented using the `openssl` package from the Ubuntu software repositories. All the data the CA maintains is stored under `/etc/ssl/iMoviesCA`. `openssl` maintains an index of issued and revoked certificates as well as some other data it needs to ensure correct working.
All issued certificates are signed by a 2048 bit self signed RSA key. The self signed root certificate is valid for ten years unless revoked earlier.

Web Server An Apache2 webserver is used to serve the client and CA administrator web user interface (web UI) of the CA. It is configured to serve two virtual hosts, the user web interface and the admin interface. The web server serves the client UI on port 443, i.e. the standard `https` port, while the CA administrator web interface is accessible through port 4433. Apache is configured to accept only `https` traffic on both ports. The configuration is stored under `/etc/apache2` and error and access logs are kept in `/var/log/apache2`.

Web UI The web interfaces are both implemented using `PHP` version `5.5.5` and `HTML`. The relevant source files are located at `/var/www/user_interface` and `/var/www/admin_interface`.

User Database A MySQL database is used to store all user information. For each user it contains the user id, the first and last name, the email address as well as a `sha1` hash of the password. A second table is used to associate a user's id to the serial numbers of his issued and revoked certificates.

Key Backup All the keys signed by the CA are stored in a folder under `/etc /ssl/iMoviesCA`. To associate the key with the corresponding certificate both files use the serial number of the certificate as file names. The key backup is secured using standard Linux Access Control Lists (ACL) against unauthorized access.

System Administration System administrators can remotely access the system using `SSH` via port 22. Public key authentication is used to secure against unauthorized access. Additionally a daily cron job is run to back up important configuration and logging files of the system.

Firewall The core server is running a firewall, namely `iptables`. It is configured to accept only incoming TCP traffic on ports 22, 443 and 4433. Outgoing traffic is only accepted if it belongs to an already established TCP connection. No connection initiated by the core server itself is let through.

1.3.2 Firewall System

The firewall system is a separate Ubuntu server acting as a gateway between iMovies intranet and `ca-net`. All the traffic between clients/admins and the core server is routed through the firewall system. The firewall is configured to forward incoming TCP packets destined for the core server only on ports 22, 443 and 4433. Outgoing traffic is only accepted if it belongs to an already established connection to the core server. No connection initiated by the core server is let through. To implement this policy `iptables` is used. To maintain the firewall system, system administrators can access it on port 22 using `SSH`.

1.3.3 Client

Client systems are the workstations, laptops, mobile devices etc. used by the employees of iMovies. At the very least they all have a web browser, an email client and an anti-virus software installed. The client systems belong to the iMovies intranet which is a class C subnet in the range `10.1.0.0/24`. If a client is authorized to access the admin web interface of the CA, a special certificate is installed in its web browser used to authenticate the client to the admin interface.

1.4 Interfaces

This section describes every interface in the system and how they are made secure against malicious users.

1.4.1 Connecting to the Core Server

The core server resides in a different network than its clients. Every connection from the 'outside' to the core server needs to pass through the firewall system. The firewall policy implemented by the firewall is described in 1.3.2. The packets are then forwarded to the core server where a second firewall, implementing the same policy, needs to be passed before they are delivered to the respective service. The approach minimizes the attack surface for a potential attacker and by deploying two separate firewalls there is no single point of failure.

1.4.2 Client/Server Interface

A client can access the web interface by connecting to `https://10.0.0.2:443`. This connection is secured by SSL/TLS providing confidentiality, server authenticity and optionally client authenticity. The server authenticates itself to the client by a certificate signed by the iMovies CA. The web browser on the client has to trust the CA to set up an authentic connection. Optionally the client can use his certificate to authenticate himself to the server, however, to access the web UI, he still needs to login with his user credentials.

1.4.3 Admin/Server Interface

An admin of the CA can access the web interface by connecting to `https://10.0.0.2:4433`. Like the client/server connection this connection also uses

SSL/TLS to provide confidentiality and authenticity. The difference to the client/server connection is the mandatory admin authentication via a certificate signed with particular signing key. The web server verifies the validity of the presented certificate and grants only access to an admin with a valid certificate.

1.4.4 System Administrator Interface

A system administrator can access the core server as well as the firewall system connecting to the respective system with `SSH` through port 22. He authenticates himself using either his password or his public/private key pair. `SSH` provides a secure channel to the destination system. Once authenticated a system administrator has full control over it.

1.4.5 Web Server/CA Interface

Whenever a user issues a new certificate or revokes one, the web server has to interact with the CA. This is done via `PHP`'s `shell_exec()` function, which allows the web server to execute shell commands privileged as the user it is running as (`www-data`). `shell_exec()` takes the command string as argument and returns the output of the command on success or `NULL` on error (or no output). To secure against command injection attacks, the argument string has to be properly escaped. `PHP` provides `escapeshellarg()` for this purpose.

1.4.6 Web Server/Database Interface

The web server accesses and updates user information by querying the underlying MySQL database. This connection is done by using the `mysqli` module shipped with `PHP` which allows querying a MySQL database from `PHP` code. To access the database, MySQL login credentials are needed which are hardcoded in the code.
There are two security risks involving the MySQL database, namely SQL Injection and persistent Cross Site Scripting (XSS) attacks. To prevent SQL Injection attacks the web server uses prepared statements every time it accesses the database. In order to prevent XSS attacks the web server has to sanitize all the user given information before displaying it on the web interface. `PHP` provides `htmlspecialchars()` for this purpose.

2 Risk Analysis and Security Measures

The analysis is conducted in the company's point of view. The analysis does not include assets like file server, mail server, video production rooms, storage space of expensive audio and video equipment etc., as they are not directly or indirectly affected by introducing a certificate authority (CA). We assume an analysis of those assets has been conducted at an earlier point in time. Existing assets/persons will only be reevaluated if they are directly affected or the importance of said asset changed, i.e. increased.

2.1 Stakeholders

Running a certificate authority in the context of the iMovies company involves three stakeholders.

Informants: The informants play a crucial role in investigative reporting, as they can provide information which is very difficult/impossible to get without them. Informants may risk their jobs or even more by providing those kind of information. Thus they expect to be able to verify (with digital signatures) that they are actually exchanging emails with an employee of iMovies and not with some, potentially malicious, third party.

Clients/Employees: The employees of iMovies may stay in contact with informants for an extended period of time and informants may also recommend this employee to other potential informants as trustworthy. Thus it is vitally important that the employee can ensure nobody is able to impersonate him, i.e. nobody but him (and the system admins) should be able to access his certificates and private keys.

iMovies: This company is known for its accurate investigations and turning the gained information into high quality movies. Proper handling of their employees information and providing a way to securely communication via email is an integral part to further increase credibility of this company.

2.2 Information Assets

2.2.1 Physical Assets

Client Machines: Client machines are the workstations, laptops, mobile devices etc. used by the employees of iMovies. The components (fan, processor, graphic card, CD/DVD-ROM, etc.) might be in normal operation mode or might be defective, affecting the function of the corresponding machine.

Core Server/Router/Firewall: The core server, router and the firewall are located in a separate lockable rack in iMovies' basement.

iMovies Intranet/ca-net: The internal networks of iMovies are Ethernet local area networks. The Ethernet subnetworks are distributed using layer 2 switches. The firewall routes traffic between the networks. The internal networks' proper operation is essential for iMovies' ability to maintain the CA's integrity. Additionally it ensures network connectivity to the Internet.

Internet Connection: The router that connects to the service provider's (enterprise grade) network is placed in the same rack as the firewall. It connects with a Gigabit Ethernet interface to the firewall and over fiber to the service provider's backbone. Internet connection is essential for iMovies since it is the main communication medium to the informants. With the introduction of the CA its importance has increased since the access to the certificate revocation list by the informants is critical.

2.2.2 Logical Assets

Core Server: The Core Server runs Ubuntu 12.04 LTS server edition. Software running on the core server includes MySQL for the database, Apache2 and `PHP` for the web server and OpenSSL for the CA system. This software needs to be regularly updated by a system administrator in order to prevent

exploitation of known vulnerabilities in old versions. Security updates for the underlying operation system need to be installed as soon as possible.

Firewall: The firewall runs Ubuntu 12.04 LTS server edition and uses `iptables` to configure the tables provided by the Linux kernel firewall and the chains and rules it stores. The firewall system needs to be updated whenever a security update is available by a system administrator.

Client Machine: The client machines need to have a web browser, an email client and an anti-virus software installed. System administrators need to update this software regularly. Also, the operating system needs regular updates. If a client is authorized to access the admin web interface of the CA a special certificate is installed in its web browser used to authenticate the client to the admin interface.

User Database: The user database is confidential. Only system administrators are able to view it. A user is only able to view and change his own data. Proper Unix access control mechanisms need to be configured for the database.

2.2.3 Persons

Reporters: The reporters of iMovies doing the investigative reporting are very important for the company. It should be guaranteed to them that their reports remain confidential.

CA Administrators: The CA administrators are responsible for the CA system itself. They know the CA system very well and should guarantee the proper functionality of the system.

System Administrators: The system administrators are responsible for maintaining all the systems concerning iMovies. They have access to the systems and need to update them regularly.

2.2.4 Intangible Goods

Informant Confidence: Since informants may risk a lot by talking to reporters of iMovies, informant confidence is a necessary prerequisite for investigative reporting.

2.3 Vulnerabilities

2.3.1 Vulnerabilities of Physical Assets

Electronic equipment is sensitive to environmental factors like heat, water, physical shock etc. Its functioning depends on availability of electricity. Storage devices can break resulting in loss of data and network cables can be cut or unplugged (intentionally or unintentionally) leading to loss of network connectivity. There is always the possibility of breaking equipment by use of force.

2.3.2 Vulnerabilities of Logical Assets

Software may always suffer from programming errors leading to exploitable vulnerabilities with varying impact depending on the type of vulnerability and the software that suffers from it. Known vulnerabilities can usually been patched within a few days after detection, however, unknown vulnerabilities leave the

systems exposed to a skilled adversary.
Another source of vulnerabilities is the misconfiguration of system or application software such as firewalls and web servers.
In terms of logical assets, the worst case scenario involves an attacker gaining access to the CA system which would allow him to issue bogus certificates and use them to trick legitimate users of the system into trusting him. Another serious breach would be the ability to issue certificates on a legitimate user's behalf, for example by gaining access to the CA's web interface in the user's context.

2.4 Threat Sources

Natural Disasters: Natural disasters should always be considered, since they may happen at any time. The company building is not located near any kind of waters, so flood is no thread source. However, fire and earthquakes are a possibility to consider.

Employees: Employees of iMovies are an important threat source, because they have more access to the system than an outsider. Especially the system administrators may be a threat source (not necessarily intentionally, they might just make a critical mistake), since they have access to the whole system.

Competitors: Competitor movie companies might have interest in harming the system of iMovies for profit reasons. They might cooperate with skilled hackers to try to harm the system of iMovies.

Investigated Entities: If by some mishap, an entity (person, group of persons, company etc.) might notice that iMovies investigates on something they do not want to get public, they might try to harm the system, possibly cooperating with skilled hackers. If the investigated entity is a government then even governmental agencies might target iMovies.

Script Kiddies: Since the systems considered are connected to the Internet, they are exposed to attacks by script kiddies.

Skilled Hacker: Skilled hackers might pose a serious threat to the system, however, independent hackers will likely not attack it, but rather contracted ones from competitors/governments.

Malware: Directed or undirected malware might be a problem if it reaches a system within iMovies.

2.5 Risks and Countermeasures

Impact	
Impact	Description
High	The event may destroy or harm any assets of the system in such a way that the future of the company is in danger. This means, either parts of the systems or employees receive major persistent damage (e.g. a physical asset is permanentely lost or an employee dies) or the reputation or the mission of the company is significately harmed.
Medium	If the event occurs, parts of the systems or employees receive damage which might lead to high costs or the reputation or the mission of the company is harmed. However, the company should be able to recover from the damage eventually.
Low	If the event occurs, parts of the systems or employees receive slight damage which might lead to some costs or the reputation or the mission of the company is harmed slightly. The company should not be affected for a long time from this event.

Likelihood	
Likelihood	Description
High	Exploiting the vulnerability might lead to a huge success for the adversary, i.e. there is a lot of motivation for the threat source to exploit the vulnerability. Moreover, this vulnerability is relatively easy to exploit.
Medium	There is motivation for threat sources to exploit the vulnerability, but it is protected good enough that it is not easily exploited.
Low	Either there is only low motivation for a vulnerability to be exploited or the asset is protected very highly against the exploit of this vulnerability.

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Note that we grouped similar assets together, because some threats are applicable to multiple assets. The threats described in one section are referring to all assets mentioned in the title of the section.

2.5.1 *Evaluation of Core Server / Firewall*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	Nature: Earthquake or fire might damage physical machine	Install good fire protection system (fire extinguishers etc.)	*Low*	*High*	*Low*
2	Nature: Components might break, render it unusable	Service contract with the manufacturer, spare machines	*Low*	*Medium*	*Low*
3	Physical access to the core server/firewall by employees leading to physical damage to the systems	Limit physical acccess for non-administrative personnel	*Medium*	*Medium*	*Medium*

2.5.2 *Evaluation of Client Systems*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
4	Nature: Earthquake or fire might damage physical machine	Install good fire protection system (fire extinguishers etc.)	*Low*	*Low*	*Low*
5	Nature: Components might break, render it unusable	Service contract with the manufacturer, spare machines	*Low*	*Low*	*Low*
6	Employees: Might accidently or intentionally damage the client physically	Spare machines	*Low*	*Low*	*Low*

2.5.3 *Evaluation iMovies Intranet / ca-net / Internet Connection*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
7	Nature: Earthquake or fire might disrupt connections	Install good fire protection system (fire extinguishers etc.)	*Low*	*Medium*	*Low*
8	Employees: Might accidently damage the connections physically	Have spare machines (e.g. modems) and redundant connections, limit physical access to networking hardware	*Low*	*Medium*	*Low*
9	Directed Malware: Directed malware might disturb connections (e.g DDoS attack)	Install good and regularly updated anti-virus software on all machines in order to prevent malware from entering the system	*Low*	*Medium*	*Low*

2.5.4 *Evaluation of Core Server Software*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
10	System Administrator: Might accidently or intentionally leave vulnerability open, e.g. by misusing protection software or misconfigured server configurations	Have multiple system administrators in our team and make sure that they are competent and know everything about the system	*Medium*	*High*	*Medium*
11	Web programmer: Might accidently or intentionally leave vulnerability open, e.g by not following standard security patterns	Have code reviews from security specialists before deploying any new code	*High*	*High*	*High*
12	Competitors/Investigated Entities: Might try to harm the system intentionally (e.g by exploiting software vulnerabilities)	Install good and regularly updated protection software, make sure that the firewall has no loopholes in it and the core system is only reachable through the firewall	*Medium*	*High*	*Medium*
13	Malware: Undirected malware may reach the system and do harm to it	Install good and regularly updated antivirus software on all machines in order to prevent malware from entering the iMovies system	*Low*	*Medium*	*Low*

2.5.5 *Evaluation of Firewall Software*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
14	System Administrator: Might accidently or intentionally leave vulnerability open, by misconfiguring the firewall	Have multiple system administrators in our team and make sure that they are competent and know everything about the system	*Medium*	*High*	*Medium*
15	Competitors/Investigated Entities: Might try to gain access to firewall and open holes in it	Limit access to firewall system to SSH only	*Low*	*High*	*Low*
16	Malware: Undirected malware may reach the system and does harm to it	Install good and regularly updated antivirus software on all machines in order to prevent malware from entering the iMovies system	*Low*	*Medium*	*Low*

2.5.6 *Evaluation of Client Software*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
17	Employee: Might accidently or intentionally leave vulnerability open, e.g by misconfiguring software	Have strong protection mechanisms for all critical infrastructure, regularly train employees	*Medium*	*Medium*	*Medium*
18	Competitors/Investigated Entities: Might try to gain access to a client system (e.g by exploiting software vulnerabilities, social engineering)	Install good and regularly updated protection software, let system administrators manage software on client	*Medium*	*Medium*	*Medium*
19	Malware: Undirected malware may reach the client and does harm to it	Install good and regularly updated antivirus software on all machines in order to prevent malware from entering the iMovies system	*Low*	*Medium*	*Low*

2.5.7 *Evaluation of User Database*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
20	Employees: Might try to get the user information of another employee intentionally, e.g. because of a personal conflict	Make sure to only have trustworthy employees and try to keep them in the company as long as possible, make sure the database is secured properly	*Low*	*Low*	*Low*
21	Competitors/Investigated Entities: Might try to get the confidential data in order to damage the reputation of iMovies or delete user data in order to harm the company	Make sure the database is secured with appropriate access control mechanisms and that there is no way of inserting SQL injections	*Medium*	*Medium*	*Medium*
22	Malware: Undirected malware may reach the core system and do harm to the database	Install good and regularly updated antivirus software on all machines in order to prevent malware from entering the iMovies system	*Low*	*Medium*	*Low*

2.5.8 *Evaluation of Persons*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
23	Nature: Illness, accident or other event might prevent the employee from working at iMovies (temporarily or even permanently)	Have other employees ready to take over the job of this employee temporarily	*Low*	*Medium*	*Low*
24	Competitors/Investigated Entities: Might try to bribe employees to give them confidential data	Have all employees sign a contract to obey the policies of iMovies	*Medium*	*High*	*Medium*

2.5.9 *Evaluation of Informant Confidence*

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
25	Confidential information might be leaked leading to loss of informant confidence and reputation	Have trusted employees and ensure confidentiality when talking to them	*Medium*	*High*	*Medium*

2.5.10 Risk Acceptance

No. of threat	Proposed countermeasure including expected impact
3	The core server, router and the firewall are located in a separate lockable rack in iMovies' basement. Only authorized personnel has access to this part of the building.
10	Hire an external company to perform a penetration test to further harden the system.
11	Make sure state-of-the-art security mechanisms to prevent XSS, CSRF, SQL Injection etc. are in place, perform penetration testing (see 10)
12	see 10/11
14	Formally verify firewall configuration, let external security experts review the configuration
17	Schedule regular mandatory security seminars, raise security awareness of employees, create a likeable working environment to keep employees in the company
18	Install security updates for client software, let system administrators manage client software
21	see 10/11
24	create a likeable working environment to keep employees loyal, encourage employee to speak up about internal issues
25	For this threat, we need to make sure that the certificates issued by the CA are really trustworthy. This therefore concerns the security of the whole CA system, therefore all countermeasures from the software threats can be applied here too (regular updates, state-of-the-art security mechanisms, penetration test, formal verification, trained employees and system administrators).