Review

Marc Gähwiler Leonhard Helminger Fabian Zeindler

12.12.13

Contents

Chapter 1

Review of the External System

1.1 Background

Developers of the external system: *Thomas Knell, Danny Schweizer, Samuel Hitz*

Date of the review: 01.12.2013

1.2 Completeness in Terms of Functionality

In this section we review the system according to the requirements given in the assignment. We compare each of the requirements stated with the report of group 3 and their implementation.

1.2.1 Functional requirements

Certificate issuing process

- Use of legacy database, verifying authorized certificate request on basis of this database ✓
- Login with user ID and password ✓
- Display user info from database ✓
- A logged in user can alter his user information ✓
- Issuing certificate on basis of data in database ✓
- Download cerated certificate in PKCS#12 format ✓

Certificate revocation process

- Authentication via user certificate or user ID/password ✓
- Certificate gets revoked ✓
- CRL published ✓

Administrator interface

- Authentication with certificate ✓
- Displays # of issued certificates, # of revoked certificates and current serial number ✓

Key backup

All certificates and corresponding private keys are stored in an archive ✓

System administration and maintenance

- Secure interfaces for remote access ✓
- Automated backup for logging and configuration information ×
  - Only events of the core server are logged
  - Only logs and configurations of the core server are backed up
  - Backup location is on the same host as the original data

Components to be provided

- Web server: user interfaces, certificate requests, certificate delivery etc. ✓
- Core CA: management of user certificates, CA configuration, CA certificates & keys, functionality to issue new certificates, etc. ✓
- MySQL database: legacy database according to provided schema ✓
- Client: Sample client that allows to test the CA's functionality ✓

1.2.2 Security requirements

- Access control on data (configs, keys, etc.) ✓
- Secrecy and integrity of keys in the key backup ×
  - Keys are not encrypted
  - No integrity checks
  - Backup location is on the same host
- Secrecy and integrity with respect to user data ✓
- Access control on all component IT systems ✓

1.3 Architecture and Security Concepts

1.3.1 General system architecture

The system is implemented with a security in depth approach when checking the source and destination of communication on two separate machines to ensure only valid traffic. However we consider the placement of the core functionality, the CA, on the same machine as the web server as not optimal. The web server is publicly accessible and should therefore be separated from the core server and the database with the user information. Another point that we consider problematic when combining all functionality on one server is the backup. Backing up data on the same server is not really a backup.

1.3.2 Risk analysis and security measures

Definition of impact an likelihood

We cannot find fault with the definition if Impact. It is loosely based on the NIST definition but with an emphasis on the reputation of the company which seems to be particularly important when doing investigative journalism.

The definition of likelihood however in our opinion lacks one important ability of the thread source, the capability of the attacker. In the definition of high likelihood it says the motivation of the thread source to exploit the vulnerability is high and/or the vulnerability is easy to exploit. We think it is important to also empathize the possibility that the capability of the thread source to exploit the vulnerability is especially high in this particular case. E.g. including the possibility that the vulnerability is hard to exploit but the thread source is not only extremely motivated but also extremely capable.
The same is true for the definition of medium and low likelihood were the possibility that the thread source is not that capable or completely lacks the knowledge/capability to exploit the vulnerability should be included.

The definition of risk follows the general notion and seems appropriate with regard to the definition of impact and likelihood.

Stakeholders, assets and threat sources

The important stakeholders are listed but we think one could include the investigated party since it is also mentioned as potentially malicious third party in the description of other stakeholders.

All important physical assets were considerate. However, the client machines have two states associated, normal operating mode or defective which ignores the state were a machine could be functioning but be compromised. All other physical assets do not have states associated with them.

Logical assets describe the software running on the physical assets. Here also, no states were associated with the assets and the iptables on the core server were not mentioned. Regarding logical assets we miss the information assets which are not specified. The user database is listed which could be understood as the user data asset but other assets like certificates or private keys are not specified although they are integer parts of the CA system.

The listing of thread sources is complete for the context of the iMovies CA system. However it would have been nice to state why other thread sources were not considerate.

Risks and countermeasures

In the listing of risks, only risks that where not threated with countermeasures during the implementation and risks to physical assets are listed which we consider wrong, as the risk analysis should state all risks and describe the proposed as well as the implemented countermeasures. Risks to information assets like private keys, communication or certificates are missing since they are not listed as assets or because apparently the authors did not include any threats to the assets that they think they dealt with during the implementation.

The evaluation of risks to the physical assets seems to be complete. For the rest, several things came up that we consider problematic. Three times the use of anti virus software is mentioned, but in the implementation we could not find any (document and vms). Also many of the proposed countermeasures are formulated very generic. The use of g̈ood softwareẅas suggested 7 times without specifying what good software is. Furthermore for example in risk number 17, the proposed countermeasure is having strong protection mechanisms for all critical infrastructure, where the means of strong protection and a more detailed description of critical infrastructure can nowhere be found. Risk number 21 where the countermeasure is to make sure the database is secured with appropriate access control mechanisms is another example.

The same is true for the proposed countermeasures in the risk acceptance section where state-of-the-art security measures are proposed. Other countermeasures as for example suggesting external

security audits or mandatory security seminars seem to be valid countermeasures. Overall, the expected impact is not described for any of the listed threats.

1.4 Implementation

In this section we will list the countermeasures who's implementations differ from the description in the documentation. Additionally we cater to implementations we encountered that we consider security risks or bugs. At the end we summarize some of our testing of the system that proved to be not successful in terms of breaking the system or finding vulnerabilities.

- In the system the possibility to change user information is implemented as vaguely described in the project assignment. We consider the fact, that a user can change all its information without audit a security risk. The user could change his information completely and thus impersonate another user. It is the responsibility of a CA to ensure the validity of the user information. Also should old certificates of a user automatically get revoked when the information on the corresponding user changes.
- In the documentation it is stated, that for a change of the user name the user password is needed. There is a password field, but the input to this field is not verified.
- When describing system administration and maintenance the documentation states that Apache access and error logs are daily backed up using logrotate. Logrotate does not back up data, it just rotates the logs (but does not move them to another location). According to the configuration logs are rotated every week and stored for a year. The same is true for MySQL logs which are rotated daily and stored for a week.
- Backups in general are done with a daily cron job. Configurations are taken from /etc/ and backed up to /home/sysadmin/backup on the same server. Logs and data are not backed up.
- As specified in the documentation under system administration the backup is done with a daily cron job. The cron job invokes rsync which copies configurations (but no logging like stated in the documentation). This copy procedure overwrites old backup files which is usually not desired.
- In addition to the above, no configuration or logging data from the firewall is backed up, only data from the core server.
- The documentation also lists public key authorization for ssh as a security measurement against unauthorized access, but there are no known keys or public key functionality in place. However sshd is configured to accept public key authentication, but it also allows remote access for root which we consider unnecessary.
- Key backup as described in the documentation is not a real backup as described earlier in this section. In addition the keys are protected solely via linux access control but not encrypted or protected by other means.
- In addition to that the certificates and corresponding private keys (.crt, .crs, .p12) are stored in /tmp/ during creation and not deleted afterwards.
- When trying to get information about the system, we could obtain the version of SSH, the operating system, via index.php detailed information about the used PHP, the version of the Apache webserver, etc.

The system seems to be protected adequately against SQL injection attacks. XSS is possible to some extent and discussed further in the Backdoors section. Nmap reviled the ports 433, 4433 and 22 to be open on both the firewall and the server as described in the documentation. In

addition port 1234 seems to be open on the firewall from within the server network to the outside (more details in the Backdoors section). As described above, we managed to obtain the kind and version of operating systems, weblanguage, webserver, ssh etc. with tools like nmap or OpenVAS. But OpenVAS as well as Metasploit did not find any other exploitable vulnerabilities.

When reviewing the system in detail by looking at the servers and software written, we found several potential security risks as described in the list above.

1.5 Backdoors

WRITE HERE ABOUT: Describe all backdoors found on the system. It may be that you also find unintended backdoors, which cannot be distinguished from intentionally added backdoors.

php selber compiled
/ext/standart/exec.c
/usr/bin/rshell
www/user/batman.jpg
www/user/protectedimage.php
open port 1234 on firewall from inside out
XSS/CSRF in general

1.6 Comparison

Comparing the both systems, the first thing that we noticed was the lack of separation in the reviewed system. They also have a designated firewall which filters traffic but they have combined all functionality (webserver, CA core and even backup) on one single server where our system has four different zones, the internet, the network where employees hate their workstations, the DMZ which hosts the webserver and is the only machine accessible from outside by non administrators, as well as the intranet which hosts the CA functionality on one server an the backup and key archive on another server. The access control to all those networks is handled by the firewall.

For remote access our system provides we use VPN where the reviewed systems just forwards the SSH ports which both seems to work.

Another major difference is the handling of user data change. Where in the reviewed system users can change data as they like and thus potentially impersonate other people, our system implements a review of user data changes other than the password to ensure the authenticity of a certificate.

WRITE SOMETHING ABOUT THAT: Are there any remarkable highlights in your system or the external system?