System Description and Risk Analysis

Cyrill Krhenbhl Silvan Egli Lukas Bischofberger

Contents

1 System Characterization

1.1 System Architecture

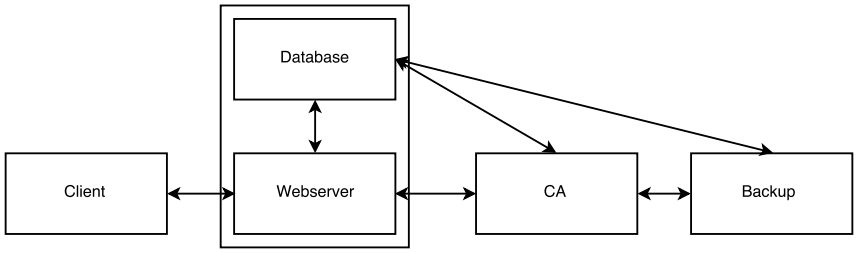

Figure 1: System overview

1.2 Components

client: angular application webserver&db server: django on top of nginx, communicating with a mysql database on the same server ca server: core ca, handles all openssl commands and stores certificates and keys backup server: backup of certificates, keys and the mysql database

1.3 Information Flows

- client authentication: client sends username/pw or certificate to webserver. webserver checks username and password in the db. the certificate is checked by nginx (valid, revoked?). django then responds with a token

- client certificate creation: client sends certificate name to webserver. webserver checks if name is present already, otherwise requests cert from ca server (based on info from database). the ca server creates certificate and key and stores them safely. returns locations of these assets. webserver inserts the certificate information into the database and offer the user to download the assets.

- certificate revocation: client sends revocation request to webserver. webserver asks ca server to revoke the certificate. ca server responds with updated certificate list.

2 Risk Analysis and Security Measures

2.1 Assets

- certificates - user data - webserver/dbserver - ca server - backup server - availability of service

2.2 Threat Sources

threats ——

- key leakage - user data leakage - compromise of webserver, ca server. backup server - unavailability - misbehaviour of trusted entities - sysadmin access to system

vulnerabilites ————-

- misconfiguration of used software - bad passwords - badly implemented software (eg. access control) - zero days in used software - lack of security awareness of employees - sys admin access privileges