Security Certificates

an overview

Xavier Belanger
January 24, 2015

You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
- **No additional restrictions** — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

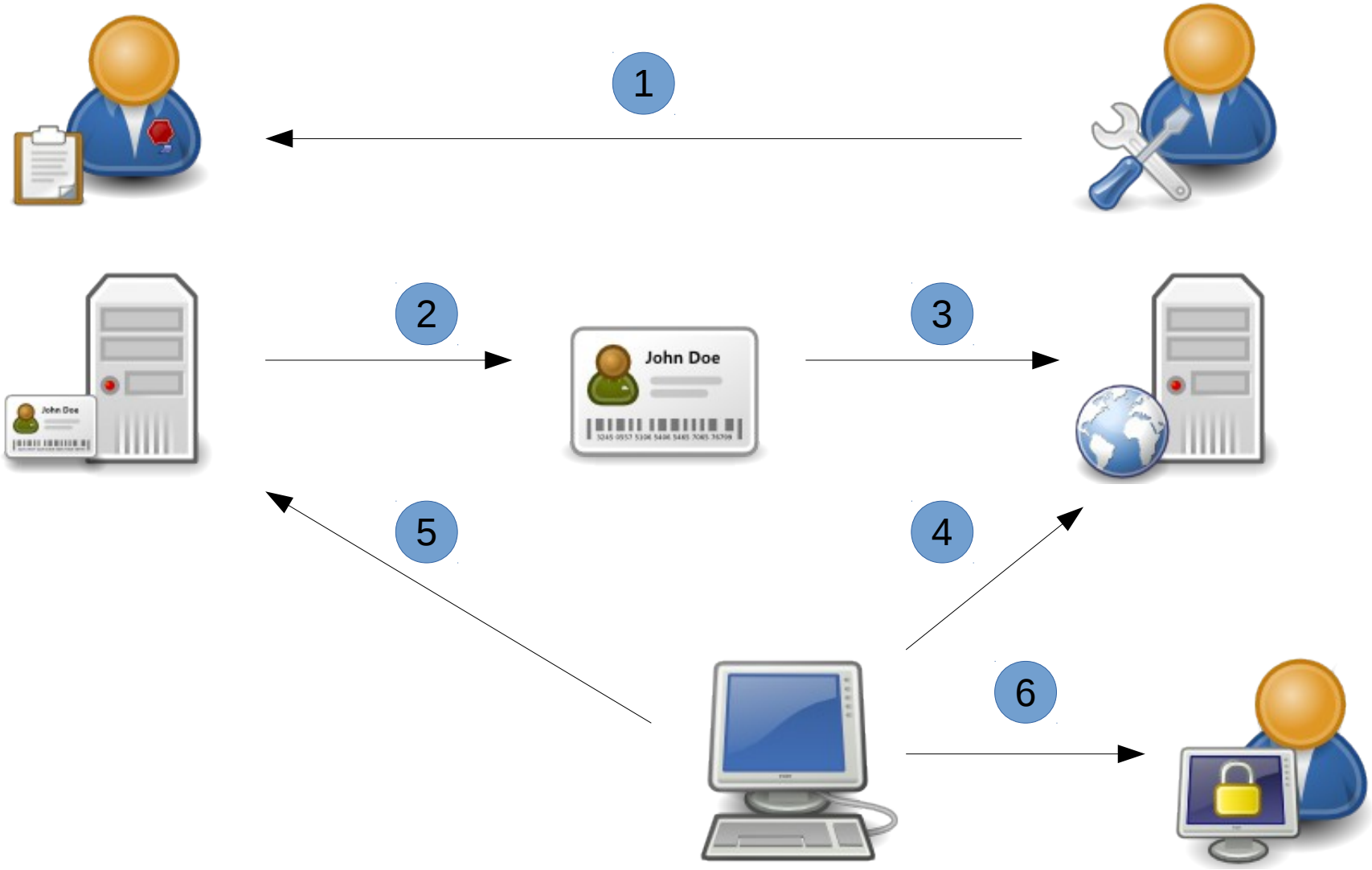
What is a certificate?

- It came from the X500 norm, created for electronic directory services, to list and describe an entity.
- Out of the X500 norm, X509 is the one about authentication.
- Think about a certificate like an ID card: it can be used by anyone to identify a server or a service as an element from an organization.

What is a security certificate?

- Human beings may be able to check a certificate, but computers need something different, that can be proven (in a logical, mathematical way).
- A couple of cryptographic keys (one private, one public) are attached to a certificate and linked to a root certificate managed by the organization.
- From the root certificate you can check the validity of a security certificate:
  it is a chain of trust.

Chain of Trust



What is the goal of a security certificate?

- It is a way to authenticate the server or service that you are using.
- It is also used to encrypt all your communications with the server.
  No one else is able to pry on what you are doing.
- This is used for more and more online services, the most visible piece are secure websites (using HTTPS) but it is also used by mail servers, chat/video-conferencing, ...

What does it looks like?

- A security certificate can be stored or displayed in many forms (depending how it is used), it is a collection of “field = value” couples.

  Name = “Server”
  Address = 192.168.1.1
  Signature = “FB56FAE570C1A”

- When accessing a secure website, your web browser is able to display all the information in a “friendly” manner.

Vocabulary

- **SSL**: Secure Sockets Layer (a socket is communication point between two computers). This is an old protocol, with three different versions. Version 1 and 2 are weak, obsolete and insecure. Version 3 is not really better but still in use.
- **TLS**: Transport Layer Security. This has been built on the top of SSL; three versions are in use.

How to get a security certificate?

- An organization can create his own root certificate and issue security certificates as needed. Problem: all the clients need to know about that root certificate and to trust it.
- The common solution is to rely on a third party, a certificate authority, who can generate everything and who is trusted by default by the clients.

What are the issues?

- You need to trust the certificate authorities. And there is a lot of them around; some are reliables, some I’m not sure and some others, well...
- All the cryptographic parts (cyphers, keys) need to use up-to-date techniques.

What can we do?

- Check security certificates, at least for important websites and services.
- Ask the service provider to improve the security when needed.

Resources

- **Information Security - Before, During and After Public-Key Cryptography with Whitefield Diffie**
  https://www.youtube.com/watch?v=1BJuuUxCaaY&html5=true
- **Qualys SSL Labs - SSL Server Test**
  https://www.ssllabs.com/ssltest/index.html
- **Bulletproof SSL and TLS - Ivan Ristic**
  https://www.feistyduck.com/books/bulletproof-ssl-and-tls/
- https://calomel.org/
- https://www.madboa.com/

Resources

- Extensions for Mozilla Firefox:
  - **Calomel SSL Validation**
  - **Certificate Patrol**
- https://addons.mozilla.org/

- This presentation has been created with LibreOffice 4.3.5.
- Fonts:
  - *Source Sans Pro Semibold* for the titles
  - *DejaVu Sans* for the text
- Icons from the *Open Security Architecture Icon Library*:

  http://www.opensecurityarchitecture.org/cms/library/icon-library