Certificates - Continued

Review

- What is the DN property on a certificate?
- How is this different from a CN?
- What is a certificate authority?
- Why have a public key in a certificate?
- What would happen if we visit a site and the certificate expired?
- What is X.509?
- What is "Let's Encrypt"?https://it.slashdot.org/story/24/09/11/1749259/security-researcher-exposes-critical-whois-vulnerability?utm_source=rss1.0mainlinkanon&utm_medium=feed

Certificate Authorities - Key Terms

- Certificate Authority (CA)
  - Signs certificates
  - Needs to be trusted by operating system in order to trust certificates they sign
- Root CA
  - Self-signed, installed in Operating System
- Intermediate CA
  - Signed by Root CA
  - Used to issue certificates
- Much easier to replace an intermediate CA instead of a Root CA

Exercise

- Who issued the root CA for eff.org?
  - How long is the root CA valid for?
- What about the intermediate CA?
  - Who issued it?
  - How long is it valid for?
- What about the actual certificate?
  - How long is it valid for?

Certificate Revocation

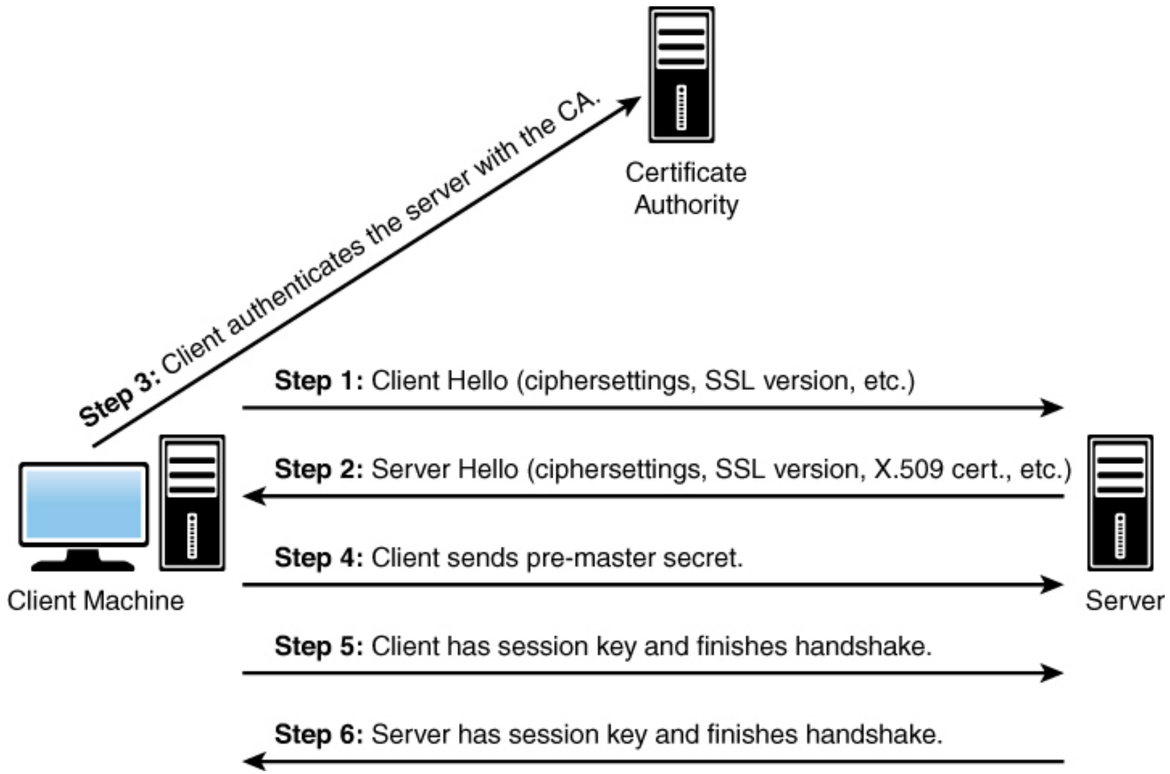
- If a private key is compromised or some other vulnerability is discovered, a certificate may be revoked
- There are two main mechanisms to do this:
  - CRL - Certificate Revocation List
    - Managed by CA, these are pulled to determine if a certificate is not valid (they can be pushed as well)
  - OCSP - Online Certificate Status Checking Protocol
    - Real time check if a certificate is valid

SSL / TLS

- Using certificates, provides a protocol to establish a secure connection to maintain confidentiality
  - Certificates do not do this automatically, they are part of this
- History
  - SSL 1 - Never released
  - SSL 2 - 1995
  - SSL 3 - 1996
  - TLS 1.0 - 1999
  - TLS 1.1 - 2006
  - TLS 1.2 - 2009
  - TLS 1.3 - 2018
  - https://www.rfc-editor.org/rfc/rfc8446

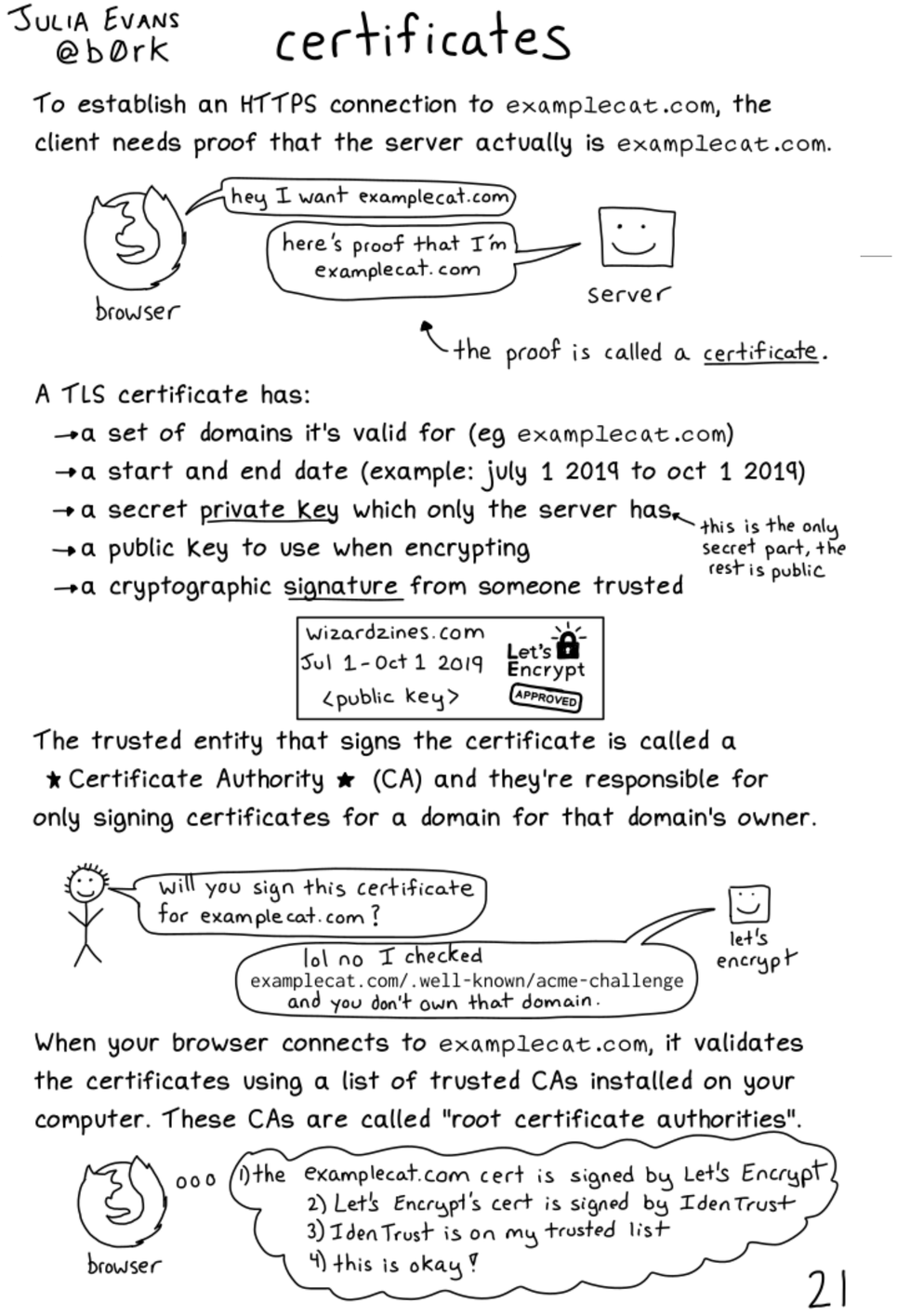
SSL / TLS - Protocol

- Client and server negotiate ciphers (e.g. aes-256) as well as hash functions (e.g.
- Public and Private Key (asymmetric) used to exchange symmetric key
  - Symmetric is faster, but we don't have a shared key yet
- CA key is used to verify the signature on the certificate
- Pre-master key is used to create a session key (AES)



Julia Evans

- Creates insightful comics to help understand CS concepts
- Follow her on Mastodon:
  - @b0rk@jvns.ca
- She has a re-runs bot as well that publishes comics:
  - @b0rk_reruns@jvns.ca



Pretty Good Privacy (PGP)

- Created by Phil Zimmerman
- Used to encrypt email and messages
- It is old, but it is known to be very secure
- You have to know who is sending
- Combines symmetric and asymmetric encryption
  - Use the public key of a person you want to send an email to encrypt a session key (symmetric key) and the message
- Why not just use asymmetric encryption?
  - It is slow, so by sending the symmetric key, the receiving party can quickly decrypt the message
- Certificates are not issued by a CA, no way to have third party verification
- You as a person communicating with someone using PGP must have a way to verify the certificate
  - Some services, like Proton Mail, can do this for you
  - More info here: https://proton.me/blog/what-is-pgp-encryption

Quiz

- Passcode is "salt"
- 5 Minutes

Assignment

- Password Manager