Mutually Endorsing CA Infrastructure

- Don't treat Symptoms: Improve the PKI System
- Combine PKI with Web-Of-Trust / Notary ideas
- Each CA should run a dynamic Vouching Service
- Vouching for network visibility of:
    - DNS information: Hostname <=> IP
    - Certificate in use: IP/Port <=> Certificate
    - Current Revocation information (OCSP)
- Vouching Service combines network information, current timestamp and adds a digital signature

Vouching architecture

- Twice a day, each server requests a current voucher from each CA and will use it for the next 24 hours
- Client picks two acceptable candidate Vouching Authorities (either by random or based on region)
- Clients request vouchers from servers as part of the SSL/TLS protocol handshake
- Server certificate and voucher: From different CAs
- Clients verify voucher signature and freshness
- Clients compare own network view with voucher information

Benefits related to Hacking

- Hacking a single CA will no longer be sufficient
- Hacking two CAs give you success only in a small number of connections, everyone else will be alarmed, allowing quick detection of compromises
- Ability to globally revoke trust from CAs within one day: Inform the Vouching Authorities about the compromise, and they will stop issuing vouchers for related certificates. As soon as clients can no longer obtain vouchers, they will stop trusting the servers that use compromised certificates.

Additional Benefits / Properties

- Clients could anonymously submit statistics about certificate mismatches
- Information about mismatches could be centrally evaluated to learn about regional attacks
- Reduced uptime requirements of OCSP servers (outages of a couple of hours are acceptable)
- Limited performance requirements for Vouching Servers, because only servers connect to them
- As with OCSP stapling: no OCSP privacy issue; works at captive portals / hotspots prior to login

Additional Idea: Automatic Failover

- Introduce optional redundancy into SSL/TLS
- Instead of always using a single server certificate, enhance the SSL/TLS protocol to allow a list of two alternative server certificates
- Servers could be configured to use two certificates from two different CAs (same keypair for both?)
- If a root CA gets revoked because of a compromise, and clients fail to validate a server's certificate (e.g. no valid voucher), clients can fall back to use the alternative certificate

Mutually Endorsing CA Infrastructure

kuix.de/mecai

Kai Engert

Red Hat employee
Mozilla contributor