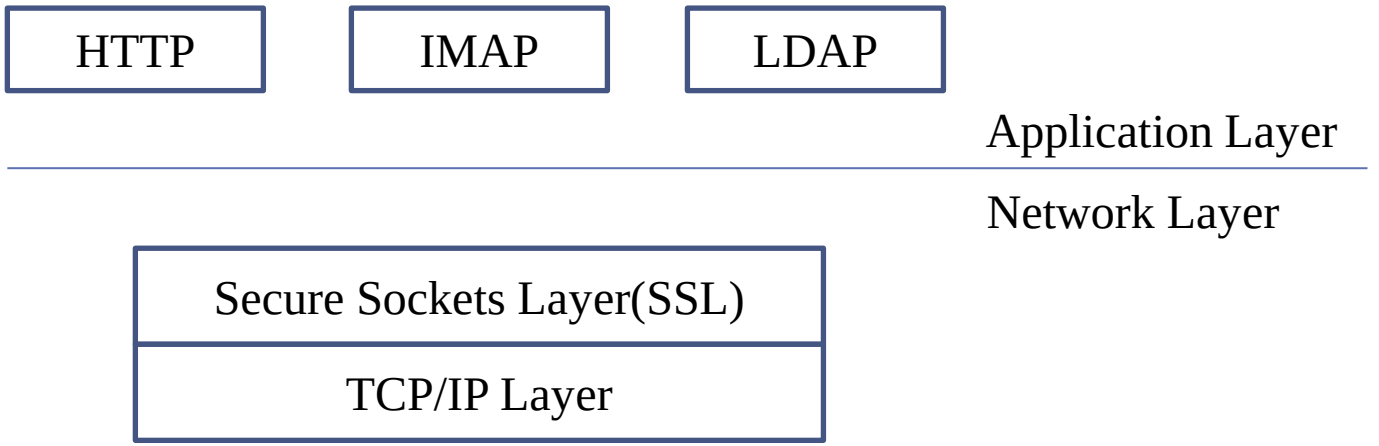
SSL, PKI and Secure Communication

Aditya Marella

20th March, 2014

Secure Sockets Layer (SSL)

- Developed by Netscape
- Sits on top of TCP and below application level protocols



What are the typical use-cases of SSL?

- HTTPS
  - Secure web communication
  - Enhances privacy by allowing encrypted data transfer
- Application (binary) Signing
- Email Certificates
- VPN

What does SSL offer?

- **Confidentiality**: encrypts data in transit
- **Integrity**: uses message authentication codes to detect tampering
- **Authentication**: public key cryptography to authenticate peers (X.509 certificates)

All of these are dependent on the trust model (PKI)

Problems

Problems observed with SSL

- Many SSL related issues are actually software bugs
  - Implementation flaws (Remote timing attacks, PRNG Seeding)
  - Oracle Attacks (reverse engineering or predicting victim's protocol implementation)
  - Protocol Level Attack (ciphersuite downgrade attack, version downgrade attack, renegotiation attack)
  - Weak Crypto Primitives
    - Weak encryption (40, 56, 64 bit encryptions subject to brute force attack)
    - Weak Hash Functions (MD5)

Jeremy Clark and Paul C. van Oorschot. SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, 2013. (S&P '13 / Oakland '13)

SSL Trust Model or What is PKI?

The Trust Model

- Root Certificate Authorities (CAs) **rule**
- CAs **sell** certificates to entrust companies and users
- CAs **delegate trust** to other CAs for a price (creating a "chain of trust")
- There is **validation process** when they sell you a certificate

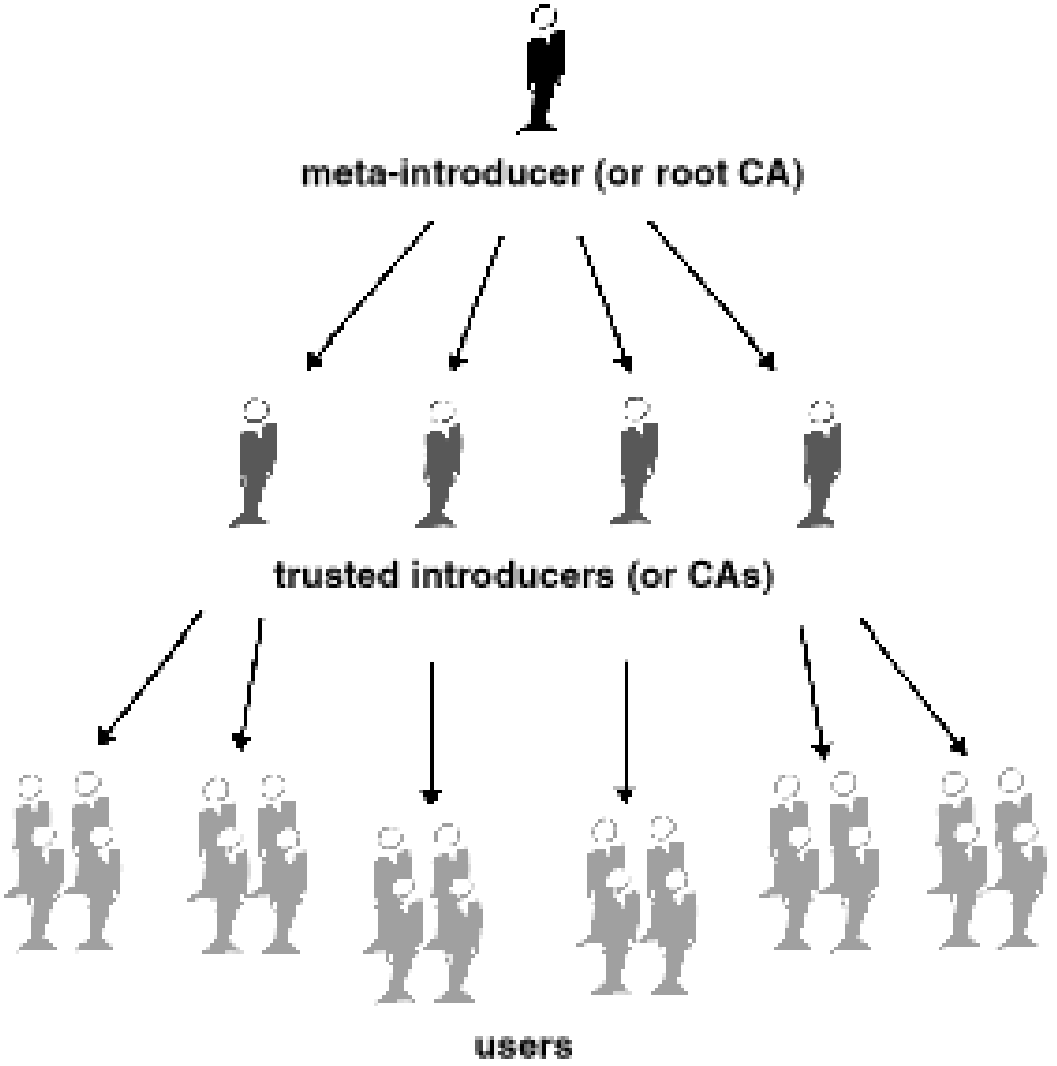
End user certificate validation

- **Server:** this is my certificate, this is the chain of trust leading upto the root CA
- **Client**: let's see if any of these certificates have been revoked/expired..

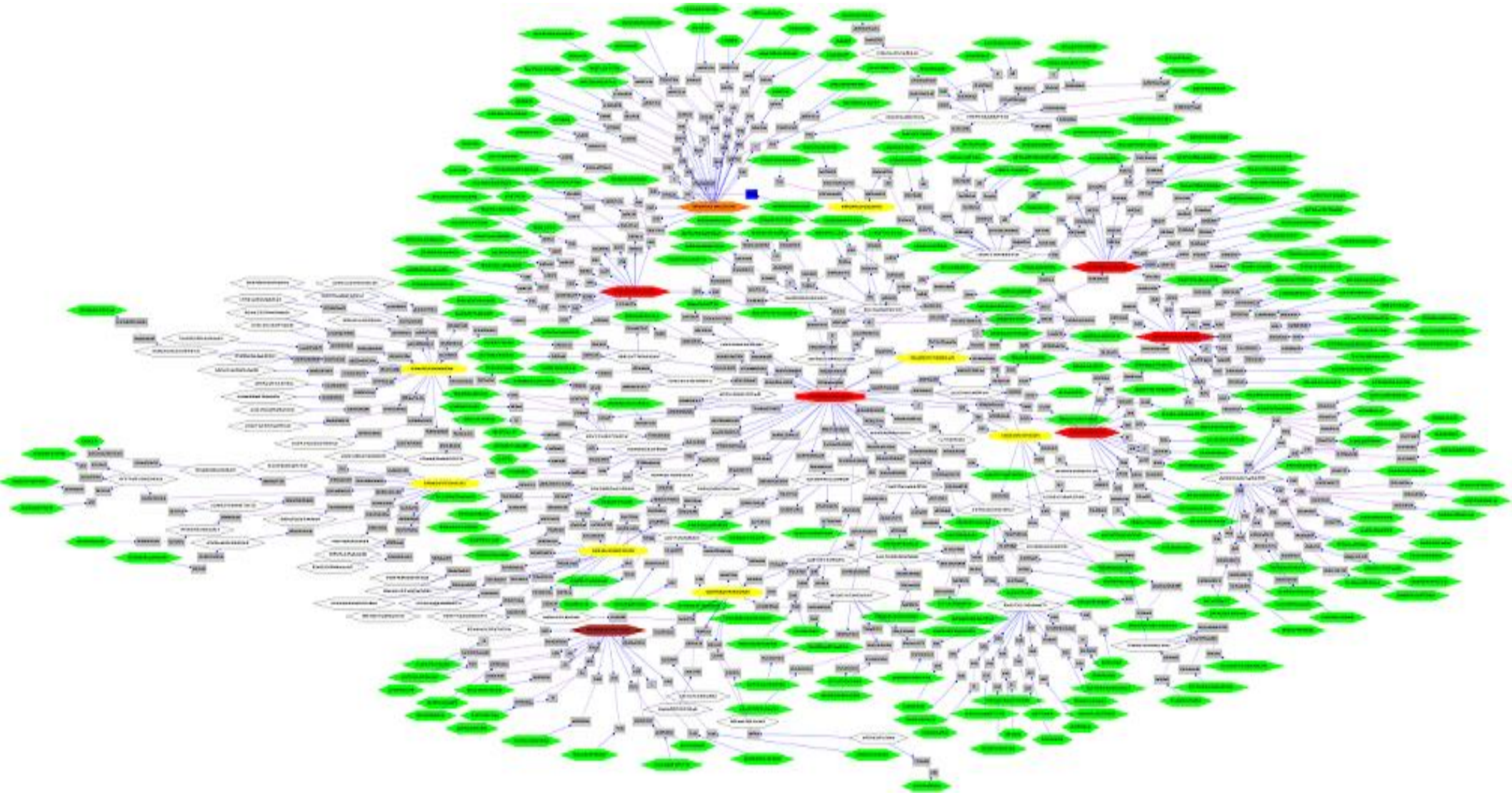
If all the certificates in the chain are valid and linked to a trusted CA (Accepted)

Revoked/expired certificates or certificate doesn't match host or don't trust the CA (Rejected)

Chain of trust (in principle)



Chain of trust (in practice)



Trust Model Issues

- **Single point(s) of failure** (Root Certificate Authority)
  - CAs themselves get hacked (**Diginotar)**
  - CAs could be malicious (**cannot be trusted**)
  - CAs could have malicious employees (**Insider threats**)
- **Not Agile**
  - CA hacks are very hard to recover from
- **Profit driven** model
  - Entity with more money/influence gets to choose what can be trusted (big companies, governments)

Trust Model Issues

- **Compelled certificate creation attack** (Soghoian et al)
  - Govt. agencies force CAs to issue false certificates
  - Intelligence agencies use these certificates to spy secure web communication

Christopher Soghoian and Sid Stamm. Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. In *Proceedings of the 15th international conference on Financial Cryptography and Data Security* (FC '11)

The Trust Model

Now what?

Solution: Certificate Transparency (from Google)

- **Log servers** hold append only logs of all issued certificates (as Merkle Trees)
  - CA sends its cert to a log server and gets timestamp as response
- **Monitor servers** check log servers periodically and flags unauthorized certificates
- **Auditors** (browsers) check any cert and timestamp they receive appears in the log

Solution: Public key pinning

- **Extending HTTP** to allow websites to instruct browsers to **remember**("pin") the hosts public keys for a given period of time
- During this time, browsers will require hosts to present a certificate chain including at least one public key that matches one of the pinned ones

IETF Proceedings 88(http://www.ietf.org/proceedings/88/slides/slides-88-wpkops-0.pdf)

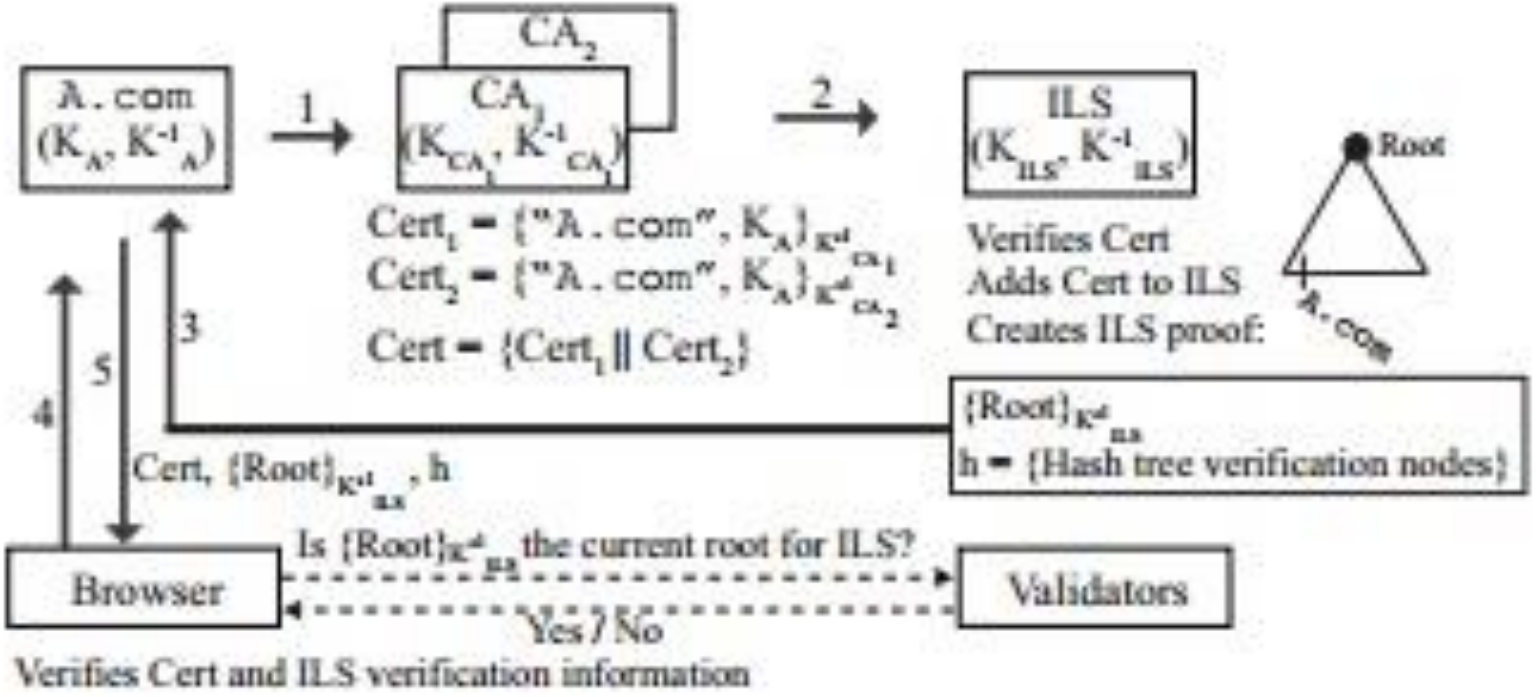
Solution: Convergence

- Several ***notaries*** can vouch for a single site
- If the notaries disagree, user can go for ***Majority vote*** or they can also be content with single notary
- Voting method can be controlled using a setting in the browser plugin
- No single point of failure

BlackHat USA 2011: SSL And The Future Of Authenticity
http://www.youtube.com/watch?v=Z7Wl2FW2TcA

Solution: Accountable Key Infrastructure

- Reduces the amount of trust placed in one CA



Solution: HTTP Strict Transport Security (HSTS)

- Allowing websites to say that they are only contactable using HTTPS
- HTTP response header contains sites security policy
- Browser remember policy and strictly enforces it
- This stops users “clicking through” security warnings of web sites that the browser does not trust

IETF Proceedings 88(http://www.ietf.org/proceedings/88/slides/slides-88-wpkops-0.pdf)

Extending SSL in Appified World

- Transparent development of SSL in the applications
- Central deployment of SSL validation strategies and infrastructures (Certificate Transparency, Convergence, AKI) instead of each application developer separately implementing it

Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Matthew Smith. Rethinking SSL Development in an Appified World. In*Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, 2013. (CCS '13)

"Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography"

— Roger Needham and Butler Lampson

taken from Ross Anderson. Chapter 21: Network Attack and Defense In *Security Engineering* (Second Edition). Wiley, 2008