Certificate Transparency with Privacy

Saba Eskandarian, Eran Messeri, Joe Bonneau, Dan Boneh
Stanford, Google, NYU, Stanford
Certificate Authorities

Certificate

Public Key

Certificate

CA
An update on attempted man-in-the-middle attacks
August 29, 2011

FINAL REPORT ON DIGINOTAR HACK SHOWS TOTAL COMPROMISE OF CA SERVERS
apo-CA-lypse

An update on attempted man-in-the-middle attacks
August 29, 2011

FINAL REPORT ON DIGINOTAR HACK SHOWS TOTAL COMPROMISE OF CA SERVERS

Distrusting WoSign and StartCom Certificates
October 31, 2016
Certificate Transparency (CT)

**Idea**: public, verifiable log of all certificates
Certificate Transparency (CT)

**Idea:** public, verifiable log of all certificates
Certificate Transparency (CT)

**Idea:** public, verifiable log of all certificates
Certificate Transparency (CT)

**Idea**: public, verifiable log of all certificates
Certificate Transparency (CT)

Idea: public, verifiable log of all certificates
Certificate Transparency (CT)

**Idea:** public, verifiable log of all certificates

CT logging required by chrome for all sites starting April 2018!
Transparency and Privacy?
Our Contributions

- Redaction of private subdomains
- Privacy-preserving proof of misbehavior
Redaction: keeping secrets on a public log

Problem: secret.facebook.com is publicly visible on the log!
Redaction: keeping secrets on a public log

Request Certificate
secret.facebook.com

Precertificate
Redacted.facebook.com

Certificate, SCT
Redacted.facebook.com

Certificate, SCT
secret.facebook.com

Log

Problem: secret.facebook.com is publicly visible on the log!
Subdomain Redaction via Commitments

Request Certificate

secret.facebook.com
secret.facebook.com

CA

Log
Subdomain Redaction via Commitments

Request Certificate

secret.facebook.com
secret.facebook.com

CA

Precertificate

secret.facebook.com

Log

...
Subdomain Redaction via Commitments

Request Certificate

secret.facebook.com

secret.facebook.com

Pre-certificate

secret.facebook.com

SCT

secret.facebook.com

CA

Log

...
Subdomain Redaction via Commitments

- Request Certificate
  - secret.facebook.com
  - secret.facebook.com

- Precertificate
  - secret.facebook.com

- Certificate
  - secret.facebook.com

- SCT
  - secret.facebook.com
  - SCT Opening:

- Log
  - ...
Subdomain Redaction via Commitments

Page Request: secret.facebook.com
Subdomain Redaction via Commitments

Page Request: secret.facebook.com

Certificate

secret.facebook.com

SCT: secret.facebook.com

SCT Opening: 🔐
Subdomain Redaction via Commitments

Page Request: secret.facebook.com

Certificate
secret.facebook.com

SCT: secret.facebook.com
SCT Opening:

Verify( , secret, )
Security

Why can’t a malicious site or CA reuse an existing redacted SCT?

   Binding property of commitment

How can a monitor still check the log?

   Knowledge of number of entries per domain owner reveals extra certificates
Privacy-Compromising Proof of Exclusion

Log

1  2  3  4  5  6  7  8  9  10

Excluded
SCT

secret.facebook.com
Privacy-Compromising Proof of Exclusion

Log
1  2  3  4  5  6  7  8  9  10

Excluded SCT
secret.facebook.com
Our Privacy-Preserving Approach

- Auditor proves to vendor that an SCT is missing from log
- Auditor does not reveal domain name, vendor only learns that log is misbehaving
Our Privacy-Preserving Approach

- Auditor proves to vendor that an SCT is missing from log
- Auditor does not reveal domain name, vendor only learns that log is misbehaving

Then:

- Vendor can investigate log
- Vendor can **blindly** revoke missing certificate (by pushing a revocation value to all browsers)
Our Privacy-Preserving Approach

- Auditor proves to vendor that an SCT is missing from log
- Auditor does not reveal domain name, vendor only learns that log is misbehaving

Then:

- Vendor can investigate log
- Vendor can **blindly** revoke missing certificate (by pushing a revocation value to all browsers)

Main tool: zero knowledge
Our Privacy-Preserving Approach

- Auditor proves to vendor that an SCT is missing from log
- Auditor does not reveal domain name, vendor only learns that log is misbehaving

Then:

- Vendor can investigate log
- Vendor can **blindly** revoke missing certificate (by pushing a revocation value to all browsers)

Main tool: zero knowledge

Assumption: timestamps in order
## Performance Numbers

**Online Costs**
- Proof Size: 333 kB
- Time to generate: 5.0 seconds
- Time to verify: 2.3 seconds

**Offline Costs (storage)**
- Growth of log entry: 480 bytes
- Growth of SCT: 160 bytes
- Revocation notice size: 32 bytes
Summary

- CT is an exciting new feature of our web infrastructure
- Transparency raises new privacy concerns
- Work on privacy-preserving solutions to two issues:
  - Compatibility between CT and need for private domain names
  - Reporting CT log misbehavior without revealing private information