Certificate Transparency with Privacy

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

Public Key
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
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
Outline

● Certificate Transparency
● Redaction of private subdomains
● Privacy-preserving proof of misbehavior
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 October 2017!
Transparency and Privacy?
Outline

- Certificate Transparency
- 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

Problem: secret.facebook.com is publicly visible on the log!
Tools: Commitments

Usage:

c ← Commit(m, r)

Verify(c, m, r)

Security Properties:

**Hiding**: given commitment \(\text{Commit}(m, r)\), can’t find \(m\)

**Binding**: given commitment \(\text{Commit}(m, r)\), can’t decommit to \(m' \neq m\)
Tools: Commitments

Usage:

\[
c \leftarrow \text{Commit}(m, r)
\]
\[
\text{Verify}(c, m, r)
\]

Security Properties:

**Hiding**: given commitment Commit(m, r), can’t find m

**Binding**: given commitment Commit(m, r), can’t decommit to m' \(\neq m\)
Tools: Commitments

Usage:

\[ c \leftarrow \text{Commit}(m, r) \]

\[ \text{Verify}(c, m, r) \]

Security Properties:

**Hiding**: given commitment \( \text{Commit}(m, r) \), can’t find \( m \)

**Binding**: given commitment \( \text{Commit}(m, r) \), can’t decommit to \( m' \neq m \)
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

Precertificate
secret.facebook.com

SCT
secret.facebook.com

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:

CA

Log
...

.facebook.com
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

How can a monitor still check the log?

Knowledge of number of entries per domain owner reveals extra certificates

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

Binding property of commitment
Outline

- Certificate Transparency
- Redaction of private subdomains
- Privacy-preserving proof of misbehavior
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
Goals

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

- 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)
Goals

- 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)

Assumption: timestamps in order
What Does Auditor Prove?

Log

1 2 3 4 5 6 7 8 9 10

Excluded
SCT
What Does Auditor Prove?

Assumption: timestamps in order
What Does Auditor Prove?

Assumption: timestamps in order
What Does Auditor Prove?

Log

1  t=4
2  t=18
3  t=21
4  t=27
5  t=30
6  t=38
7  t=41
8  t=42
9  t=50
10 t=59

3  t=21
4  t=27

3  t=21
4  t=27
5  t=30
6  t=38
7  t=41
8  t=42
9  t=50
10 t=59
What Does Auditor Prove?

Log

1 t=4  2 t=18  3 t=21  4 t=27  5 t=30  6 t=38  7 t=41  8 t=42  9 t=50  10 t=59

What about privacy?!
Tools: Additively Homomorphic Commitments
Tools: Additively Homomorphic Commitments

\[ \text{val}_1 + \text{val}_2 \]
Tools: Additively Homomorphic Commitments
Tools: Zero-Knowledge Proofs
Tools: Zero-Knowledge Proofs
Tools: Zero-Knowledge Proofs

\[ 0 < A < 5 \]
Tools: Zero-Knowledge Proofs

0 < A < 5

A = B
Tools: Zero-Knowledge Proofs

\[ 0 < A < 5 \]
Tools: Zero-Knowledge Proofs

$0 < A < 5$

$A = B$
Proof of Exclusion

What about privacy?!

Log

1  t=4
2  t=18
3  t=21
4  t=27
5  t=30
6  t=38
7  t=41
8  t=42
9  t=50
10 t=59
Proof of Exclusion

Log:
1 t=4
2 t=18
3 t=21
4 t=27
5 t=30
6 t=38
7 t=41
8 t=42
9 t=50
10 t=59

What about privacy?!
Proof of Exclusion
Proof of Exclusion

\[ \text{Index}(X) + 1 = \text{Index}(Z) \]

\[ \text{Time}(X) < \text{Time}(Y) < \text{Time}(Z) \]
Proof of Exclusion

Index(X) + 1 = Index(Z)

Time(X) < Time(Y) < Time(Z)
Proof of Exclusion

\[ X + 1 = Y + 1 \leq Z \]
Proof of Exclusion

\[ \text{Index}(X) + 1 = \text{Index}(Z) \]

\[ \text{Time}(X) < \text{Time}(Y) < \text{Time}(Z) \]

Are these numbers really from the log?
Proof of Exclusion

\[ X + 1 = Z \]

hehehe...
Proof of Exclusion

Needed for proof

Index(X)  Time(X)
Proof of Exclusion

New signatures from log

$H(x) + \text{Index}(X)$

$H(x)$

$H(x) + \text{Time}(X)$

Needed for proof

Index($X$)

Time($X$)
Proof of Exclusion

New signatures from log

\[ H(x) + \text{Index}(X) \]

\[ H(x) \]

\[ H(x) + \text{Time}(X) \]

Needed for proof

\[ \text{Index}(X) \]

\[ \text{Time}(X) \]
Proof of Exclusion

New signatures from log

H(x) + Index(X) \[ sk_i \]

H(x) \[ sk_H \]

H(x) + Time(X) \[ sk_T \]

Needed for proof
Proof of Exclusion

New signatures from log

H(x)+Index(X) \( sk_i \)

H(x) \( sk_H \)

H(x)+Time(X) \( sk_T \)

H(x)+Index(X) + H(X) + H(x)+Time(X)

Index(X)

Time(X)
Proof of Exclusion

New signatures from log

Needed for proof
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