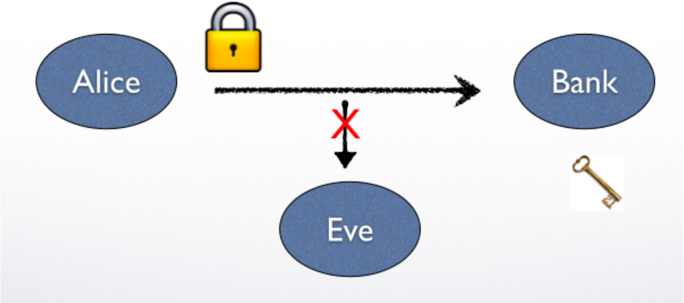
Distributed Transparent Key Infrastructure

Jiangshan Yu, Vincent Cheval, and Mark Ryan

School of Computer Science
University of Birmingham

Dec. 2013

Secure communication



Certificate

A certificate is a digital signed statement that binds a public key to a subject's identity detail. (*Example*)

Certificate

A certificate is a digital signed statement that binds a public key to a subject's identity detail. (*Example*)

CA/B trust model

- browser defines a set of CAs;
- browser accepts all certificates issued by any one of them.

Mozilla Firefox browser initially trusts 57 root CAs.
The EFF SSL Observatory : $\sim$ 1500 of CAs in total.

Issues

Problems

- Any CA can certify public keys for any domain.
- CA/B cannot detect mis-issued certificate.

Issues

Problems

- Any CA can certify public keys for any domain.
- CA/B cannot detect mis-issued certificate.

Example of Attacks:

- Comodo was attacked and fake certificates were issued for popular domains (e.g. Google, Yahoo, Skype, etc.). (2011)
- DigiNotar issued 531 fake certificates for more than three hundred domains, including most of major Internet communications companies. (2011)

Issues

Another concern

Monopoly.

- CAs are American dominated; and
- it is hard to become a browser-accepted CA because of the strong trust assumption that it implies.

Existing Proposals

Table: Taxonomy of existing solutions

Taxonomy	**Existing Proposals**
PGP adoption	MonkeySphere;
DNS extension	DANE
Difference observation	SSL Observatory; Certificate Patrol; Perspectives;
	DoubleCheck; CertLock; Covergence;
	TACK.
Public log adoption	Sovereign Keys; Certificate Transparency;
	AKI; DTKI

Existing Proposals

Table: Taxonomy of existing solutions

Taxonomy	**Existing Proposals**
PGP adoption	MonkeySphere;
DNS extension	DANE
Difference observation	SSL Observatory; Certificate Patrol; Perspectives;
	DoubleCheck; CertLock; Covergence;
	TACK.
Public log adoption	Sovereign Keys; Certificate Transparency;
	AKI; DTKI

Public log adoption protocol

Basic idea:

- All certificates issued by a CA should be recorded in a public log.
- Browsers only accept certificates which are included in the log.
- Domain owners can detect mis-issued certificates by checking the log.

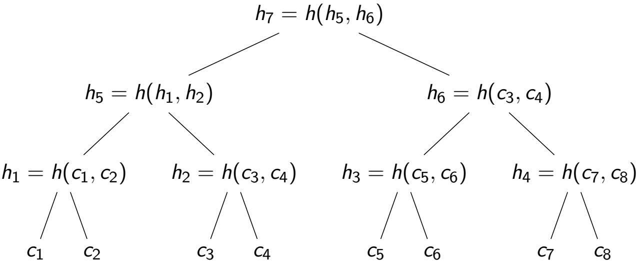
Public Log

Desired proofs:

- **Proof of presence** proves that a certificate is included in a public log.
- **Proof of extension** proves that the current public log is an extension of previous versions.
- **Proof of currency** proves that the public key of a subject is the latest one in the public log.
- **proof of absence** proves that no certificate in the log is issued for the given subject.

Certificate transparency [Laurie, Kasper, Langley]

Append-only public log – Merkle tree.



$h_7 = h(h_5, h_6)$

$h_5 = h(h_1, h_2)$ $h_6 = h(c_3, c_4)$

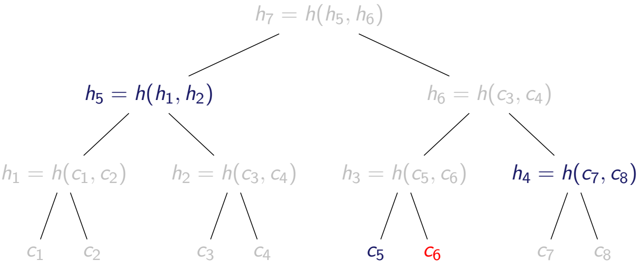
$h_1 = h(c_1, c_2)$ $h_2 = h(c_3, c_4)$ $h_3 = h(c_5, c_6)$ $h_4 = h(c_7, c_8)$

c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8

IETF RFC6962 (June 2013)

Certificate transparency [Laurie, Kasper, Langley]

Append-only public log – Merkle tree.



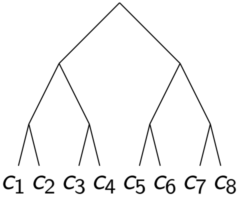
Proof of	Complexity
presence	$O(log\, n)$
extension	$O(log\, n)$
currency	$O(n)$
absence	$O(n)$

IETF RFC6962 (June 2013)

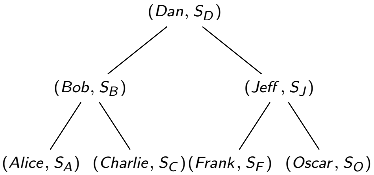
An improvement

Certificate Issuance and Revocation Transparency [Ryan 2013]

ChronTree



LexTree



Proof of		
presence	$O(log\, n)$	$O(log\, n)$
extension	$O(log\, n)$	$O(n)$
currency	$O(n)$	$O(log\, n)$
absence	$O(n)$	$O(log\, n)$
consistency	$O(n)$	

Consistency Proof

- Monitors.
- Random checking by clients.

Problems

Informal description

- Formalisation.
- Formal verification.

Difficulty with multiple public logs

- **Efficiency**
- **Security**.

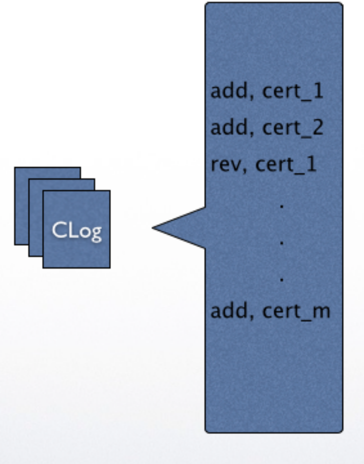
DTKI

Distributed **T**ransparent **K**ey **I**nfrastructure

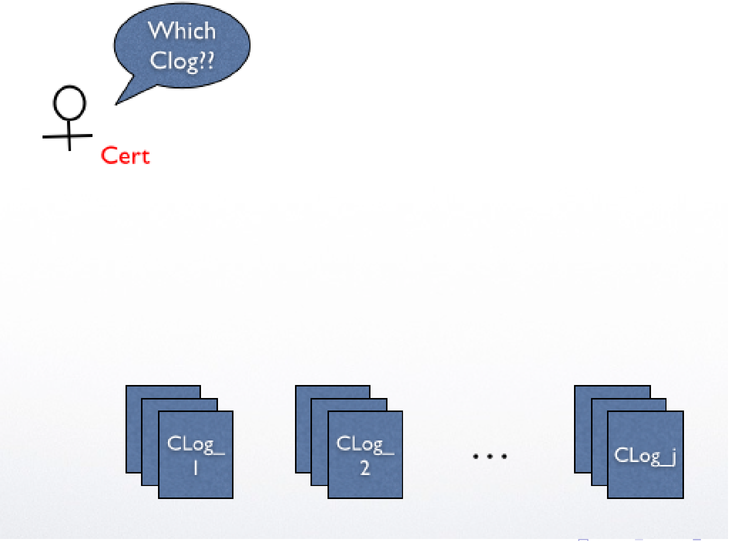
- Formalisation of data structure
- Proofs of data structure properties
- Minimisation of monopoly
- Reduction of trusted parties

DTKI

Certificate log (Clog)

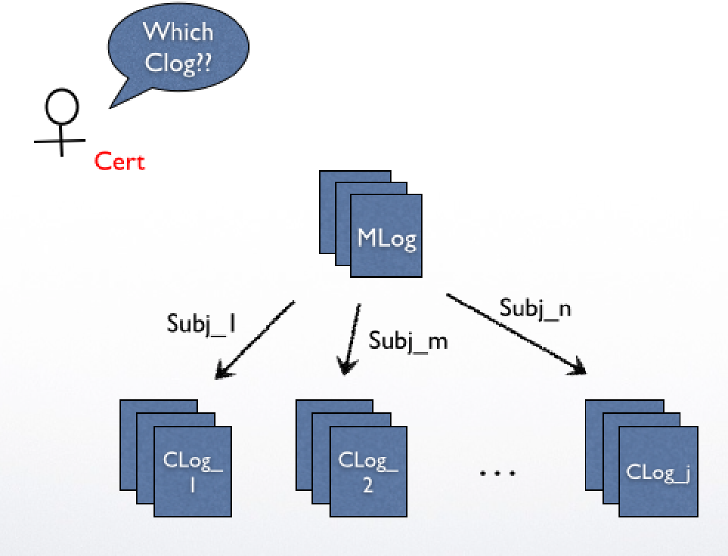


DTKI



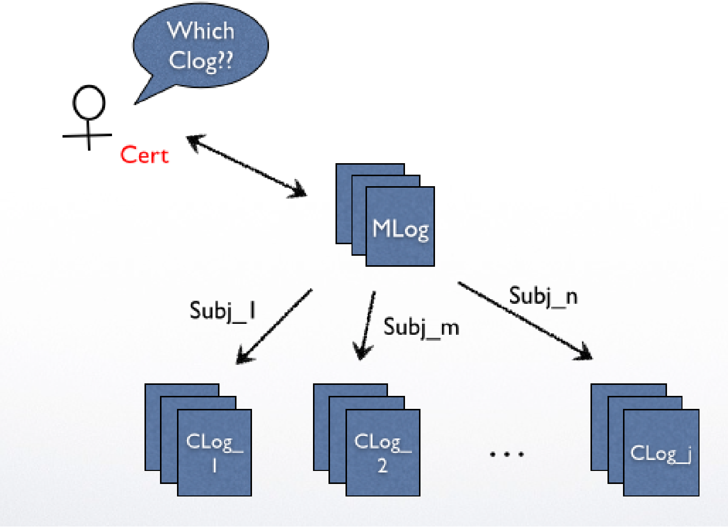
DTKI

Mapping log (Mlog)



DTKI

Mapping log (Mlog)



DTKI

Map=(Log(ID),RegX).

DTKI

Map=(Log(ID),RegX).

Example:

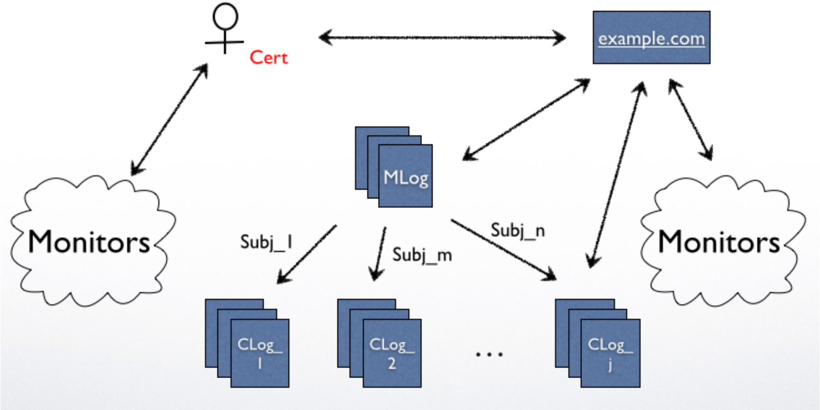
$$(add, Log(ID_1), www\backslash. * \backslash.org)$$

$$(add, Log(ID_1), www\backslash. * \backslash.uk)$$

$$(rev, Log(ID_1), www\backslash. * \backslash.uk)$$

$$(add, Log(ID_{127}), www\backslash. * \backslash.uk)$$

DTKI


Cert
example.com
MLog
Monitors
Subj_l
Subj_m
Subj_n
Monitors
CLog_ 1
CLog_ 2
. . .
CLog_ j

Thank You!