Certificates-as-an-Insurance (CaaI): Incentivizing Accountability in SSL/TLS

Stephanos Matsumoto (CMU/ETH Zurich)

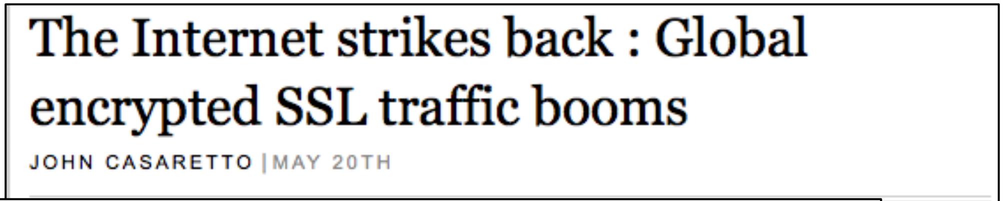
Raphael M. Reischuk (ETH Zurich)

Workshop on the Security of Emerging Network Technologies (SENT)

8 February 2015

Introduction

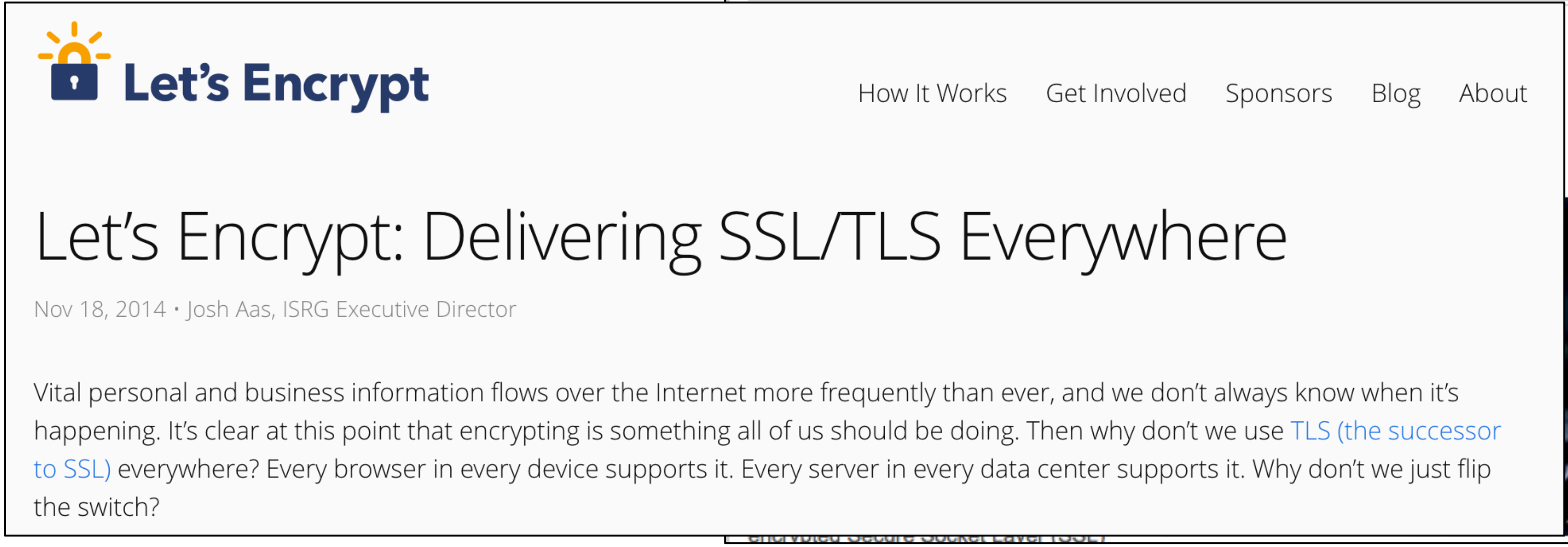
- Authentication of public keys is *critical to end-to-end encryption*



The Internet strikes back : Global encrypted SSL traffic booms

JOHN CASARETTO | MAY 20TH

[2]



Let's Encrypt: Delivering SSL/TLS Everywhere

Nov 18, 2014 • Josh Aas, ISRG Executive Director

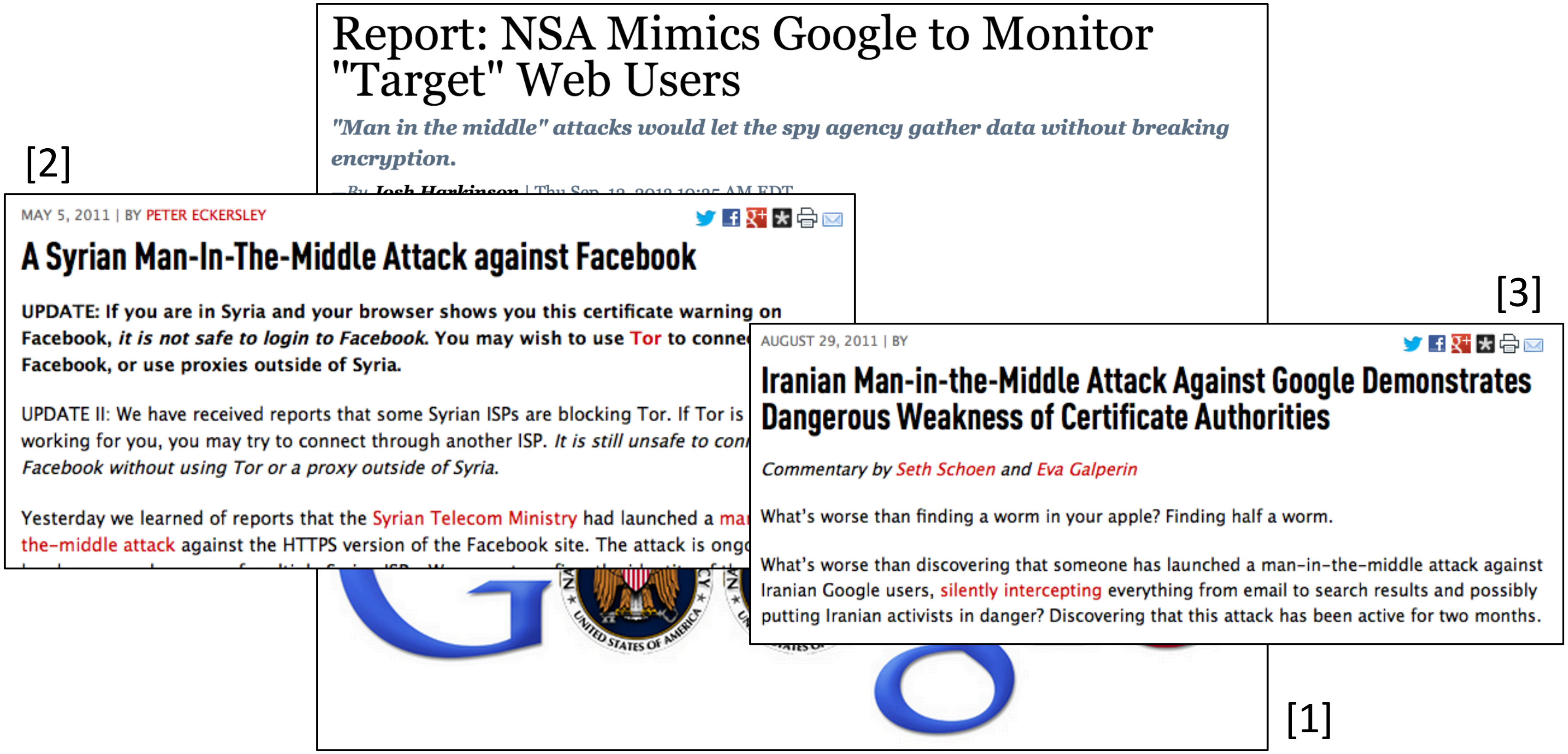
Vital personal and business information flows over the Internet more frequently than ever, and we don't always know when it's happening. It's clear at this point that encrypting is something all of us should be doing. Then why don't we use TLS (the successor to SSL) everywhere? Every browser in every device supports it. Every server in every data center supports it. Why don't we just flip the switch?

[1]

[1] http://siliconangle.com/blog/2014/05/20/the-internet-strikes-back-global-encrypted-ssl-traffic-booms/
[2] https://letsencrypt.org/

Introduction

- Authentication of public keys is *attacked*



Report: NSA Mimics Google to Monitor "Target" Web Users

"Man in the middle" attacks would let the spy agency gather data without breaking encryption.

—By **Josh Harkinson** | Thu Sep. 12, 2013 10:35 AM EDT

[1]

MAY 5, 2011 | BY PETER ECKERSLEY

A Syrian Man-In-The-Middle Attack against Facebook

UPDATE: If you are in Syria and your browser shows you this certificate warning on Facebook, *it is not safe to login to Facebook.* You may wish to use Tor to conne Facebook, or use proxies outside of Syria.

UPDATE II: We have received reports that some Syrian ISPs are blocking Tor. If Tor is working for you, you may try to connect through another ISP. *It is still unsafe to con Facebook without using Tor or a proxy outside of Syria.*

Yesterday we learned of reports that the Syrian Telecom Ministry had launched a ma the-middle attack against the HTTPS version of the Facebook site. The attack is ong

[2]

AUGUST 29, 2011 | BY

Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities

Commentary by Seth Schoen and Eva Galperin

What's worse than finding a worm in your apple? Finding half a worm.

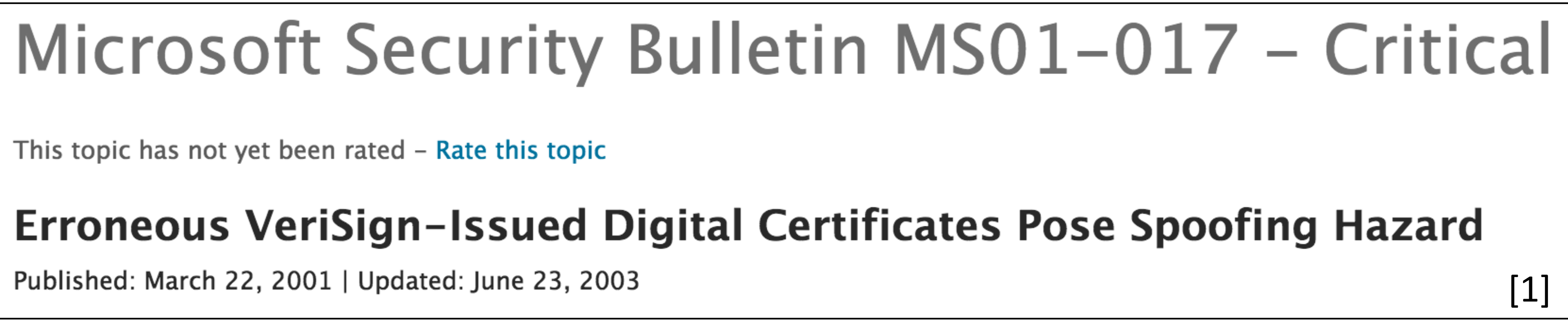
What's worse than discovering that someone has launched a man-in-the-middle attack against Iranian Google users, silently intercepting everything from email to search results and possibly putting Iranian activists in danger? Discovering that this attack has been active for two months.

[3]

[1] http://www.motherjones.com/politics/2013/09/flying-pig-nsa-impersonates-google
[2] https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook
[3] https://www.eff.org/deeplinks/2011/08/iranian-man-middle-attack-againstgooglev

Introduction

- Current TLS authentication is *fragile*



Microsoft Security Bulletin MS01-017 - Critical

This topic has not yet been rated - Rate this topic

Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard

Published: March 22, 2001 | Updated: June 23, 2003

[1]

> "Zusman requested the DV SSL certificate from CA Thawte using the email address SSLCertificates@Live.com, which he registered with the free Live.com webmail service." [2]

[1] https://support.microsoft.com/kb/293818

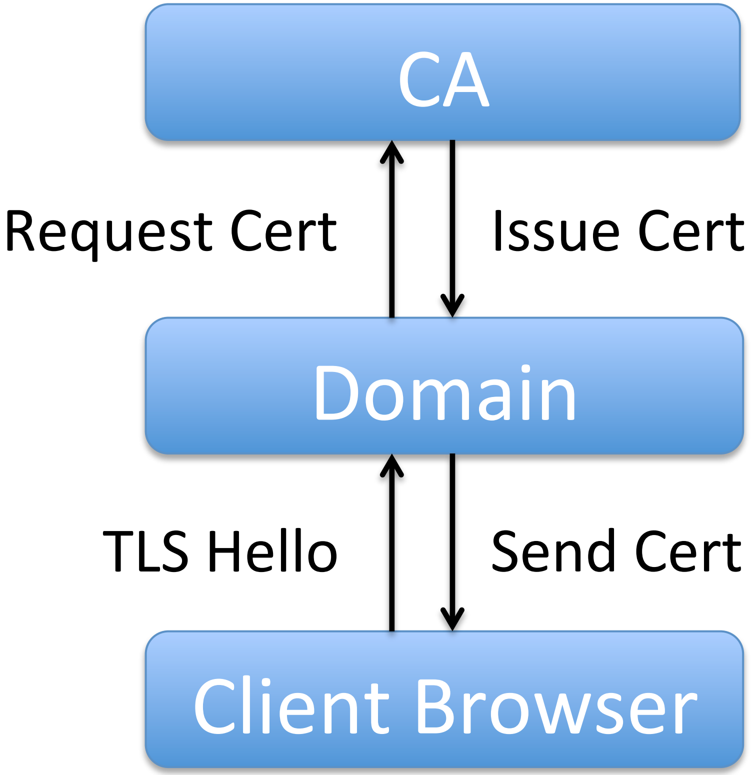
[2] M. Zusman, A. Sotirov. "Sub-Prime PKI: Attacking Extended Validation SSL. BlackHat '09.

Introduction

- How can we incentivize CAs to more carefully check a domain's control of a key?
- Contributions:
  - Study *shortcomings in CA accountability*
  - Model *certificates-as-an-insurance (CaaI)* as a way to provide enforceable accountability
  - Propose *challenges and possible instantiations* of the CaaI model

Background

- SSL/TLS
  - SSL (Netscape, 1994)
  - TLS (IETF, 1999)
- *Confidentiality* through end-to-end encryption
- *Authenticity* through CA-based certification



Check Cert, Verify CA Signature

Background

- Other proposals
  - DANE
  - EV Certs

  Enhance assurance with existing infrastructures and extra checks

  - Network perspective
  - Log-based proposals
  - Pinning

  Mechanisms to detect unauthorized certificates

- Accountability is insufficiently addressed

Shortcomings in Accountability

1. Lack of enforceable accountability
2. Imbalance of control and liability
3. Disincentives for accountability

1. Lack of enforceable accountability

- Domains and users still trust breached CAs

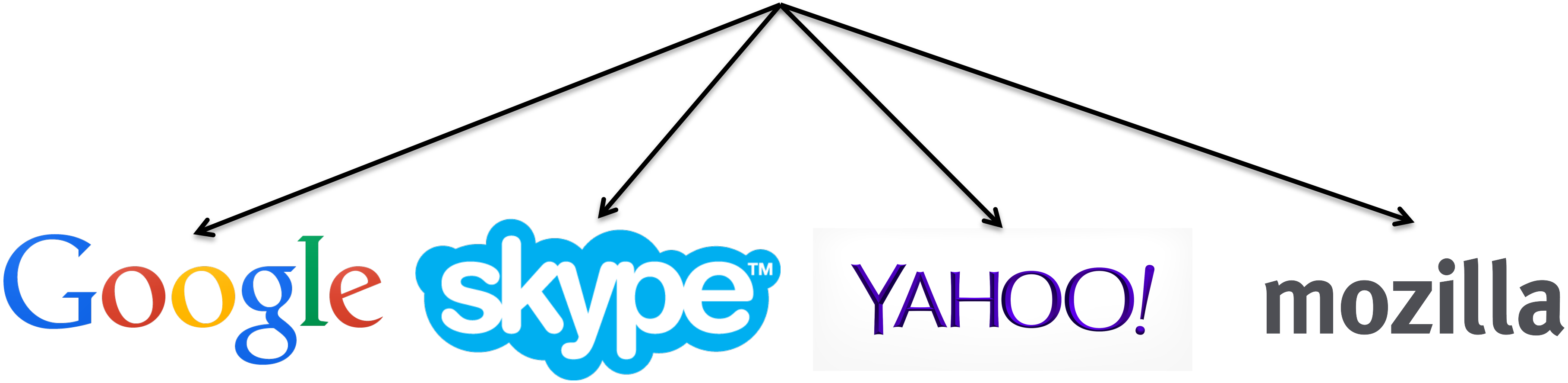
Hacked, 2011
Bankrupt

COMODO
Creating Trust Online™

Hacked, 2011
30.7% Market Share, 2015 [1]

VeriSign®
(now Symantec)

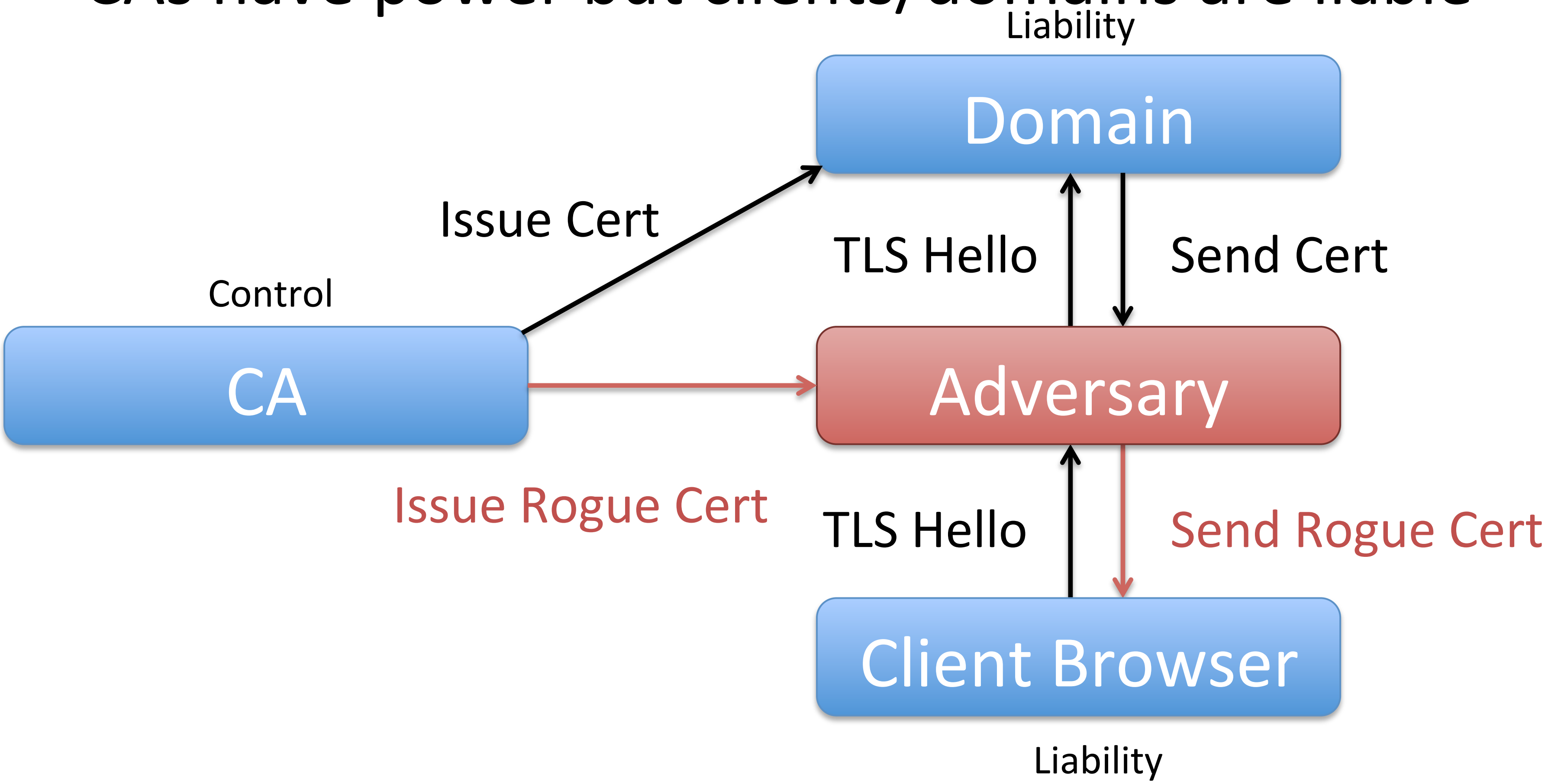
Hacked, 2010
33.9% Market Share, 2015 [1]



[1] http://w3techs.com/technologies/overview/ssl_certificate/all, accessed 1 Feb 2015

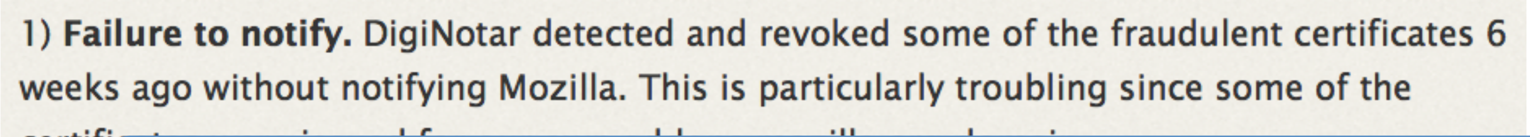
2. Imbalance of control and liability

- CAs have power but clients/domains are liable



3. Disincentives for accountability

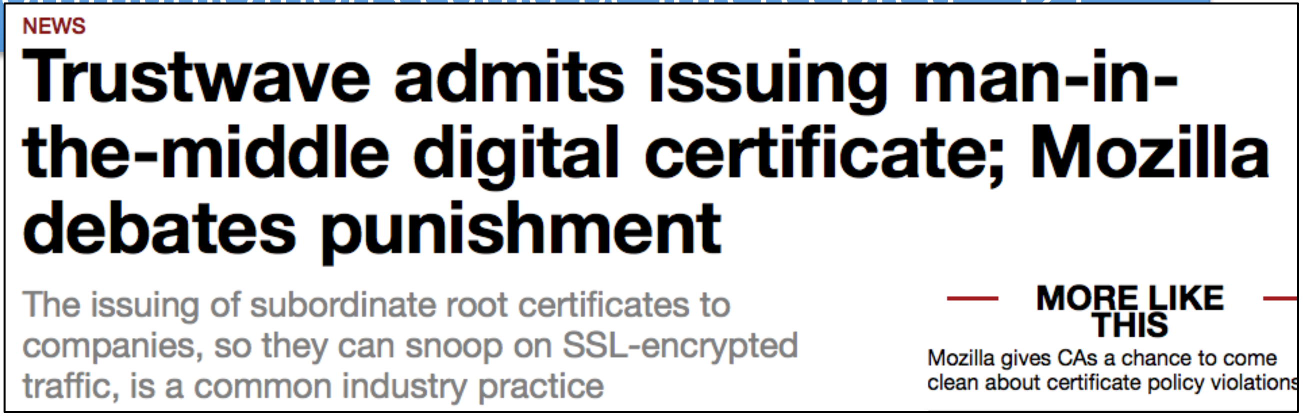
- Lack of accountability can benefit CAs



1) **Failure to notify.** DigiNotar detected and revoked some of the fraudulent certificates 6 weeks ago without notifying Mozilla. This is particularly troubling since some of the certifi

[1]

“DigiNotar did not immediately report the cyber-attack to customers or government authorities…for 2 months, private communications could be intercepted.” [2]



NEWS

Trustwave admits issuing man-in-the-middle digital certificate; Mozilla debates punishment

The issuing of subordinate root certificates to companies, so they can snoop on SSL-encrypted traffic, is a common industry practice

MORE LIKE THIS
Mozilla gives CAs a chance to come clean about certificate policy violations

[3]

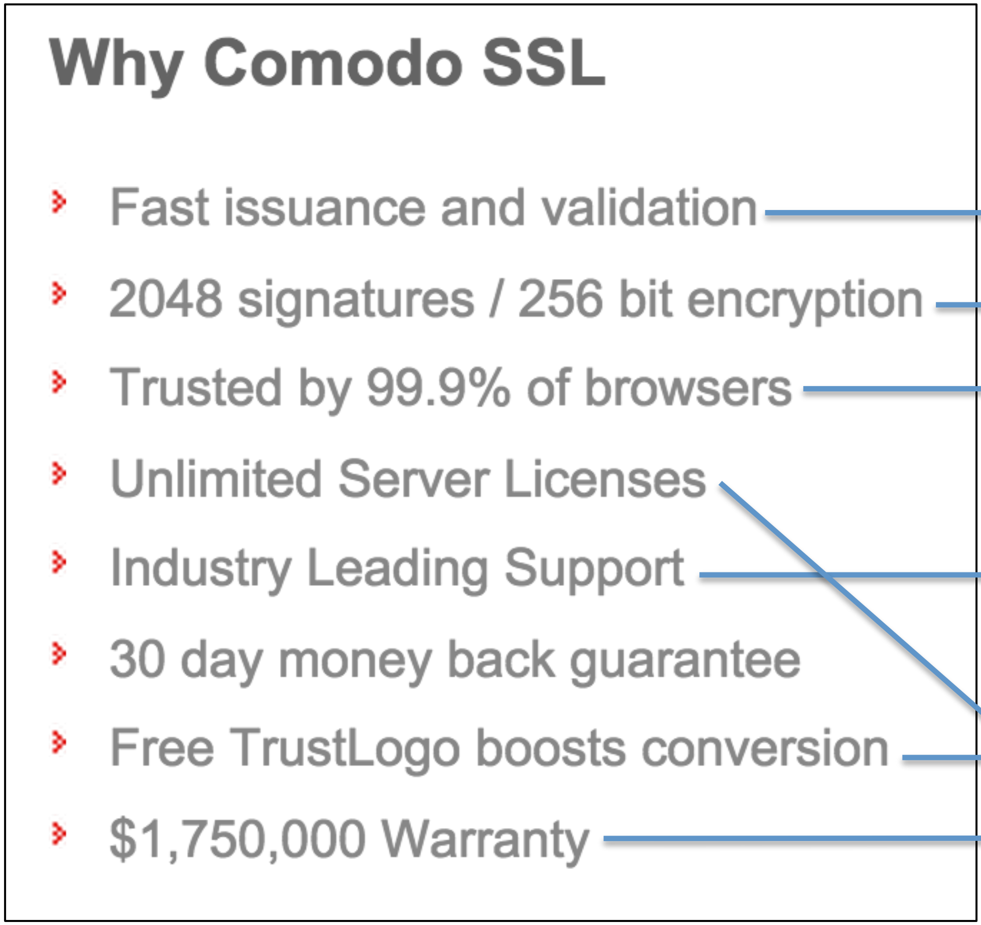
[1] https://blog.mozilla.org/security/2011/09/02/diginotar-removal-follow-up/

[2] https://www.enisa.europa.eu/media/news-items/operation-black-tulip

[3] http://www.computerworld.com/article/2501291/internet/trustwave-admits-issuing-man-in-the-middle-digital-certificate--mozilla-debates-punishment.html

3. Disincentives for accountability

- CAs sell certificates by bundling features



Why Comodo SSL

- Fast issuance and validation
- 2048 signatures / 256 bit encryption
- Trusted by 99.9% of browsers
- Unlimited Server Licenses
- Industry Leading Support
- 30 day money back guarantee
- Free TrustLogo boosts conversion
- $1,750,000 Warranty

Speed, not carefulness, of validation

Features that most CAs offer

Reputation is a selling point

Support bundled with cert

Extra services bundled with cert

Warranty

https://ssl.comodo.com/, accessed 2 Feb 2015

Research Questions

1. Enforceable CA Accountability
2. Collocated Control and Liability
3. Incentives for Trustworthy Behavior

1. Enforceable CA Accountability

- Goal: efficient, effective *enforcement*
- Method 1: Certificate revocation
  - Revoke the domain's or the CA's certificate
  - Challenge: avoid collateral damage to other certs
- Method 2: Out-of-Band Solutions
  - e.g. legal claims, lawsuits
  - Challenge: many jurisdictions, slow legal process

2. Collocated Control and Liability

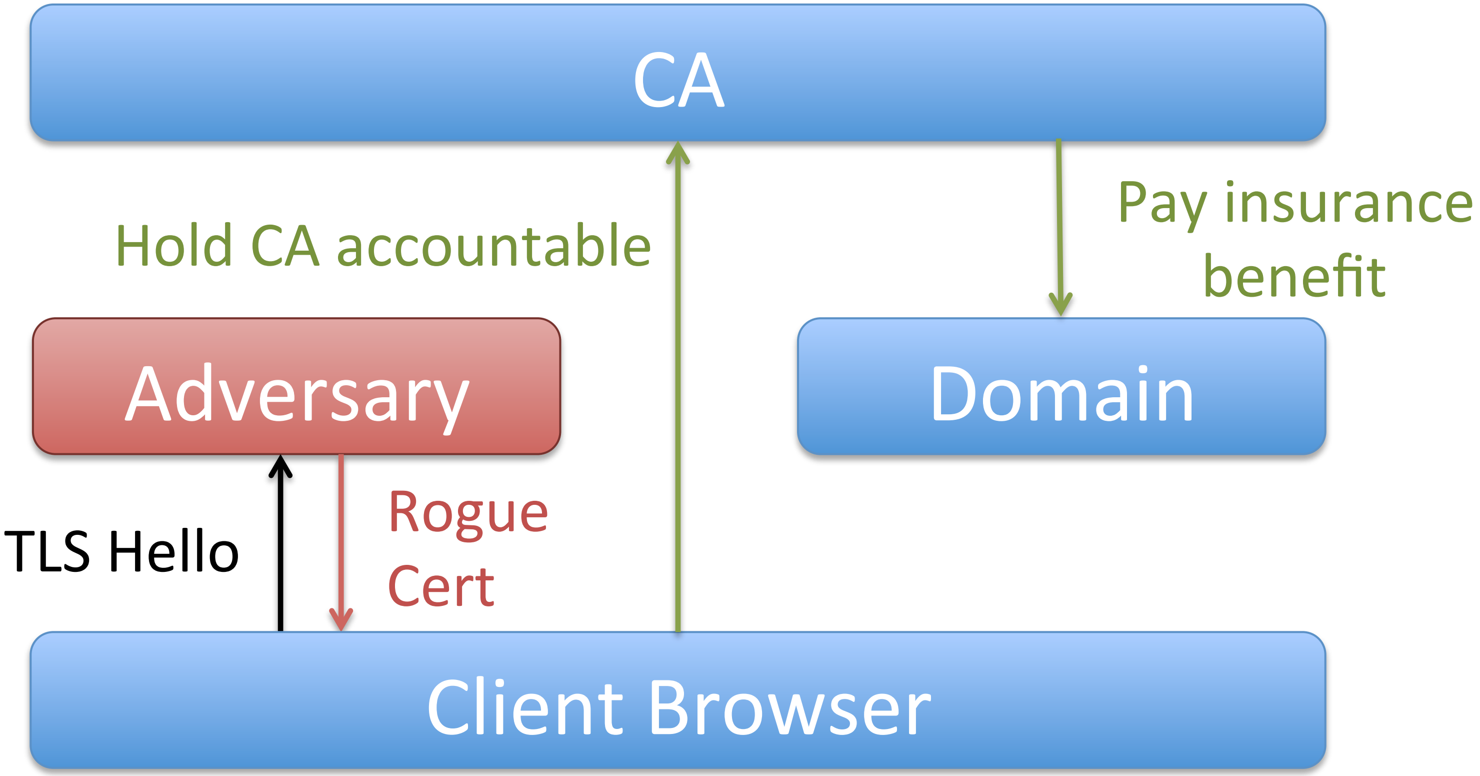
- Goal: transfer control to domains and clients
  - e.g. through trust agility, network perspective
  - Challenge: who has control over what aspects?
- Goal: transfer liability to CAs and browsers
  - Challenge: how to quantify damages?
  - Challenge: whom does the CA pay?

3. Incentives for Trustworthy Behavior

- Goal: incentivize more careful checks
  - CAs should want to hold themselves accountable
  - Enforceable accountability, balanced control and liability would provide these incentives
- Likely economic incentives
  - Disincentives against hiding breaches, lax checks
  - Incentives for strict checks such as EV

Proposal: Certificates-as-an-Insurance

- Our Caal Model



Check Cert, Verify CA Signature

Caal Goals

- *Prevent CA laziness*: CAs should not benefit from failing to carefully check domains’ keys
- *Ensure CA penalty*: misbehaving CAs should not be able to prevent an insurance payout
- *Prevent insurance fraud*: Triggering a payout without misbehavior should not be possible

Possible Approach: Secret Sharing

- Overview
  - Insurance payout (e.g. an electronic check) is split using secret sharing
  - Threshold number of shares proves misbehavior and triggers payout
- Challenges
  - Who manages the shares?
  - How do we define and identify misbehavior?

Possible Approach: Public Commitments

- Overview
  - CA makes a public commitment (e.g. in the cert)
  - Bitcoin payment to some set of domains if CA misbehavior is proved
- Challenges
  - Ensuring commitments are public and consistent
  - Negotiation and expression of conditions/proofs
  - Claiming and enforcing payout

Conclusions

- We must move towards making CAs voluntarily hold themselves accountable
- Caal provides incentives for greater accountability
- We encourage future work to address the details of instantiating Caal

Thank you! Questions?