The SSL/TLS Public-Key Infrastructure (PKI)

Terminology, Certificates, Problems, Certificate Transparency, Key Pinning, Revocation

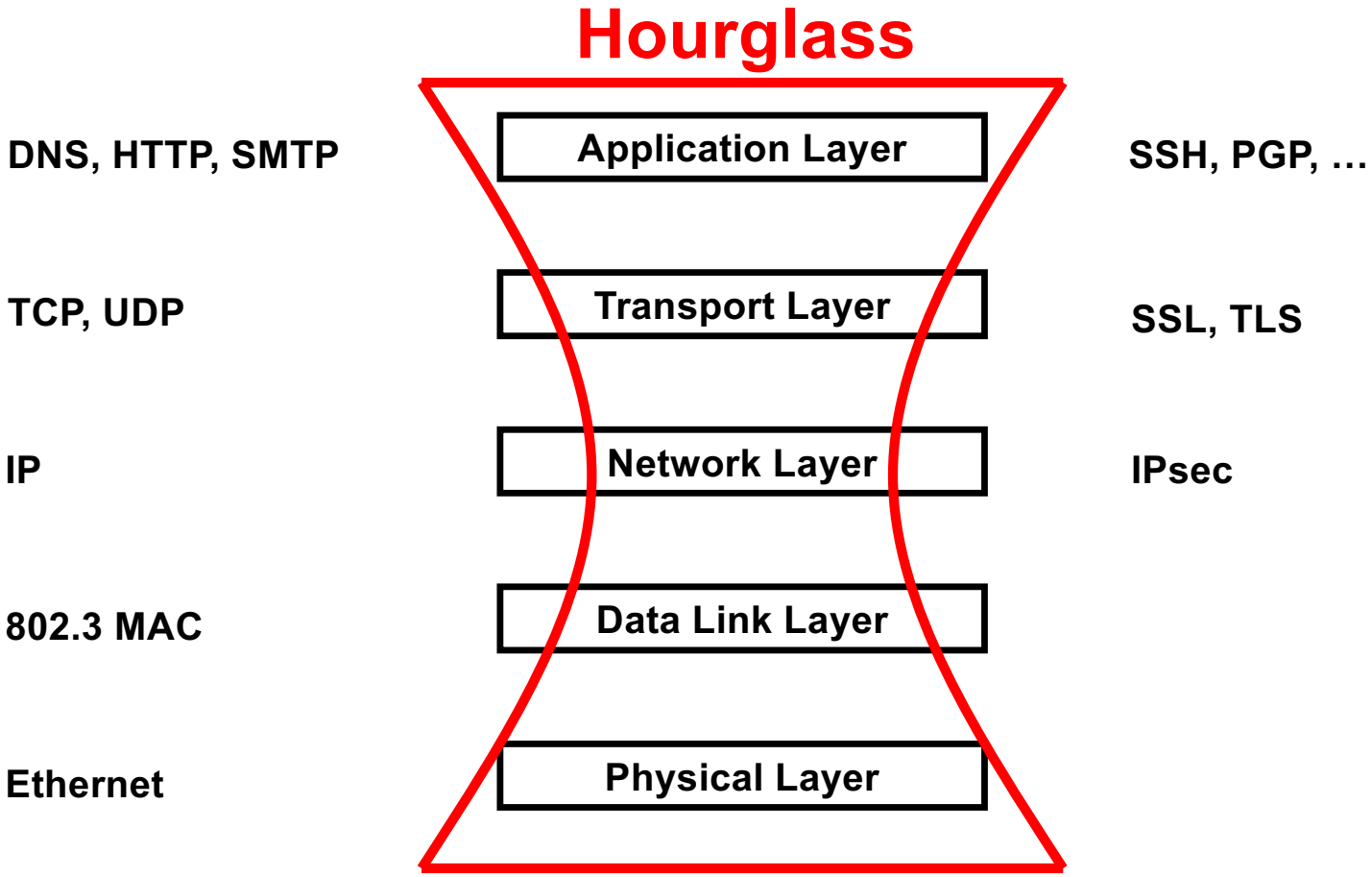
Network Security AS 2020

22 September 2020

Adrian Perrig
Laurent Chuat

ETH zürich

Position of Security in Protocol Stack



Brief SSL/TLS Overview

- Goal: Secure Internet communication
  - Secure bank transactions
  - Secure online purchases
  - Secure login (e.g., mail, social networks)
- Security requirements
  - Secrecy to prevent eavesdroppers to learn sensitive information
  - Entity and message authentication to prevent message alteration / injection

Sample TLS 1.2 Session

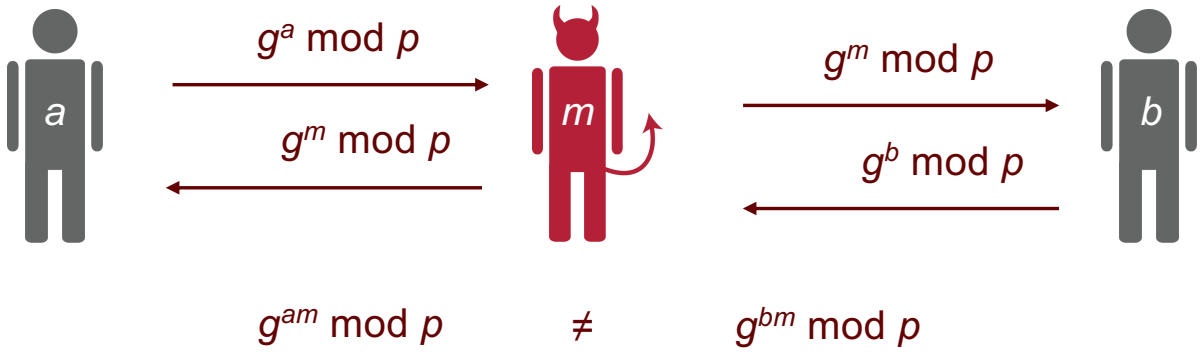
- Client has no certificate, only server authenticated
- C → S: client_hello
- S → C: server_hello
  - Ephemeral DH key exchange, RC4 encryption, MD5-based MAC
- S → C: Server certificate, containing RSA public key
  - Client checks validity + verifies that the URL matches the certificate
- S → C: Server_key_exchange: g, p, g^s, $\{H(g, p, g^s)\}_{K_S^{-1}}$
- S → C: server_hello_done
- C → S: client_key_exchange: g^c
- C → S: change_cipher_spec
- C → S: finished
- S → C: change_cipher_spec
- S → C: finished

Diffie–Hellman Key Agreement

- Public values: large prime p, generator g
- Alice has secret value a, Bob has secret b
- A → B: $g^a \pmod p$
- B → A: $g^b \pmod p$
- Bob computes $(g^a)^b = g^{ab} \pmod p$
- Alice computes $(g^b)^a = g^{ab} \pmod p$
- Eve cannot compute $g^{ab} \pmod p$

Problem: Man-in-the-Middle Attack

- Public values: large prime p, generator g
- Problem: in Man-in-the-Middle attack, Mallory impersonates Alice to Bob and Bob to Alice



PKI Overview

- In symmetric cryptography, main challenge is key distribution as keys need to be distributed via *confidential and authentic* channels
- In public-key systems, main challenge is key authentication (i.e., which key belongs to whom) as keys need to be distributed via *authentic channels*
- Public-key infrastructures (PKIs) provide a way to validate public keys

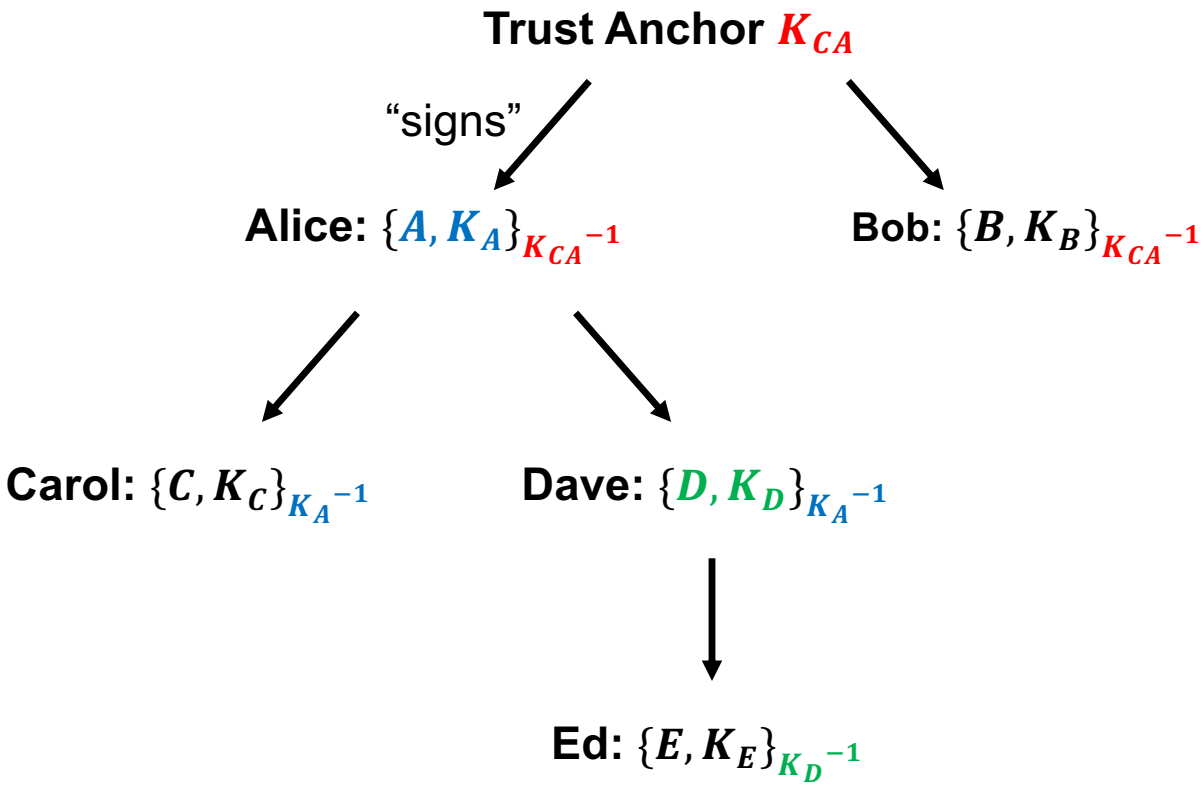
PKI Terminology

- *PKI*: Public-Key Infrastructure
- *CA:* Certification Authority
- A *public-key certificate* (or simply *certificate*) is signed and binds a name to a public key
- *Trust anchor, trust root:* self-signed certificates of public keys that are allowed to sign other certificates
- *X.509:* standard format of digital certificate

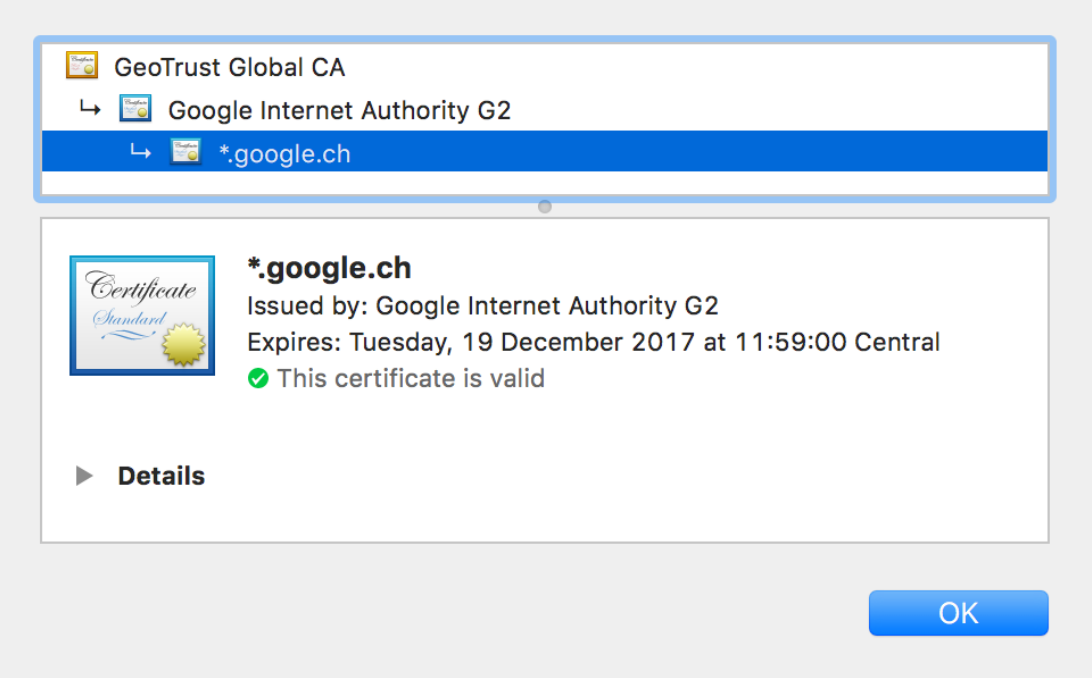
Trust Establishment

- Central questions
  - How can we establish trust in a public key certificate?
  - How do we know that we indeed have a secure connection?
  - How can we bind certificate to an *entity*? (Individual, corporation, government entity, web site, movie, …)
- Observations
  - You cannot establish trust out of thin air
  - *Root of trust* is used to establish trust in other entities
  - *Cryptographic operations enable transfer of trust from one entity to another*
- Metrics
  - Size of trust root (i.e., how many entities need to be trusted?)
  - Number of malicious entities that can be tolerated

Trust Anchors



Certificate Hierarchy



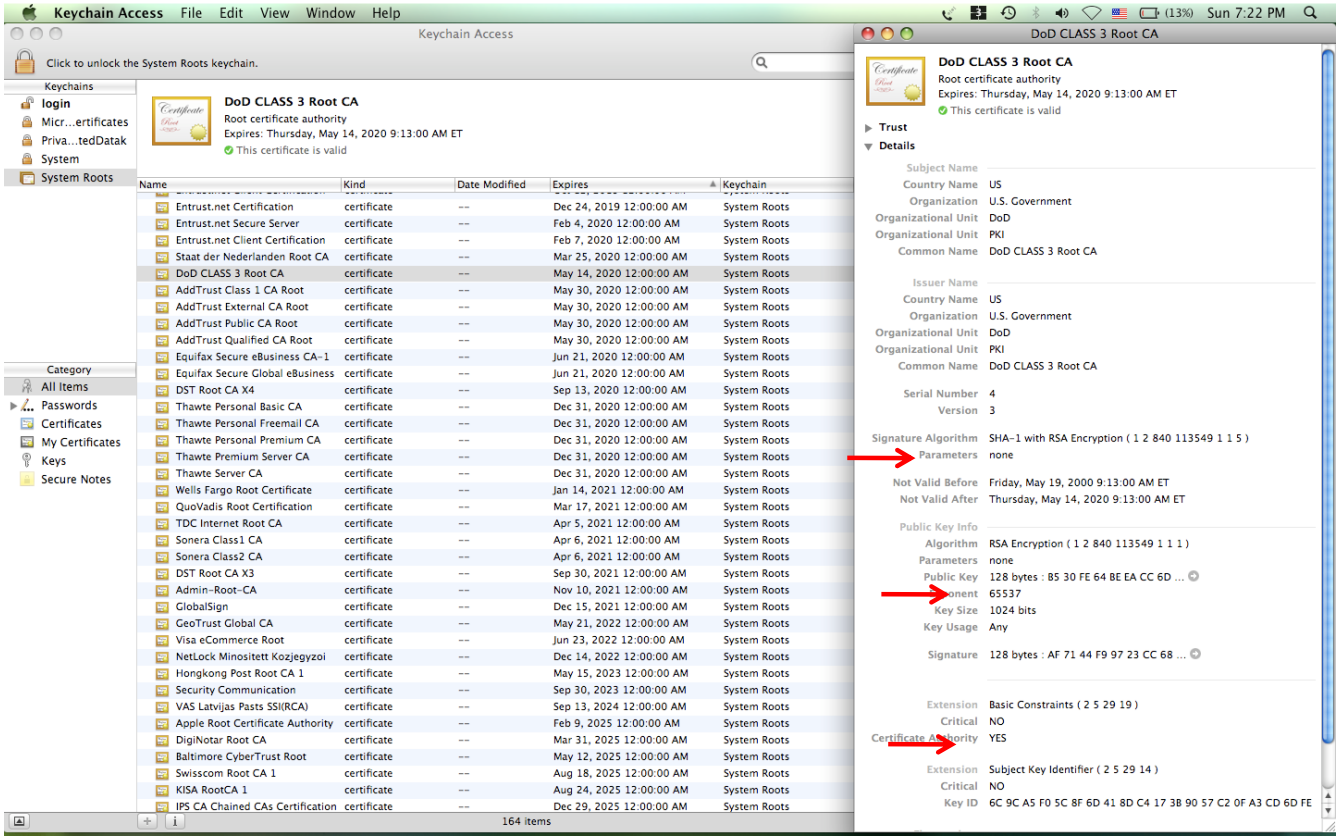
X.509

- X.509 was issued by the International Telecommunications Union (ITU) in July 1988, in association with the X.500 electronic directory services standard
- X.509 defines a structure for public key certificates
  - Two sections: data and signature section
  - A CA assigns a unique name to each user and issues a signed certificate
  - Often name is the domain or Email address
- Basic structure is very simple, but end up being very complex in any reasonable application

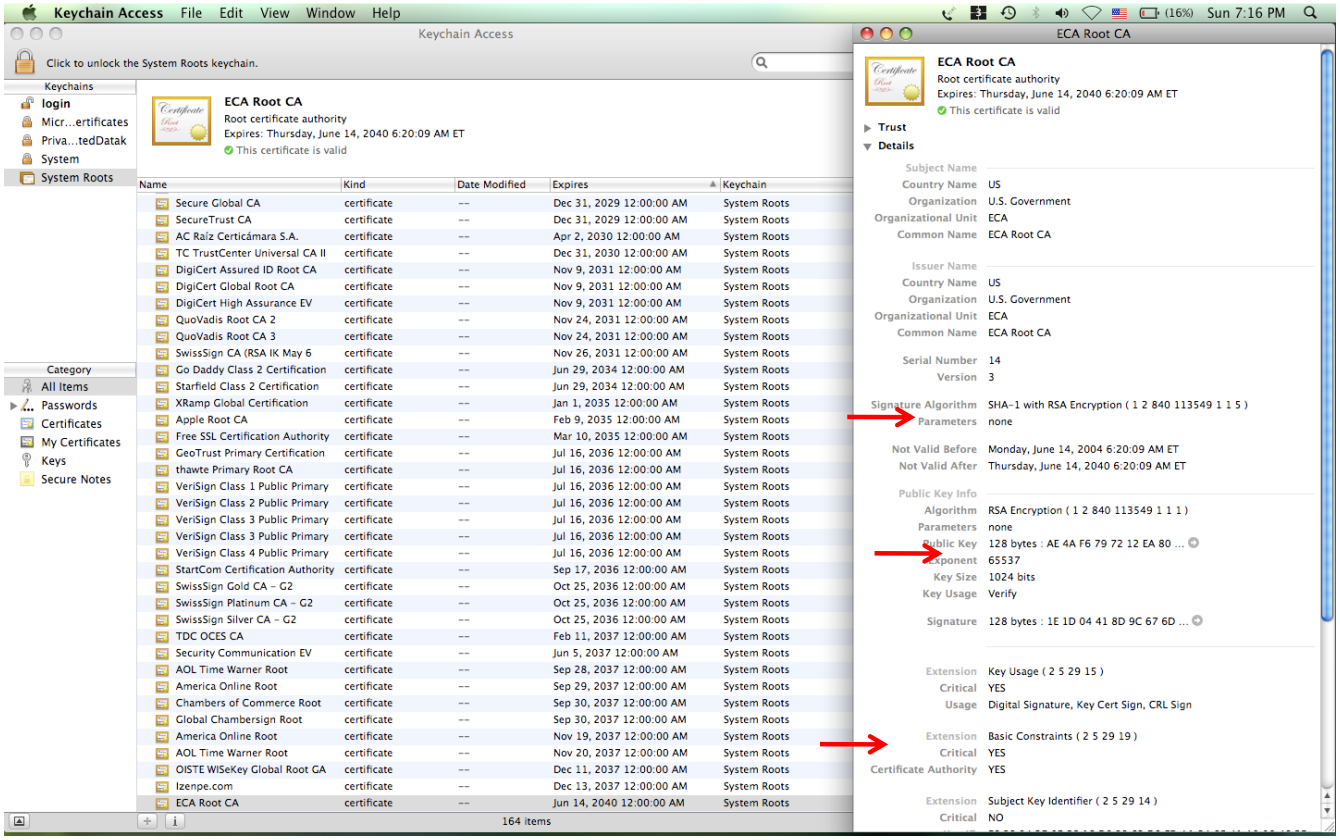
Trusted Root CA Certificates

A-Trust-nQual-01	certificate	--	Dec 1, 2014 12:00:00 AM	System Roots
A-Trust-nQual-03	certificate	--	Aug 18, 2015 12:00:00 AM	System Roots
A-Trust-Qual-01	certificate	--	Dec 1, 2014 12:00:00 AM	System Roots
A-Trust-Qual-02	certificate	--	Dec 3, 2014 12:00:00 AM	System Roots
AAA Certificate Services	certificate	--	Jan 1, 2029 12:59:59 AM	System Roots
AC Raíz Certicámara S.A.	certificate	--	Apr 2, 2030 11:42:02 PM	System Roots
Actalis Authentication Root CA	certificate	--	Sep 22, 2030 1:22:02 PM	System Roots
AddTrust Class 1 CA Root	certificate	--	May 30, 2020 12:38:31 PM	System Roots
AddTrust External CA Root	certificate	--	May 30, 2020 12:48:38 PM	System Roots
AddTrust Public CA Root	certificate	--	May 30, 2020 12:41:50 PM	System Roots
AddTrust Qualified CA Root	certificate	--	May 30, 2020 12:44:50 PM	System Roots
Admin-Root-CA	certificate	--	Nov 10, 2021 8:51:07 AM	System Roots
AdminCA-CD-T01	certificate	--	Jan 25, 2016 1:36:19 PM	System Roots
AffirmTrust Commercial	certificate	--	Dec 31, 2030 3:06:06 PM	System Roots
AffirmTrust Networking	certificate	--	Dec 31, 2030 3:08:24 PM	System Roots
AffirmTrust Premium	certificate	--	Dec 31, 2040 3:10:36 PM	System Roots
AffirmTrust Premium ECC	certificate	--	Dec 31, 2040 3:20:24 PM	System Roots
America Onli...ation Authority 1	certificate	--	Nov 19, 2037 9:43:00 PM	System Roots
America Onli...ation Authority 2	certificate	--	Sep 29, 2037 4:08:00 PM	System Roots
AOL Time W...cation Authority 1	certificate	--	Nov 20, 2037 4:03:00 PM	System Roots
AOL Time W...cation Authority 2	certificate	--	Sep 29, 2037 1:43:00 AM	System Roots
Apple Root CA	certificate	--	Feb 9, 2035 10:40:36 PM	System Roots
Apple Root Certificate Authority	certificate	--	Feb 10, 2025 1:18:14 AM	System Roots
Application CA G2	certificate	--	Mar 31, 2016 4:59:59 PM	System Roots
ApplicationCA	certificate	--	Dec 12, 2017 4:00:00 PM	System Roots
Autoridad de...l CIF A62634068	certificate	--	Dec 31, 2030 9:38:15 AM	System Roots
Autoridad de...tado Venezolano	certificate	--	Dec 18, 2030 12:59:59 AM	System Roots
Baltimore CyberTrust Root	certificate	--	May 13, 2025 1:59:00 AM	System Roots
Belgium Root CA	certificate	--	Jan 27, 2014 12:00:00 AM	System Roots
Belgium Root CA2	certificate	--	Dec 15, 2021 9:00:00 AM	System Roots
Buypass Class 2 CA 1	certificate	--	Oct 13, 2016 12:25:09 PM	System Roots
Buypass Class 2 Root CA	certificate	--	Oct 26, 2040 10:38:03 AM	System Roots
Buypass Class 3 CA 1	certificate	--	May 9, 2015 4:13:03 PM	System Roots
Buypass Class 3 Root CA	certificate	--	Oct 26, 2040 10:28:58 AM	System Roots
CA Disig	certificate	--	Mar 22, 2016 2:39:34 AM	System Roots
CA Disig Root R1	certificate	--	Jul 19, 2042 11:06:56 AM	System Roots
CA Disig Root R2	certificate	--	Jul 19, 2042 11:15:30 AM	System Roots

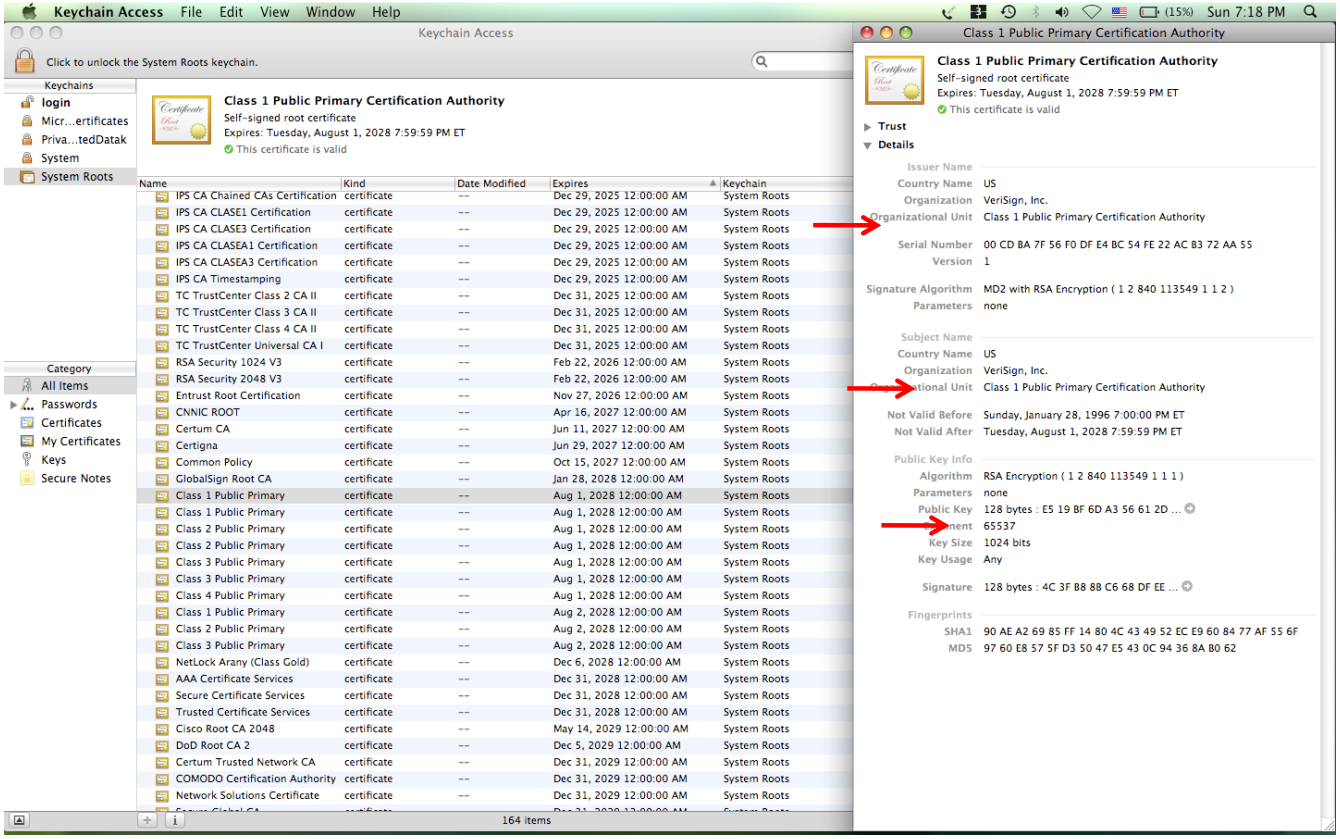
Sample CA Certificate 1



Sample CA Certificate 2



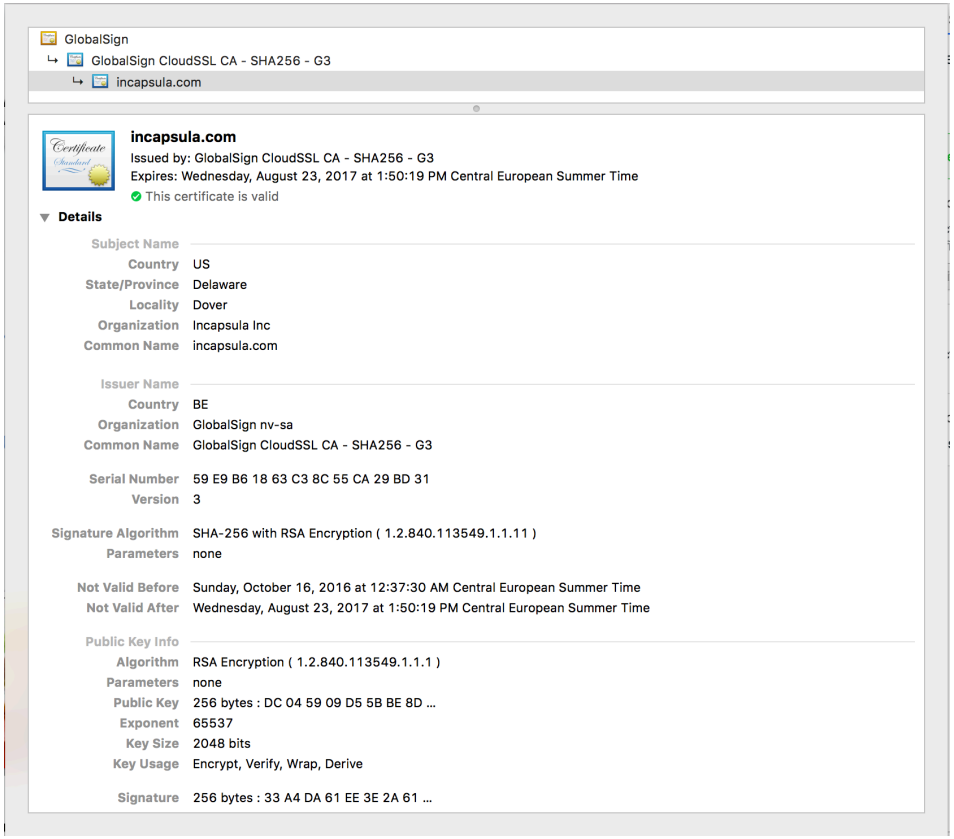
Sample CA Certificate 3



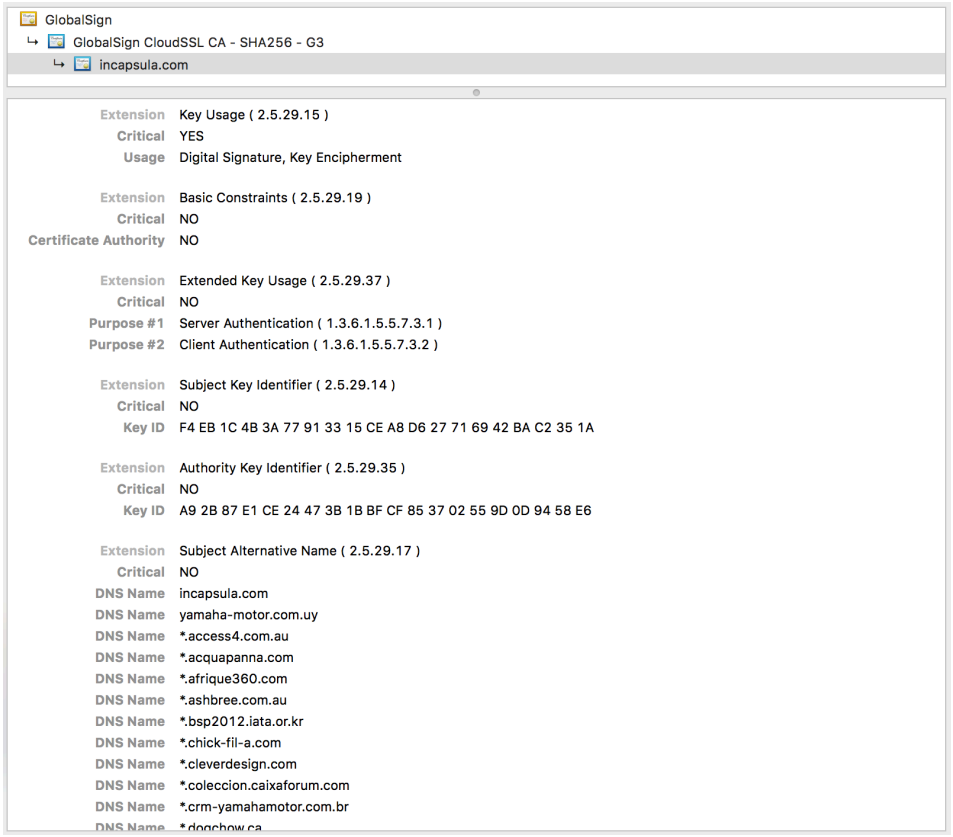
Multi-Domain Certificates by CDNs

- Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem by Cangialosi et al., ACM CCS 2016
- Problem 1: Content Delivery Networks (CDN) are hosting web sites for domains and thus need a certificate to service content
- Problem 2: CDNs are obtaining a single certificate for multiple domains

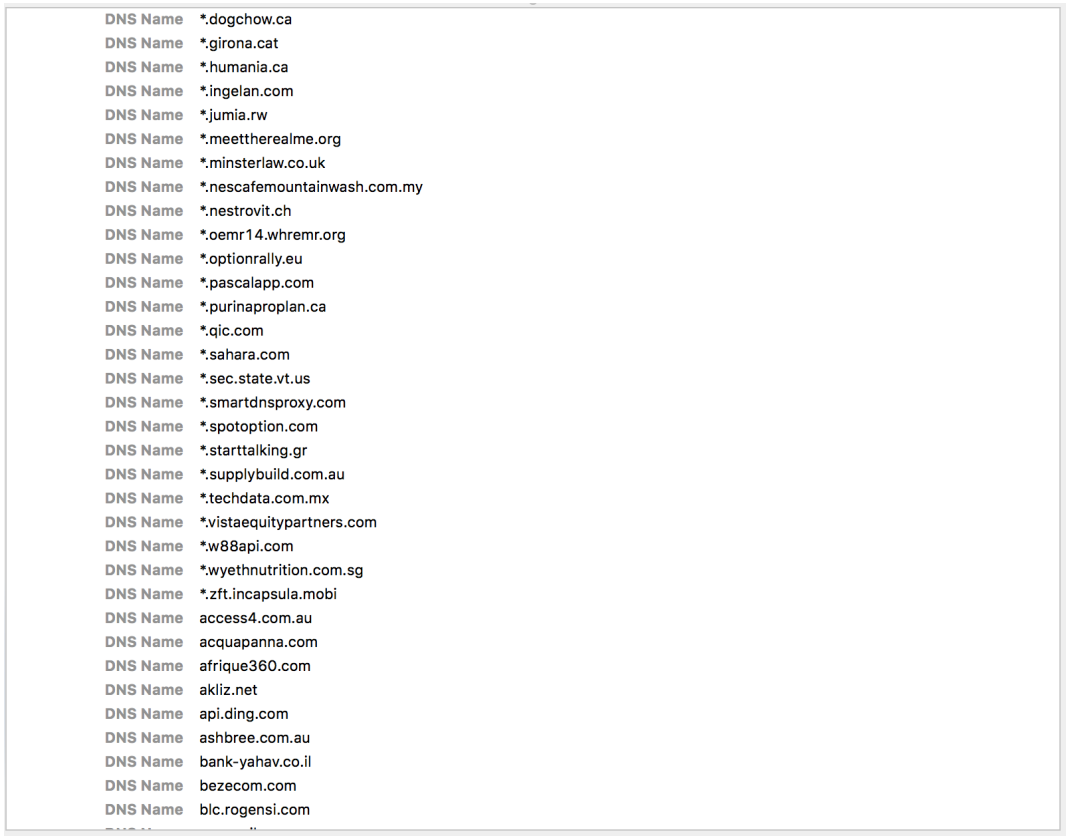
Sample Certificate by Incapsula.com (1/5)



Sample Certificate by Incapsula.com (2/5)

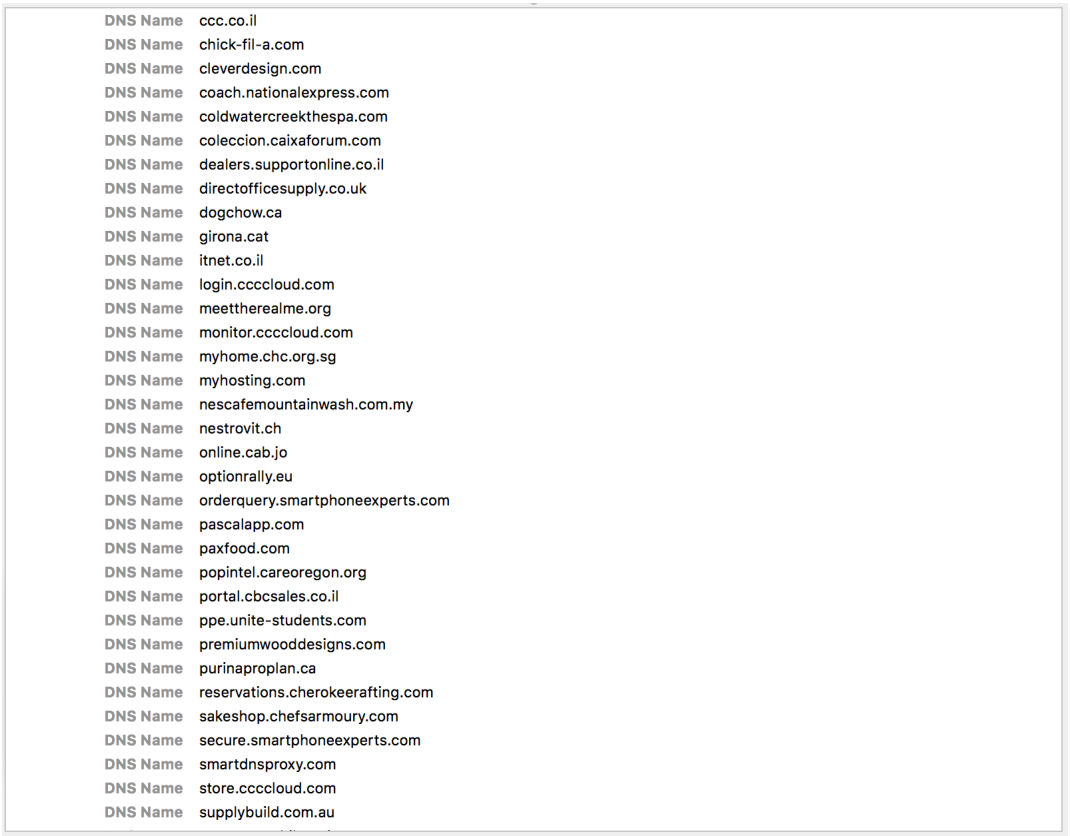


Sample Certificate by Incapsula.com (3/5)



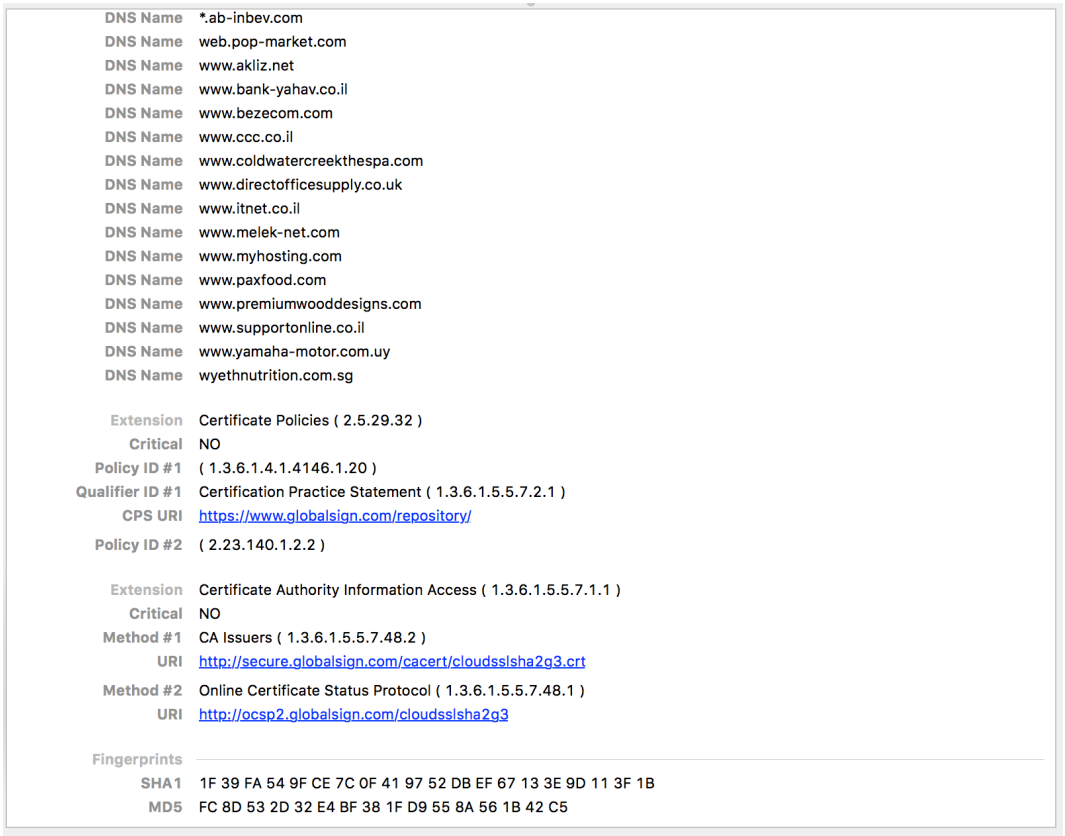
DNS Name	*.dogchow.ca
DNS Name	*.girona.cat
DNS Name	*.humania.ca
DNS Name	*.ingelan.com
DNS Name	*.jumia.rw
DNS Name	*.meettherealme.org
DNS Name	*.minsterlaw.co.uk
DNS Name	*.nescafemountainwash.com.my
DNS Name	*.nestrovit.ch
DNS Name	*.oemr14.whremr.org
DNS Name	*.optionrally.eu
DNS Name	*.pascalapp.com
DNS Name	*.purinaproplan.ca
DNS Name	*.qic.com
DNS Name	*.sahara.com
DNS Name	*.sec.state.vt.us
DNS Name	*.smartdnsproxy.com
DNS Name	*.spotoption.com
DNS Name	*.starttalking.gr
DNS Name	*.supplybuild.com.au
DNS Name	*.techdata.com.mx
DNS Name	*.vistaequitypartners.com
DNS Name	*.w88api.com
DNS Name	*.wyethnutrition.com.sg
DNS Name	*.zft.incapsula.mobi
DNS Name	access4.com.au
DNS Name	acquapanna.com
DNS Name	afrique360.com
DNS Name	akliz.net
DNS Name	api.ding.com
DNS Name	ashbree.com.au
DNS Name	bank-yahav.co.il
DNS Name	bezecom.com
DNS Name	blc.rogensi.com

Sample Certificate by Incapsula.com (4/5)



DNS Name	ccc.co.il
DNS Name	chick-fil-a.com
DNS Name	cleverdesign.com
DNS Name	coach.nationalexpress.com
DNS Name	coldwatercreekthespa.com
DNS Name	coleccion.caixaforum.com
DNS Name	dealers.supportonline.co.il
DNS Name	directofficesupply.co.uk
DNS Name	dogchow.ca
DNS Name	girona.cat
DNS Name	itnet.co.il
DNS Name	login.ccccloud.com
DNS Name	meettherealme.org
DNS Name	monitor.ccccloud.com
DNS Name	myhome.chc.org.sg
DNS Name	myhosting.com
DNS Name	nescafemountainwash.com.my
DNS Name	nestrovit.ch
DNS Name	online.cab.jo
DNS Name	optionrally.eu
DNS Name	orderquery.smartphoneexperts.com
DNS Name	pascalapp.com
DNS Name	paxfood.com
DNS Name	popintel.careoregon.org
DNS Name	portal.cbcsales.co.il
DNS Name	ppe.unite-students.com
DNS Name	premiumwooddesigns.com
DNS Name	purinaproplan.ca
DNS Name	reservations.cherokeerafting.com
DNS Name	sakeshop.chefsarmoury.com
DNS Name	secure.smartphoneexperts.com
DNS Name	smartdnsproxy.com
DNS Name	store.ccccloud.com
DNS Name	supplybuild.com.au

Sample Certificate by Incapsula.com (5/5)

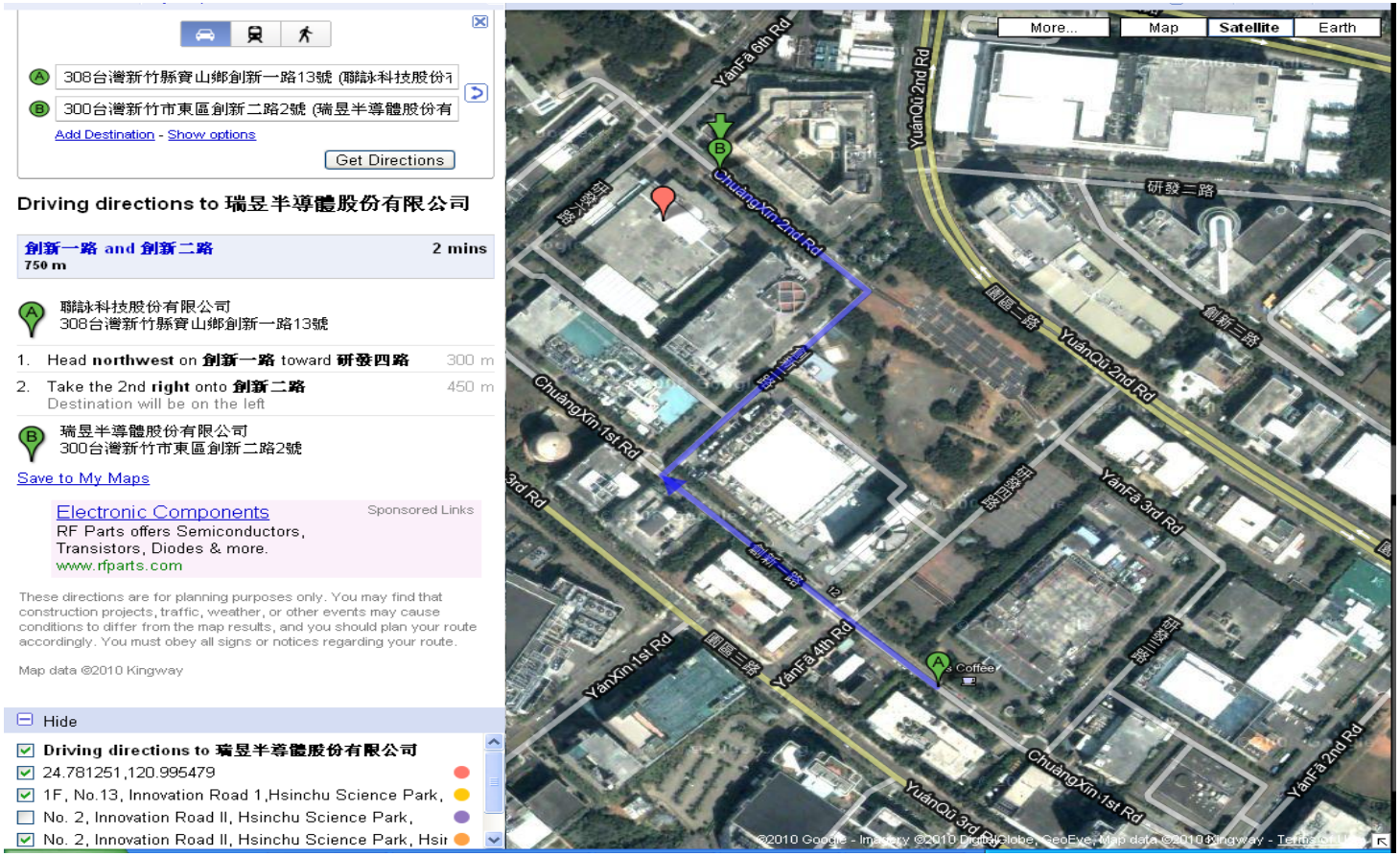


DNS Name	*.ab-inbev.com
DNS Name	web.pop-market.com
DNS Name	www.akliz.net
DNS Name	www.bank-yahav.co.il
DNS Name	www.bezecom.com
DNS Name	www.ccc.co.il
DNS Name	www.coldwatercreekthespa.com
DNS Name	www.directofficesupply.co.uk
DNS Name	www.itnet.co.il
DNS Name	www.melek-net.com
DNS Name	www.myhosting.com
DNS Name	www.paxfood.com
DNS Name	www.premiumwooddesigns.com
DNS Name	www.supportonline.co.il
DNS Name	www.yamaha-motor.com.uy
DNS Name	wyethnutrition.com.sg
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.4146.1.20)
Qualifier ID #1	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI	https://www.globalsign.com/repository/
Policy ID #2	(2.23.140.1.2.2)
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://secure.globalsign.com/cacert/cloudsslsha2g3.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp2.globalsign.com/cloudsslsha2g3
Fingerprints	
SHA1	1F 39 FA 54 9F CE 7C 0F 41 97 52 DB EF 67 13 3E 9D 11 3F 1B
MD5	FC 8D 53 2D 32 E4 BF 38 1F D9 55 8A 56 1B 42 C5

Compromised/Misbehaving CAs

- Famous case: false Microsoft ActiveX certificate issued by VeriSign in January 2001
- VeriSign Hacked, Successfully and Repeatedly, in 2010
  - VeriSign attacks were revealed in a quarterly U.S. Securities and Exchange Commission filing in October 2011
- March 2011: Attack on Commodo reseller, several fraudulent certificates were issued: mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com
  - Suggested that attack originated from Iranian IP address
  - http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
- August 29, 2011: news broke that DigiNotar, a Dutch CA, improperly issued a certificate for all Google domains to an external party
  - Claim: 250 certificates for an unknown number of domains were released
  - Iranian government spied on Iranian citizens' communications with Google email during the month of August 2011
- Stuxnet used the certificates of 2 Taiwanese CAs

Stuxnet Exploited 2 Taiwanese CA Keys



The TURKTRUST Story

- August 2011: TURKTRUST CA mistakenly issues two intermediate CA certs.
  - “CA: True” is just one bit in a regular certificate.
- *.google.com cert issued by the intermediate detected December 24th 2012.
- Cert revoked December 25th 2012.

Compelled Certificates

- Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL by Christopher Soghoian and Sid Stamm
  - http://files.cloudprivacy.net/ssl-mitm.pdf
- Compelled certificate: public/private key pair for *law enforcement* (MitM attacks on TLS) with CA certificate enabling private key to sign additional certificates
- Danger?

MitM Device using Compelled Certificates

PACKET FORENSICS VOLUME 1 • NO. 1 • 2009

Technical Details

Man-in-the-Middle Capabilities

Intercept any communication within Secure Socket Layer (SSL) or Transport Layer Security (TLS) sessions

All Packet Forensics targeting and policy capabilities can operate within the encrypted tunnel

Operational Configurations

In-line with hardware bypass / failsafe

Import any certificate / public key or generate your own for presentation

Availability

Available in firmware releases after August 31st, 2009 for all Packet Forensics platforms

Available under customization program

Contacts

Offices in Virginia and Arizona, USA

Headquarters

420 S Smith Rd
Tempe, AZ 85281
United States of America

Telephone & E-mail

Domestic US +1 (800) 807 6140
International +1 (757) 320 2002
salesteam@packetforensics.com

PACKET FORENSICS

HOW DOES IT WORK?

Deployment and Capabilities

Just as it sounds, engaging in a man-in-the-middle attack requires the interception device to be placed in-line between the parties to be intercepted at some point in the network. This could be at the subscribers' telecom operator or even on-premises, close to the subject. Packet Forensics' devices are designed to be inserted into and removed from busy networks without causing any noticeable interruption. Even the failure of a device due to power loss or other factors is mitigated by our hardware bypass fail-safe system. Once in place, devices have the capability to become a go-between for any TLS or SSL connections in addition to having access to all unprotected traffic. This allows you to conditionally intercept web, e-mail, VoIP and other traffic at-will, even while it remains protected inside an encrypted tunnel on the wire. All the same capabilities as other Packet Forensics products are still available, including the ability to extract pen/trap details only.

Technical Considerations: PKI

Using "man-in-the-middle" to intercept TLS or SSL is essentially an attack against the underlying Diffie-Hellman cryptographic key agreement protocol. To protect against such attacks, public key infrastructure ("PKI") is often used to authenticate one or more sides of the tunnel by exchanging certain keys in advance, usually out-of-band. This is meant to provide assurance that no one is acting as an intermediary. Secure web access (HTTP-S) is the best example of this, because when an unexpected key is encountered, a web browser can warn the subject and give them an opportunity to *accept* the key or *decline* the connection.

To use our product in this scenario, users have the ability to import a copy of any legitimate key they obtain (potentially by court order) or they can generate "look-alike" keys designed to give the subject a false sense of confidence in its authenticity.

Of course, this is only a concern for communications incorporating PKI. For most other protocols riding inside TLS or SSL tunnels—where no PKI is employed—interception happens seamlessly without any subscriber knowledge or involvement.

HOW CAN YOU USE IT?

Government Security

IP communications adoption dictates the need to examine encrypted traffic at-will, especially transiting government networks.

Investigations

Your investigative staff will likely collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VoIP encryption.

Product Testing and Evaluation

All network products should be tested diligently for phone-home capabilities with encryption.

PACKET FORENSICS

SMALL DEVICES. BIG OPPORTUNITIES.

INTRODUCING THE 5-SERIES

Packet Forensics 5-Series are the most flexible tactical surveillance devices in the world of IP networks. Designed for defense and (counter) intelligence applications, they are fully-embedded without moving parts and available in a variety of sizes, shapes and power footprints, all customized for the client. In under five minutes, they can be configured and installed in-line without knowledge of existing network topology. **Capabilities include:** Keyword, RADIUS, DHCP and **behavior-based** session identification; filtering, modification and injection of packets; compatibility with existing collection systems. With this modular platform, Packet Forensics creates **mission packages** based on customer requirements. Best of all, they're so cost effective, they're disposable--that means less risk to personnel.

Introduction

The 5-Series is a turnkey intercept solution in an appliance platform. Offering the most flexible approach to network surveillance and novel approaches to rapid deployment and stealthy reporting of captured data, the 5-Series devices are unmatched in the industry.

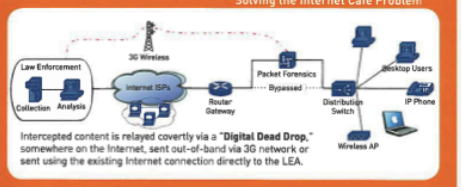
An attractive feature of the 5-Series is its ability to passively discover network topology--this allows an individual to deploy it with no prior knowledge of the target network. The device can be placed in-line and immediately act as a passive bridge while performing its mission. As intelligence is being gathered and the device has an understanding of the network, it uses its stealth reporting techniques to return captured information or accomplish a variety of other missions.

The 5-Series has no MAC address or IP address; it dynamically masquerades as the most appropriate host that sits topologically behind it. The 5-Series can be used to intercept and record matching sessions to internal flash-memory, or report them upstream using a variety of protocols. In the most hostile environments, this upstream reporting can be accomplished using a technique that makes the 5-Series' presence undetectable using standard network security methods.

The Internet Cafe

The 5-Series is an ideal solution to the "Internet Cafe Problem." Quick deployment and remote control minimize personnel risk and maximize collection capabilities. Small footprint and minimal power requirements make installation easy.

Solving the Internet Cafe Problem



Intercepted content is relayed covertly via a **"Digital Dead Drop,"** somewhere on the Internet, sent out-of-band via 3G network or sent using the existing Internet connection directly to the LEA.

Key Advantages

- **Customized** mission packages
- Small form-factor, solid-state (as small as 4 square inches)
- No moving parts, highly reliable
- Battery, PoE or wired power
- Hardware bypass, fail-safe
- Tamper detection, fail-secure
- Up to Gb/sec throughput
- Deployable with **no knowledge of target network topology**
- Supports **stealth upstream reporting** (practically **undetectable**)
- **"Digital Dead Drop"** delivery
- Triggers intercepts based on **keywords, RADIUS, DHCP, behavior** or other subject criteria
- **Probe** and **Mediation** capabilities
- Performs **dialed digit extraction**
- Packet **modification, injection** and **replay** capabilities
- Packet Forensics software stack and PeerTalk™ technology
- Advanced firmware-update keeps software up-to-date

Statistics

- From EFF SSL Observatory, 2010 / 2011
- CA statistics
  - 1,482 CA root keys trusted with Microsoft or Mozilla software
  - 1,167 distinct Issuer strings
  - 651 organizations
- Size of the SSLiverse
  - 16.2M IP addresses were listening on port 443
  - 11.3M started an SSL handshake
  - 4.3+M used valid cert chains
  - 1.5+M distinct valid leaves

Trust Roots for Entity Validation

- Trust roots do not scale to the world
  - Monopoly model: single root of trust
    - DNSSEC, BGPSEC / RPKI
    - Problem: world cannot agree on who controls root of trust
  - Oligarchy model: numerous roots of trust
    - SSL/TLS PKI: over 1000 trusted root CA certificates
    - Problems
      - Weakest-link security: single compromised entity enables man-in-the-middle attack
      - Not trusting some trust roots results in unverifiable entities
- Current implementation of both models lacks efficient update / maintenance of roots of trust

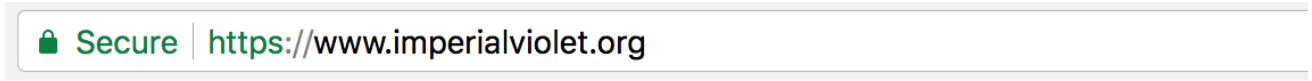
Approaches to Improve TLS

- The “Let’s Encrypt” CA
- Extended Validation (EV) certificates
- HTTP Strict Transport Security (HSTS)
- Certificate Revocation List (CRL)
- Online Certificate Status Protocol (OCSP) and OCSP Stapling
- Short-lived certificates
- Perspectives, Convergence
- Trust Assertions for Certificate Keys (TACK)
- DNS-Based Authentication of Named Entities (DANE)
- HTTP Public-Key Pinning (HPKP)
- …
- Recent approach: *log to make certificates publicly visible*
  - Google: Certificate Transparency
  - EFF: Sovereign Keys
  - CMU / ETH Zurich: AKI, ARPKI, PoliCert

- Goal: provide free certificates based on automated domain validation, issuance, and renewal
- Beta phase began in September 2015 and ended in April 2016, now fully operational
- More than 100 million certificates issued as of June 2017
- Relatively short-lived certificates: 90 days
- Many sponsors: Mozilla, EFF, Facebook, Chrome, Internet Society, Cisco, Akamai, …
- Based on ACME: Automated Certificate Management Environment
- Attack using BGP prefix hijacking: Bamboozling Certificate Authorities with BGP, Birge-Lee et al., USENIX Security, August 2018.

Levels of Trust

- No SSL/TLS



- Domain Validation (DV)

- Organization Validation (OV) / “High Assurance”

- Extended Validation (EV)

HTTP Strict Transport Security (HSTS)

- Goal: allows servers to declare that their clients should only use HTTPS (for a specified period)
- Prevents some “downgrade”, “SSL stripping”, and “session hijacking” attacks
- Implemented with an HTTPS header. Example:
  - `Strict-Transport-Security: max-age=31536000`
- Browsers should automatically redirect to HTTPS or display a warning message.

HTTP Public-Key Pinning (HPKP)

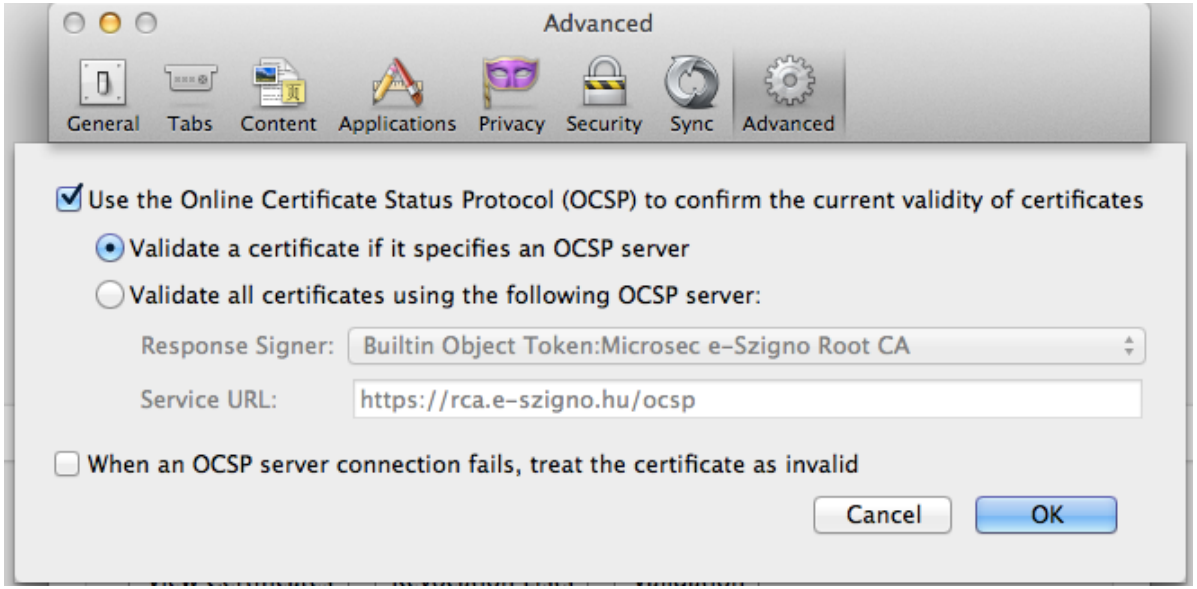
- The server sends a set of public keys to the client. These keys should be the only ones used for connections to this domain.
- Implemented with an HTTPS header. Example:
  - `Public-Key-Pins: max-age=2592000;`
  - `pin-sha256="…";`
  - `pin-sha256="…";`
  - `report-uri="…";`

Certificate Revocation

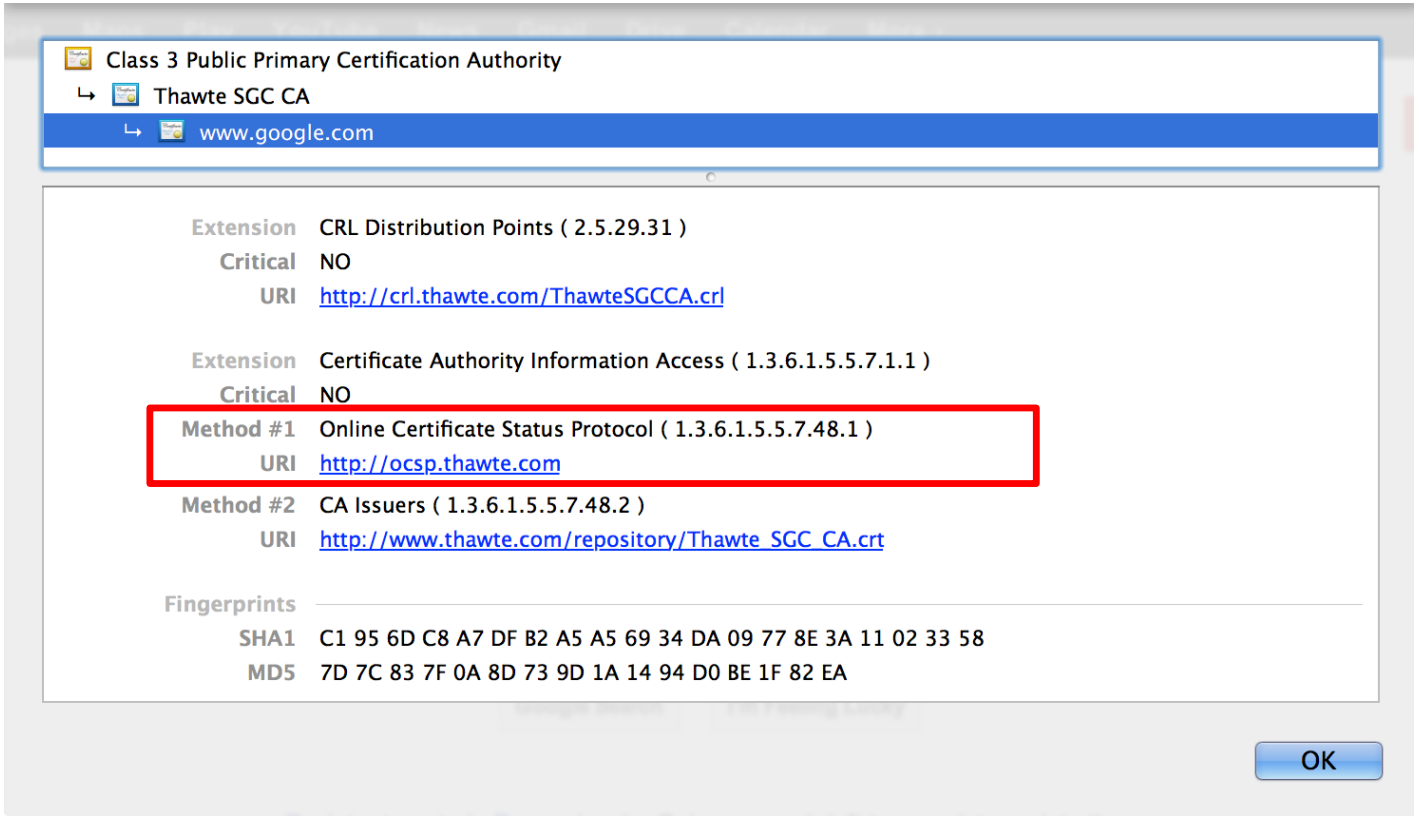
- Certificate revocation is a mechanism to invalidate certificates
  - After a private key is disclosed
  - Trusted employee / administrator leaves corporation
  - Certificate expiration time is usually chosen too long (to reduce effort for updating certificates)
- CA periodically publishes Certificate Revocation List (CRL)
  - Delta CRLs only contain changes
  - What to do if we miss CRL update?
- What is general problem with revocation?
  - CAP theorem (Consistency, Availability, tolerance to Partition): impossible to achieve all 3, must select one to sacrifice!

OCSP

- Online Certificate Status Protocol (OCSP) to verify certificate status, ensure certificate is valid and has not been revoked
  - Certificate contains OCSP responder
- Problems and issues?



OCSP Information in Certificate



OCSP Performance Issues

- OCSP servers can be slow!
- From “The Case for Prefetching and Prevalidating TLS Server Certificates” by Stark et al. @ NDSS 2012:

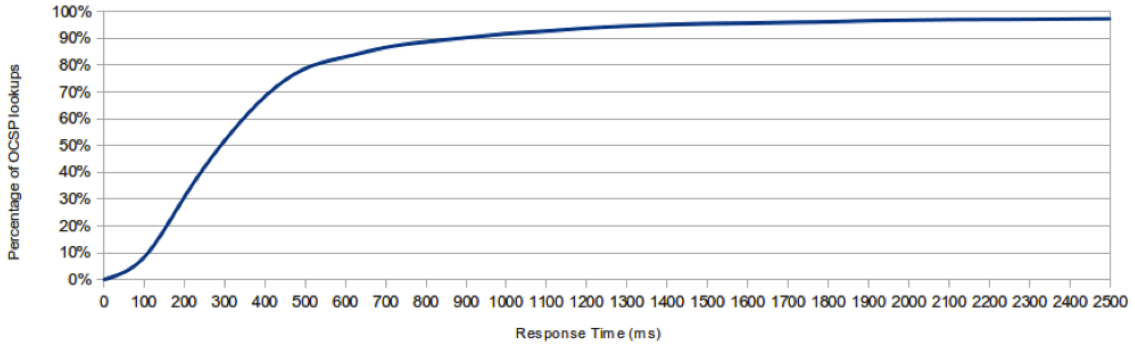


Figure 3. Cumulative distribution of OCSP lookup response times.

OCSP responder	Number of lookups	Response time			
		Median (ms)	Min (ms)	Max (ms)	Standard deviation
http://EVSecure-ocsp.verisign.com	938	167	25	7235	610.76
http://ocsp.digicert.com	1372	252	12	12303	759.64
http://ocsp.godaddy.com/	741	101	20	4832	515.53
http://ocsp.thawte.com	4209	564	10	12376	976.09
http://ocsp.verisign.com	1389	279	21	10209	743.53

Table 2. Response times of OCSP responders.

OCSP Issues

- “Optimistic” treatment of OCSP failure information
  - Some browsers ignore bogus OCSP responses
  - All browsers avoid treating OCSP errors as fatal
- After Comodo and Diginotar breaches, browser vendors relied on browser patches (SW update) to remove compromised certs instead of relying on revocation!
- OCSP stapling (web server provides OCSP information) would help with privacy and latency
  - But: multi-stapling needed for intermediate CAs
  - However: responses may be too large to fit in initial TCP congestion window and still require multiple round-trips
- OCSP can leak browsing information outside of private browsing mode as Microsoft’s CryptoAPI and Apple’s Security Framework API cache OCSP responses in OS

DANE

- DNS-Based Authentication of Named Entities
- Goal: authenticate TLS servers without a certificate authority (CA)
- Idea: use DNSSEC to bind certificates to names
- Use cases:
  - *CA constraints:* clients should only accept certs by these CAs
  - *Cert constraints:* clients should only accept this cert
  - *Trust anchor assertion:* clients should use domain-provided trust anchor to validate certificates for that domain

DANE (cont.)

- Can prevent DigiNotar's attack on Google who can express:
  - DigiNotar is *not* one of Google's trusted CAs, or
  - Enclosed cert is the *only* legitimate cert

- *Issue:* Heavy reliance on DNSSEC

Certificate Transparency (CT)

- Certificate Transparency will make all public end-entity TLS certificates public knowledge, and will hold CAs publicly accountable for all certificates they issue
- And it will do so without introducing another trusted third party

(CT slides credit: Emilia Kasper)

CT: Log Design

A CT log is an append-only list of certificates

- The log server
  - Verifies the certificate chain
    - CA attribution for certificate misissuance
    - Spam control
- Periodically append all new certificates to the append-only log and sign that list
- Publish all updates of the signed list of certificates (“the log”) to the world

CT: Log Properties

A CT log is not a “Super CA”

- The log does not testify to the “goodness” of certificates; it merely notes their presence
- The log is public: everyone can inspect all the certificates
- The log is untrusted: since the log is signed, the fact that everyone sees the same list of certificates is cryptographically verifiable

CT: Data Structure

- Merkle hash tree

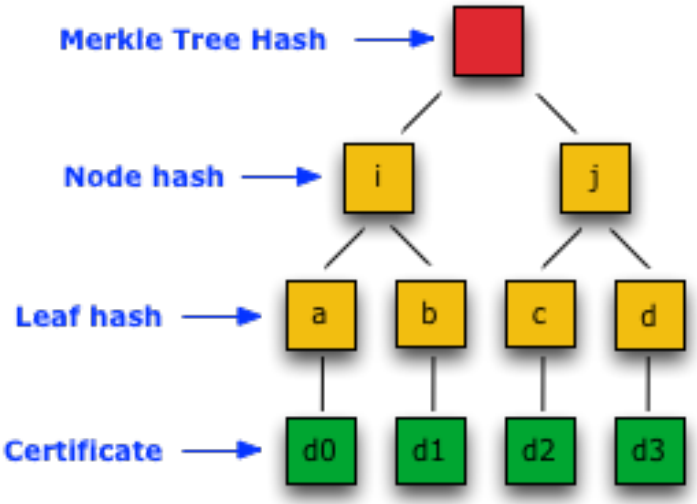


Figure 1

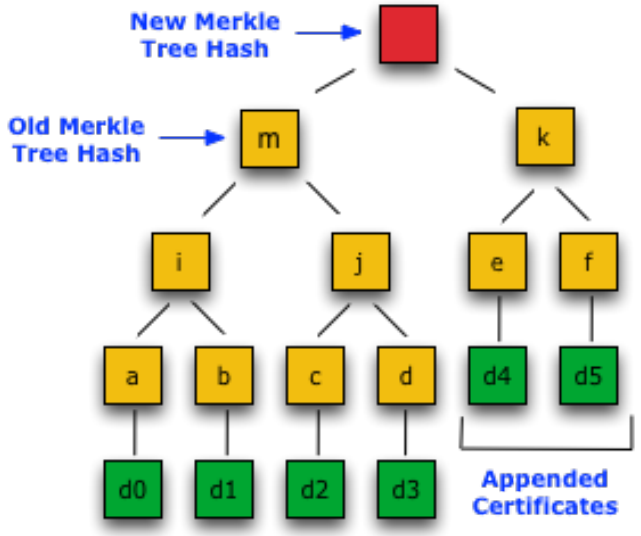
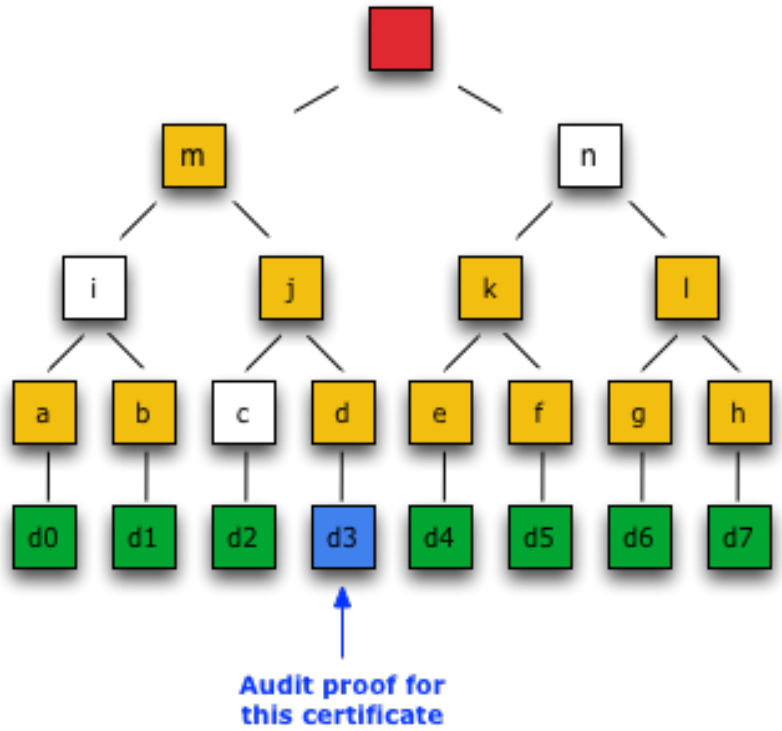


Figure 2

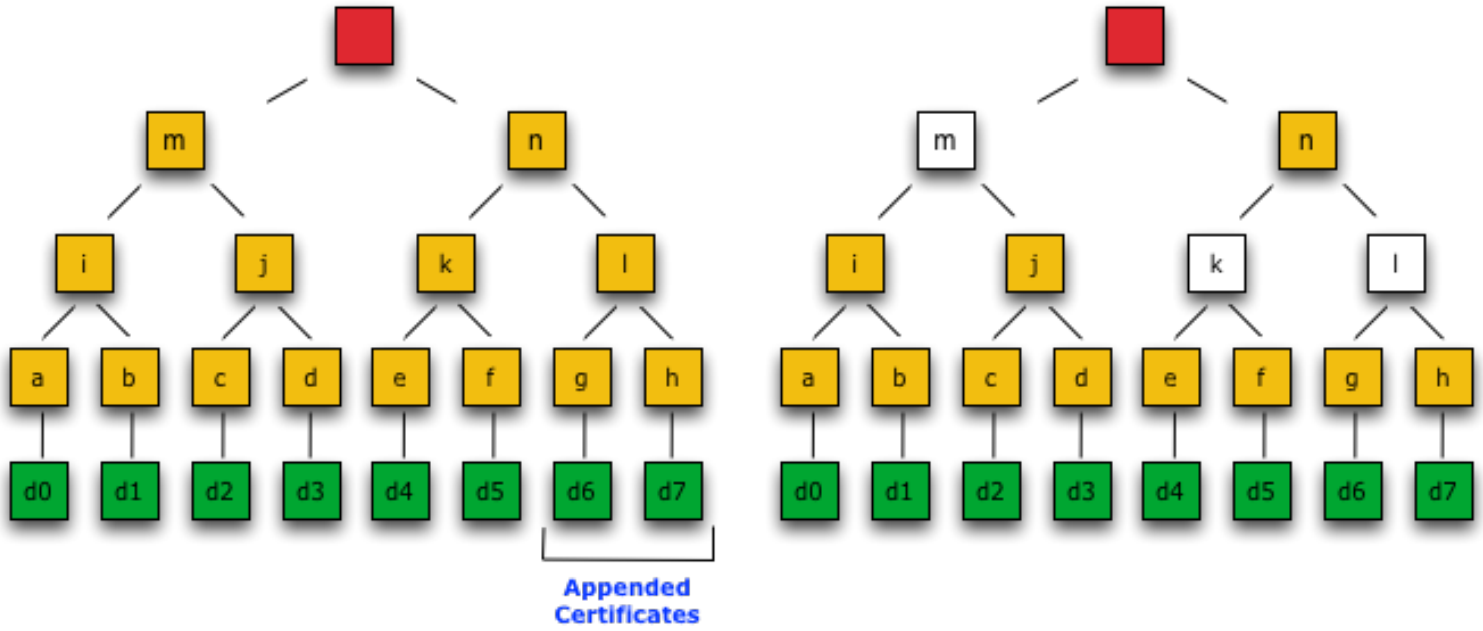
CT: Proof of Inclusion

- Proving that a certificate appears in the log is easy with a Merkle tree:



CT: Proof of Consistency

- Proving that the log is append-only is also easy with a Merkle tree:



TLS with Certificate Transparency

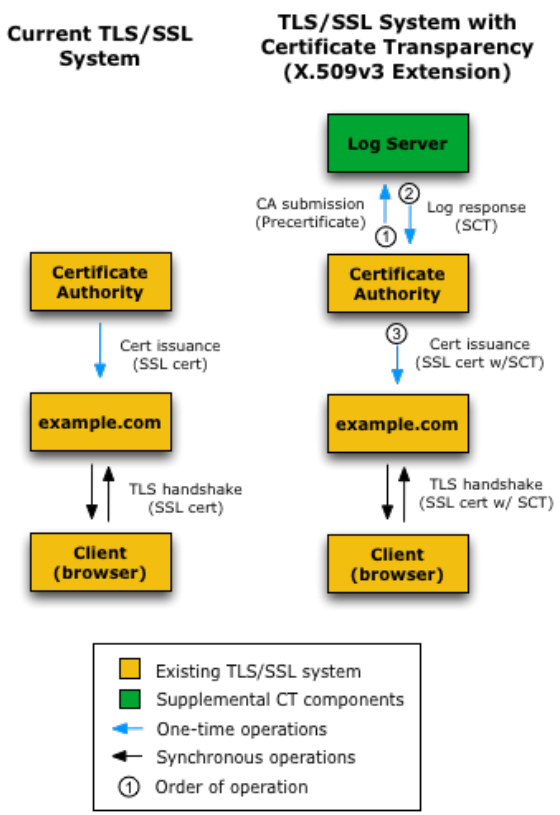


Figure 1

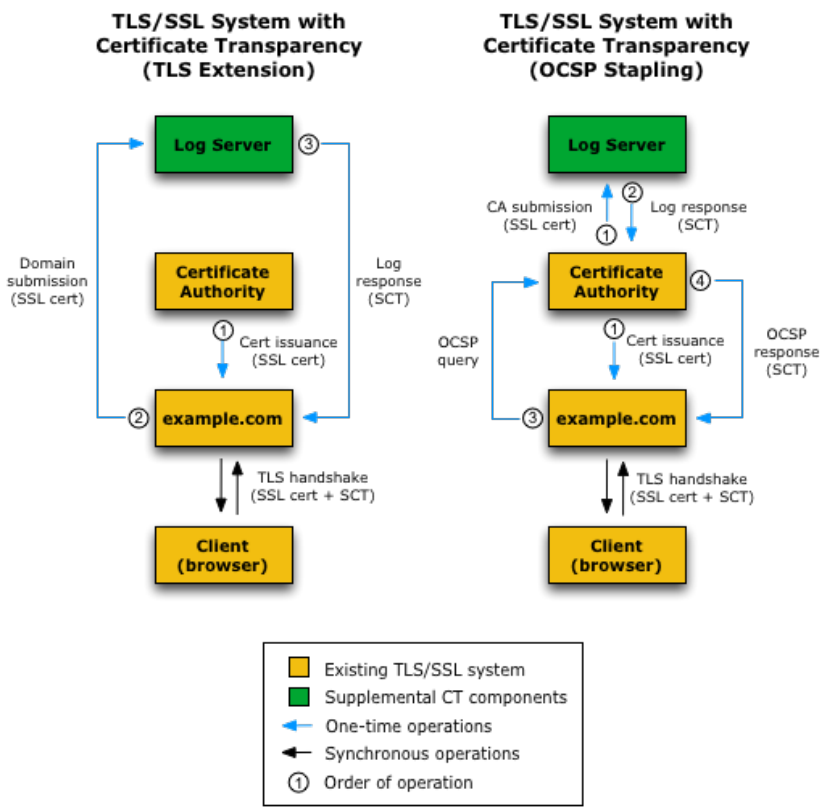
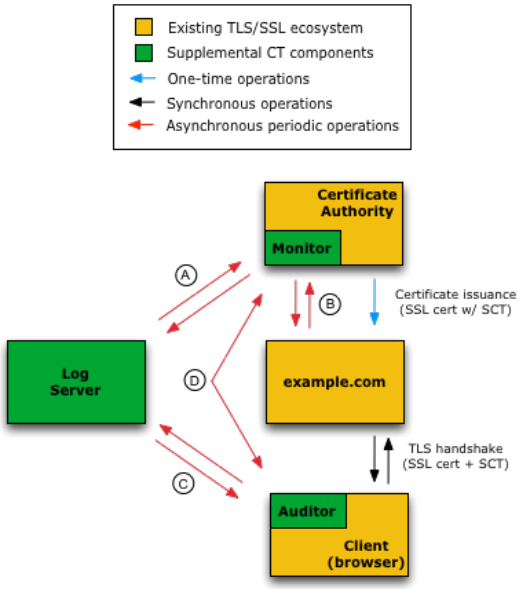


Figure 2

Who participates in the protocol?



(A) Monitors watch logs for suspicious certs and verify that all logged certs are visible.

(B) Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.

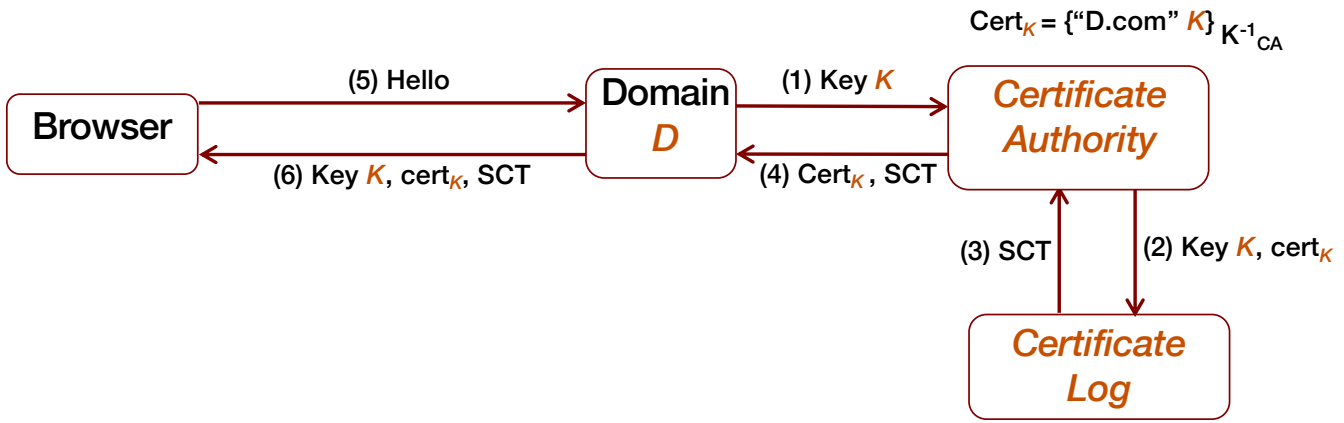
(C) Auditors verify that logs are behaving properly; they can also verify that a particular cert has been logged.

(D) Monitors and auditors exchange information about logs to help detect forked or branched logs.

Figure 3

CT: Summary

- Certificate logs
  - Append-only logs (similar to a timestamping server)
  - Merkle hash tree (MHT) to implement log
  - Entry = certificate
  - Periodically appends new entries and signs the root (Signed Tree Head, STH)
- Upon receiving a certificate chain from domain or CA
  - Log verifies the certificate
  - Log issues Signed Certificate Timestamp (SCT)
    - Promise to add the new certificate to the MHT



Security of CT

- How CT improves security
  - Browser would require SCT for opening connection
  - Browser contacts log server to ensure that certificate is listed in log
- Consequence
  - Attack certificate would have to be listed in public log
  - Attacks become publicly known → deterrence
- Advantages
  - CT is fully operational today
  - No change to domain's web server required
- Disadvantages
  - MitM attacks can still proceed (but can be detected externally)
  - Browser still needs to contact Log eventually to verify that certificate is listed in log
  - Current CT does not support revocation
  - Malicious Log server can add bogus certificate
  - Management of list of trusted log servers can introduce a kill switch

Lessons Learned / Challenges

- Cannot tolerate additional latency of contacting additional server during SSL / TLS handshake
- A key has to be immediately usable and verifiable after initial registration
- Users shouldn't be bothered in the decision process if certificate is legitimate
- Need to cover entire certificate life cycle, including revocation, handling stolen and lost certificates

Conclusions

- Secure crypto and secure protocols are insufficient!
  - Numerous failure possibilities, e.g., CA compromise
  - User interface security and certificate management are critically important!
- Developing a secure real-world protocol is very challenging