CS 578: CYBER-SECURITY

PART I: ECOSYSTEMS AND APPLICATIONS – MORE

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL
Secure AI Systems Lab

ANNOUNCEMENT

- Call for actions
  - Homework 1 due today
  - Homework 2 will be out tomorrow
  - In-class presentation sign-up
    - Choose the paper your team will present by the end of this week

CERTIFICATE TRANSPARENCY (CT)

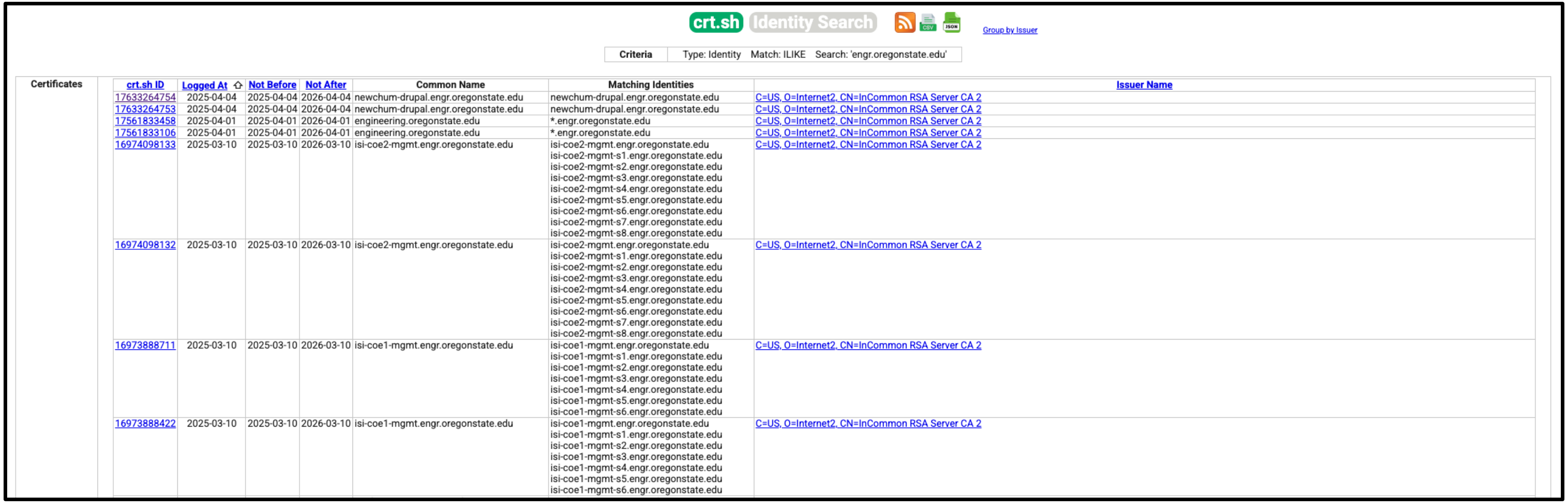
CERTIFICATE TRANSPARENCY

- A system that
  - Makes the issues of certificates publicly auditable and verifiable
  - Is append-only (certificate issuance logs cannot be removed)
- CT prevents
  - Enhanced compliance (through the increased transparency and accountability)
  - Early detection of mis-used certificates (faster revocation, …)
  - Protection against rogue CAs

[1] https://crt.sh, Search with 'engr.oregonstate.edu'

CERTIFICATE TRANSPARENCY

- A system that
  - Makes the issues of certificates publicly auditable and verifiable
  - Is append-only (certificate issuance logs cannot be removed)



crt.sh Identity Search

Group by Issuer

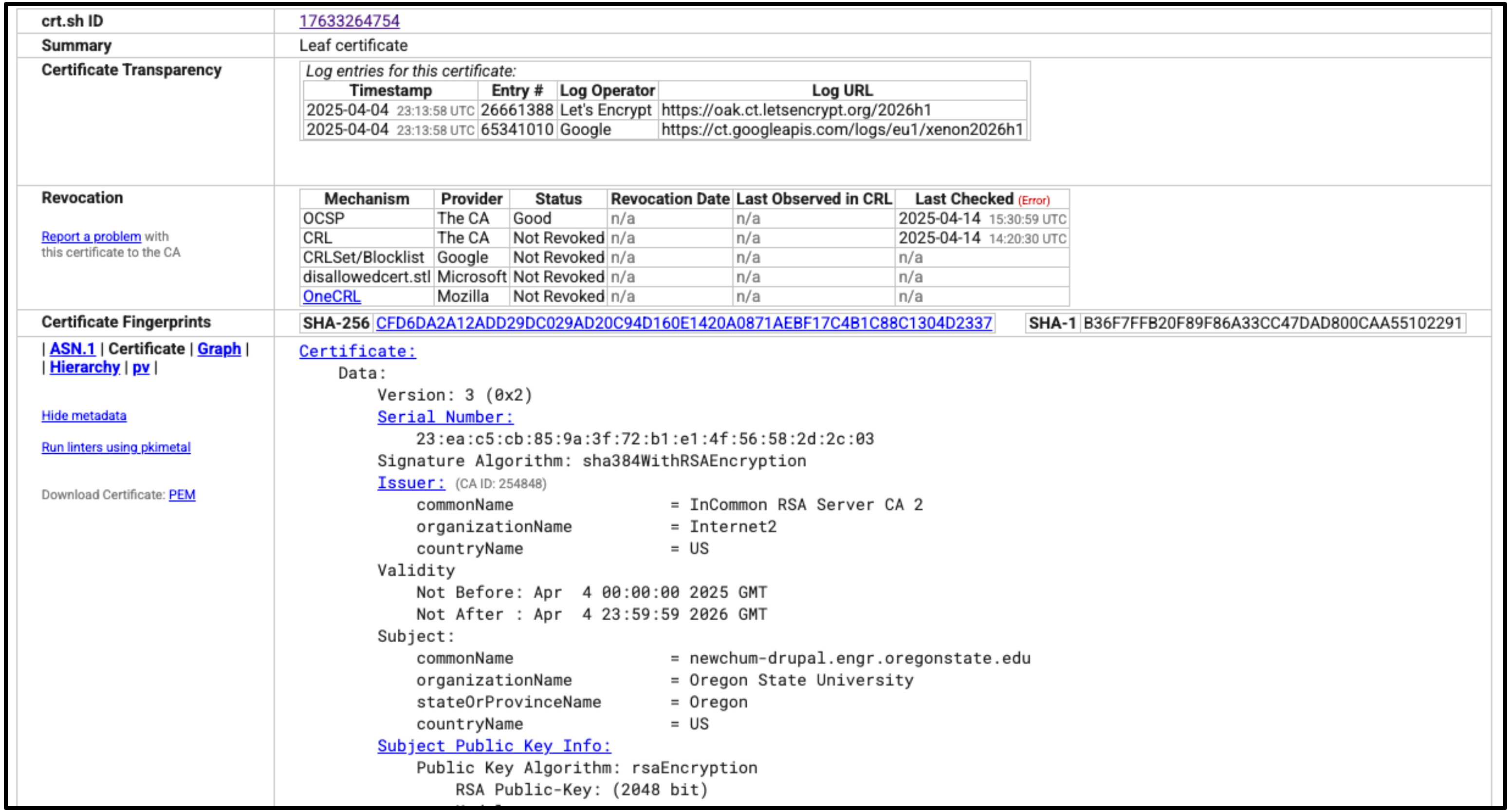
Criteria	Type: Identity Match: ILIKE Search: 'engr.oregonstate.edu'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
17633264754	2025-04-04	2025-04-04	2026-04-04	newchum-drupal.engr.oregonstate.edu	newchum-drupal.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
17633264753	2025-04-04	2025-04-04	2026-04-04	newchum-drupal.engr.oregonstate.edu	newchum-drupal.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
17561833458	2025-04-01	2025-04-01	2026-04-01	engineering.oregonstate.edu	*.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
17561833106	2025-04-01	2025-04-01	2026-04-01	engineering.oregonstate.edu	*.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
16974098133	2025-03-10	2025-03-10	2026-03-10	isi-coe2-mgmt.engr.oregonstate.edu	isi-coe2-mgmt.engr.oregonstate.edu isi-coe2-mgmt-s1.engr.oregonstate.edu isi-coe2-mgmt-s2.engr.oregonstate.edu isi-coe2-mgmt-s3.engr.oregonstate.edu isi-coe2-mgmt-s4.engr.oregonstate.edu isi-coe2-mgmt-s5.engr.oregonstate.edu isi-coe2-mgmt-s6.engr.oregonstate.edu isi-coe2-mgmt-s7.engr.oregonstate.edu isi-coe2-mgmt-s8.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
16974098132	2025-03-10	2025-03-10	2026-03-10	isi-coe2-mgmt.engr.oregonstate.edu	isi-coe2-mgmt.engr.oregonstate.edu isi-coe2-mgmt-s1.engr.oregonstate.edu isi-coe2-mgmt-s2.engr.oregonstate.edu isi-coe2-mgmt-s3.engr.oregonstate.edu isi-coe2-mgmt-s4.engr.oregonstate.edu isi-coe2-mgmt-s5.engr.oregonstate.edu isi-coe2-mgmt-s6.engr.oregonstate.edu isi-coe2-mgmt-s7.engr.oregonstate.edu isi-coe2-mgmt-s8.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
16973888711	2025-03-10	2025-03-10	2026-03-10	isi-coe1-mgmt.engr.oregonstate.edu	isi-coe1-mgmt.engr.oregonstate.edu isi-coe1-mgmt-s1.engr.oregonstate.edu isi-coe1-mgmt-s2.engr.oregonstate.edu isi-coe1-mgmt-s3.engr.oregonstate.edu isi-coe1-mgmt-s4.engr.oregonstate.edu isi-coe1-mgmt-s5.engr.oregonstate.edu isi-coe1-mgmt-s6.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2
16973888422	2025-03-10	2025-03-10	2026-03-10	isi-coe1-mgmt.engr.oregonstate.edu	isi-coe1-mgmt.engr.oregonstate.edu isi-coe1-mgmt-s1.engr.oregonstate.edu isi-coe1-mgmt-s2.engr.oregonstate.edu isi-coe1-mgmt-s3.engr.oregonstate.edu isi-coe1-mgmt-s4.engr.oregonstate.edu isi-coe1-mgmt-s5.engr.oregonstate.edu isi-coe1-mgmt-s6.engr.oregonstate.edu	C=US, O=Internet2, CN=InCommon RSA Server CA 2

[1] https://crt.sh, Search with 'engr.oregonstate.edu'

CERTIFICATE TRANSPARENCY



crt.sh ID	17633264754
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2025-04-04 23:13:58 UTC	26661388	Let's Encrypt	https://oak.ct.letsencrypt.org/2026h1
2025-04-04 23:13:58 UTC	65341010	Google	https://ct.googleapis.com/logs/eu1/xenon2026h1

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Good	n/a	n/a	2025-04-14 15:30:59 UTC
CRL	The CA	Not Revoked	n/a	n/a	2025-04-14 14:20:30 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	CFD6DA2A12ADD29DC029AD20C94D160E1420A0871AEBF17C4B1C88C1304D2337	**SHA-1**	B36F7FFB20F89F86A33CC47DAD800CAA55102291

| **ASN.1** | Certificate | **Graph** |
| **Hierarchy** | **pv** |

Hide metadata

Run linters using pkimetal

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            23:ea:c5:cb:85:9a:3f:72:b1:e1:4f:56:58:2d:2c:03
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: (CA ID: 254848)
            commonName                = InCommon RSA Server CA 2
            organizationName          = Internet2
            countryName               = US
        Validity
            Not Before: Apr  4 00:00:00 2025 GMT
            Not After : Apr  4 23:59:59 2026 GMT
        Subject:
            commonName                = newchum-drupal.engr.oregonstate.edu
            organizationName          = Oregon State University
            stateOrProvinceName       = Oregon
            countryName               = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

[1] https://crt.sh, Search with 'engr.oregonstate.edu'

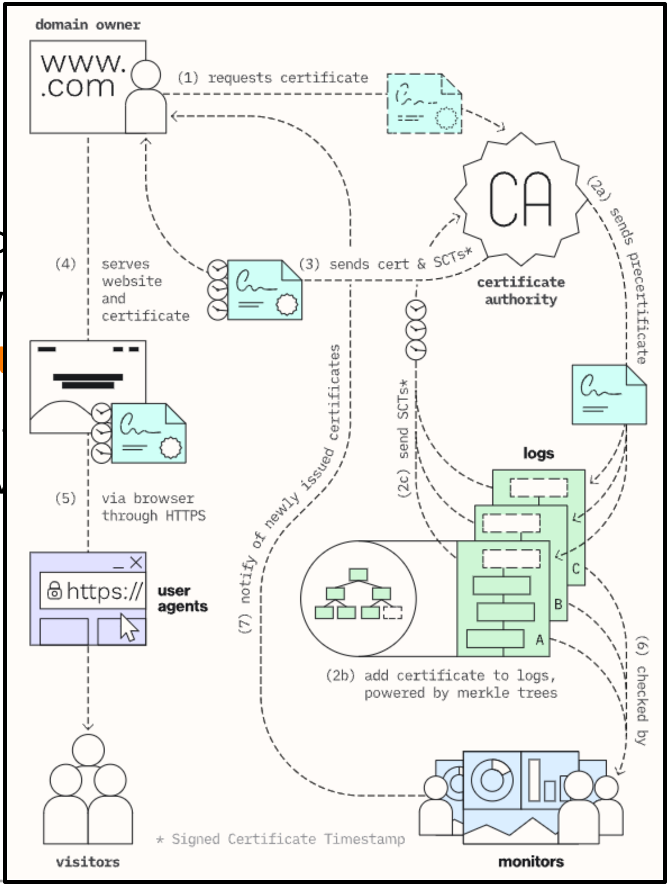
CERTIFICATE TRANSPARENCY

- Certificate issue with CT
  - Request a certificate to CA
  - CA issues a pre-certificate
  - CA also sends the pre-certificate to the transparency logs
  - Pre-certificate(s) are appended to the transparency logs
  - The transparency returns a signed certificate timestamp (SCT)
  - CA sends a certificate to the requester that contains the SCT
  - Users when accessing the requester's website can validate the certificate

[1] https://certificate.transparency.dev/howctworks/

CERTIFICATE TRANSPARENCY

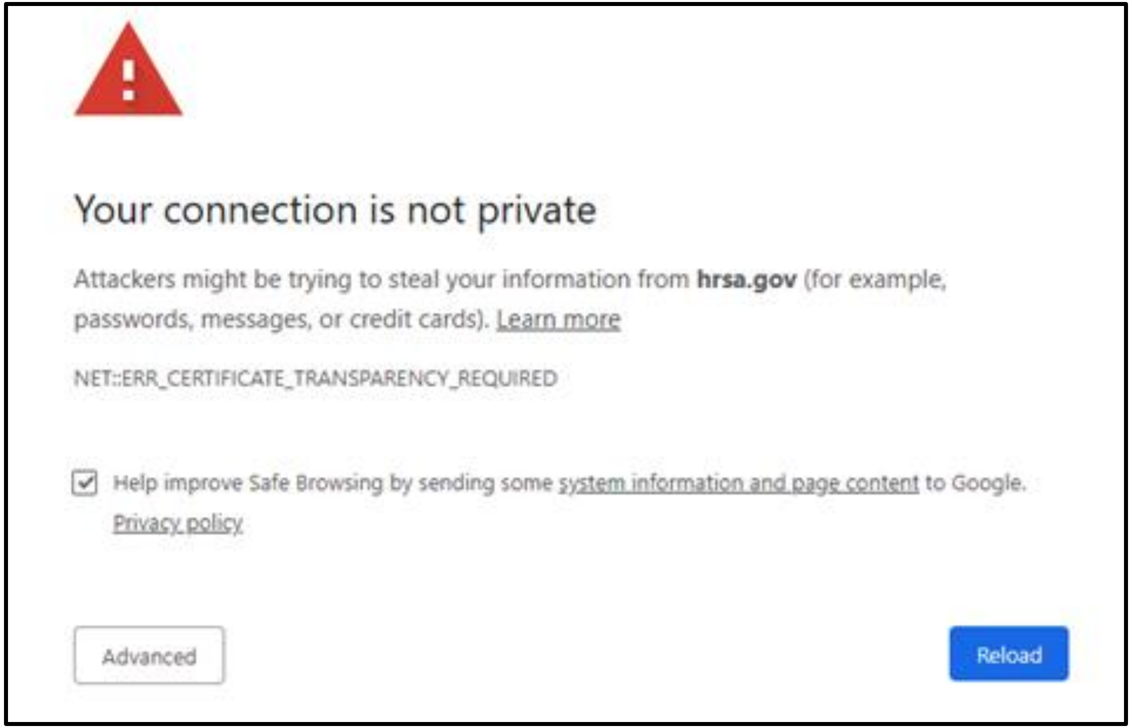
- Certificate issue with CT
  - Request a certificate to CA
  - CA issues a pre-certificate
  - CA also sends the pre-certificate to the transparenc
  - Pre-certificate(s) are appended to the transparency
  - The transparency returns a signed certificate timest
  - CA sends a certificate to the requester that contain
  - Users when accessing the requester’s website can v



[1]https://certificate.transparency.dev/howctworks/

CERTIFICATE TRANSPARENCY

- What if the certificate is not in the CT chain
  - Most browsers will show warnings
  - It’s your risk from now on



Your connection is not private

Attackers might be trying to steal your information from **hrsa.gov** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

☑ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Domain name systems (DNS)

DOMAIN NAME SYSTEM

- A hierarchical and distributed name service that
  - Offers a naming system for computers, services, and other resources on the Internet
  - Associates various information (e.g., IPv4 addr.) to domain names

- “Records”: the associations
  - Each record has a time-to-live (TTL), e.g., in cache
  - It supports different types, e.g.,
    - A/AAAA record: name to IPv4/IPv6 (such as sanghyun-hong.com to 123.456.789.012)
    - CNAME record: name to canonical name (myspace.* to facebook.com/alice)
    - MX record: main exchanger records
    - NS record: nameserver records
    - TXT record: text record (e.g., _github-pages-challenge… to c578365nsjd…)

DOMAIN NAME SYSTEM – CONT'D

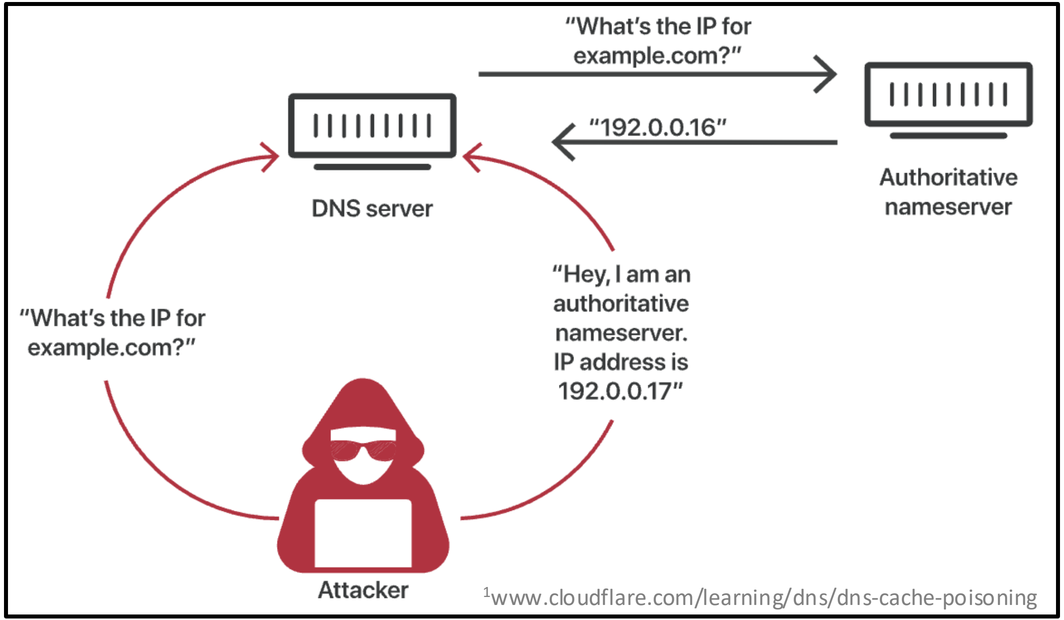
- How does it work?
  - You enter www.sanghyun-hong.com
  - Your browser searches its, OS, or router caches
    - If the value (e.g., IPv4 of the website) is found, then access it -> Done
  - Your browser access to DNS resolver
  - The DNS resolver finds out and accesses
    - The name servers for the TLD (.com)
    - The authoritative name servers for the domain (sanghyun-hong.com)
    - The domain name server for my website (www.sanghyun-hong.com)
    - The IPv4 (or IPv6) address of my website
    - Returns the IP address
  - Your browser accesses the IPv4 and receives my webpages

DOMAIN NAME SYSTEM – CONT'D

- How does it work?
  - DNS packets use UDP by default
  - DNS can use TCP packets as a fallback
  - Port #53

DOMAIN NAME SYSTEM – VULNERABILITIES

- DNS cache poisoning/spoofing
  - An adversary may impersonate the DNS nameservers
  - If impersonate the TLD server, ask the IP of sanghyun-hong.com
  - If impersonate the authoritative nameserver, returns a fake IP


"What's the IP for example.com?"
"192.0.0.16"
DNS server
Authoritative nameserver
"What's the IP for example.com?"
"Hey, I am an authoritative nameserver. IP address is 192.0.0.17"
Attacker

[1]www.cloudflare.com/learning/dns/dns-cache-poisoning

DOMAIN NAME SYSTEM – VULNERABILITIES

- DNS cache poisoning/spoofing
  - An adversary may impersonate the DNS nameservers
  - If impersonate the TLD server, ask the IP of sanghyun-hong.com
  - If impersonate the authoritative nameserver, returns a fake IP

- Once poisoned
  - User requests to sanghyun-hong.com
  - The DNS server (resolver) will reply with the fake IP
  - The fake IP is highly likely to be associated with malicious website

[1] www.cloudflare.com/learning/dns/dns-cache-poisoning

DOMAIN NAME SYSTEMS SECURITY EXTENSIONS (DNSSEC)

DNSSEC

- A security extension that
  - Secures data exchanged in the DNS in networks
  - Adds cryptographic signatures to existing DNS records
  - Stores digital certificates with “records” (e.g., A, AAAA, CNAME, etc.)

- DNSSEC requires a few more DNS records
  - RRSIG record: contains cryptographic signatures
  - DNSKEY record: contains a public key for signing signatures
  - DS record: contains the hash of a DNSKEY record
  - NSEC (NSECC3): explicit denial-of-existence of a DNS record
  - CDNSKEY (CDS): a child zone that requests updates to DS records in the parent

DNSSEC – How it works?

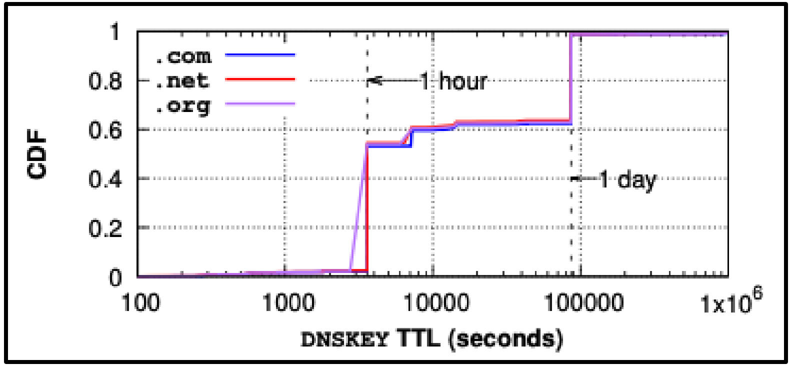
- DNS Zone owner
  - Generates a private (key signing key) and public key (zone signing key)
  - The private key is used to sign all DNS records within the zone
  - Each signed DNS record is accompanied by an RRSIG record (containing the signature)
  - The public key(s) are published in the DNS zone

- User / client
  - The DNS resolver retrieves the signed DNS records and their RRSIG records
  - The resolver retrieves the public key from the DNS zone
  - The resolver uses the public key to validate the signature on the DNS record
  - The resolver runs this validation through the DNS hierarchy
  - Upon completion of the validation, the resolver will send the records

DNSSEC – DEPLOYMENT AND MANAGEMENT

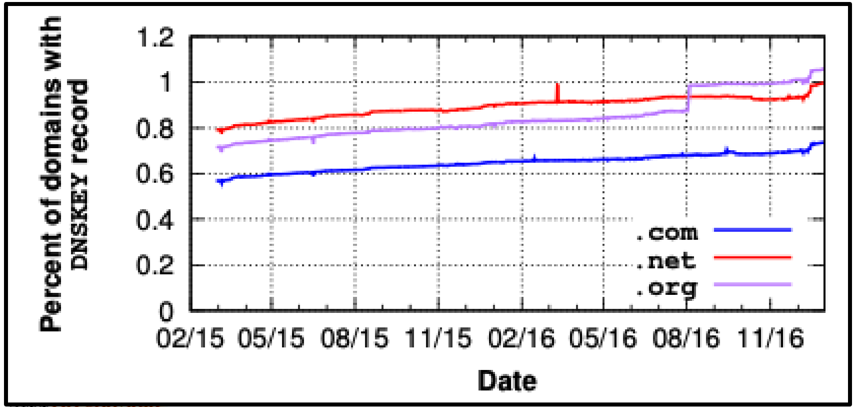
- Research questions
  - How widely is DNSSEC deployed?
  - How often are DNSSEC records correctly published and managed?
  - How are DNSSEC cryptographic keys managed and maintained?

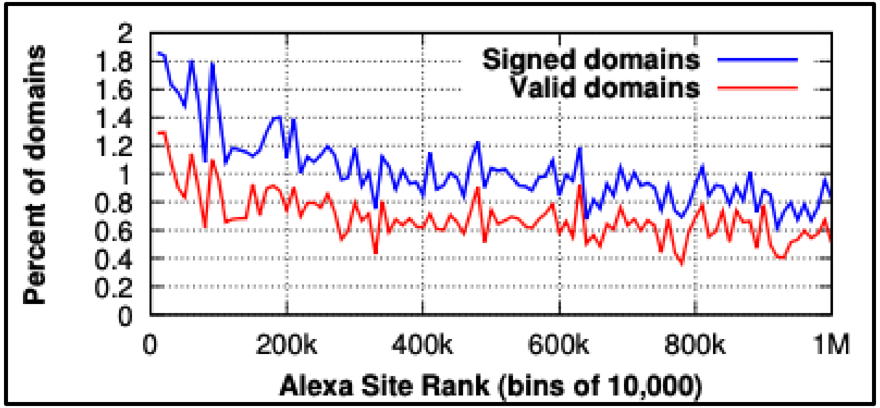
- Dataset
  - .com, .net and .org TLDs (150M domains)
    - 64% of the Alexa Top-1M
    - 75% of the Alexa Top-1K
  - Daily dataset : Mar 1, 2015 – Dec 31, 2016
  - Hourly dataset: Sep 29, 2016 – Dec 31, 2016



DNSSEC – Deployment and management

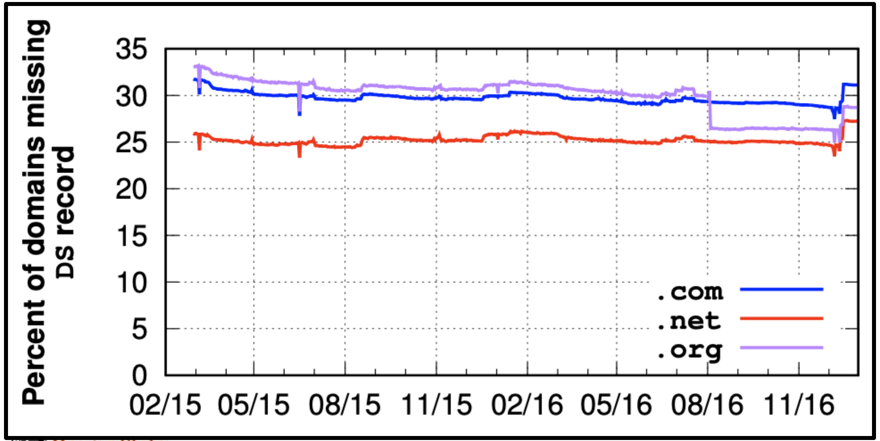
- Prevalence
  - DNSSEC deployment is rare (0.6 – 1.0% of domains, .com and .org respectively)
  - The deployment increases over time (0.75 to 1.0%)
  - There are spikes due to actions by a few authoritative name servers (.org)
  - But this means that a few authoritative name servers are responsible for the dep.
  - Popular websites are more likely to sign their domains

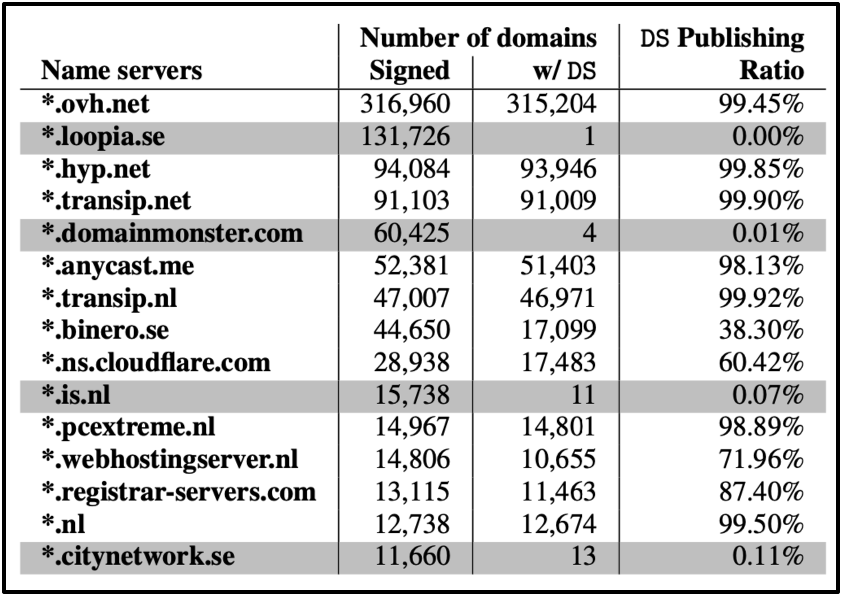




DNSSEC – DEPLOYMENT AND MANAGEMENT

- Missing records
  - 28 – 32% domains do not have a DS record
  - 15 authoritative name servers cover 83% of domains collected
  - 4 authoritative name servers fail to publish DS records for nearly all of their domains
  - Drop in .org is due to hyp.net publishing 11k signed domains, and spike was caused by Domain Monster, 37k new domains





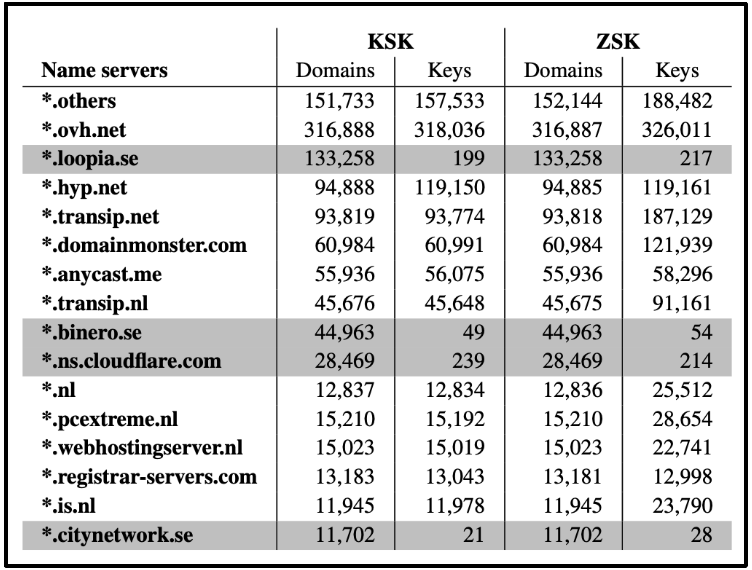
Name servers	Number of domains Signed	w/ DS	DS Publishing Ratio
*.ovh.net	316,960	315,204	99.45%
*.loopia.se	131,726	1	0.00%
*.hyp.net	94,084	93,946	99.85%
*.transip.net	91,103	91,009	99.90%
*.domainmonster.com	60,425	4	0.01%
*.anycast.me	52,381	51,403	98.13%
*.transip.nl	47,007	46,971	99.92%
*.binero.se	44,650	17,099	38.30%
*.ns.cloudflare.com	28,938	17,483	60.42%
*.is.nl	15,738	11	0.07%
*.pcextreme.nl	14,967	14,801	98.89%
*.webhostingserver.nl	14,806	10,655	71.96%
*.registrar-servers.com	13,115	11,463	87.40%
*.nl	12,738	12,674	99.50%
*.citynetwork.se	11,660	13	0.11%

DNSSEC – Deployment and management

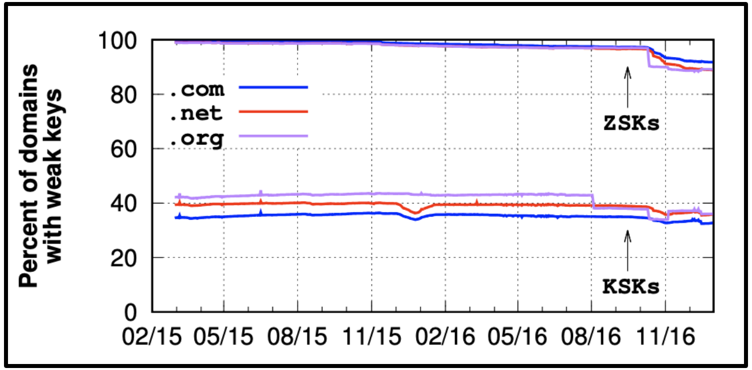
- Incorrect records
  - 99.5% of domains, where RRISG validation for SOA records fails, are valid
  - 99.9% of DS records are valid

DNSSEC – Deployment and management

- Key management
  - Two domains share a privacy key?
    - 99.95% of keys are used for one domain
    - 0.04% private keys and 0.05% public keys are shared by more than one domain
    - One private and public keys are shared over 132k domains
  - Weak keys?
    - < 1024-bit RSA keys are weak
    - < 2048-bit DSA keys are weak



Name servers	KSK Domains	KSK Keys	ZSK Domains	ZSK Keys
*.others	151,733	157,533	152,144	188,482
*.ovh.net	316,888	318,036	316,887	326,011
*.loopia.se	133,258	199	133,258	217
*.hyp.net	94,888	119,150	94,885	119,161
*.transip.net	93,819	93,774	93,818	187,129
*.domainmonster.com	60,984	60,991	60,984	121,939
*.anycast.me	55,936	56,075	55,936	58,296
*.transip.nl	45,676	45,648	45,675	91,161
*.binero.se	44,963	49	44,963	54
*.ns.cloudflare.com	28,469	239	28,469	214
*.nl	12,837	12,834	12,836	25,512
*.pcextreme.nl	15,210	15,192	15,210	28,654
*.webhostingserver.nl	15,023	15,019	15,023	22,741
*.registrar-servers.com	13,183	13,043	13,181	12,998
*.is.nl	11,945	11,978	11,945	23,790
*.citynetwork.se	11,702	21	11,702	28



Thank You!

Sanghyun Hong

https://secure-ai.systems/courses/Sec-Grad/current

Oregon State University

SAIL

Secure AI Systems Lab