Stale TLS Certificates

Investigating Precarious Third-Party Access to Valid TLS Keys

Zane Ma (he/him)
Oregon State University
2024.10.08

Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric*, Michael Bailey, Angelos Keromytis, Fabian Monrose, Manos Antonakakis

Georgia Institute of Technology *Stanford University

Public-key crypto

TLS Certificate

Key challenge: linking cryptographic identity (public-key) with semantic identity

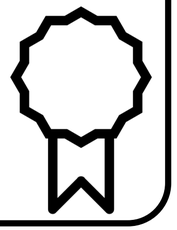
TLS certificate = cached attestation

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…



TLS Certificate

Stale TLS certificates

Stale TLS Certificate

New TLS Certificate

Stale certificates arise from **certificate invalidation events**: changes to attested information (e.g., subject / issuer info) while certificate is still valid

Stale TLS certificates

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…

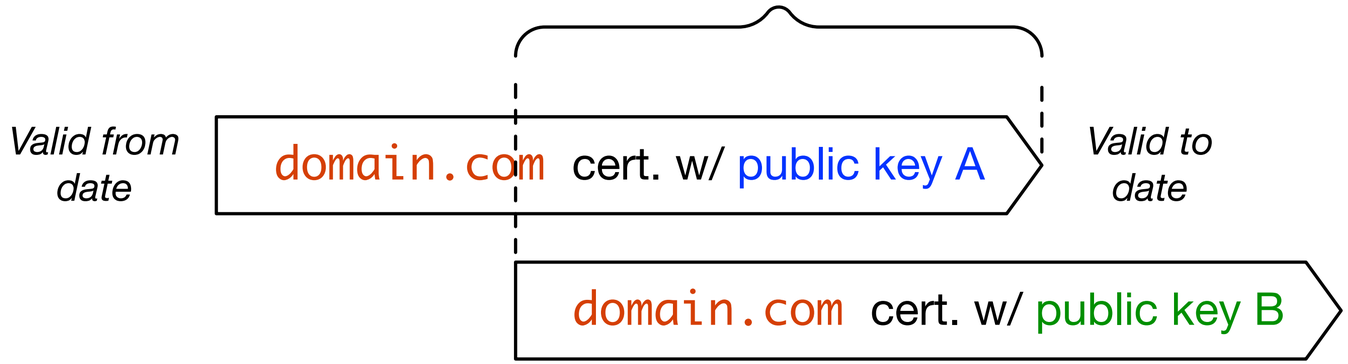
Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 00c946d6e746f1…

Validity: 2023-10-25 to 2024-11-24

Issuer Signature: 19574503953e…

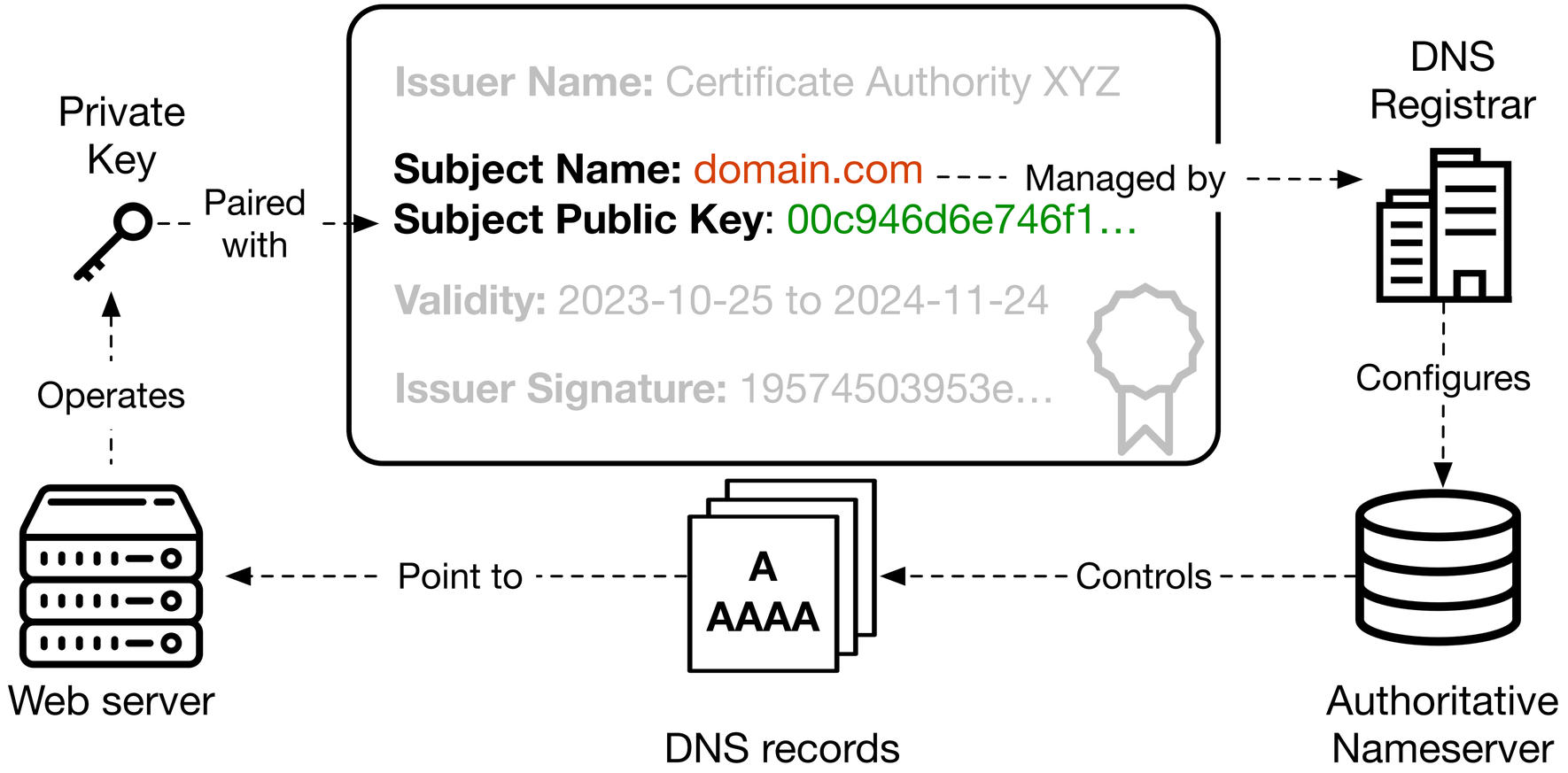
Stale TLS Certificate **Stale period** *New TLS Certificate*



Certificate Information Taxonomy

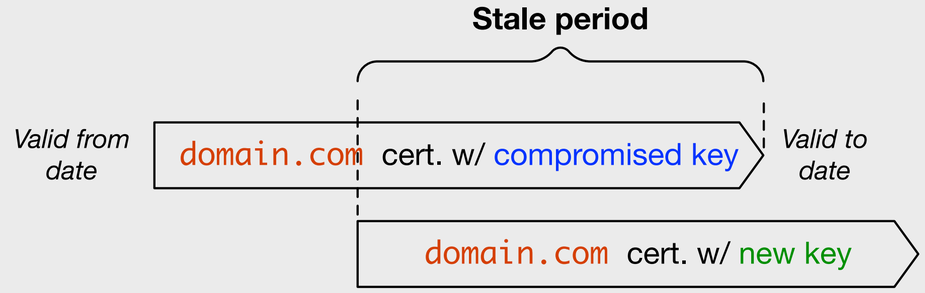
Information category	Description	Relevant fields
Subscriber authentication	Subscriber identifiers: domain + cryptographic keys	Subject Name, SAN, Subj. Public Key, Subj. Key ID
Key authorization	Permissions + constraints on key utilization	Basic Constraints, Key Usage, EKU
Issuer information	Details of CA that issued certificate	Issuer Name, Auth. Key ID, Signature, CRL Dist. Points, Auth. Info Access, Cert. Policy
Certificate metada	Meta-info about certificate itself	Serial #, Precert, Poison, SCTs

Domain-to-key operational gap

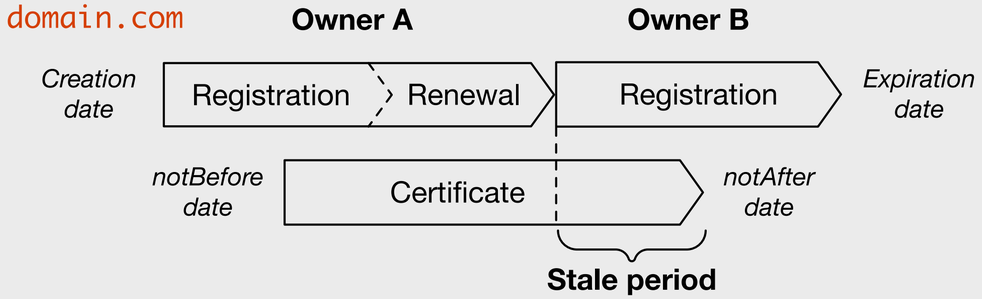


Third-party access to valid TLS keys

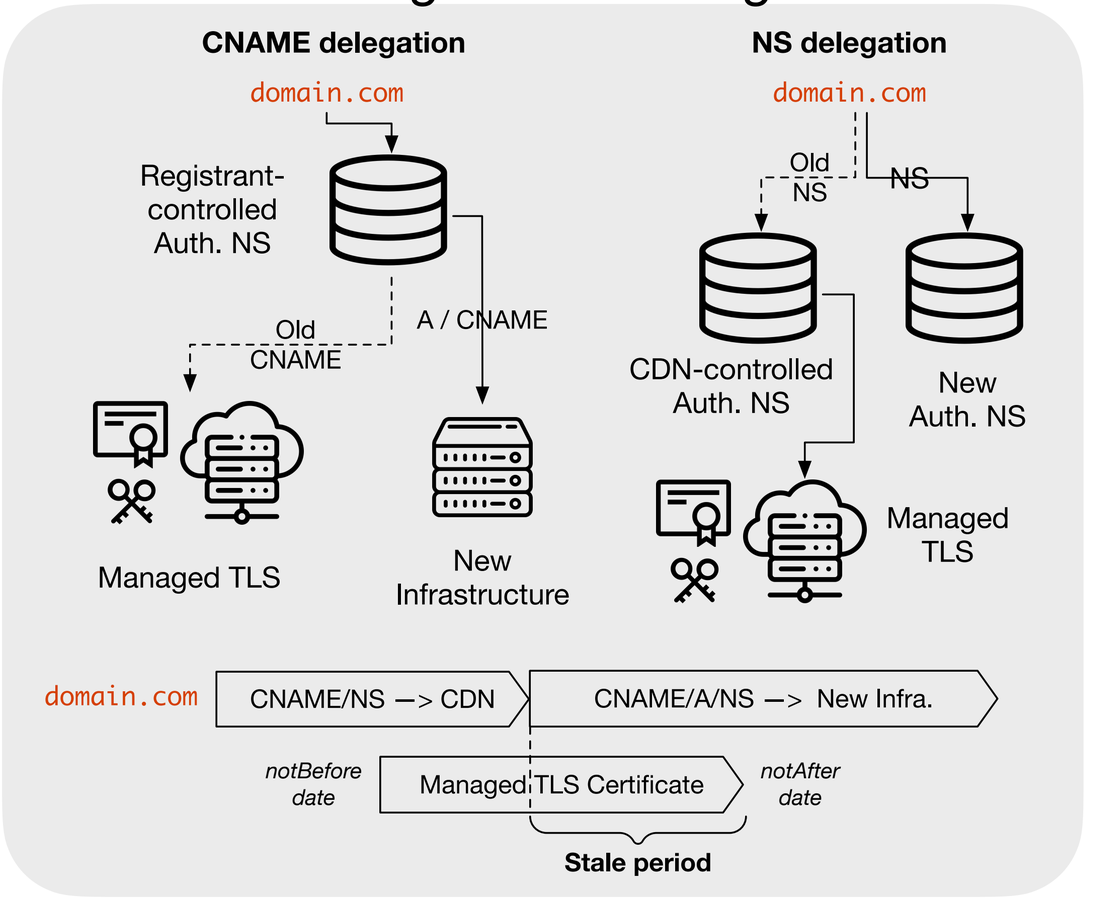
Compromised key change



Domain owner change



Managed TLS change



Revocation to the rescue?

Web browsers

Chrome has CRLsets primarily for “emergency situations”

Firefox OCSP checking fails open
OCSP Must-Staple fails closed, but low adoption

No revocation checking for most leaf certificate revocation

Non-browser TLS clients

openSSL, curl, API libraries, email servers, messaging clients

OpenSSL Cryptography and SSL/TLS Toolkit

curl://

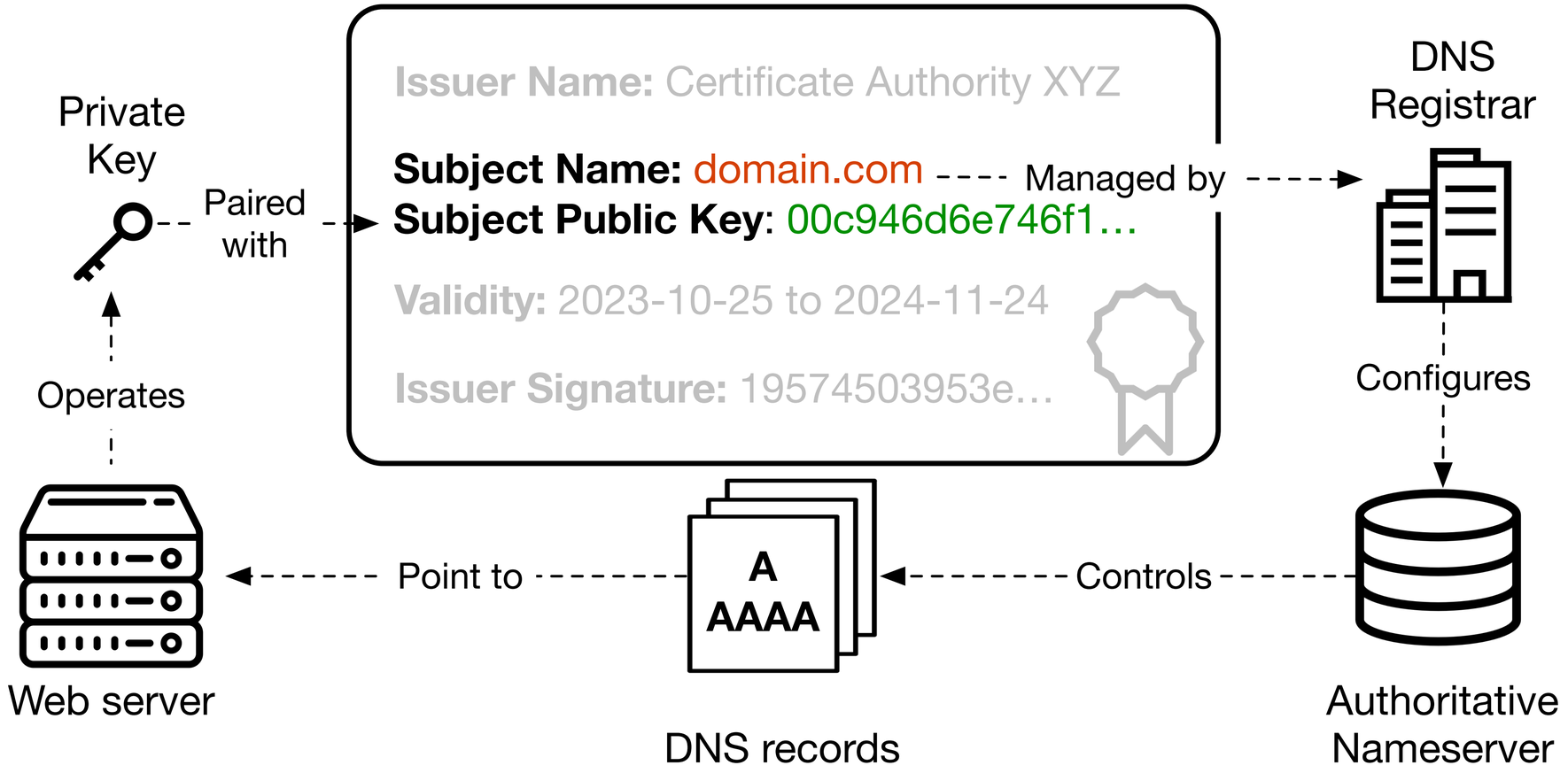
OkHttp **LibreSSL** **GnuTLS**

Mbed TLS **BoringSSL**

Minimal-to-no revocation checking

Revocation is sparse and unreliable

Domain-to-key operational gap



Internet-wide staleness

5B TLS certificates

4B WHOIS records

27B DNS records

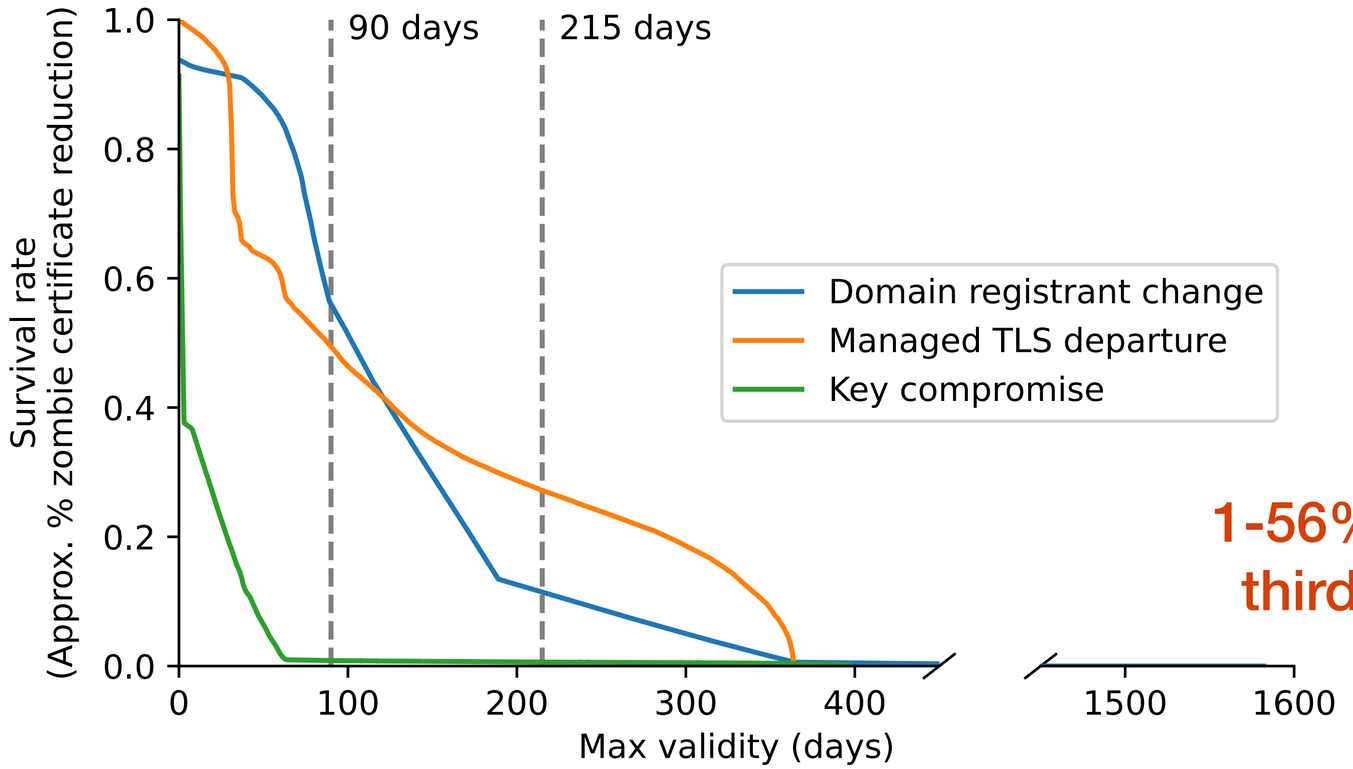
31M Revocations

Third-party staleness	Date range	# Certs / day	# FQDNs / day	#e2LD / day
Key compromise	2021-2023	493	787	347
Domain owner change	2013-2021	2,593	2,807	1,214
Managed TLS change	2022	9,495	18,833	7,722

Lower bound: 4.5M total 2LDs susceptible since 2013

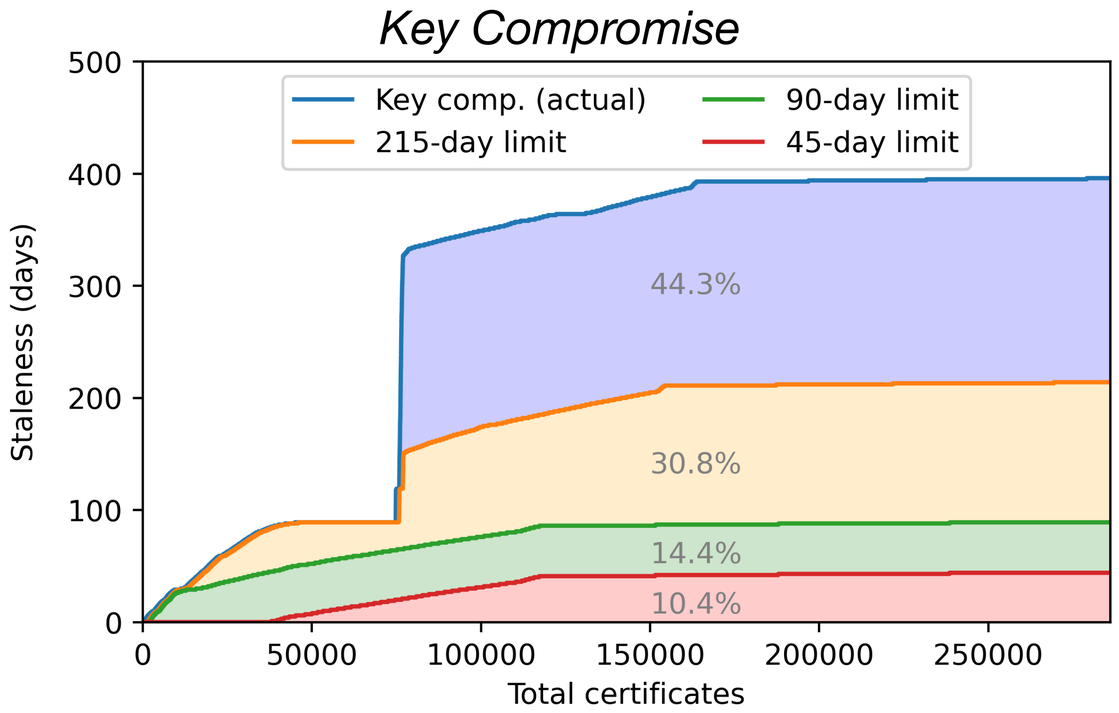
What can we do about it?

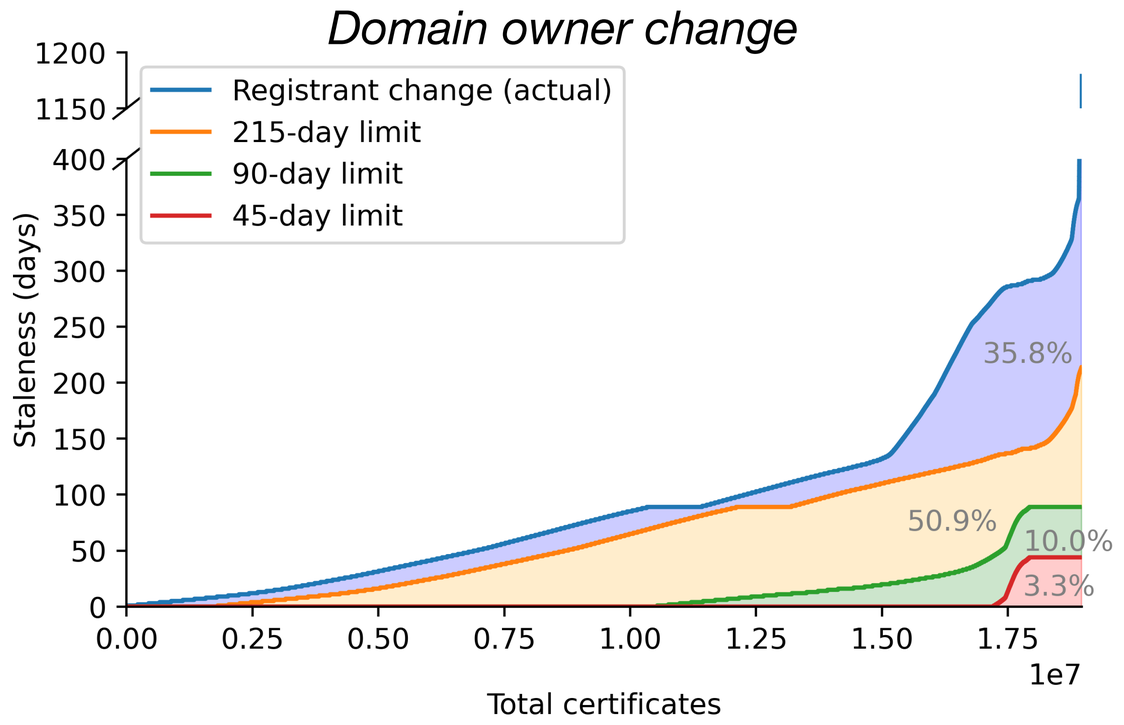
- Revocation is largely ineffective, and (unsurprisingly) poorly utilized
- Caching problem: reduce certificate lifetimes



90-day limit =
1-56% reduction in stale third-party certificates

Shortening certificate lifetimes





90-day limit =
75% decrease in time of third-party access to valid TLS keys

Takeaways for CA/Browser Forum

- # of stale third-party certificates is growing (4M domains and counting)! More third-parties are gaining precarious access to valid TLS keys
  - % HTTPS adoption plateauing, but total # of HTTPS websites is growing
  - Increasing dynamicity of the web
- Solutions?
  - Practical: decrease certificate lifetimes
  - Practical - hard: make revocation work (been trying for years)
  - Idealistic: move keys operationally closer to names (e.g., DANE)

Stale TLS Certificates

Investigating Precarious Third-Party Access to Valid TLS Keys

Zane Ma (he/him)
Oregon State University
2024.10.08

Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric*, Michael Bailey, Angelos Keromytis, Fabian Monrose, Manos Antonakakis

Georgia Institute of Technology *Stanford University