OOTB.NET

# Long Live Short-Lived Certificates!

## Updates on Public Key Infrastructure

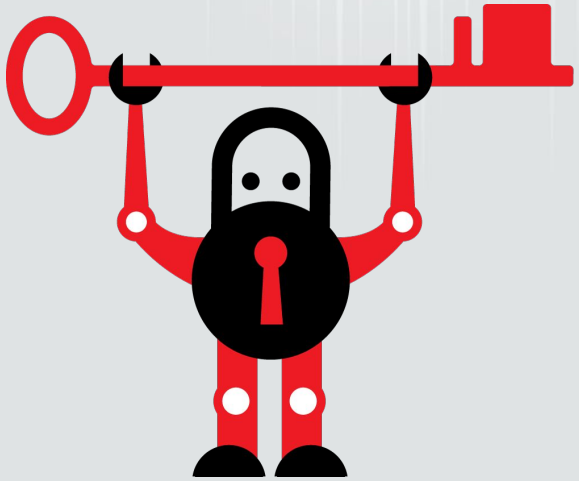
By Alexis Hancock
Director of Engineering @ the Electronic Frontier Foundation

Out of The Box, Bangkok
20 - 21 August 2025

# Why Am I Talking Right Now?

## Encrypting the Web is my “Thing”


- I manage the Certbot project. A client that uses the ACME protocol.
- The ACME (Automated Certificate Management Environment) protocol (RFC 8555) assists in automating TLS (Transport Layer Security) certificates for web servers.
- Certbot uses ACME to accomplish setting up TLS certificates through an easy to use interface.
- 5.3M installations maintaining 29 million certs for 42 million domains



# Jargon/Terms

## I apologize for the alphabet soup


- CA = Certificate Authority (issues certificates)
- TLS = Transport Layer Security (protocol for securing data in transit)
- HTTPS = Hypertext Transfer Protocol (Secure)
- Root Store = Usually a storage mechanism on the OS or Browser level that contains a list of all trusted CAs for that system
    - All browsers have a Root Store Program
- CT = Certificate Transparency (Publicly available & auditable information on issued certificates)
- OCSP = Online Certificate Status Protocol (real time certificate status checks)
- CRL = Certificate Revocation List (list of revoked certificates)
- CA/B = Certificate Authority and Browser forum

# Short Timeline of Related Events for Certificate Lifetimes


August 2011 - DigiNotar

↓

November 2011 - Google deploys Perfect Forward Secrecy

↓

November 2015 - Let's Encrypt Launches (90 day FREE certificates)

↓

April 2025 - 47 Day Certificates in CA/B Baselines for TLS

↓

January 2025 - Six Day and IP Address Certificate Options in 2025

# Diginotar Incident


June 2011 - Compromise detected via Audit

July 2011 - Rogue *.google.com certificate issued

Iran MITM attack

More rogue certificates issued 11th-20th.

July 27 - OCSP Request for rogue *.google.com

August 2011 - *.google.com revoked

September 2011 - Diginotar files for bankruptcy

# Why Are Short-Lived Certificates a Good Thing?


- If a certificate's private key is compromised, that compromise can't last as long.
- Shorter life spans for the certificates, automation is encouraged.
  - Which facilitates robust security of web servers (especially @ scale).
- Certificate revocation is historically flaky and at times unreliable or slow.
  - Lifetimes 10 days and under *prevent the need to invoke the revocation process* and deal with *continued usage of a compromised key*.
  - While CRLs are better, this approach helps to avoid them during a security incident, allowing Incident Response to possibly “skip a step” while triaging.

# Concerns


- How short is too short?
- Way more certificates than usual for CT Logs to keep track of.
- More certificates for system admins to keep track of.
- Legacy systems potentially not being able to keep up with requirements.

Short answer: Automation helps!

# How Could Have Diginotar Went Differently?


June 2011 - Intermediate CA key compromise detected via audit

July 2011 - Rogue *.google.com certificate issued Attackers would have about 6 days to act

Iran MITM attack This campaign would have been short or not have happened at all

More rogue certificates issued 11th-20th. Targets could have been limited by time constraint because certificates would have been useless

Ongoing Attack Ends - Incident Response continues…

July 27 - OCSP Request for rogue *.google.com

More requests to OCSP show the expanse of compromise

August 2011 *.google.com revoked The manual nature of revocation and longer lived certificates impacted the ability to wrangle and revoke these certificates.

September 2011 - Diginotar files for bankruptcy

# How Could Have Diginotar Went Differently?


> Short key compromise times don't only allow for better triage but also helps provide the ability to give customers a shorter scope of impact. Possibly preserving reputation.

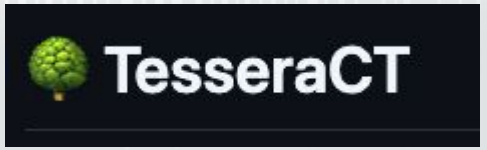
> Modern TLS and automation allows for another way to take inventory of what is open on your network, legacy systems you have, and the ability to use tools like CT logs to measure scope and impact of compromise.

# Short-Lived Certificates and CT Logs


CT Logs are becoming more resilient then they used to. However, challenges still exist.

Older storage formats caused fickle logs and poor reliability

New implementations allow for better storage mechanisms and higher uptimes.

# Proactive Protection and CT Logs


> CT Logs can help locate forgotten or neglected services

> Monitor phishing attacks with suspicious domains and track campaigns

> Monitor third party vendors and development partners that access to your systems

# ACME Renewal Information API


ARI is available with Let's Encrypt and support is being added to Certbot*

ARI makes it possible to handle certificate revocation and renewal as easily and automatically as the process of getting a certificate in the first place.

ARI can signal that renewal needs to happen prior to the revocation. Reducing service down time.

# ACME Profiles


Configured with your ACME client (Like Certbot)

With ACME profiles you can have the default or “classic” Let’s Encrypt experience (90 days) or start actively using other profile types through Certbot with the --preferred-profile and --required-profile flags. For six day certificates in the near future, you can choose the “shortlived” profile. This provides flexibility for legacy systems and other types like IoT devices.

# Notes on Internal PKI systems


- Legacy systems and outdated systems
  - Visibility is better than resignation
  - Usually more security issues than just lack of automation
- BACKUPS
- Security hardware has more variety now
  - Cloud based HSMs
  - Security keys (FIPS available)
- Use internal tools that support ACME

OOTB.NET

# Thank You

alexis@eff.org