Certificate Transparency

Kazuhiro NISHIYAMA

LILO&東海道らぐオフラインミーティング
2018/05/03

Certificate Transparency とは?

- CT, RFC 6962
- 証明書の透明性
- 証明書発行のログを CT ログサーバーに記録

何ができるか

- 意図しない証明書が発行されていないか監視
- 不正な証明書の発行を防げるわけではない

対応状況

- Google Chrome で EV (Extended Validation) 証明書では早くから必須だった
- Google、Certificate Transparency（CT）の適用範囲をすべての証明書タイプに拡大へ｜DigiCert Blog 日本語版｜DigiCert
  - 2017年10月からは DV (Domain Validation) 証明書, OV (Organization Validation) 証明書も必須

SCT: Signed Certificate Timestamp の提供方法

- 証明書に埋め込む (CA 側の対応)
- TLS Extension (mod_ssl_ct, nginx-ct など Web サーバー側で対応)
- OCSP Stapling を利用 (CA 側の対応)

Let’s Encrypt の対応

- Chain of Trust - Let’s Encrypt - Free SSL/TLS Certificates
- ログサーバーへの登録自体は以前から対応
- 2018年3月29日以降埋め込みに対応

問題点

- Pre-certificate という変なものがある (省略)
- ログに公開されている FQDN から情報漏洩の懸念
- 参考文献の PDF 参照

検索サイト

- https://transparencyreport.google.com/https/certificates?hl=ja
  - サブドメイン部分だけなどの検索ができない
- https://crt.sh/
  - 柔軟な検索ができる
  - IP アドレスでの検索もできる (1.1.1.1 など)

GitHub Pages

カスタムドメインの証明書が発行されていた。

- GitHub Pages generated a (rogue?) TLS cert for my own domain!

自分のドメインでも発行されていたので、 GitHub に確認したところ、いくつかのドメインで試験的にやっているという返事がきた。

発表後追記

5月1日から正式対応になっていました。
https://blog.github.com/2018-05-01-github-pages-custom-domains-https/

参考文献

- http://www.jnsa.org/seminar/pki-day/2016/data/1-2_oosumi.pdf
- Let’s EncryptのCertificate Transparency対応 - Apache 2.4系でHTTP/2対応サーバを構築してみるテスト。
- Certificate Transparency の仕組みと HPKP から Expect-CT への移行 | blog.jxck.io