LET'S ENCRYPT

LE TRUBLION DU HTTPS

Evolix – Jérémy Lecour & Victor Laborie – VVT 2017

HTTPS, TLS/SSL, CA

C'EST QUOI CETTE JUNGLE ?

HTTP + CHIFFREMENT = HTTPS

- motivé surtout par le e-commerce
- émergence du marché des certificats
- adoption lente entre 90's et 2010

OBSTACLES À L'ADOPTION MASSIVE

- crypto-guerre
- coût CPU
- coût réseau
- technicité de mise en place
- frais d'acquisition des certificats

LA DONNE CHANGE

- Firesheep
- Snowden
- Google
- HTTP/2

COMMENT ÇA MARCHE ?

- les CA créent des clés et certificats racine
- … qui servent à signer les certificats des sites
- ils sont dans les navigateurs, OS, Java…
- ça forme un réseau de confiance en arbre

Let’s Encrypt

Créer un web plus sécurisé,
respectueux de la vie privée.

PRINCIPES FONDAMENTAUX

- gratuit
- automatique
- sécurisé
- transparent
- ouvert
- collaboratif

D'OÙ ÇA VIENT

- 2 projets fusionnés
- ISRG créé en 2014
- ouverture publique en novembre 2015

QUI FINANCE ET CONTRÔLE ?

- financé à 100% par les dons
- Mozilla, EFF, Akamai, Cisco, Google Chrome, OVH…
- Conseils d'administration et technique variés

COMMENT ENTRER DANS LA DANSE ?

- Ajout dans les "trust stores"
- signature croisée
- méfiance de l'industrie

UN PEU DE TECHNIQUE

LE PROTOCOLE : ACME

- échanges client/serveur REST + JSON
- conçu pour être un standard IETF

LE CLIENT : CERTBOT

- client de référence, écrit en Python
- disponible sur les OS courants
- implémente la totalité du protocole
- et plus : config du serveur web …

LE SERVEUR : BOULDER

- gère toute la partie CA, écrit en Go
- implémente la totalité du protocole

COMMENT OBTENIR UN CERTIFICAT ?

- demande de certificat par le client
- challenge(s) de vérification par le CA
- création du certificat
- renouvellement et révocation simplissimes
- environnements "staging" et "production"

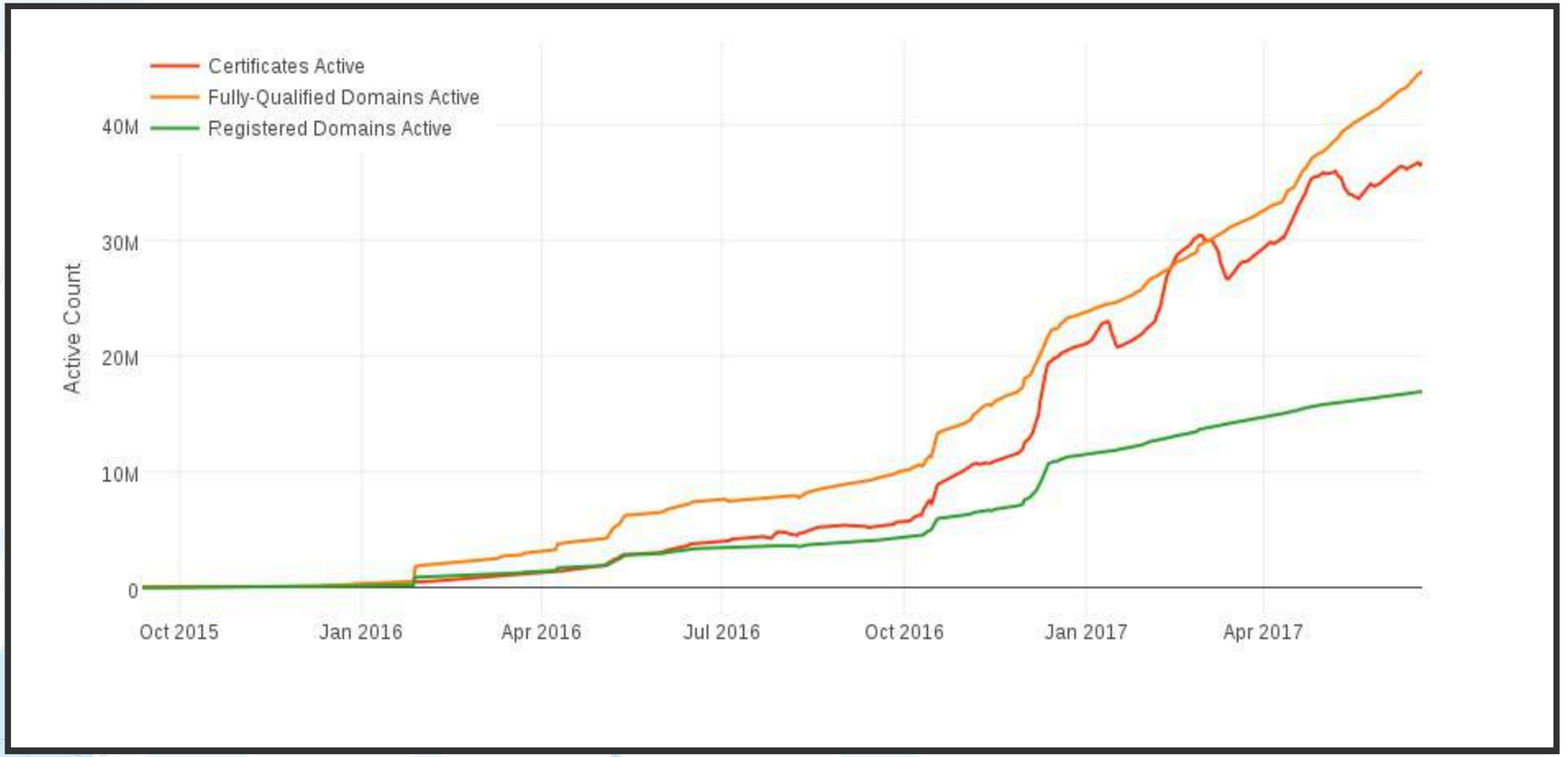
CHALLENGES DE VÉRIFICATION

- ressource HTTP en clair
- signature dans un certificat TLS temporaire
- signature dans un enregistrement DNS

DURÉE DE VIE DE 90 JOURS

- limiter la casse
- favoriser l'automatisation

STATISTIQUES D'ADOPTION



LIMITATIONS

- Pas de wildcard
- pas de OV/EV
- pas de support garanti
- pas de signature de code, mail…

LET'S ENCRYPT CHEZ EVOLIX

ADOPTION PROGRESSIVE

- premier tests internes ; fin 2015
- prod interne ; début 2016
- clients pilotes ; été 2016
- prod clients (manuel) ; fin 2016
- début de généralisation aux outils ; courant 2017

CERTBOT, OU PAS

- certbot automatise tout
- scripts maison "make-csr" et "evoacme"
- certbot limité aux échanges avec la CA
- en cas de faille/bug de certbot, les clés sont protégées

LET'S ENCRYPT ET ANSIBLE

- un module officiel existe, en beta
- on a fait des rôles maison, avec *evoacme*
- mise en place idempotente non triviale
- on est encore au stade de test

MERCI

À VOS QUESTIONS