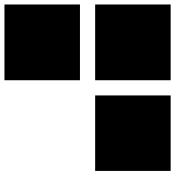
SYNACKTIV
DIGITAL SECURITY



TCP Fast Open

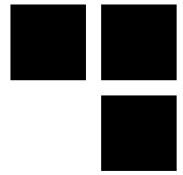
Bypassing pigs/suricates like a synack~~psh~~tiv ninja

Présenté 05/06/2014

Pour SSTIC 2014

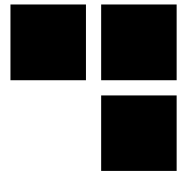
Par Nicolas Collignon et Renaud Dubourguais

TCP à la rescousse de HTTP



- **HTTP/1.0**
  - 1 handshake TCP par requête HTTP
- **HTTP/1.1**
  - Ajout de l'en-tête HTTP *keep-alive*
  - Plusieurs requêtes HTTP sur 1 handshake TCP
- **YouTube**
  - Toujours trop lent !

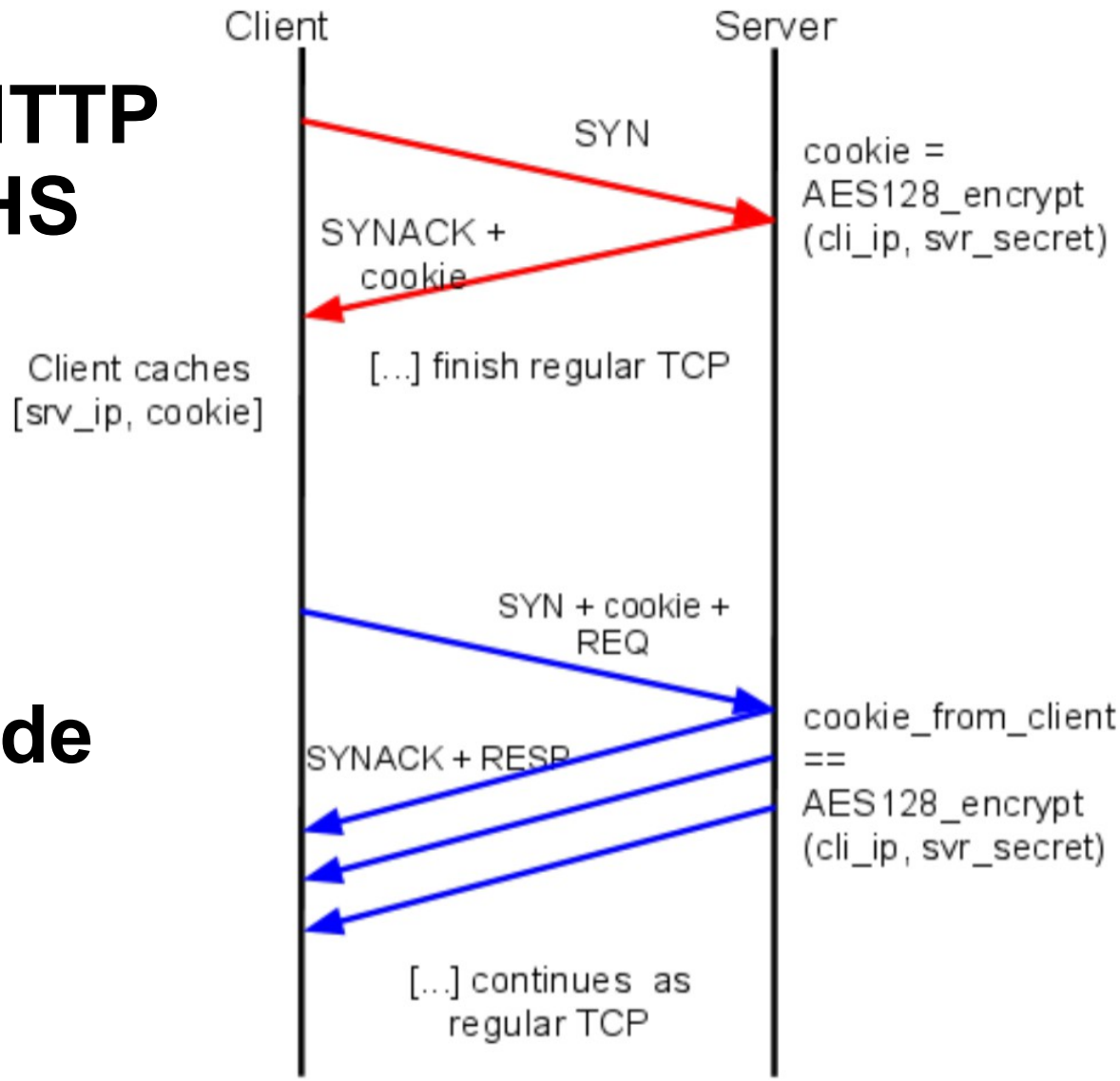
TCP Fast Open



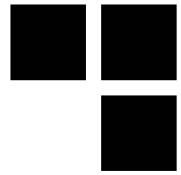
- **Norme à l'état de brouillon IETF**
  - Supporté sous Linux depuis 3.6
  - TFO côté client activé par défaut depuis 3.13
- **Impact sur l'API des sockets**
  - Client : connect() → sendto(MSG_FASTOPEN)
  - Serveur : setsockopt(TCP_FASTOPEN)

TFO handshake

- **1ère connexion HTTP nécessite un 3WHS**
- **Génération d'un cookie**
- **Ensuite échange de données avec un 3WHS**



TFO c'est bien, mais il faut faire attention !



- **Les données sont dans le SYN**
- **TFO est transparent pour les équipements de routage intermédiaires**
- **Les IDS ne « voient » pas les données**

Démo

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY