TCP Fast Open

Bypassing pigs/suricats like a synackṣṭiv ninja

Presented in the 05/06/2014
During the SSTIC 2014
By Nicolas Collignon and Renaud Dubourguais
Fixing TCP to help HTTP

- **HTTP/1.0**
  - 1 HTTP request = 1 TCP handshake

- **HTTP/1.1**
  - "Keep-Alive" HTTP header
  - Multiple HTTP requests = 1 TCP handshake

- **YouTube**
  - Still too slow!
  - We need something else...
TCP Fast Open

- **IETF draft**
  - The aim is to speed up connections establishment
  - Allows data transmission in the TCP handshake
  - Supported since Linux 3.6
  - Client-side TFO is enabled by default since Linux 3.13

- **Impacts on the socket API**
  - Client-side: `connect() → sendto(MSG_FASTOPEN)`
  - Server-side: `setsockopt(TCP_FASTOPEN)`
TFO handshake

- The first HTTP connection requires a regular 3WHS with the TFO TCP option enabled.
- The server generates a TFO cookie and sends it to the client in the SYN-ACK.
- Next, the client can send data during the following 3WHS.
TFO vs IDS

- Data is in the SYN packet
- Intermediate devices don't care about TFO
- IDS don't analyse data in SYN packets
Demo!

- TFO vs SNORT = TFO wins
- TFO vs Suricata = TFO wins