TLS Proxies

draft-mcgrew-tls-proxy-server

D. McGrew
D. Wing
P. Gladstone
Y. Nir

Current Practice

- TLS Proxies are middleboxes that inspect and optionally modify TLS traffic
- They are “client-side” in that they decrypt and inspect all traffic for a particular client
- They do this by replacing a single TLS connection with two connections, and performing a handshake with both the client and the server, and copying the requests and responses from one connection to the other.
- In HTTP terminology, they are “transparent proxies”

Current Practice

- They work for TLS connections that have server authentication by generating a key-pair, and signing an ephemeral certificate with that key for the real server.
- Uses include:
  - Detecting malware going through HTTP
  - Detecting HTTP attacks (XSS, CSRF)
  - Filtering content
  - Data leakage prevention
  - Botnet detection
  - Lawful (?) interception (not covertly)

Current Practice

- Firewalls have long inspected and filtered traffic
- So-called “next generation firewalls” do deeper inspection and look into HTTP streams
- HTTPS is great for keeping data private on the Internet, but interferes with filtering.
- TLS proxies allow those next-generation firewalls to work on encrypted connections.
- TLS proxies have been available from various vendors for over 6 years.

Current Practice

- TLS proxies have to be CAs
  - They need to sign certificates on the fly.
- Clients have to trust these CAs
  - Otherwise you get the warning screens in browsers
- When the CA certificate is added to the trust anchor store of the client, the user experience is flawless, unless the user actually views the server certificate.
- Some browsers detect proxies, and disable certificate pinning.

Problems with TLS Proxies

- Getting all clients to trust the proxy CA is hard
  - It's fairly easy in an environment where all clients are Windows boxes running Internet Explorer and connected to a single domain, but...
  - Today there are multiple browsers and OS
  - There are phones and other devices connecting to the network
  - There are guests and contractors who are allowed to use the network.

Problems with TLS Proxies

- The client doesn't get to see the real server certificate.
  - Extended Validation certificates cannot be checked and the green indication is gone.
  - Certificate pinning schemes don't work
    - cert-pinning, DANE
  - Revocation checking is at the option of the proxy.

Problems with TLS Proxies

- Clients cannot enforce their policy
  - TLS version
  - RI support
  - Trusted CAs
  - Algorithms
  - Forward secrecy

Problems with TLS Proxies

- The server never finds out about the proxy
- The server administrator cannot enforce a no-proxy policy.

Problems with TLS Proxies

- Client certificates (for mutual authentication) don't work
- The client trusts the certificates signed by the proxy CA, but the server does not, so the proxy cannot sign a certificate for the client
- The proxy cannot present the client certificate, because the CertificateVerify message would fail verification
- OBC don't work
- WebID (FOAF+SSL) doesn't work
- Some forms of BrowserID don't work

Need one solution

- There have been some proposals to fix this:
  - Use an extension to give the client information about the server-side connection
  - Have the client send encryption keys to the proxy
- In all cases, at least the proxy and client have to be modified.
- We can't ask browser makers to implement a bunch of proprietary extensions for this.
- There can only be one.

Requirements

- Dynamic discovery of TLS proxies
  - Make it possible for clients to choose whether to trust proxies or not
- Client gets server certificates, ciphersuites, TLS version, and other important information
- Mutual authentication works

Our Solution

- ServerHello extension from the proxy holds server cert and other information about the server-side connection.
- Similarly, an extension notifies the server that a proxy is present.
- The CertificateVerify message is modified to sign only the information that the proxy includes in the extension.
- more info in draft-mcgrew-tls-proxy-server

Questions?