LIVE DETECTION AND ANALYSIS OF HTTPS INTERCEPTION

HTTPS Interception

Example: anti-virus, enterprise-level middlebox, malware
Security Impact:
- Removal of PFS ciphers
- Introduction of export-grade ciphers
- ...

Client ID Derivation
Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
name="Firefox" version="57.0" os="Windows 7"

Fingerprint Comparison

version
suites
extensions
0x0303
0xa, 0xb, 0xc
0, 5, 10, 13, 21
observed fingerprint
0x0303
0xd, 0xc, 0xa, 0xb
stored fingerprint
Legend: added/removed/reordered/ignored

Fingerprint Learning

Motivation: automatically build database of trusted fingerprints
Collect fingerprint variants as possible fingerprint candidates
Check trust for each variant in regular intervals
Single trusted variant: trusted fingerprint, else undecided

Security Impact

Mobile clients are intercepted much less often (0.8%) compared to desktop clients (11%)

Results

Overall Interception Rates

Security Impact

50% of TLS proxies remove security-critical extended master secret extension, 8% remove a preferred PFS cipher suite

Future Work

Reducing Undecided Results
- If two or more variants are trusted, regard match of most common as not intercepted (instead of undecided)
- Find interception product fingerprints and distrust them explicitly

Live Analysis
- Setup for live traffic interception detection
- Perform client-side tests with JavaScript
- Test middlebox certificate validation
- Confirm interception using unsupported TLS configuration
- Find location of intercepting system

Add Fingerprint Parameters
- Compression methods
- Content of some TLS extensions (e.g. ECC, SNI)


Tobias Brunnwieser, Oliver Gasser, Sree Harsha Totakura, Florian Wohlfart, and Georg Carle | brunnwie | gasser | totakura | wohlfart | carle j@net.in.tum.de