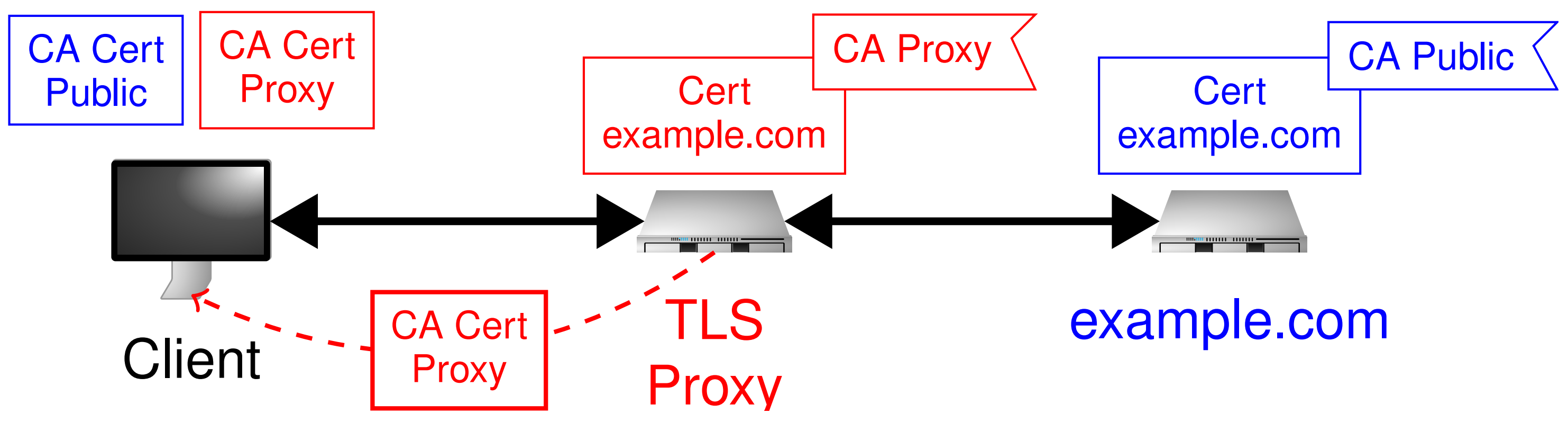
Live Detection and Analysis of HTTPS Interception

HTTPS Interception



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

Interception Detection

Client ID Derivation

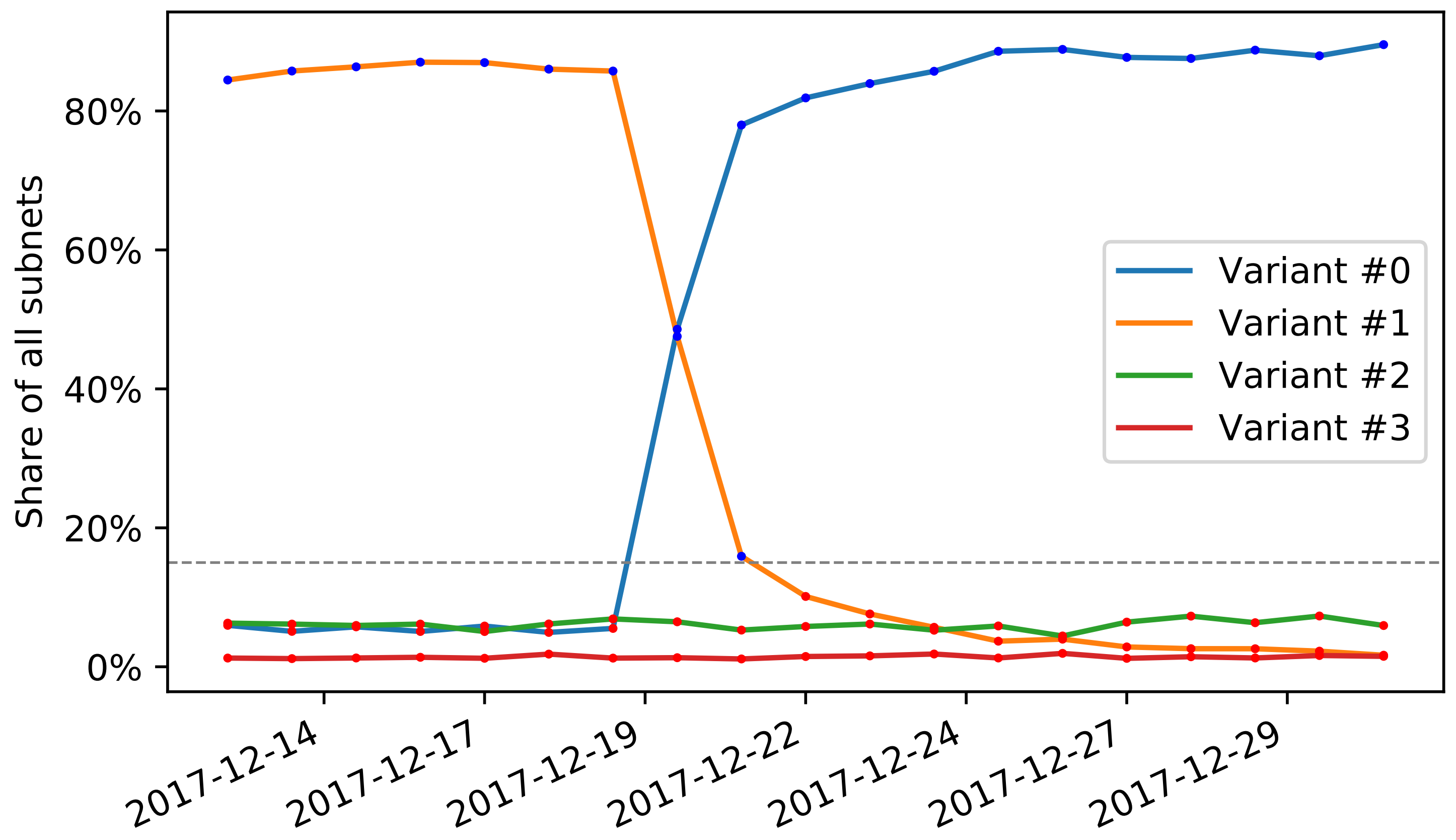
```
Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
⇩
name="Firefox" version="57.0" os="Windows 7"
```

Fingerprint Comparison

	observed fingerprint	stored fingerprint
version	0x0303	0x0303
suites	0xa, 0xb, 0xc	0xd, 0xc, 0xa, 0xb
extensions	0, 5, 10, 13, 21	0, 5, 10, 15, 13

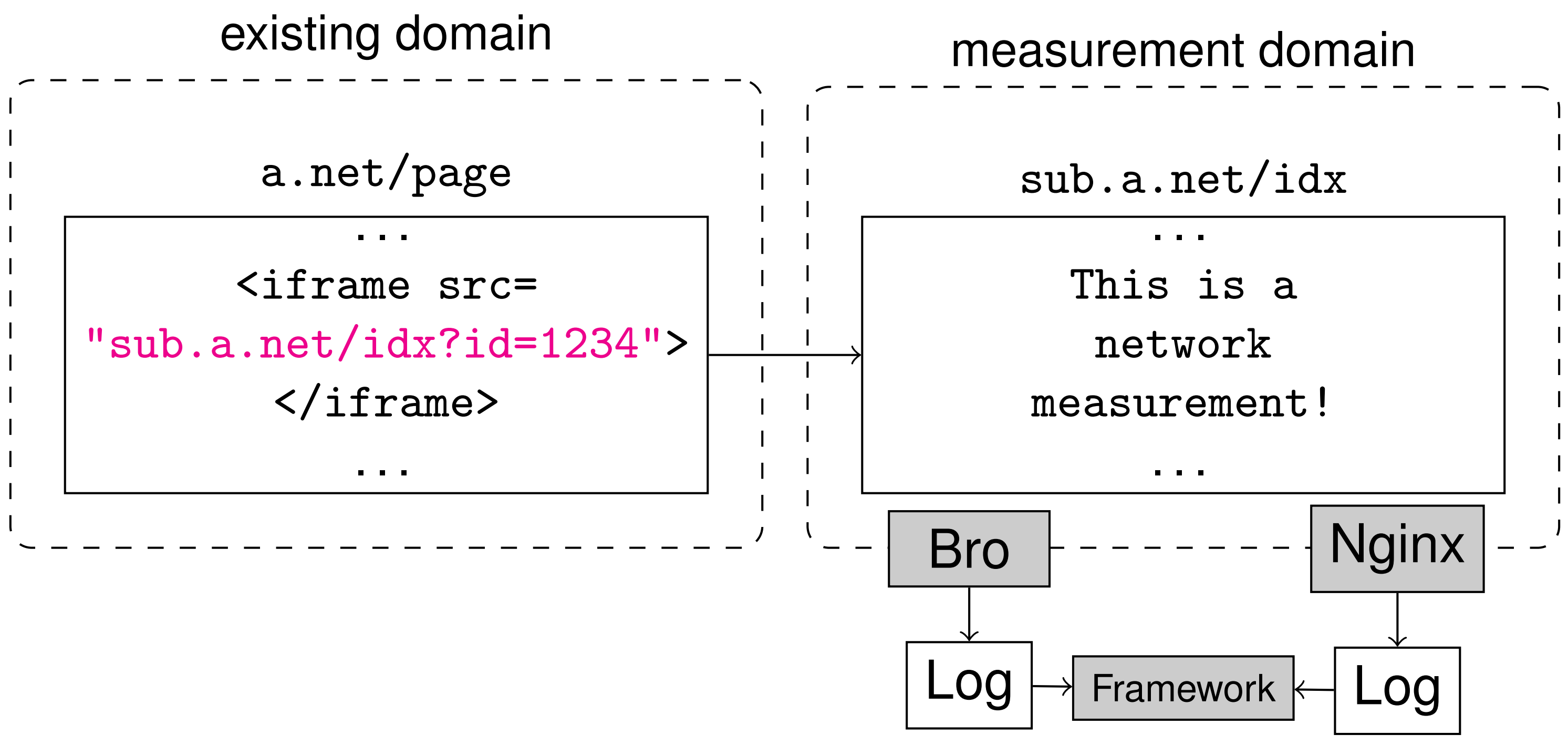
Legend: added/removed reordered ignored

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*

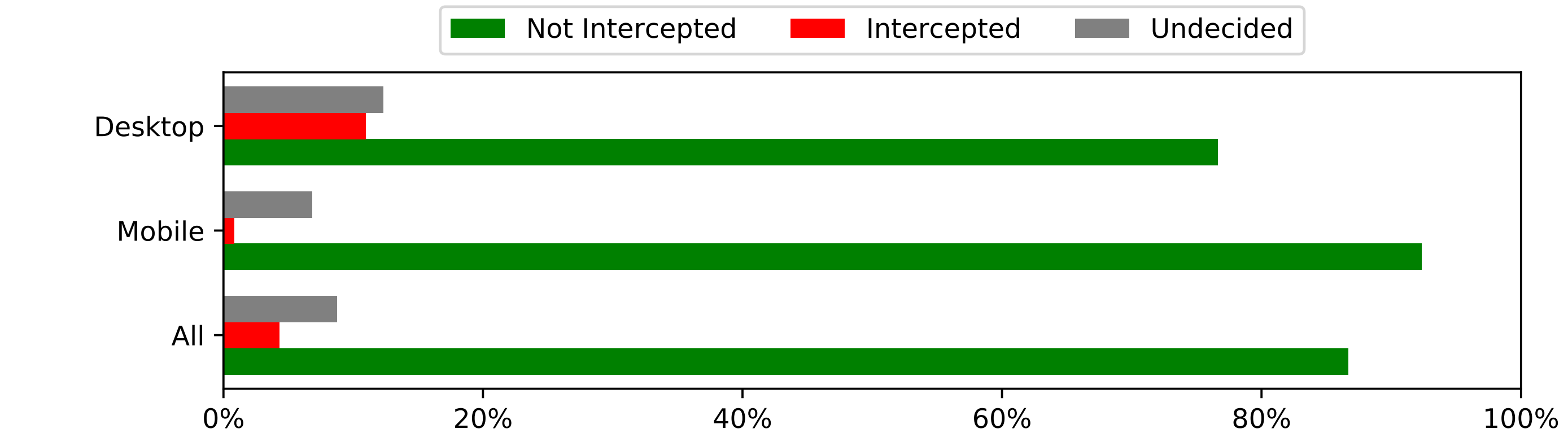
Measurement Setup



- Hidden `iframe`: *isolation* from existing domain, easy integration
- Measurements from *multiple* sites possible
- Option to pass parameters to `iframe` (e.g. anonymous user ID)
- Measurements performed at PPRO site with ~ 26k unique connections/day

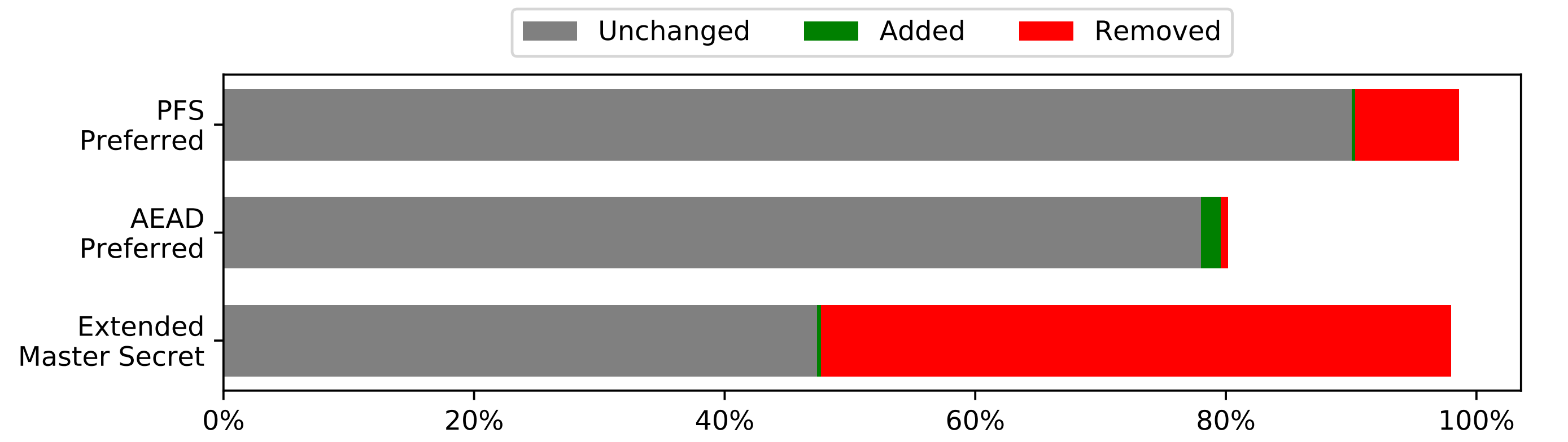
Results

Overall Interception Rates



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

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)

[1] Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Nailey, J. A. Halderman, and V. Paxson. The Security Impact of HTTPS Interception. In *Proceedings of the 2017 Symposium on Network and Distributed System Security*, San Diego, CA, USA, 2017.

[2] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson. Analyzing Forged SSL Certificates in the Wild. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2014.

[3] M. O'Neill, S. Ruoti, K. Seamons, and D. Zappala. TLS Proxies: Friend or Foe? In *Proceedings of the 2016 Internet Measurement Conference*, New York, NY, USA, 2016.

Tobias Brunnwieser, Oliver Gasser, Sree Harsha Totakura, Florian Wohlfart, and Georg Carle

{ brunnwie | gasser | totakura | wohlfart | carle }@net.in.tum.de