Combinatorial Methods and Models for Privacy

Dimitris E. Simos, Bernhard Garn, Stefan Zauner, Rick Kuhn, Raghu Kacker

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

MATRIS

Combinatorial Methods in the Context of Privacy

Combinatorial Browser Fingerprinting

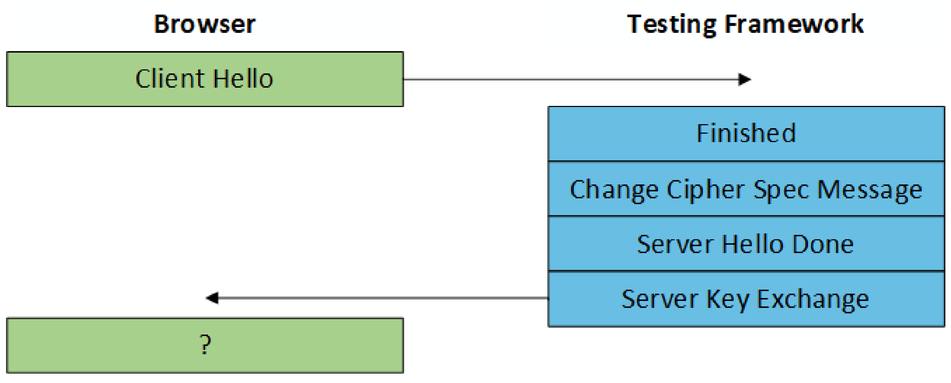
- Distinguish between Browsers using TLS-Handshake messages.
- Novel approach that does not need JavaScript.

Anonymity Networks

- Combinatorial design structures for analysis and as building blocks.
- Analysis of anonymity networks with Design of Experiments.

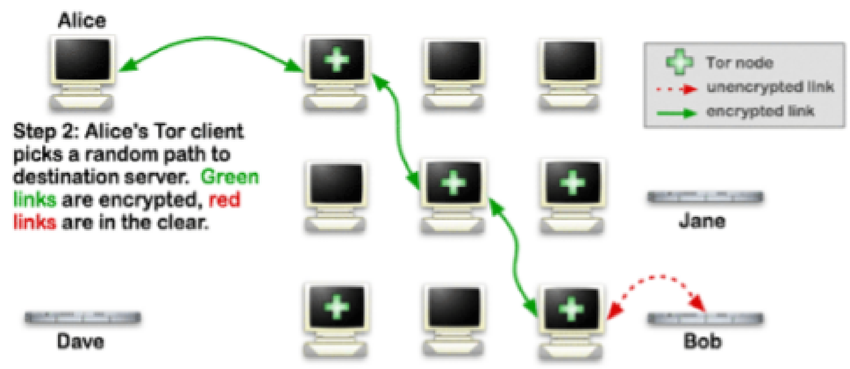
Browser Fingerprinting

- Browsers are widely used to consume services over the Internet.
- Transport Layer Security (TLS) is used to keep connection secure.
- Different TLS-Implementations expose different behaviour, especially when exposed to manipulated Handshakes.
- This allows distinction between browsers.



Anonymity Networks

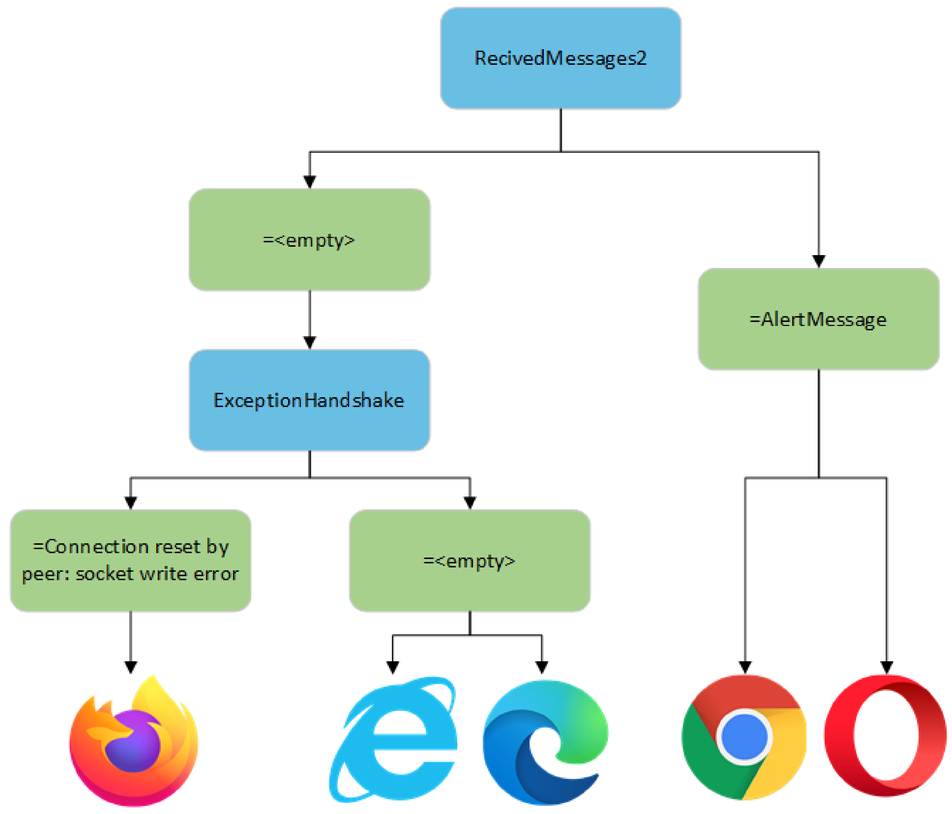
- Analysis of low-latency anonymity overlay networks.
- **T**he **O**nion **R**outer (Tor) de-facto standard for online anonymity.
- Hides IP addresses of hundreds of thousands of users every day.
- Combine flow-networks and block designs for new attacks.



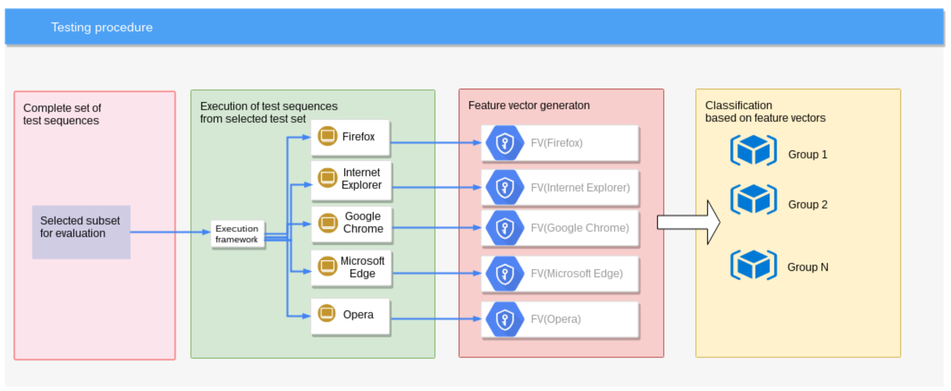
Sequences

- The six server-side TLS handshake messages are regarded as a set of six abstract events $\mathcal{M}$.
- $\mathcal{M}$ = {*ServerHello*, *Cert*, *ServerKeyExchange*, *ServerHelloDone*, *ChangeCipherSpec*, *Finished*}.
- All permutations of any non-empty subset ***E*** of $\mathcal{M}$ are tested, therefore all SCAs defined over the elements ***E*** are included.
- A row in a SCA created in such a way is a test sequence that can be transformed to a sequence of actual TLS handshake messages.
- Example: $\{0, 3, 2, 1\}$ translates to {*ServerHello*, *ServerHelloDone*, *ServerKeyExchange*, *Cert*}.

Decision Tree Based on a Single Test



Testing Methodology



Testing Framework:

- Java-based software that automatically records behaviour of Browsers
- Uses TLS-Attacker to execute manipulated TLS Handshakes
- Only the sequence of the six server-side TLS messages is altered
- All possible $\sum_{i=1}^{6} \binom{6}{i} \cdot i! = 1956$ permutations were tested

Evaluation

- Five Browsers were tested (Chrome, IE, Edge, Firefox and Opera).
- The best possible splitting was based on the browser families: {Chrome, Opera} {IE, Edge} {Firefox}.
- Distinguished by pairwise comparison of their feature vector.
- The best possible distinction was achieved even using sequences of length 2 (higher-strength sequences also yielded this outcome).

Bernhard Garn, Dimitris E. Simos, Stefan Zauner, Rick Kuhn, and Raghu Kacker. Browser fingerprinting using combinatorial sequence testing. In *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, HotSoS '19, New York, NY, USA, 2019. Association for Computing Machinery.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.