Combinatorial Testing of TLS, X.509 and IoT protocols

Dimitris E. Simos, Bernhard Garn, Manuel Leithner, Dominik Schreiber, Yu Lei, Franz Wotawa

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

SBA Research

MATRIS

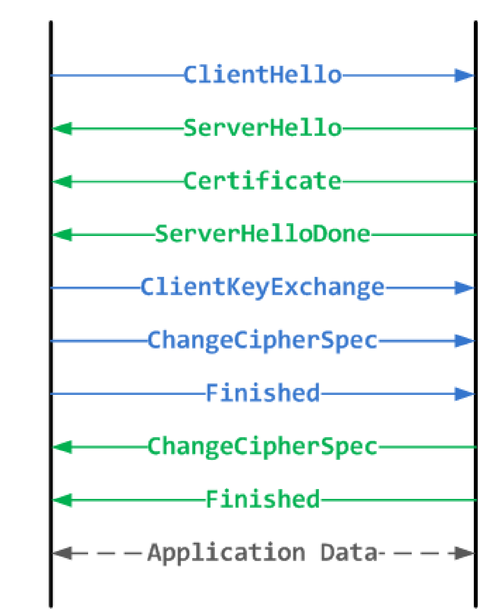
Transport Layer Security (TLS/SSL)

- Most common communications security protocol on the Internet.
- Provides confidentiality via symmetric encryption.
- Authenticity of servers provided via X.509 certificates:
  - Client authenticity optionally provided through client certificate
- Integrity of exchanged data verified through Message Authentication Codes.

Attacks

High-profile protocol, thus valuable target.

- Protocol-version downgrades (FREAK and Logjam).
- Compression-based (CRIME and BREACH).
- Padding oracle-based (POODLE and Lucky Thirteen).
- ...



Our Contribution

- Differential testing of implementations.
- Combinatorial testing of X.509 certificate parsers:
  - All libraries should parse certificates the same way
  - Endpoint equivalence undecidable
  - Different behavior between implementations ⇒ possible vulnerabilities
- Combinatorial (sequence) testing:
  - Focus on handshake or entire TLS session
  - Hierarchical Input Parameter Models
  - Weighted t-way sequences
  - AI-based planning support in test generation

Target Implementations

- OpenSSL
- GnuTLS
- NSS
- ...

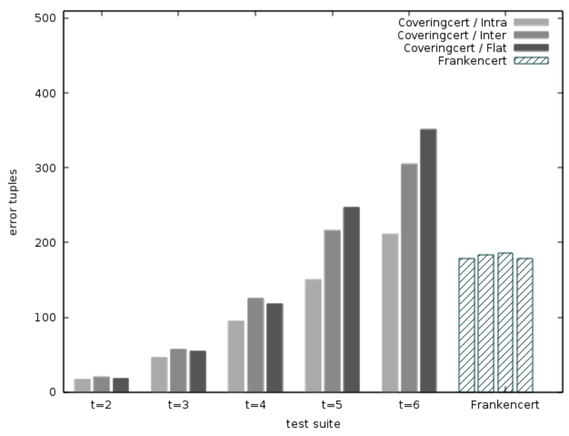
Contributions

CoveringCerts

Combinatorial generation of X.509 certificates and differential testing of parsers.

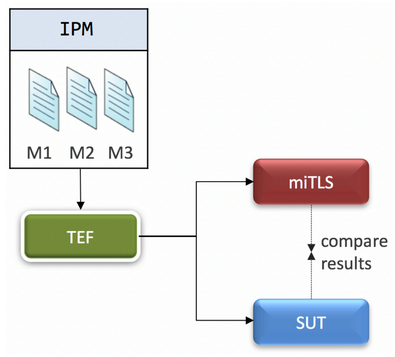
- Modeling of certificate contents.
- Generation of concrete certificates.
- Differential testing of implementations

⇒ More detailed and efficient results than previous approaches.



Hierarchical Input Parameter Models

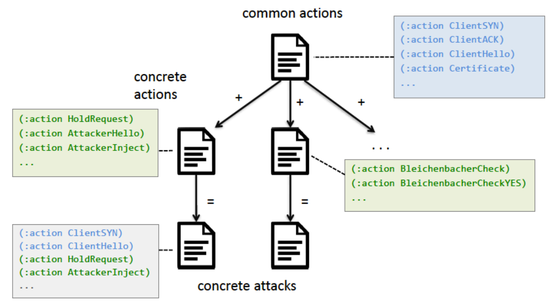
- Naive/flat approach:
  One model for all attributes of all messages in TLS handshake.
- Hierarchical approach:
  Intra-message model for each message,
  Inter-message model to combine results
  ⇒ Enables higher-strength testing.
- Comparison with miTLS, a verified reference implementation of TLS.



Sequence Testing

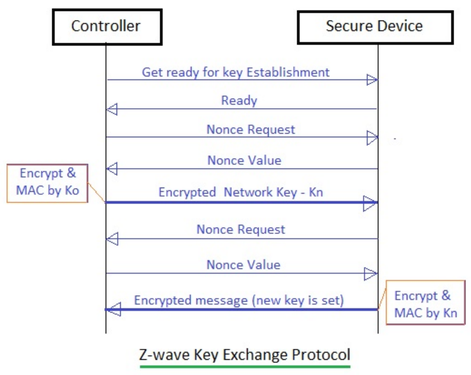
Modify attributes and order of TLS messages in handshake.

- Handshake testing as a sequence testing problem.
- Differential testing of implemented TLS state machines.
- AI-based planning to generate attack sequences.
- Weighted t-way Sequences:
  - Assign weights, derived from occurrences in bug reports, to events (TLS messages)
  - Event selection for candidate sequences based on integer partitions

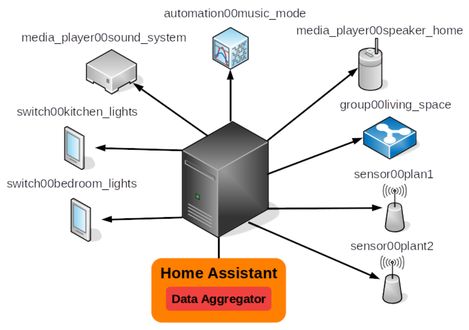


Future focus: Internet of Things

- Rapid adoption:
  - Home automation / Smart Home
  - Medical assistance
  - Infrastructure management
- Resource constrained devices.
- Emerging protocols:
  - Z-Wave
  - NFC/RFID
  - Bluetooth Low Energy Mesh



Z-wave Key Exchange Protocol



Multi-faceted Attack Surface

- Attacks on web interfaces.
- Commonly backed by REST services.
- Focus on usability.
- Weakened cryptography.
- Increased privacy risk.

Rapidly changing technology
⇒Automated testing required.

- K. Kleine and D. E. Simos, "Coveringcerts: combinatorial methods for x. 509 certificate testing," in *2017 IEEE International conference on software testing, verification and validation (ICST)*. IEEE, 2017, pp. 69–79.
- D. E. Simos, J. Bozic, F. Duan, B. Garn, K. Kleine, Y. Lei, and F. Wotawa, "Testing tls using combinatorial methods and execution framework," in *IFIP International Conference on Testing Software and Systems*. Springer, 2017, pp. 162–177.
- B. Garn, D. E. Simos, F. Duan, Y. Lei, J. Bozic, and F. Wotawa, "Weighted combinatorial sequence testing for the tls protocol," in *2019 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*. IEEE, 2019, pp. 46–51.
- D. E. Simos, J. Bozic, B. Garn, M. Leithner, F. Duan, K. Kleine, Y. Lei, and F. Wotawa, "Testing tls using planning-based combinatorial methods and execution framework," *Software quality journal*, vol. 27, no. 2, pp. 703–729, 2019.

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.