Combinatorial Testing of TLS, X.509 and IoT protocols

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

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).
- ... (continued)

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
- Naïve/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 mTLS, 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 z-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
- Multi-faceted Attack Surface
  - Attacks on web interfaces.
  - Commonly backed by REST services.
  - Focus on usability.
  - Weakened cryptography.
  - Increased privacy risk.
  ⇒ Automated testing required.