

# Automated Security Analyses of the TLS Ecosystem

Marcel Maehren

## Abstract

The Transport Layer Security (TLS) protocol is one of the most prevalent cryptographic protocols, particularly through its role in securing web traffic sent in HTTPS. TLS aims to ensure confidentiality, authenticity, and integrity of transmitted data. However, weaknesses in the protocol design and faulty implementations have threatened these goals in the past. This dissertation advances the understanding of the TLS ecosystem through publications developing automated techniques for analyzing implementations, establishing foundational data sets, and uncovering critical security flaws. To this end, the included publications study TLS libraries in the lab and deployments on the Internet, providing the following contributions:

- An analysis of the protocol compliance of 13 open-source TLS clients and servers across varying parameters, offering a comprehensive assessment and revealing critical issues.
- An analysis of DTLS protocol features and a study providing the first large-scale data set on the distribution of DTLS hosts on the Internet, their protocol properties, and the prevalence of known vulnerabilities.
- An analysis of implementation pitfalls in the TLS session ticket resumption mechanism and a large-scale Internet scan uncovering exploitable weaknesses which allow attackers to decrypt sessions.
- An analysis of timing side channels in open-source TLS implementations and the development of a new statistical test for detecting such leaks.
- A study collecting the first large-scale data set on real-world TLS state machines and a novel methodology for their automated analysis identifying vulnerabilities.

The insights gained from these individual studies contribute to the future development of robust and secure TLS implementations, improving the overall safety of the ecosystem.

# Automated Security Analyses of the TLS Ecosystem

Marcel Maehren

## Kurzfassung

Das Transport Layer Security (TLS) Protokoll gehört zu den am weitesten verbreiteten kryptographischen Protokollen, insbesondere durch seine Rolle bei der Absicherung von Daten über HTTPS. TLS verfolgt dabei das Ziel, Vertraulichkeit, Authentizität und Integrität der übertragenen Daten sicherzustellen. Frühere Schwächen im Protokolldesign sowie fehlerhafte Implementierungen haben diese Ziele jedoch in der Vergangenheit gefährdet. Diese Dissertation trägt zu einem tieferen Verständnis des TLS Ökosystems bei, indem automatisierte Techniken entwickelt werden, mit denen TLS Implementierungen untersucht, grundlegende Datensätze erhoben und Schwachstellen identifiziert werden. Die enthaltenen Publikationen betrachten dabei Implementierungen im Labor und im Internet und liefern damit die folgenden Beiträge:

- Eine Analyse von 13 Open-Source TLS Clients und Servern, die die Protokollkonformität über verschiedene Parameterkombinationen untersucht und darüber kritische Schwachstellen aufdeckt.
- Eine Analyse der DTLS-Protokollfunktionen sowie eine Studie, die erstmals einen Datensatz zur Verbreitung von DTLS Hosts im Internet, deren Protokolleigenschaften und Anfälligkeit gegenüber bekannter Schwachstellen erhebt.
- Eine Analyse möglicher Implementierungsfehler im TLS Resumption-Mechanismus über Session Tickets sowie ein großflächiger Internet-Scan, der ausnutzbare Schwächen aufdeckt, die es Angreifern erlauben, TLS Verbindungen zu entschlüsseln.
- Eine Analyse von Timing-Seitenkanälen in Open-Source TLS Implementierungen sowie die Entwicklung eines neuen statistischen Tests zur Erkennung solcher Schwachstellen.
- Eine Studie, die erstmals einen umfangreichen Datensatz realer TLS-Zustandsmaschinen erhebt und mittels einer neuen Analysemethodik automatisiert Schwachstellen darin identifiziert.

Die aus den Studien gesammelten Erkenntnisse unterstützen die zukünftige Entwicklung robuster und sicherer TLS Implementierungen und tragen so zur allgemeinen Sicherheit des TLS Ökosystems bei.