Universität Hamburg

Fachbereich Informatik

Entwurf vom
23. Mai 2015

Exposé

Bachelorarbeit über TLS (1.3)

vorgelegt von

Tom Petersen

geb. am 13. Dezember 1990 in Hannover

Matrikelnummer 6359640

Studiengang Informatik

eingereicht am 23. Mai 2015

1 Motivation

TLS ist das wohl am meisten genutzte Sicherheitsprotokoll im Internet. Aus diesem Grund wurde es im Laufe seiner Entwicklung oft untersucht und angegriffen. Dabei sind viele einfache und elegante Angriffe gefunden worden, die zeigen, wie wirksam die kleinsten Schwächen in Protokollen ausgenutzt werden können und das auch scheinbar unbedenkliche Stellen zu Sicherheitslücken führen können. Daher ist TLS auch ein gutes Beispiel für Dinge, die bei der Erstellung eines Protokolls bedacht werden müssen.

Weiterhin ist TLS ein sehr

und verbessert, um diese Angriffe zu verhindern.

2 Richtung der Bachelorarbeit

3 SSL und TLS - ein Überblick

SSL (Secure Socket Layer) bzw. TLS[1] (Transport Layer Security) ist ein zustandsbehaftetes Protokoll, das auf dem TCP-Protokoll der Transportschicht des TCP/IP-Protokollstapels aufbaut[2].

Hauptaufgaben von TLS sind Authentifikation der Kommunikationspartner, Verschlüsselung der Kommunikation sowie die Sicherstellung der Integrität der übertragenen Nachrichten. Die hierbei verwendeten kryptographischen Verfahren werden erst zu Beginn der Kommunikation festgelegt.

Viele Protokolle der Anwendungsschicht nutzen TLS zur sicheren Datenübertragung, so beispielsweise HTTPS oder FTPS und auch viele Anwendungen übertragen ihre Daten TLS-gesichert.

SSL wurde von der Firma Netscape entwickelt und nachdem es starke Verbreitung gefunden hatte, durch die IETF als TLS 1.0 standardisiert (TLS 1.0 entspricht SSL 3.1). Aktuell ist die TLS-Version 1.2 und an Version 1.3 wird gearbeitet. [Sch09]

TLS 1.0 RFC 2246 - http://tools.ietf.org/html/rfc2246

TLS 1.1 RFC 4346 - http://tools.ietf.org/html/rfc4346

TLS 1.2 RFC 5246 - http://tools.ietf.org/html/rfc5246

TLS Extensions RFC 3546 - http://tools.ietf.org/html/rfc3546,
RFC 3466 - http://tools.ietf.org/html/rfc4366,
RFC 6066 - http://tools.ietf.org/html/rfc6066

TLS 1.3 Draft - https://tools.ietf.org/html/draft-ietf-tls-tls13-05

1. Im weiteren Verlauf dieser Arbeit wird der Einfachheit halber lediglich von TLS gesprochen. Bei etwaigen Unterschieden wird explizit auf diese eingegangen.
2. DTLS (Datagram Transport Layer Security) ist ein auf TLS basierendes Protokoll, dass auch per UDP Daten übertragen kann

4 Funktionsweise und Teilprotokolle

Die Informationen in diesem Abschnitt stammen überwiegend aus der TLS 1.2-Spezifikation([**?**]). Für einen ersten Überblick wurde [Eck13] genutzt.

RFC in BibTex

Zum Einstieg grobe Funktionsbeschreibung, evtl. schon mit Grafik über Verbindungsaufbau?, Grafik der TLS-Protokolle

4.1 Record-Protokoll

TLS besteht selbst aus zwei Schichten. In der unteren Schicht befindet sich das *Record-Protokoll*, das die Daten von den Teilprotokollen der oberen Schicht entgegennimmt, diese Protokolldaten fragmentiert (maximale Paketgröße 2^{14} Byte) und optional komprimiert. Danach wird je nach aktuell verhandelten krypographischen Funktionen die Integrität der Daten durch Berechnen und Anhängen eines MACs gesichert und die Nachricht verschlüsselt. [1].

Nach http://crypto.stackexch schlägt Schneier in Cryptography Engineering MAC-then-encrypt aus Gründen der Komplexheit von Encrypt-then-MAC vor. Nachlesen! Gibt es in der Informatik-Bibliothek: T FER 45399

Der Macwird auf die folgende Weise berechnet:

```
1 MAC(MAC_write_key, seq_num ||
2                     TLSCompressed.type ||
3                     TLSCompressed.version ||
4                     TLSCompressed.length ||
5                     TLSCompressed.fragment);
```

Reihenfolge anpassen

Bei den in TLS verwendeten Cipher Suites wird das HMAC-Verfahren zur Berechnung des MACs genutzt. Details hierzu sind in [KBC97] zu finden. Die für dieses Verfahren verwendete Hashfunktion wird in der Cipher Suite angegeben. Bei SSL 3.0 wurde hier noch eine HMAC-ähnliche Konstruktion verwendet.

Der Record-Header enthält Informationen über die verwendete SSL/TLS-Version, den Content-Type (Handshake, Alert, ChangeCipherSpec, ApplicationData) und die Länge des Klartextfragments.

Aus dem nach Ausführung des Handshake-Protokolls (siehe nächsten Abschnitt) beidseitig bekannten master-secret werden Schlüssel für die Erstellung des MACs sowie für die Kommunikation zwischen Client und Server berechnet (also insgesamt vier Schlüssel). Dazu werden solange Schlüsselblöcke nach dem folgenden Verfahren erstellt, bis alle Schlüssel konstruiert werden können.

```
1 key_block = PRF(SecurityParameters.master_secret,
2                 "key expansion",
3                 SecurityParameters.server_random +
4                 SecurityParameters.client_random);
```

Hierbei werden die folgenden Funktionen genutzt:

1. Achtung: hier wird MAC-then-Encrypt angewendet. Laut [BN00] ist Encrypt-then-MAC vorzuziehen. In [Kra01] wird dieses Ergebnis bestätigt, aber auch die Sicherheit von authenticate-then-encrypt unter bestimmten Voraussetzungen gezeigt.

```
PRF(secret, label, seed) = P_hash(secret, label + seed)

P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) +
                       HMAC_hash(secret, A(2) + seed) +
                       HMAC_hash(secret, A(3) + seed) + ...

A(0) = seed
A(i) = HMAC_hash(secret, A(i-1))
```

4.2 Protokolle der oberen Schicht

In der oberen Schicht sind vier Teilprotokolle spezifiziert: *Handshake-, ChangeCipherSpec-, Alert-* und *ApplicationData-Protokoll*.

Das *Handshake-Protokoll* dient zur Herstellung einer gesicherten Verbindung. Hierbei werden kryptographische Verfahren zwischen den Kommunikationspartnern vereinbart, ihre Identität authentifiziert und ein Schlüssel (das sogenannte pre-master-secret) für die bereits beschriebene Erstellung der - später während der eigentlichen Kommunikation verwendeten - Schlüssel übertragen oder berechnet. Der Handshake kann folgendermaßen ablaufen (hier illustriert für keine Nutzung einer existierenden Sitzung und kein Clientzertifikat):

als ordentliche Grafik ohne Clientverifikation

- –>client-hello mit
  $H_C = ($4 Byte Zeitstempel, 28 Byte Zufallszahl, Sitzungsidentifikator (!= Null bei bereits existierender Sitzung), Cipher Suite List$)$
- <– server-hello mit
  $H_S = ($4 Byte Zeitstempel, 28 Byte Zufallszahl, Sitzungsidentifikator (falls vom Client gewünschte Sitzung bedient werden kann), Cipher Suite, die vom Server unterstützt wird$)$
- <– Server Zertifikat (inklusive öffentlichem Schlüssel des Servers, meist nach X.509v3)
- Client: Zertifikatverifikation
- –> Generierung und Senden von pre-master-secret (48 Byte) verschlüsselt mit öffent. Schlüssel des Servers (bei RSA) oder Diffie-Hellman-Verfahren
- Client und Server: aus Zufallszahl des Clients R_C aus H_C, Zufallszahl des Servers R_S aus H_S und pre-master-secret wird das master-secret berechnet.

  ```
  master_secret = PRF(pre_master_secret, "master secret",
                  ClientHello.random + ServerHello.random)[0..47];
  ```

- –> Change Cipher Spec-Nachricht (kein Bestandteil des Handshake-Protokolls -> eigener Record)
- –> Handshakeabschluss: finished mit MAC über alle bisher ausgetauschten Handshake-Nachrichten

  ```
  verify_data = PRF(master_secret, finished_label,
      Hash(handshake_messages)) [0..verify_data_length-1];
  ```

- <– Change Cipher Spec-Nachricht

- <– Handshakeabschluss, wie Client-Nachricht

Das *Change Cipher Spec-Protokoll* dient dazu, die vereinbarten kryptographischen Verfahren zu ändern. Es enthält lediglich eine Nachricht mit dem Wert 1, die für das Übernehmen der während des Handshakes ausgehandelten Verfahren steht.

Das *Alert-Protokoll* dient dazu, auftretende Fehler zu versenden, die während des Datenaustausches auftreten. Hierbei kann es sich zum Beispiel um fehlgeschlagene Überprüfung von entschlüsselten Nachrichten (bad_record_mac) oder fehlerhafte Zertifikatsüberprüfung (bad_certificate) handeln. Unterschieden wird zwischen Fehlern (fatal alert), die sofort zum Schließen der Sitzung führen, und Warnungen(warning alert). Eine Übersicht über alle Fehler findet sich in Abschnitt 7.2 von [**?**].

Das *Application Data-Protokoll* ist zuständig für das Durchreichen von Anwendungsdaten, die von der Anwendungsschicht gesendet werden sollen.

4.3 Sitzungs- und Verbindungskonzept

TLS erstellt beim ersten Handshake eine Sitzung zwischen Client und Server. Hierbei wird ein Sitzungsidentifikator erstellt, der beim server-hello mitgesendet wird. Weiterhin wird sich in der Sitzung das Zertifikat des Gegenübers, optional das Kompressionsverfahren, die Cipher Suite und das master-secret gemerkt.

Ein Client kann nun, wenn er den Sitzungsidentifikator beim client-hello mitschickt, eine alte Sitzung in Form einer neuen Verbindung wiederaufnehmen oder mehrere Verbindungen parallel aufbauen. Eine Verbindung wird dabei durch Client- und Server-Zufallszahlen R_C und R_S, die generierten Schlüssel, je nach verwendeten Verschlüsselungsverfahren einen Initialisierungsvektor, sowie aktuelle Sequenznummern beschrieben.

Beim Verbindungsaufbau kann so ein verkürzter Handshake genutzt werden, bei dem weniger Nachrichten gesendet werden müssen. Es kann dabei auf Neuberechnung des master-secret, Server- und Client-Validierung und Aushandlung der Cipher Suite verzichtet werden.

Grafik des verkürzten Handhakes

5 Angriffe auf SSL und TLS

Eine gute Übersicht zu bisherigen Angriffen auf TLS findet sich in [MS13]. Viele Schwächen früherer Protokollversionen bis SSL 3 sind in [WS96] zu finden.

JEDEN Angriff auf angreifbare Version und Änderungen in neuen Versionen überprüfen.

5.1 Version Rollbacks [nette Übersetzung?]

Ein Angreifer kann eine SSL 3-konforme client-hello-Nachricht so modifizieren, dass der Server eine SSL 2-Verbindung aufbaut. So kann der Angreifer alle Schwächen der älteren Protokollversion ausnutzen. Abhilfe schafft die Einbindung der SSL-Version in das per RSA übertragene pre-master-secret.

Ein Schwachpunkt könnte laut [WS96] immer noch die Wiederaufnahme einer SSL 3-Sitzung durch eine SSL 2-client-hello-Nachricht sein. Dieses sollte in Implementationen verhindert werden.

5.2 Ciphersuite Rollback

Ein für SSL 2.0 bestehender Angriff ermöglichte aktiven Angreifern die während des Handshake-Protokolls übertragenen Listen von unterstützten Cipher Suites zu verändern, so dass schwache kryptographische Verfahren erzwungen werden konnten (oftmals exportgeschwächte Verfahren mit kürzeren Schlüsselängen).

In SSL 3.0 wird dieser Angriff dadurch verhindert, dass die finished-Nachrichten von Client und Server jeweils einen mit dem master-secret berechneten MAC über die Nachrichten des *Handshake*-Protokolls enthalten, der die Integrität dieser Nachrichten bestätigt.

Eine detaillierte Übersicht ist in [WS96] zu finden.

5.3 Verhindern der Change Cipher Spec-Nachricht

Im Sonderfall einer SSL-Verbindung, die lediglich die Integrität der Nachrichten schützen soll, aber nicht verschlüsselt, lässt sich ausnutzen, dass der in der finished-Nachricht gesendete MAC die Change Cipher Spec-Nachricht nicht mit einschließt. Dadurch kann ein aktiver Angreifer diese Nachrichten abfangen und nicht weiterleiten, sodass die Verbindungspartner die Integritätsprüfung nicht einsetzen. Ein Angreifer ist so in der Lage, gesendete Nachrichten zu verändern.

Theoretisch wäre der Angriff unter bestimmten Voraussetzungen und schwacher Kryptographie auch bei verschlüsselten Verbindungen möglich, unter praktischen Gesichtspunkten aber eher unwahrscheinlich.

Die TLS 1.0-Spezifikation verhindert diesen Angriff dadurch, dass sie eine Change Cipher Spec-Nachricht vor der finished-Nachricht explizit vorschreibt.

Details zu diesem Angriff sind in [WS96] zu finden.

5.4 Schwache Cipher Suites

5.5 Bleichenbacher-Angriff und darauf basierende Angriffe

Daniel Bleichenbacher stellte 1998 in [Ble98] einen Adaptive Chosen Ciphertext Angriff gegen RSA-basierte Protokolle vor.

Der Angriff basiert auf dem festen Format nach PCKS #1 formatierter Nachrichten.

Weiter ausformulieren

5.6 Vaudenay in 2002? Padding Oracle

In [Vau02] beschreibt der Autor einen Angriff zur Erlangung des Klartextes, bei dem das für Blockchiffren nötige Padding im CBC-Modus ausgenutzt wird. Durch das vorgegebene Format des Paddings und da das Padding bei TLS nicht durch den MAC geschützt ist (MAC - then PAD - then Encrypt) ermöglicht es theoretisch in einer relativ kleinen Zahl von Anfragen die Berechnung des Klartextes. Praktisch konnte das Verfahren nicht eingesetzt werden, da SSL 3.0 für Padding- und Entschlüsselungsfehler gleiche Fehlermeldungen ausgibt (TLS 1.0 nicht?) und bei Paddingfehlern mit einem decryption_failed-error die Sitzung abbricht.

Mal gucken

nachschauen!

In [CHVV03] beschreiben die Autoren eine Umsetzung des Angriffs auf TLS-gesicherte IMAP-Verbindungen zur Erlangung von Passwörtern. Hierbei wird das Problem ununterscheidbarer und verschlüsselter Fehlermeldungen durch einen Timing-Angriff umgangen. Außerdem bedenken die Autoren das Abbrechen der Sitzung durch Nutzung vieler paralleler Sitzungen mit dem gleichen verschlüsselten Aufruf (wie es bei der Authentifizierung im IMAP-Protokoll der Fall ist).

Begirff: Padding Oracle einbauen

5.7 Lucky Thirteen

In [AFP13] stellen die Autoren weitere auf [Vau02] basierende Angriffe vor, die ebenfalls auf Timing-Attacken zur Erkennung falschen Paddings und mehrere Verbindungen setzen.

5.8 Bard - IV? Chosen Plaintext Attacks

In [Bar04] stellt der Autor einen Angriff vor, der die Art ausnutzt, wie die für den CBC-Modus nötigen Initialisierungsvektoren (IV) von TLS bereitgestellt werden. Durch die Nutzung des letzten Ciphertextblocks der letzten Nachricht als IV der neuen Nachricht lässt sich unter bestimmten Vorraussetzungen ein Chosen-Plaintext-Angriff durchführen. Der Autor beschreibt eine Möglichkeit unter Nutzung von Browser-Plugins über HTTPS übertragene Passwörter oder

PINs herauszufinden. In [Bar06] verbessert der Autor seinen Angriff durch nie Nutzung von Java-Applets anstelle von Browser-Plugins.

Seit TLS 1.1 werden explizite IV vorgeschrieben. Hierzu besteht jede Nachricht aus einem Ciphertextblock mehr als Klartextblöcken. Dieser erste Block bildet den IV für die restliche Verschlüsselung. Da dieser IV nicht vor dem Senden der Nachricht bekannt ist, wird der hier beschriebene Chosen-Plaintext-Angriff verhindert.

5.9 BEAST

In [DR11] und in einem Konferenzbeitrag auf der ekoparty Security Conference 2011 wurde von den Autoren das Tool BEAST vorgestellt, dass die Ideen aus [Bar04] aufgreift. Die Autoren erweiterten den Angriff jedoch auf einen sogenannten block-wise chosen-boundary Angriff, bei dem der Angreifer die Lage der Nachricht in den verschlüsselten Blöcken verändern kann. Die Autoren zeigten auch die praktische Umsetzbarkeit am Beispiel des Entschlüsselns einer über HTTPS gesendeten Session-ID.

5.10 CRIME

Auf der ekoparty Security Conference 2012 stellten die Entdecker des BEAST-Angriff einen weiteren Angriff vor, der die (optionale) Kompression in TLS nutzt, um beispielsweise Cookiedaten zu stehlen.

5.11 Poodle

In [MDK14] nutzen die Autoren den erneuten Verbindungsversuch mit älteren Protokollversionen wenn der Handshake fehlschlägt (SSL 3.0 Fallback), der in vielen TLS-Implementationen eingesetzt wird. Darauf aufbauend beschreiben sie einen Angriff, der bestehende Schwächen in der RC4-Chiffrebzw. in der Nicht-Prüfung von Padding im CBC-Modus in SSL 3.0 ausnutzt, um Cookiedaten zu stehlen.

RC4 noch irgendwo unterbringen? Vllt bei den Ciphersuites?

5.12 FREAK

Eine Gruppe von Pariser Wissenschaftlern entdeckte eine Möglichkeit, wie ein Angreifer die Kommunikationspartner während des Handshakes zur Nutzung schwacher Kryptographie (RSA export cipher suite) bringen kann. Weiterhin zeigten sie in [BDLF+] die Machbarkeit der Faktorisierung der entsprechenden RSA-Module und die Praxistauglichkeit des Angriffs.

5.13 logjam

In [ABD+] beschreiben die Autoren mehrere Angriffe gegen die Nutzung von Diffie-Hellman(DH)-Schlüsselaustausch während des TLS Handshakes. Ein Angriff richtet sich gegen kleine DH-Parameter (DHE-EXPORT), ein weiterer nutzt die weite Verbreitung von standardisierten DH-Parametern, um mittels Vorberechnung bestimmter Werte schneller diskrete Logarithmen für beim DH-Verfahren gesendete Nachrichten zu berechnen.

5.14 Probleme bei Zertifikatvalidierung und bei CAs und Diebstahl privater Schlüssel

Viele Probleme, die in den letzten Jahren aufgetreten sind, betreffen nicht das TLS-Protokoll direkt, sondern die Erstellung und Validierung von (insbesondere) Server-Zertifikaten, und seien deshalb nur am Rande erwähnt. Ein guter Überblick ist in [MS13] zu finden.

Viele dieser Angriffe richteten sich gegen mangelnde Zertifikatvalidierung in TLS-Implementierungen (keine Validierung, keine Überprüfung des Servernamens, Akzeptanz unsignierter oder abgelaufener Zertifikate, ...) oder wenig Sorgfalt bei der Zertifikaterstellung durch Certificate Authorities (Nutzung von MD5, fehlerhafte Validierung von übermitttelten Servernamen, fehlerhafte Ausgabe von intermediate-Zertifikaten, mangelhaft abgesicherte Server, ...).

Der Vollständigkeit halber sei hier auch noch die notwendige Sicherheit des privaten Serverschlüssels erwähnt. Gelangt ein Angreifer in seinen Besitz, so kann er den Datenverkehr problemlos mitlesen oder verändern.

6 Protokollversion 1.3

Literaturverzeichnis

[ABD+] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. Zugriff am 22.05.2015.

[AFP13] N. J. Al Fardan and K. G. Paterson. Lucky thirteen: Breaking the tls and dtls record protocols. *2014 IEEE Symposium on Security and Privacy*, 0:526–540, 2013.

[Bar04] Gregory V. Bard. Vulnerability of ssl to chosen-plaintext attack. Technical report, 2004.

[Bar06] Gregory V. Bard. A Challenging But Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL. In *SECRYPT 2006, Proceedings of the international conference on security and cryptography*, pages 7–10. INSTICC Press, 2006.

[BDLF+] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, Santiago Zanella-Béguelin, Jean-Karim Zinzindohoué, and Benjamin Beurdouche. FREAK: Factoring RSA Export Keys. https://www.smacktls.com/#freak. Zugriff am 22.05.2015.

[Ble98] Daniel Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1. In *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '98, pages 1–12, London, UK, 1998. Springer-Verlag.

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In *Advances in Cryptology - ASIACRYPT 2000*. Springer Berlin Heidelberg, 2000.

[CHVV03] Brice Canvel, Alain P. Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a ssl/tls channel. In *Advances in Cryptology - CRYPTO 2003*, volume 2729, pages 583–599. Springer, 2003.

[DR11] Thai Duong and Juliano Rizzo. Here Come The XOR Ninjas. 2011.

[Eck13] Claudia Eckert. *IT-Sicherheit - Konzepte, Verfahren, Protokolle*. Oldenbourg Verlag, München, 2013.

[KBC97] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997.

[Kra01] Hugo Krawczyk. The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?). In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 310–331, London, UK, 2001. Springer-Verlag.

[MDK14] Bodo Möller, Thai Duong, and Krzysztof Kotowicz. This POODLE Bites: Exploiting the SSL 3.0 Fallback, 2014.

[MS13] Christopher Meyer and Jörg Schwenk. SoK: Lessons Learned From SSL/TLS Attacks. In *The 14th International Workshop on Information Security Applications*, 2013.

[Sch09] Klaus Schmeh. *Kryptographie - Verfahren, Protokolle, Infrastrukturen*. dpunkt.verlag, Heidelberg, 2009.

[Vau02] Serge Vaudenay. Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS... In *Advances in Cryptology - EUROCRYPT 2002*, pages 534–545. Springer, 2002.

[WS96] David Wagner and Bruce Schneier. Analysis of the SSL 3.0 Protocol. In *The Second USENIX Workshop on Electronic Commerce*, pages 29–40. USENIX Association, 1996.