Verschlüsselung der Kommunikation zwischen Rechnern

Stand: 11. Mai 2007

Rechenzentrum Hochschule Harz

Sandra Thielert

Hochschule Harz
Friedrichstr. 57 – 59
38855 Wernigerode
03943 / 659 – 0

Inhalt

Abkürzungen

SSL	Secure Socket Layer
TLS	Transport Layer Security
HTTP	Hypertext Transport Protocol
S-HTTP	Secure Hypertext Transport Protocol
RC4	Rivest Cipher 4
DES	Data Encryption Standard
RSA	Rivest, Shamir, Adleman
CA	Certificate Authority

1 Einleitung

Für den Betrieb eines Servers müssen verschiedene Sicherheitsmaßnahmen vorgenommen werden, um den Serverbetrieb und die auf dem Server befindlichen Daten zu schützen. Hierbei spielen die Vergabe von Benutzer- und Gruppenrechten sowie die Konzeptionisierung der Zugriffsbeschränkungen eine wichtige Rolle. Bei der Integrierung eines Servers in ein Netzwerk kommen weitere Sicherheitsregeln hinzu. Diese sind zum Einen die Beschränkung bzw. Koordinierung der externen Zugriffe auf den Server und zum Anderen die Gewährleistung das übertragene Daten nicht von Dritten abgehört werden können.

Um eine sichere Übertragung von sensiblen Daten, wie z.B. Nutzername und Passwort, über eine unsichere Verbindung, wie z.B. das Internet, zu gewährleisten wurden verschiedenste Verfahren entwickelt.

Als Standard wird derzeit das SSL (Secure Socket Layer) Verfahren[1] bzw. der Nachfolger TLS (Transport Layer Security)[2] eingesetzt. Der Kommunikationsablauf sowie grundlegende Informationen zu diesem Verfahren werden im nächsten Abschnitt erläutert.

Das S-HTTP (Secure Hypertext Transfer Protokoll) konnte sicht nicht durchsetzen, da es nur für http anwendbar ist.

[1] ursprünglich entwickelt von Netscape

[2] wurde im RFC 2246 verabschiedet [Eilebrecht]

2 SSL (Secure Socket Layer) und sein Nachfolger TLS (Transport Layer Security)

Das zugrundeliegende Protokoll einer SSL bzw. TLS Verbindung ist das https Protokoll, welches alle Daten der gegenwärtigen Kommunikation zwischen Server und Client verschlüsselt übermittelt über seinen Standardport 443. So kann gewährleistet werden das ein unberechtigter Dritter keinen Zugriff auf sensible Daten hat. Angezeigt wird eine SSL Verbindung durch ein geschlossenes Vorhängeschloss in der Statuszeile des Browsers.

Ein großer Vorteil des SSL Verfahrens gegenüber anderen sind die weitreichenden Einsatzmöglichkeiten für die verschiedensten Arten von Diensten wie Tabelle 1 zeigt.

Schichten des OSI-Modells			**Dienste für SSL**
7	Anwendungsschicht	application Layer	Telnet, FTP, SMTP, NNTP, HTTP
6	Darstellungsschicht	presentation layer	
5	Sitzungsschicht	session layer	
4	Transportschicht	transport layer	TCP, UDP
3	Vermittlungsschicht	network layer	
2	Sicherungsschicht	data link layer	
1	Bitübertragungsschicht	physical layer	

Tabelle 1: Einsatz von SSL auf den verschiedenen Ebenen des OSI-Modells nach [Kredel]

Natürlich muss dabei beachtet werden das die Rechenleistung durch die Ver- und Entschlüsselung der zu übertragenden Daten erhöht wird.

2.1 Ablauf der Kommunikation

Beim Verbindungsaufbau vom Client zum Server wird ein Sitzungsschlüssel (Session Key) erstellt, der auf einem symmetrischen Verfahren, meist RC4 (Rivest Cipher 4) oder DES (Data Encryption Standard), basiert. Mit diesem

Sitzungsschlüssel werden die eigentlichen Daten der Kommunikation verschlüsselt bzw. entschlüsselt. Die Übertragung des Sitzungsschlüssel selbst wird abgesichert, durch eine asymmetrische Verschlüsselung mittels dem öffentlichen Schlüssel der Gegenseite.

Für den Nachweis der Identität der Rechner wird für SSL ein Serverzertifikat benötigt, welches von einer unabhängigen Zertifizierungsinstanz signiert wurde. Hierdurch wird die Identität des Rechners bzw. die Zugehörigkeit des öffentlichen Schlüssels zu diesem Rechner bestätigt. Dieses Zertifikat wird bei Verbindungsaufbau zum Gegenüber gesendet, der Gegenüber hat die Möglichkeit das Zertifikat anzunehmen bzw. abzulehnen.

Die Kommunikation zwischen zwei Rechnern kann demnach nach den drei folgenden Authentifizierungsmechsnismen [Roßbach] ablaufen.

1. Authentifizierung auf beiden Seiten
   Client und Server besitzen jeder ein eigenes Zertifikat und können sich gegeneinander authentifizieren.
2. Authentifizierung des Servers
   Bei dieser Variante besitzt nur der Server ein Zertifikat. Die Absicherung der Kommunikation verläuft nur in eine Richtung, vom Client zum Server. Der Ablauf einer solchen Kommunikation ist nachfolgend dargestellt in der Abbildung 1.
3. Authentifizierung erfolgt nicht
   Server und Client besitzen entweder kein Zertifikat oder ein vorhandenes Zertifikat wurde vom Gegenüber abgelehnt, hier kann keine Authentifizierung erfolgen. Die Datenübertragung erfolgt unverschlüsselt.

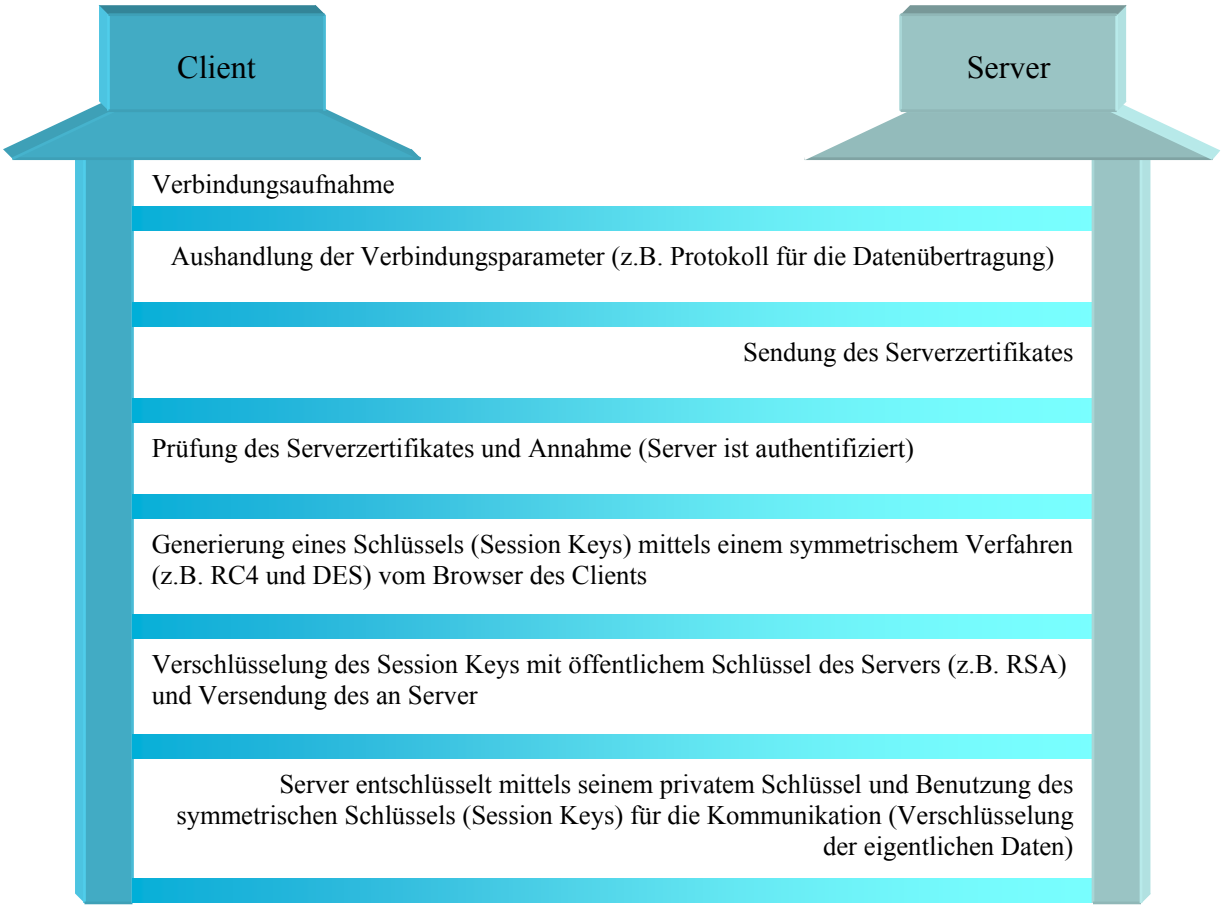

Abbildung 1: Ablauf einer verschlüsselten Kommunikation zwischen Rechnern

2.2 Technische Details des Verfahrens

Das SSL Protokoll besteht aus 2 Schichten, zum Einem die Steuerprotokolle und zum Anderen das Rekordprotokoll. Die Steuerprotokolle dienen zur Aushandlung der Verbindungsparameter, wie z.B. den kryptografischen Algorithmus für die Verschlüsselung der zu übertragenen Daten und sie dienen weiterhin zur Übergabe von Fehlermeldungen beim Verbindungsaufbau. Das Rekordprotokoll arbeitet mit den ausgehandelten Parameter und kodiert und überträgt die gewünschten Daten.

2.3 Einführung von SSL auf einen Server

Für die Einbindung von SSL wird, wie schon gesagt, ein Serverzertifikat benötigt, hierzu kann sich ein Testzertifikat erstellt werden bzw. das Zertifikat wird von einer Zertifizierungsstelle, CA (Certificate Authority), ausgestellt. Die Zertifizierungsstelle bürgt, durch ihre Signierung, für die Identität des Rechners, dadurch bekommt das Zertifikat einen offiziellen Charakter. Nachfolgend sind die Schritte für die Einbindung eines Zertifikates in eine Serversoftware aufgelistet.

Schritt 1) Generierung eines Schlüsselpaares, wenn eine Zertifizierung durch eine CA erfolgen soll müssen die Anforderungen der CA beachtet werden. Hierzu gehören die Beachtung der vorgegebenen Schlüssellängen und –algorithmen, weiterhin spielen die Sicherheitsanforderungen für die Aufbewahrung des Privaten Schlüssels eine entscheidende Rolle. SSL wird von allen gängigen Browsern unterstützt, beachtet werden müssen dabei die gegebenen Import- bzw. Exportrestriktionen einiger Länder mit einer Beschränkung auf Schlüssellängen z.B. mit hohen Schlüssellängen, wie RSA (Rivest, Shamir, Adleman) 2048 bit.

Schritt 2) Generierung eines digitalen Antrags (Certificate Requests), mit Beachtung der Vorgaben zur Namensvergabe durch die zuständige CA.

Schritt 3) Ausfüllen und Unterschreiben der verlangten Anträge.

Schritt 4) Persönliches Treffen mit einem Mitarbeiter der CA zur Prüfung der Identität und Übermittlung des Certificate Requests an die CA.

Schritt 5) Erstellung des Zertifikates von der CA

Schritt 6) Das Signierte Zertifikat wird an den Administrator des Rechners übermittelt.

Schritt 7) Einbindung des Zertifikates und des Privaten Schlüssels in die Konfiguration der Serversoftware, dabei muss darauf geachtet werden dass das Zertifikat und der Private Schlüssel vor einem Zugriff durch Dritte geschützt wird. Die Einbindung in die Konfiguration eines Servers ist, in Abhängigkeit von der jeweiligen Software, sehr unterschiedlich und ist auf die Anwendung abgestimmt.

Beispiel: Apache Webbrowser

Für eine Einbindung eines Zertifikates in den Apache Webbrowser werden folgende Pakete benötigt:

- OpenSSL,
  zur Generierung eines Schlüssels und eines Certificate Requests
- mod_ssl,
  dient als Schnittstelle zwischen Apache und OpenSSL für die dynamische Verschlüsselung bzw. Entschlüsselung der Daten. Für jede Version des Apache gibt es eine bestimmte mod_ssl Version.

Schritt 8) Privater Schlüssel im Ordner ssl.key speichern

Schritt 9) Zertifikat im Ordner ssl.crt speichern

Schritt 10) In der Konfigurationsdatei müssen die nachfolgenden Einstellungen geändert werden

a. Freischaltung Port 443 `Listen 443`

b. SSL erlauben `SSLEngine on`

c. Pfadangabe zum Zeritfikat
   `SSLCertificateFile /etc/httpd/conf/ssl.crt/Cert.pem`

d. Pfadangabe zum Privaten Schlüssel
   `SSLCertificateKeyFile /etc/httpd/conf/ssl.key/Key.key`

Literatur

[Eilebrecht] Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas: Apache Webserver Installation, Konfiguration, Administration. mitp-Verlag, Bonn, 2002.

[Roßbach] Roßbach, Stephan: Der Apache Webserver. Addison-Wesley-Verlag, Paderborn, 1999.

[Kredel] Kredel, Heinz: HTTP over SSL (HTTPS). Universität-Mannheim, Rechenzentrum, 2000. http://krum.rz.uni-mannheim.de/web-tech2000w/sess-18.html