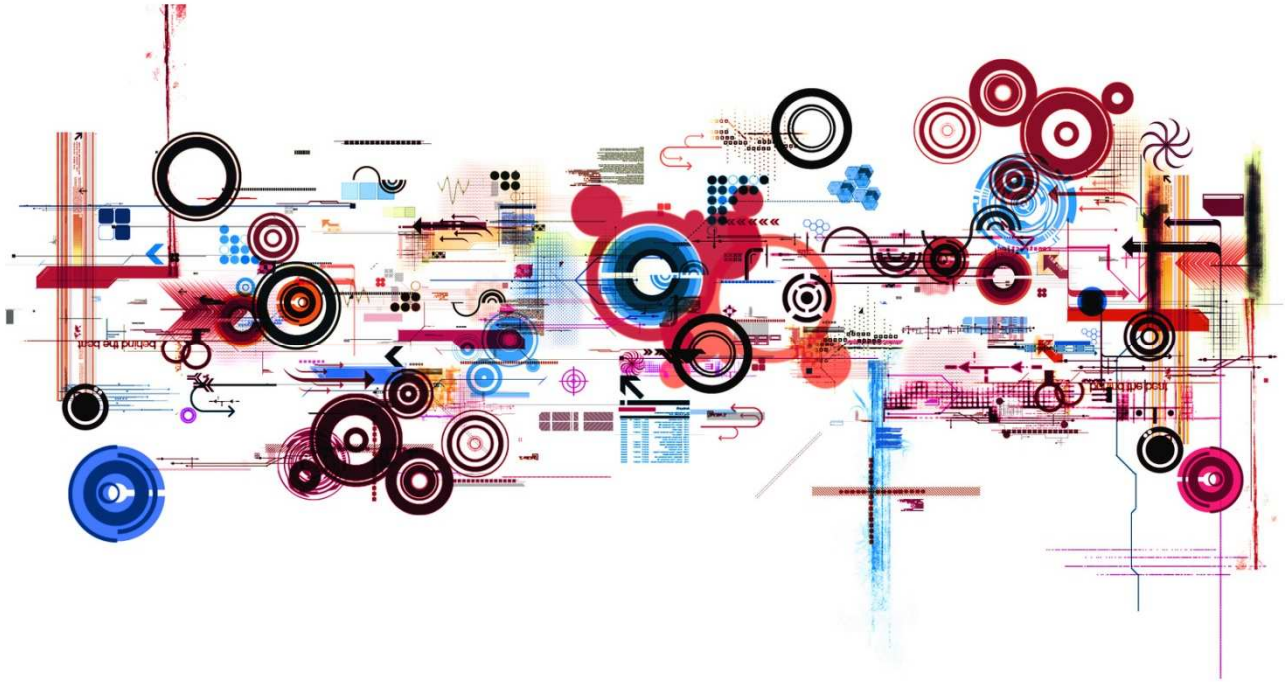
Überwachung von Unternehmenskommunikation

Am Beispiel von SSL Verbindungen



Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Warum Überwachung?

- Einsatz von Web-Anwendungen für unternehmenskritische Prozesse
- Hosting solcher Webanwendungen durch Dritte
- Einsatz von SSL Verschlüsselungen dadurch notwendig
- die Unternehmens-IT verliert durch Verschlüsselung den Einblick in Anwendungen und Transaktionen
- Verbreitung „gefährlicher“ Inhalte durch SSL-Tunnel oder Umgehung von Sicherheitsrichtlinien

Transportprotokolle

HTTPS (Hypertext Transfer Protocol Secure)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Verschlüsselte Datenübertragung
Port:	443/TCP

HTTPS im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	**SSL/TLS**				
	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 2818 (HTTP Over TLS, 2000)

[Docs] [txt|pdf] [draft-ietf-tls-rf...] [Diff1] [Diff2] [IPR] [Errata]

Updated by: 5746, 5878, 6176 — PROPOSED STANDARD
Errata Exist

Network Working Group — T. Dierks
Request for Comments: 5246 — Independent
Obsoletes: 3268, 4346, 4366 — E. Rescorla
Updates: 4492 — RTFM, Inc.
Category: Standards Track — August 2008

The Transport Layer Security (TLS) Protocol
Version 1.2

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Table of Contents

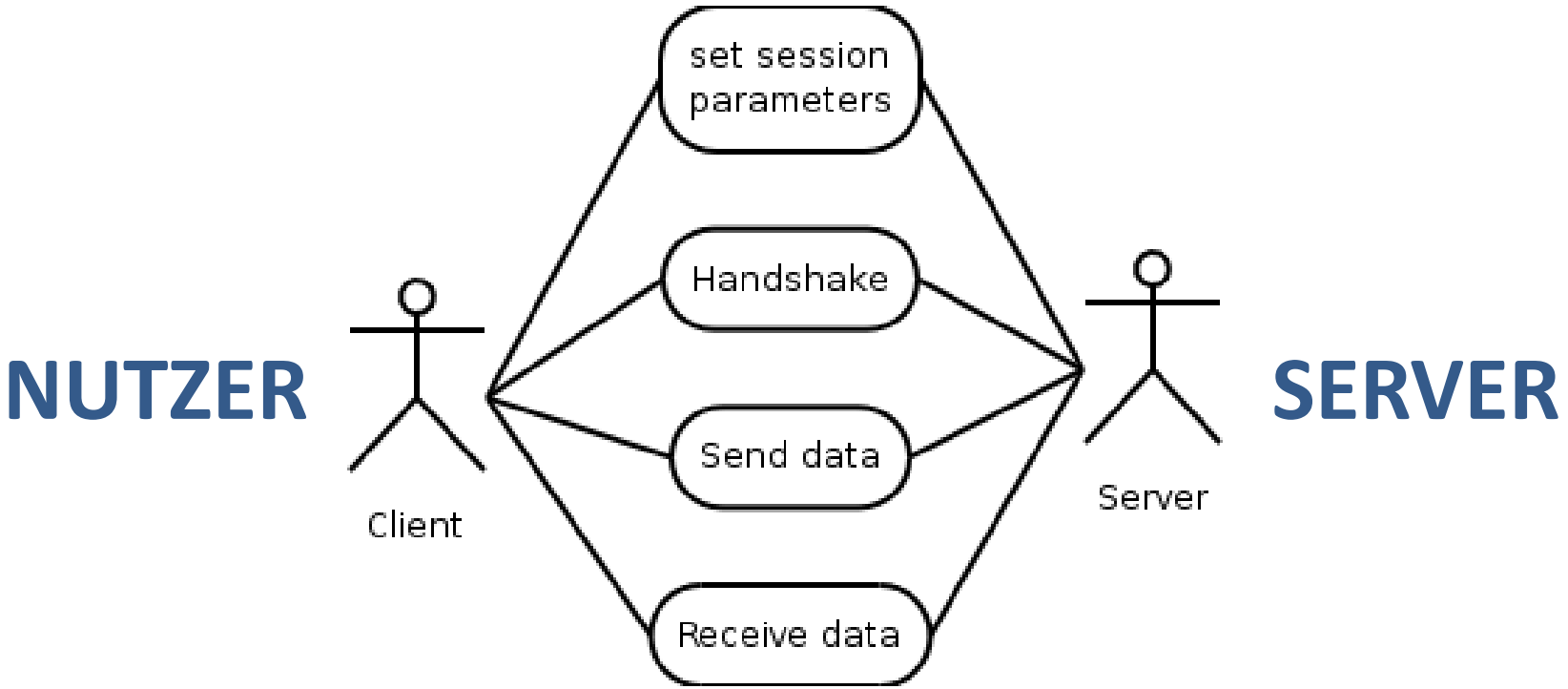
Funktionsweise des SSL/TLS Transportprotokolls

- Bei der Kommunikation werden folgende Ebenen angesprochen:

SSL im TCP/IP-Protokollstapel

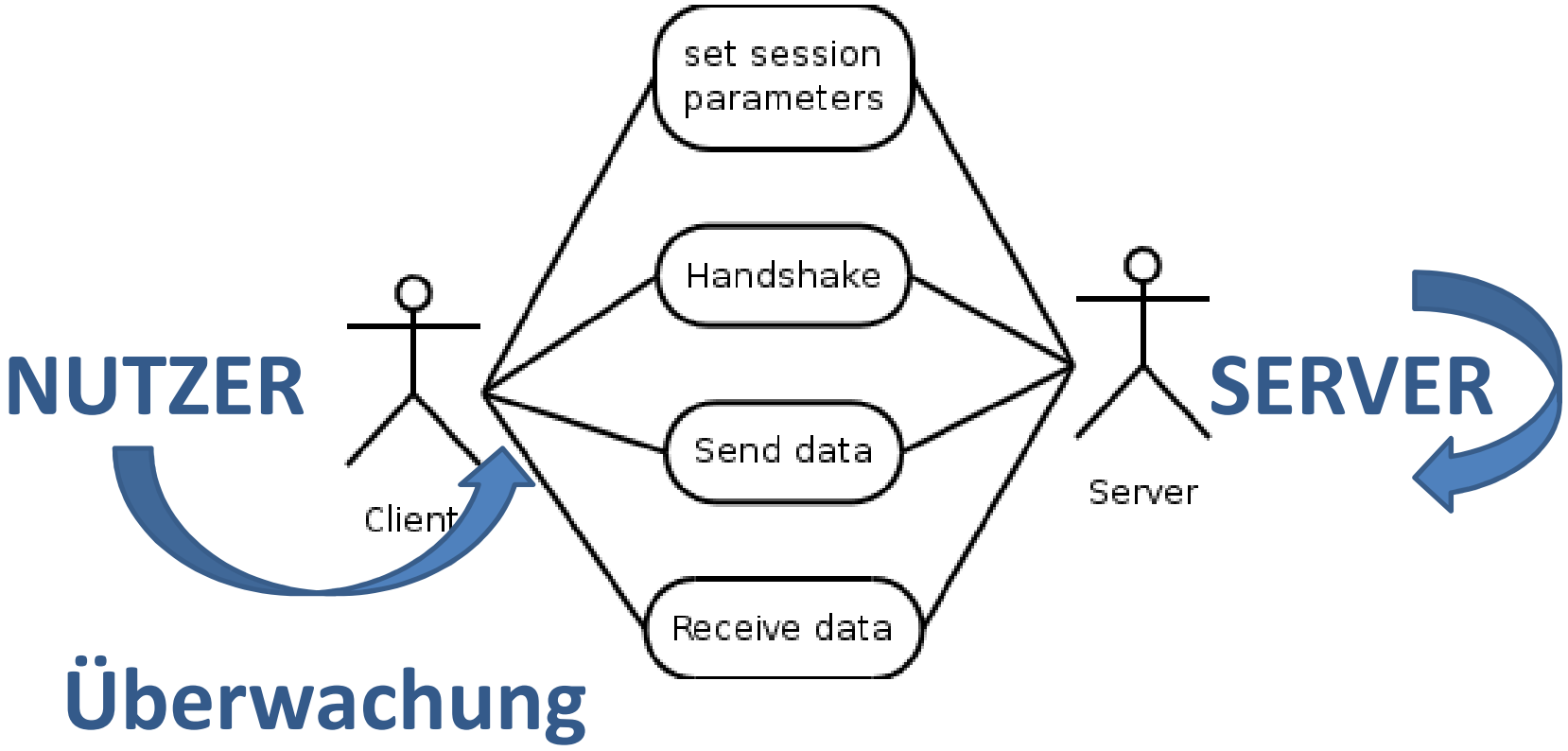
Anwendung	HTTPS	IMAPS	POP3S	SMTPS	...
Transport	**SSL/TLS**				
	TCP				
Internet	IP				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Funktionsweise des SSL/TLS Transportprotokolls



Übertragung

Überwachung des SSL/TLS Transportprotokolls



Überwachung des SSL/TLS Transportprotokolls

WWW über HTTPS

WWW
über HTTPS

Überwachung des SSL/TLS Transportprotokolls

WWW über HTTPS

WWW
über HTTPS

VPN und andere verschlüsselte Verbindungen

- Ihrem Ursprung nach bilden VPNs innerhalb eines öffentlichen Wählnetzes in sich geschlossene virtuelle Teilnetze, wobei das VPN ein reines Softwareprodukt ist.
- Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt und üblicher Weise mit SSL/TLS Verschlüsselung verschlüsselt.
- Auch wenn das virtuelle Teilnetz in einem „fremden“ Netz betrieben wird, ist grundsätzlich die Überwachung der Verbindung möglich.

Nutzerwahrnehmung von SSL Verbindungen

(Nicht nur) die Rente ist sicher!

Nutzerwahrnehmung von SSL Verbindungen

Aufgrund der hohen Verbreitung des SSL/TLS Protokolls, insbesondere durch standardmäßige Implementierung in allen verfügbaren Internet-Browsern, wird das Vorhandensein einer solchen Verbindung durch den Nutzer regelmäßig als sicher wahrgenommen.

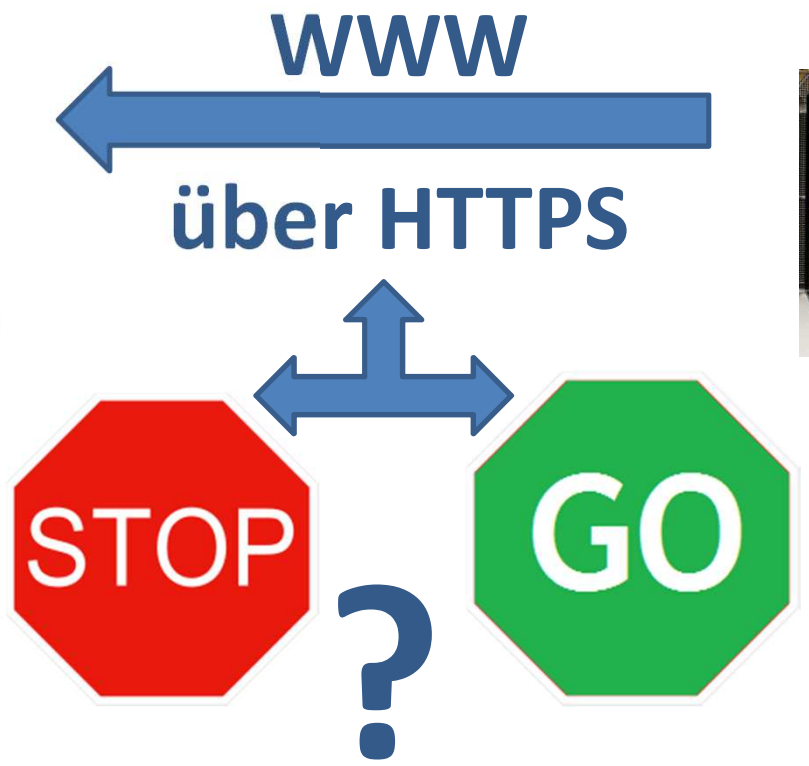
Nutzerwahrnehmung von SSL Verbindungen

Das Vertrauen des Nutzers in die SSL/TLS Verbindung wird dann grundsätzlich zunächst verletzt, wenn ein Eingriff in diese als „sicher“ angesehene Verbindung vorgenommen wird.

Schutzbereiche in der Kommunikation

- Die Integrität und die Vertraulichkeit von Daten, die im Rahmen von elektronischen Kommunikationsvorgängen übermittelt werden, sind durch verschiedene Ebenen des Rechts geschützt.
- Dabei ist bereits der Transportvorgang, in den durch die SSL/TLS Überwachung eingegriffen wird, Schutzgegenstand.
- Darüber hinaus unterliegen auch die entstehenden Daten über das Verhalten des Nutzers dem Schutz gesetzlicher Regelungen.

Einwilligung in die Überwachung?



Schutzbereiche

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

TKG ????

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.

BDSG ????

Schutzbereich

Anwendbarkeit

Einwilligungsfähigkeit

Rechtfertigungsgründe

Vertragliche Vereinbarungen

- Neben den straf- und datenschutzrechtlichen Vorschriften kommen auch noch vertragliche (oder quasi vertragliche) Vereinbarungen in Betracht, die einen besonderen Schutz und/oder ein Interesse der Vertragspartei an der „Unversehrtheit“ der SSL/TLS Verbindung begründen.

- Beispiele von Regelungen:
  - Um die Sicherheit Ihrer Informationen bei Übertragung zu schützen, benutzen wir Secure Sockets Layer Software (SSL). Diese Software verschlüsselt die Informationen, die von Ihnen übermittelt werden. (Beispiel aus Amazon und Banking AGB)
  - Du wirst dein Passwort (oder deinen geheimen Schlüssel, wenn du ein Entwickler bist) nicht weitergeben, eine andere Person auf dein Konto zugreifen lassen oder anderweitige Handlungen durchführen, die die Sicherheit deines Kontos gefährden können. (Facebook AGB)
  - Regelungen zur Geheimhaltung von Pin und Tan in den AGB für Onlinebanking.

Vertragliche Vereinbarungen

- Soweit diese vertraglichen oder quasi-vertraglichen Regelungen einseitig zugunsten des jeweiligen Nutzers gelten, kann dieser einseitig auf einzelne vertragliche Rechte verzichten. Daher ist in diesen Fällen eine Zustimmung oder Einwilligung der anderen Vertragspartei und somit des Betreibers des entsprechenden Webdienstes nicht erforderlich.
- Ein einseitiger Verzicht bei zweiseitigen Verpflichtungen der Vertragsparteien oder bei einer einseitigen Verpflichtung des Nutzers gegenüber der anderen Vertragspartei ist nach BGB jedoch nicht möglich. Hier wäre es erforderlich, dass die andere Vertragspartei zustimmt, also die Zustimmung oder Einwilligung dahingehend erteilt, dass der Nutzer die entsprechende vertragliche Verpflichtung nicht erfüllt.

Umsetzungsmöglichkeiten in Unternehmen

- Strafrechtliche Schutzbereiche einzeln prüfen und jeweils die Erteilung oder Nicht-Erteilung einer Einwilligung dokumentieren.
- Im Hinblick auf § § 203 und 204 StGB ist sicherzustellen, dass solche Mitarbeiter des Unternehmens, die in den Katalog der geschützten Berufe fallen nicht der Überwachung unterliegen.
- Weiter sollte die Einwilligungserklärung auch den Schutzbereich des § 303a StGB im Hinblick auf das Merkmal „Unterdrücken“ umfassen.

Umsetzungsmöglichkeiten in Unternehmen

- Die Einwilligung des Nutzers muss neben den Einwilligungen aus dem strafrechtlichen Bereich auch die datenschutzrechtliche Einwilligung enthalten.
- Die Einwilligung muss dem Nutzer, der die Einwilligung erteilen soll, einen ausreichenden und für ihn verständlichen Überblick über das, wozu er zustimmt gegeben werden, so dass eine entsprechende Überschaubarkeit der Tragweite seiner Entscheidung besteht.
- Wesentlich dabei ist, dass die Einwilligung – und zwar sowohl die für die strafrechtlichen, wie auch die für die datenschutzrechtlichen Schutzbereiche – jeweils auf freiwilliger Basis erfolgt und der klare zustimmende Wille des Nutzers erkennbar und dokumentiert ist.

Umsetzungsbezogene Besonderheiten

- Anpassung/Erstellung von Betriebsvereinbarungen

  Zur Umsetzung des Konzepts der Einwilligungserklärungen und eines abgestuften Überwachungskonzeptes mit Ausnahmeregelungen für einzelne Datenströme oder Ziele sind bestehende Betriebsvereinbarungen anzupassen oder neu zu erstellen.

- Einbindung des Datenschutzbeauftragten und Betriebsrates

  Bei der Umsetzung eines Konzepts von Einwilligungserklärungen und eines abgestuften Überwachungskonzeptes mit Ausnahmeregelungen für einzelne Datenströme oder Ziele ist der betriebliche Datenschutzbeauftragte einzubinden und die Zustimmung des Betriebsrates einzuholen. Dabei ist auch abzustimmen, wie die jeweilige Zustimmung des einzelnen Nutzers erfolgt und dokumentiert wird. Die Personen, die Zugang zu den entstehenden Daten haben, sind auszuwählen und zu überwachen; für den Umgang mit den Daten sind Anweisungen zu erlassen.

Vielen Dank für Ihre Aufmerksamkeit !

Für Rückfragen

ANWALTSCONTOR

Rechtsanwalt Christian R. Kast

www.anwaltscontor.de

itanwalt @ twitter