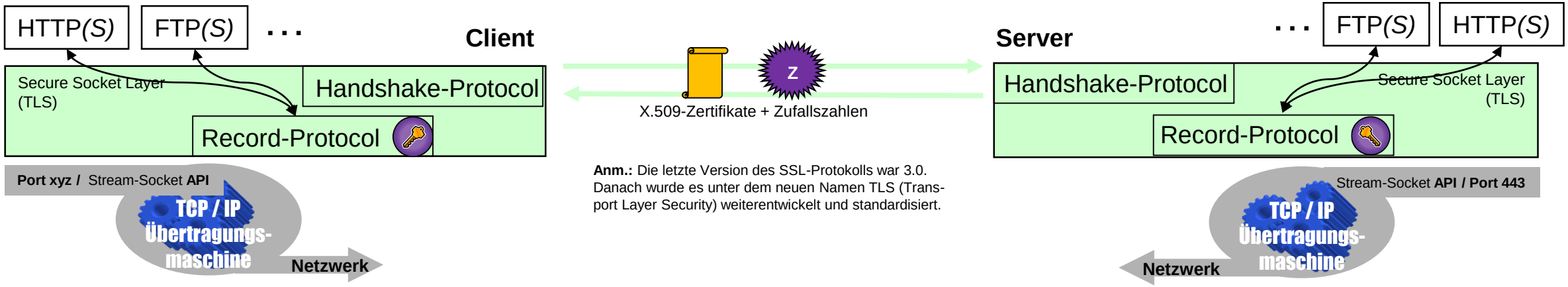
Internet-Transport / Absicherung
KURZÜBERSICHT DER TLS-ABLÄUFE

STUDIEREN AUF HÖCHSTEM NIVEAU

Prof. Nikolaus Hottong, Hochschule Furtwangen
Fakultät Digitale Medien

ABLÄUFE Verschlüsselte Socket-Übertragungen: (SSL/TLS)



Anm.: Die letzte Version des SSL-Protokolls war 3.0. Danach wurde es unter dem neuen Namen TLS (Transport Layer Security) weiterentwickelt und standardisiert.

0. Der Client baut zum Server/Port 443 mittels 3-Wege-Handshake eine bidirektionale TCP/IP-Verbindung auf. Darüber erfolgt nun ...

1. TLS-Handshake ***Client_Hello***: Der Client sendet dem Server eine Liste von Algorithmen, die von ihm unterstützt werden, sowie eine Zufallszahl, die bei der Erzeugung des Schlüssels verwendet wird. TLS unterstützt dabei eine Vielzahl von unterschiedlichen Verschlüsselungsverfahren verschiedener Qualität und Komplexität.

2. TLS-Handshake ***Server_Hello***: Der Server sucht den „sichersten" Algorithmus aus den vom Client angebotenen Verfahren aus und informiert den Client hierüber.

3. Handshake ***Certificate***: Der Server sendet seinen öffentlichen Schlüssel in einem gültigen X.509-Zertifikat an den Client („credential"). Falls eine Client-Authentifizierung per Zertifikat gefordert ist, sendet der Server zusätzlich eine Liste der akzeptierten Zertifizierungsstellen als Zertifikatanforderung.

4. Handshake ***Server_HelloDone***: Zusätzlich versendet auch der Server eine Zufallszahl, die ebenfalls bei der Erzeugung des Schlüssels benötigt wird.

5. Handshake ***ClientKeyExchange***: Der Client überprüft das Zertifikat des Servers. Dann erzeugt er eine zufällige Zeichenfolge (pre master secret) und sendet diese mit dem öffentlichen Schlüssel des Servers verschlüsselt an den Server. Auf der Grundlage der beiden von Server und Client erzeugten Zufallszahlen und des pre master secret berechnen Client und Server unabhängig voneinander die Schlüssel für die nachfolgende Verschlüsselung und die Signaturen. Der Server kann dies nur korrekt durchführen, wenn er im Besitz des zum Server-Zertifikat passenden privaten Schlüssels ist. Im Falle der Client-Authentifizierung sendet der Client zusätzlich ein passendes Client-Zertifikat sowie eine mit dem privaten Schlüssel signierte Prüfsequenz, die Client und Server im bisherigen Protokollablauf gemeinsam berechnet haben, als Berechtigungsnachweis (engl. „credential"). Der Server überprüft das Client-Zertifikat und überprüft die Prüfsequenz mit Hilfe des öffentlichen Schlüssels aus dem Client-Zertifikat.

6. ***ChangeCipherSpec***: Durch diese Nachricht teilt der Client mit, dass er in der aktiven Sitzung auf die ausgehandelte Cipher Suite (Record-Protocol) wechselt.

7. ***Handshake Finished***: Das Finished-Paket enthält eine Signatur über alle übertragenen Handshake-Nachrichten. Auf diese Weise kann der Server herausfinden, ob ein „Man in the Middle"-Angriff die originalen Pakete des Clients verändert hat.

8. Die Dienste aus den höheren Kommunikationsschichten (z.B. FTP, HTTP, QUIC, etc.) starten nun ihre Kommunikation über die zwischengeschobene TLS-Socket-API. Ihre Befehle und Nutzdaten werden beim vertikalen TLS-Durchgang als verschlüsselte Nutzlast in die TCP-Segmente eingepackt.