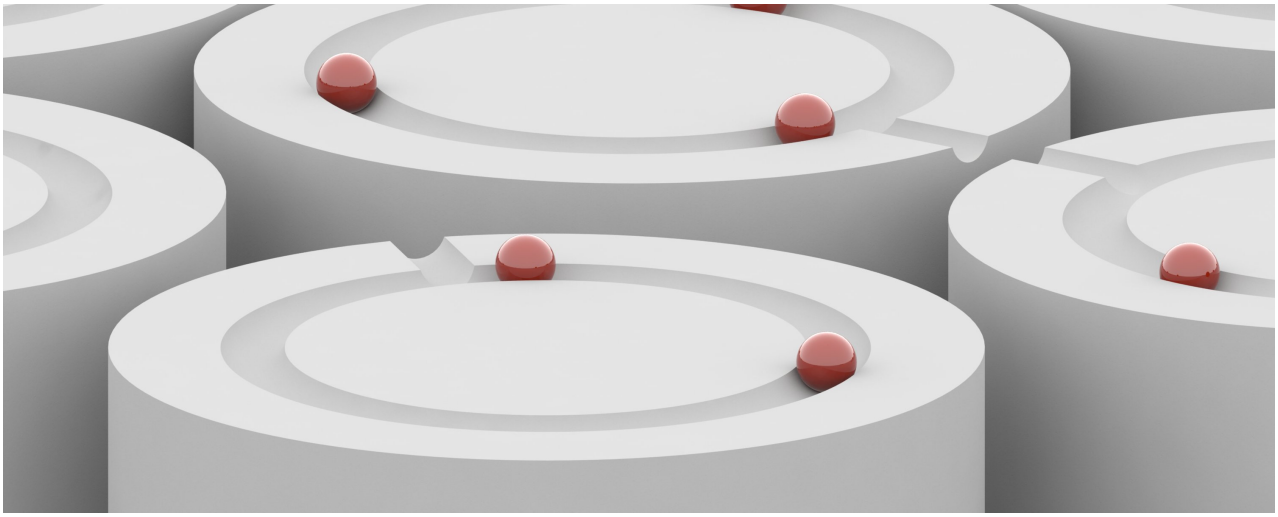


IT-/TK-NETZWERKE

Verschlüsselte VoIP-Kommunikation bei IP-Anschlüssen mittels SIP-over-TLS

Voice over IP wird in der Regel bei Massenmarktanschlüssen unverschlüsselt übertragen. Dabei werden sowohl die Signalisierungsverkehre (SIP) als auch die Medienströme (RTP) über das verbindungslose Transportprotokoll UDP ausgetauscht. Der Hauptvorteil dieses Netzwerkprotokolls liegt im schlanken Aufbau, was eine Overhead-arme und verkehrsmengenreduzierte Übertragung von Daten ermöglicht.

Ein wesentlicher Nachteil von UDP ist die fehlende Verschlüsselungsfunktionalität, der sich spätestens dann bemerkbar macht, wenn ein Service-Provider seinen VoIP-Kunden einen verschlüsselten Sprachdienst anbieten möchte. Mit DTLS besteht ein von der IETF standardisiertes Verschlüsselungsprotokoll, das speziell zur Erfüllung kryptographischer Anforderungen bei der Datenübertragung mittels UDP entwickelt wurde. Jedoch hat sich DTLS bei den Netzwerkgeräteherstellern – bis auf wenigen Ausnahmen – nicht etablieren können, sodass die meisten Vendoren stattdessen auf das im WWW-Umfeld verbreitete TLS setzen.

Die Service-Provider bieten aus vielen Gründen keine Ende-zu-Ende Verschlüsselung für die Übertragung der Voice-Verkehre an. Hierzu zählt u.a. die gesetzlich vorgeschriebene Bereitstellung eines Zugriffs auf die Telekommunikationsdaten. Die verschlüsselte Übertagung von

Signalisierungsdaten und Medienverkehre wird stattdessen vom Kundenanschluss (SIP-fähige Telefonanlage) kommend, auf dem Provider-Edge (SBC – siehe Adiccon-Blog Artikel vom 20.07.2016 link) terminiert. Dabei finden auf Transportebene SIP-over-TLS (für die Signalisierung) bzw. Secure RTP (für die Medienverkehre) Anwendung.

Die Verschlüsselung der übertragenen Daten erfolgt mittels symmetrischer Algorithmen, wie z.B. DES oder AES. Die Nachrichten-Integrität wird über Hash-Funktionen sichergestellt. Die Aushandlung der notwendigen Chiffrierungsparameter, wie z.B. Verschlüsselungsmethode und Schlüssel, erfolgt während der initialen TLS-Handshake Phase (siehe folgende Abbildung).

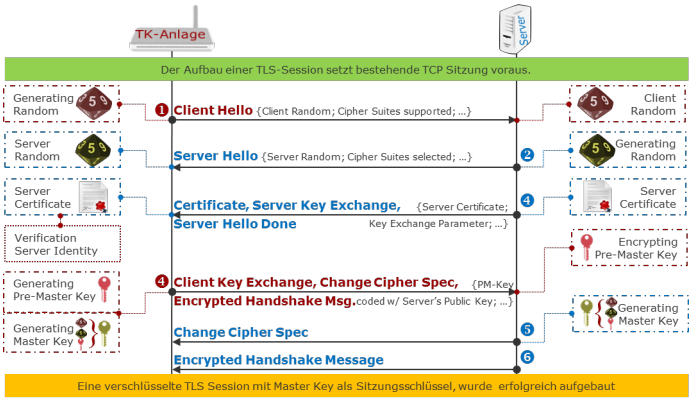


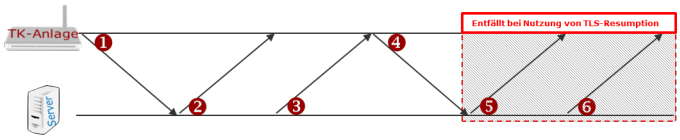
Abbildung 1 TLS-Handshake

Nach dem die TLS Sitzung erfolgreich aufgebaut wurde, erfolgt hierüber die Übertragung der symmetrischen Verschlüsselungsparameter für SRTP. Aufgrund der Abhängigkeit des Schlüsselaustauschs für Medienstrom und Signalisierungsverkehr, ist es nicht empfehlenswert, nur einen Verkehrstyp (SIP bzw. RTP) zu chiffrieren. Wird nur SIP verschlüsselt, können die ungeschützten Sprachpakete abgehört und manipuliert werden. Ist nur der Medienstrom verschlüsselt, so müssen die dafür notwendigen Schlüsselparameter über das offene TCP bzw. UDP übertragen werden und sind dadurch abgreifbar.

Trotz der großen Vorteile des TLS, wie z.B. die starke Etablierung und Verarbeitbarkeit in Middleboxen (z.B. Firewalls, NAT, usw.), birgt die Implementierung dieses Verschlüsselungsstandards auch einige Nachteile, beispielsweise seine zeitintensive Initialisierung. So setzt TLS zunächst den Aufbau einer TCP Sitzung voraus, die ihrerseits erst einen 3-Wege-Handshake ausführen muss. Hierauf folgt die Initialisierung der TLS Sitzung durch Aushandlung der kryptographischen Parameter. Kritisch wird es, wenn die Client-Server Verbindung durch einen Ausfall oder eine Störung unterbrochen wird. Im Rahmen der Wiederherstellung müssen alle TCP/TLS Aufbauvorgänge erneut durchlaufen werden, was aufgrund

des üppigen Zeitbedarfs zu einem negativen Kundenempfinden führen kann.

Eine Möglichkeit, die Wiederherstellung der TLS-Session zu beschleunigen, besteht in der Implementierung der im RFC 5077 standardisierten TLS Erweiterung – die „TLS Session Resumption". Durch die Nutzung der TLS Session Resumption wird der Vorgang der Schlüsselaushandlung abgekürzt und somit die Transportsitzung schneller wiederhergestellt (siehe folgende Abbildung). Die im Rahmen des initialen Verbindungsaufbaus ausgehandelten Verschlüsselungsparameter werden durch den Server in ein sogenanntes „Session-Ticket" verarbeitet und mit dem Servereigenen öffentlichen Schlüssel chiffriert, bevor es zum Ende des Handshakes an den Client übertragen wird. Soll die (unterbrochene) Verbindung erneut aufgebaut werden, überträgt der Client das Session-Ticket an den Server zurück. Dieser entnimmt die Verschlüsselungsparameter aus dem Ticket und setzt die Session wieder fort.



#	Ohne Resumption	Mit Resumption	#	Ohne Resumption	Mit Resumption
1	Client Hello	Client Hello (SessionTicket)	4	Client Key Exchange Change Cipher Spec Encrypted Handshake Msg.	Change Cipher Spec Client Hello Done
2	Server Hello	Server Hello	5	Change Cipher Spec	./.
3	Certificate Server Key Exchange Server Hello Done	Change Cipher Spec New Session Ticket Server Hello Done	6	Encrypted Handshake Message	./.

Abbildung 2 Prozessuale Gegenüberstellung eines TLS Verbindungsaufbaus mit und ohne Session Resumption

Die Voraussetzung für die Nutzung der TLS-gesicherten (mit und ohne TLS-Session Resumption) VoIP-Telefonie ist die Unterstützung des Transportprotokolls sowohl auf dem Provider-Edge (SBC), als auch auf der Telefonanlage. In unseren Untersuchungen mit einer Vielzahl an VoIP TK-Lösungen[1] für kleine und mittelständische Unternehmen haben wir festgestellt, dass ein Großteil der verfügbaren Produkte TLS zur Verschlüsselung von SIP und SRTP für den Medienstrom unterstützt.

Wenn Sie Fragen haben oder weitere Informationen wünschen, sind wir gerne für Sie da. Nehmen Sie Kontakt zu uns auf – wir freuen uns auf Sie!

Verwendete Abkürzungen und Referenzen

DTLS – Datagram Transport Layer Security
NAT - Network Address Translation
RFC - Request for Comments
RTP – Real-Time Transport Protocol
SBC – Session Border Controller
SIP – Session Initiation Protocol
TLS – Transport Layer Security
UDP – User Datagram Protocol
WWW – World Wide Web

[1]Zu den untersuchten SIP-fähigen Telefonanlagen gehören u.a. Produkte der Hersteller AGFEO, AVM, Bintec, LANCOM und Unify.

Veröffentlicht am Donnerstag, 07.06.2018

AUTOR
Masod Said

Vielen Dank für Ihr Interesse.
Weitere Blog Beiträge finden Sie unter adiccon.de