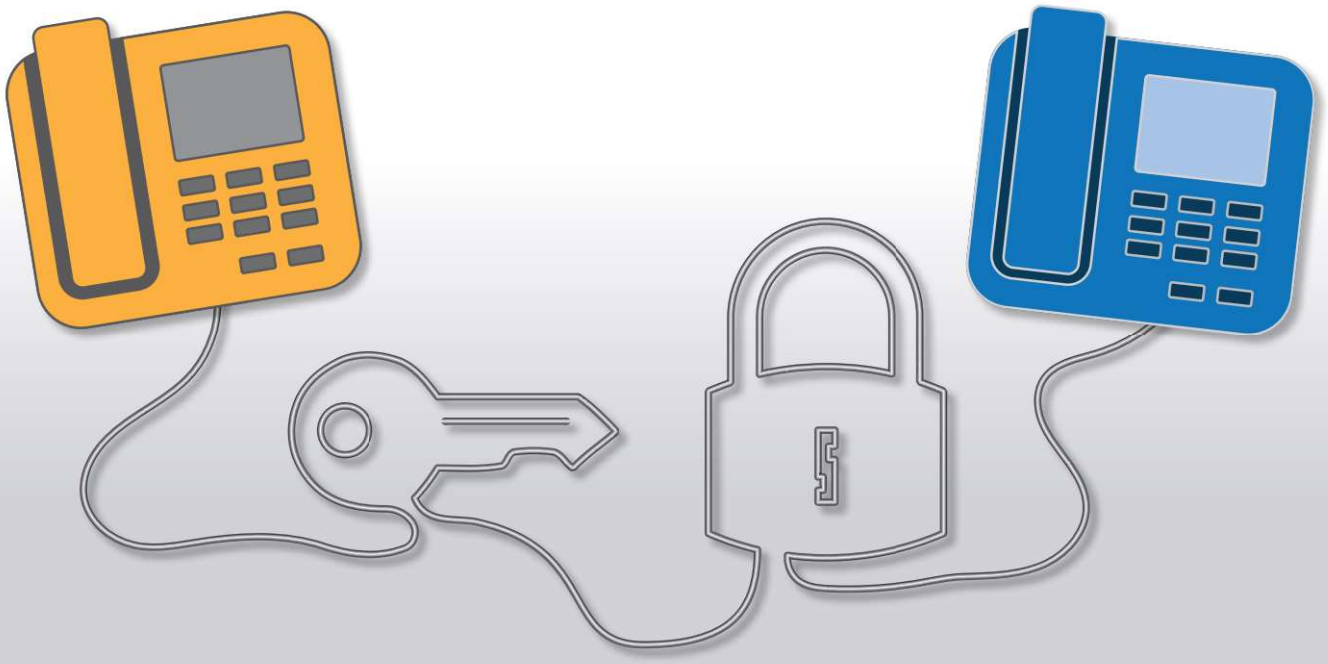
VAF | BUNDESVERBAND TELEKOMMUNIKATION

SIP- und RTP-Verschlüsselung

Eine Praxiseinführung

Gefährdungen und Schutzmaßnahmen für das aktuelle VoIP-Signalisierungsprotokoll und die zugehörigen Medienströme



Grafik: VAF

www.vaf.de

Impressum

SIP- und RTP-Verschlüsselung | Eine Praxiseinführung
Gefährdungen und Schutzmaßnahmen für das aktuelle VoIP-Signalisierungsprotokoll und die zugehörigen Medienströme

Autor:
Benjamin Pfister, Rotenburg an der Fulda

Redaktion:
Chrissanthi Nikolakudi (leitende Redakteurin), Mathias Hein (techn. Beratung), Uwe Klenner (Layout, Titelseite und Bildbearbeitung), Dr. Christian Jerger (Lektorat), Martin Bürstenbinder (für den Herausgeber, V.i.S.d.P.)

Bilder:
Benjamin Pfister; Titelseite und Bildbearbeitungen: VAF

Herausgeber:
VAF Bundesverband Telekommunikation e. V.
Otto-Hahn-Straße 16
40721 Hilden
www.vaf.de

Daniel Brosend (1. Vorsitzender), Martin Bürstenbinder (Geschäftsführer)

1. Auflage, November 2022

Inhaltsverzeichnis

SIP- und RTP-Verschlüsselung

Eine Praxiseinführung

Gefährdungen und Schutzmaßnahmen für das aktuelle VoIP-Signalisierungsprotokoll und die zugehörigen Medienströme

1. Einleitung

Die Sprach- und Videodatenübertragung über IP-basierende Netze erfolgt nach den geltenden Standards völlig ungesichert und birgt daher nicht unerhebliche Gefahren. Ohne eine Konfiguration von Schutzmaßnahmen liegen die Daten jedoch allen Beteiligten auf dem Transportweg im Klartext vor. Selbst im lokalen Netz können sich ohne passende Schutzmaßnahmen Angreifer einen Zugang zu den gewünschten Daten verschaffen. Sowohl die Signalisierung mit SIP als auch die Übertragung der Sprache mit RTP erfolgen normalerweise unverschlüsselt. Bei einem entsprechenden Zugang zum Netz können die Sprachdaten ohne spezielle Kenntnisse und mit frei verfügbaren Tools (Wireshark) einfach mitgelesen werden. Unberechtigte Dritte könnten somit laufende Gespräche abhören und mitschneiden.

Konkret geht es zunächst um die Metadaten in der Signalisierung. Darunter versteht man beispielsweise die Quell- und Zielrufnummern sowie gegebenenfalls auch Namen. Dies hat Relevanz für den Datenschutz. Es sind aber auch die Zeitpunkte des Gesprächsaufbaus und dessen Abbaus als Daten vorhanden. Aus diesen Daten lassen sich bei entsprechender Aufbereitung Kommunikationsmuster der Nutzenden ableiten. Aber auch ungewünschte Gesprächsbeendigungen durch Attacken oder von Angreifern provozierte Überlastungen bis hin zur Quittierung des Telefondienstes, sogenanntes Denial of Service, bergen Risiken. Nicht zuletzt birgt der Missbrauch der Signalisierung die Gefahr des Gebührenbetrugs.

Neben der Signalisierung liegen jedoch auch die Mediendaten, also die inhaltlichen Informationen, wie Sprache oder Video im Klartext vor. Während in Datennetzen die Verschlüsselung schon seit vielen Jahren in vielfältigen Ausprägungen und Szenarien zum Einsatz kommt, fristet sie in IP-basierenden Sprach- und Videonetzen noch ein Nischendasein. Von einer Verbreitung wie im Web, wie bei der TLS-geschützten Übertragung von HTTP über HTTPS, sind wir im Telefonieumfeld noch weit entfernt.

Erfolgreiche Angriffe auf VoIP-Plattformen werden selten öffentlich gemacht, sei es aufgrund der Sorge vor negativer Reputation oder aufgrund der Kommunikationsrichtlinien der betroffenen Unternehmen, die eine Mitteilung nach außen unterbinden. Dass die Attacken auf VoIP-Systeme auch in Europa zunehmen, kann man beispielsweise an dem massiven Angriff auf VoIP-Service-Provider in Großbritannien im Oktober 2021 erkennen.

Bei Angriffen auf VoIP-Netze stehen jedoch nicht nur die direkten Auswirkungen im Mittelpunkt. Schlecht gesicherte VoIP-Netze können bei Kompromittierung auch negative Auswirkungen auf die Datennetze haben.

Verschlüsselung stellt also einen zentralen Baustein der Absicherung in VoIP-Netzen dar.

Den Systemintegratoren muss jedoch bewusst sein, dass nicht nur die Aufwände bzw. die Zeiten für die Implementierung, den Betrieb und die Fehleranalyse, sondern auch die Abhängigkeiten von Diensten wie DNS (Domain Name System) und NTP (Network Time Protocol) bei dem Einsatz von Verschlüsselung zunehmen. Auch Kunden mussten zunächst ein Bewusstsein für die Gefährdungen entwickeln. Aufgrund der aktuellen Gefährdungslage im IT/TK-Sektor, inklusive der medialen Wirkung, verbessert sich dies jedoch. Daher gibt es auch vermehrt Anfragen zur Verschlüsselung der Telefonie. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt in seiner aktuellen Veröffentlichung »NET.4.2 für VoIP« die Verschlüsselung ab einem Schutzbedarf »Standard«.

2. Grundlagen der Verschlüsselung

Verschlüsselung bietet grundsätzlich die Möglichkeit, übertragene oder gespeicherte Daten zu schützen. Sie soll Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen.

Nicht vertrauenswürdige Dritte sollen keinen Zugang zu den verschlüsselten Informationen haben (Vertraulichkeit) und diese nicht verändern können (Integrität). Zudem soll die Betriebsbereitschaft möglichst hoch sein, ohne dass ein Dritter durch Attacken Fehlfunktionen herbeiführen kann (Verfügbarkeit). Zusätzlich geht es jedoch auch um die Sicherstellung der Identifizierbarkeit des jeweiligen Kommunikationspartners (Authentizität der übermittelten Informationen) und die Privatsphäre der Nutzenden.

Grundsätzlich baut die Verschlüsselung darauf auf, dass es einen zu schützenden und zu verschlüsselnden Inhalt gibt, seien es Informationen zur Quell- und Zielrufnummer in der Signalisierung als vertraulicher Inhalt oder ein RTP-Stream mit schützenswerter Sprache. Ein oder mehrere Schlüssel und eine zugehörige Richtlinie zu den unterschiedlichen Verschlüsselungsverfahren stellen die Grundlage für die Verschlüsselung dieser Daten dar und bieten somit entsprechenden Schutz.

Die Verschlüsselung und Entschlüsselung kosten jedoch auch Zeit und Ressourcen. So braucht es CPUs (Central Processing Units; umgangssprachlich auch Prozessoren genannt) als Ressource für die zugehörigen Berechnungen. Diese Berechnungen kosten jedoch auch Zeit, was bei Echtzeitapplikationen, wie der Übertragung von Sprache und Video, kritisch ist.

2.1 Symmetrische Kryptografie

Bei einer symmetrischen Kryptografie sind beide Kommunikationspartner im Besitz des gleichen Schlüssels. Dieser ermöglicht die Ver- und Entschlüsselung der Daten mit nur einem Schlüssel, wie **Bild 1** darstellt. Ein prominentes Beispiel stellt der Advanced Encryption Standard (AES) dar, der sehr häufig zur Anwendung kommt. Der Vorteil symmetrischer Verschlüsselung gegenüber asymmetrischer Verschlüsselung ist, dass sie ressourcenschonender ist. Entsprechend höher ist die Performanz. Es muss jedoch sichergestellt sein, dass der geheime Schlüssel über einen sicheren Weg ausgetauscht wurde.

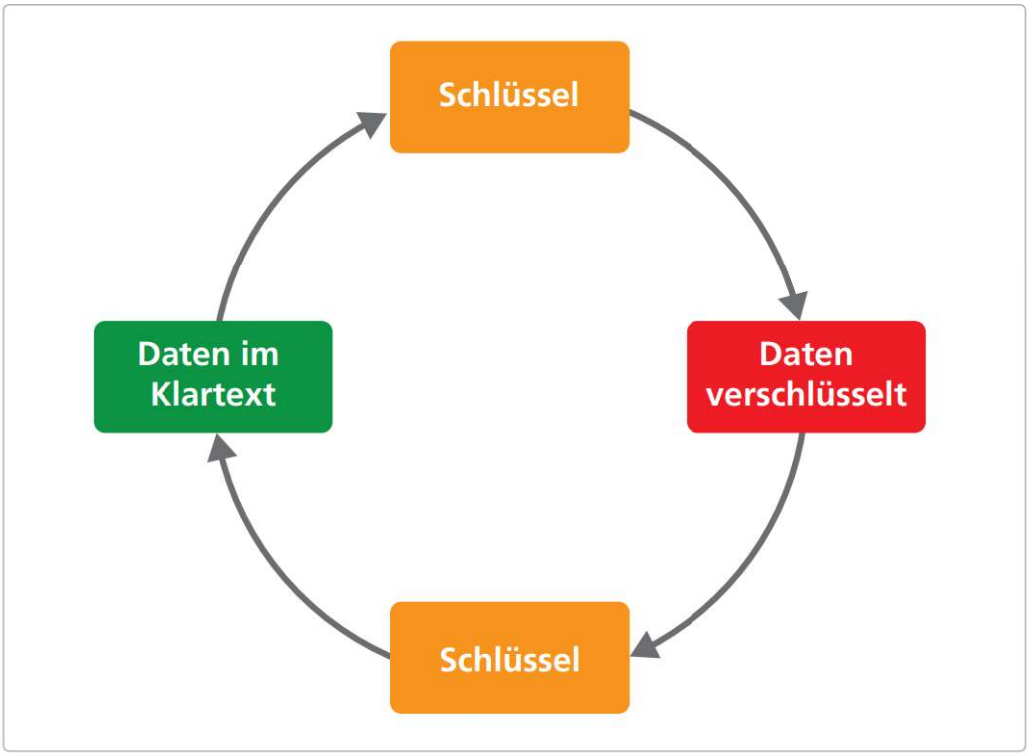


Bild 1 Konzept symmetrischer Verschlüsselung. Es kommt der gleiche Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln zur Anwendung.

2.2 Asymmetrische Kryptografie

Bei der asymmetrischen Kryptografie kommt nicht ein einzelner Schlüssel, sondern ein Schlüsselpaar zur Anwendung. Konkret handelt es sich um einen öffentlichen (Public Key) und einen privaten Schlüssel (Private Key). Das Prinzip baut mathematisch auf eine Funktion auf, die einfach zu rechnen ist. Die Umkehrung muss dagegen sehr aufwendig sein. Asymmetrische Verfahren sind wesentlich ressourcenintensiver als symmetrische Verfahren.

Der öffentliche Schlüssel dient der Verschlüsselung, der private Schlüssel der Entschlüsselung. Aus dem öffentlichen Schlüssel lässt sich der private Schlüssel nicht leicht erraten oder berechnen. Daher kann er auch der Gegenstelle bekannt gegeben werden. Wie in **Bild 2** dargestellt, verschlüsselt der Client, in diesem

Bild 2 Konzept asymmetrischer Verschlüsselung am Beispiel einer SIP-TLS-Verschlüsselung zwischen IP-Telefon und SIP-Proxy

Fall das IP-Telefon, die Daten mit dem öffentlichen Schlüssel des SIP-Proxys. Nur mithilfe des privaten Schlüssels des SIP-Proxys ist es möglich, diese Daten wieder zu entschlüsseln. Der private Schlüssel bedarf also eines besonderen Schutzes.

3. Grundlagen der digitalen Zertifikate

3.1 Anwendungsszenarien SIP

Eine wichtige Grundlage für die Verschlüsselung von SIP-Nachrichten stellen digitale Zertifikate dar. Im Tagesgeschäft von TK-Systemhäusern fallen Zertifikate meist nur auf, wenn es Probleme mit ihnen gibt. Sei es ein Provider, der seine Kunden nicht rechtzeitig über den notwendigen Tausch seines TLS-Zertifikats informiert, oder sogar gestörte UCC-Dienste, weil Zertifikate abgelaufen oder aus anderen Gründen nicht valide sind. Was im Fall von lokal beim Kunden befindlichen IP-PBX-Systemen oder UCC-Diensten zum Ausfall des entsprechenden Dienstes eines Kunden führte, führt bei immer häufiger angebotenen multimandantenfähigen Public Cloud Services zu einem Denial of Service für alle daran angebundenen Kunden – ein Super-GAU für den Dienstanbieter.

Im Geschäftlichen wie auch im Privaten basiert vieles auf Vertrauen. Fehlt es, kann keine Interaktion mit dem Gegenüber stattfinden. Wenn ein guter Freund eine Handwerksfirma empfiehlt, vertrauen wir ihm. Ähnlich geschieht dies bei digitalen Zertifikaten. Den guten Freund stellt, wie in **Bild 3** (1.) dargestellt, die Zertifizierungsstelle dar. Die Zertifizierungsstelle bestätigt über die Signierung des Serverauthentifizierungszertifikats die Identität (2.) des Servers. Die Übertragung vertraulicher Informationen findet auf Basis dieser über die Zertifizierungsstelle dargestellten Vertrauensstellung zwischen IP-Telefon und SIP-Server (3.) statt. Im digitalen Umfeld legen jedoch manchmal Dritte, wie Microsoft, Apple

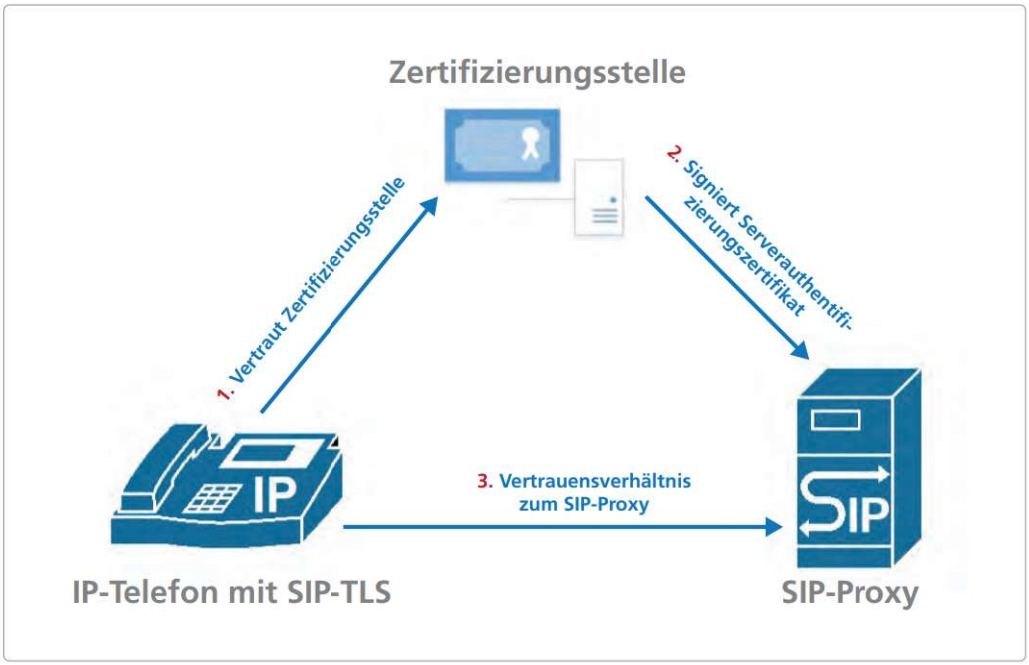


Bild 3 Beispielhafte Vertrauensstellung zwischen einem Telefon und einem SIP-Proxy