

Schwerpunktthema

Herausforderung VoIP-Sicherheit Wie sicher ist die Kommunikation von morgen

von Dr. Behrooz Moayeri

Als der Autor am folgenden Beitrag arbeitete, wurde bekannt, dass die neue französische Regierung aus Sorge vor einer eventuellen Ausspionierung durch den amerikanischen Geheimdienst National Security Agency (NSA) den Gebrauch von mobilen Geräten des Typs BlackBerry in den Ministerien Frankreichs verboten hat.

Dahinter steht die Unsicherheit, was mit Nachrichten geschieht, die in den Rechenzentren des BlackBerry-Anbieters RIM weiter vermittelt werden. Obwohl das kanadische Unternehmen RIM immer wieder beteuert, dass eine Verschlüsselung für die ausreichende Sicherheit der Kun-



daten sorgt, warnen Experten davor, sich vollständig auf diese Zusicherung zu verlassen, und empfehlen zusätzliche Verschlüsselungsmaßnahmen.

Ein ähnliches Problem wird mit der zunehmenden Nutzung von Voice over IP (VoIP) und insbesondere der zunehmenden Nutzung des Internet für die Sprachkommunikation entstehen, nämlich die Unsicherheit, über welche Wege die Gespräche übertragen werden und wer sie abhören kann.

weiter auf Seite 16

Zweitthema

Neue Flusskontrolle in Vista - 50% mehr Last, Netzwerke in Gefahr?

von Dipl.-Inform. Oliver Flüs

TCP ist immer noch auf eine 20 Jahre alte Netzwerk-Technik optimiert. Im Wesentlichen bedeutet dies, dass es versucht, Engpässe zu vermeiden, die mittlerweile nur noch in Sondersituationen vorkommen, im LAN praktisch gar nicht.

So werden große Teile der Bandbreite moderner Netzwerke gar nicht genutzt. Zum Beispiel könnten Backup-Vorgänge über das Netzwerk bei voller Nutzung des gegebenen Potenzials um bis zu 50% schneller erfolgen. So erklärt sich auch, dass viele Benutzer beim Aufrüsten von 100 Mbit/s auf Gigabit-Netzwerke eigentlich keinen messbaren Unterschied in der Performance feststellen.

Nun hat Microsoft mit Vista den „Next-Generation IP-Stack“ eingeführt. Vollerendet wird diese Neuerung mit dem Gegenstück auf der Server-Seite, wenn Longhorn auf den Markt kommt.

weiter auf Seite 5

Aktueller Kongress

**Voice-over-IP-
Forum 2007**

Geleit

**ComConsult
Certified
Voice Engineer**

Report des Monats

**Session Initiation
Protocol**

Schwerpunktthema

Herausforderung VoIP-Sicherheit

Wie sicher ist die Kommunikation von morgen?



Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Fortsetzung von Seite 1

Die auf klassische, auf Time Division Multiplexing (TDM) und Leitungsvermittlung basierende Sprachkommunikation (siehe Abbildung 1) nutzt bisher eine Infrastruktur für Telekommunikation (TK), die bestimmte Merkmale aufweist. Einige dieser Merkmale sind im Folgenden aufgeführt:

- TDM-Netze arbeiten verbindungsorientiert. Dies bedeutet, dass vor jeder Informationsübertragung zunächst explizit eine Verbindung aufgebaut werden muss. Diese Verbindungsaufbauphase (Signalisierungsphase) ist eine geeignete Phase für die Implementierung von Sicherheitsmechanismen. Zum Beispiel können bestimmte Verbindungen aus Sicherheitsgründen verhindert werden.
- Die digitalen TDM-Netze nutzen Out-of-band-Signalisierung. Dies bedeutet, dass die Informationsströme für Sprache und Signalisierung (Nutzdaten und Steuerdaten) über verschiedene Kanäle übertragen werden. Ein Beispiel dafür ist das Integrated Services Digital Network (ISDN), das zwischen B-Kanälen für Nutzdaten und D-Kanälen für

Signalisierung unterscheidet. Der jedem Teilnehmer offen stehende Zugang zum Nutzdatenkanal erfordert nicht unbedingt den Zugang zum Steuerkanal. Die Endteilnehmer können lediglich eingeschränkte Methoden zur Übertragung über Steuerkanäle nutzen, nämlich nur solche Mechanismen, die für den Auf- und Abbau von Verbindungen und für Leistungsmerkmale erforderlich sind.

- TDM-Netze bieten keine Broadcast-Mechanismen. Es ist für die Teilnehmer nicht möglich, Informationen an alle anderen Teilnehmer zu übertragen. Es gibt keinen „Shared-Medium“-Ansatz wie zum Beispiel in einigen für IP genutzten Infrastrukturen wie Wireless Local Area Networks (WLANs). In einem TDM-Netz gibt es statt eines dem Zugriff vieler Teilnehmer ausgesetzten Mediums eine Vielzahl von physikalischen Verbindungen, die explizit und in der Regel von Punkt zu Punkt aufgebaut werden. Das Abhören der Kommunikation ist ohne physikalisches oder elektromagnetisches Wiretapping (Anzapfen) kaum realisierbar.

- In TDM-Netzen gibt es keine Multicast-Mechanismen. Informationen werden in der Regel von Punkt zu Punkt übertragen. Punkt-zu-Mehrpunkt-Übertragung ist nur begrenzt und ausschließlich über spezielle Mechanismen für die Signalisierung von Konferenzen möglich (die nichts anderes sind als die Zusammenschaltung mehrerer explizit aufzubauenden Punkt-zu-Punkt-Verbindungen). Ansonsten gibt es keine „Verzweigungen“ von Informationsströmen, die von Punkt zu Punkt übertragen werden. Das „Kopieren“ von Informationsströmen mittels solcher Verzweigungen ist sehr aufwändig.
- Administratoren von TDM-Netzen nutzen in der Regel proprietäre Management-Mechanismen für den Zugriff auf diese Netze. Diese Mechanismen werden von einem eingeschränkten Personenkreis beherrscht.

Aus den genannten Merkmalen folgt ein bestimmtes Niveau der Sicherheit von klassischer TK. Der Personenkreis, der über das Know-how und die Mittel für die Durchführung von Angriffen auf die klas-

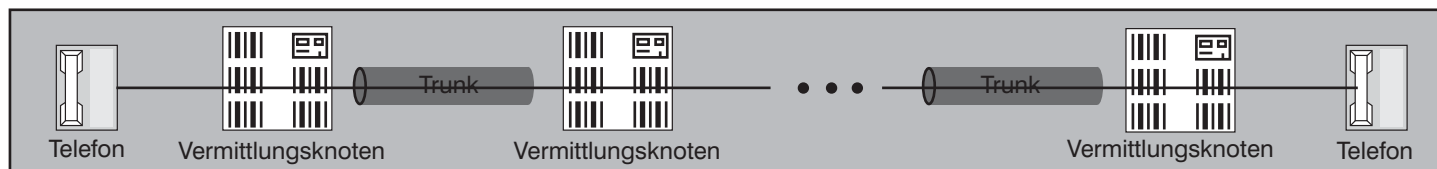


Abbildung 1: Prinzip der Leitungsvermittlung

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

sische Sprachkommunikation verfügt, ist relativ klein. Die Durchführung solcher Angriffe erfordert eine hohe kriminelle Energie bzw. ein relativ großes Budget. Beispielsweise muss ein Angreifer, der Leitungen anzapfen will, sich physikalisch in die Nähe der Leitungen begeben, die abgehört werden sollen, und entsprechende Tarnmaßnahmen ergreifen, um nicht aufzufallen.

Selbstverständlich haben es jene Angreifer leichter, die einerseits über große Budgets verfügen und andererseits selbst in dem Fall, dass sie „auffliegen“, keine größeren Risiken befürchten müssen. Das gilt zum Beispiel für Geheimdienste, insbesondere im Hoheitsgebiet ihres eigenen Staates oder der „befreundeten“ Staaten. So ist es kein Geheimnis, dass beispielsweise im kalten Krieg sehr teure Abhörstationen betrieben wurden. Es wird berichtet, dass zum Beispiel die Vereinigten Staaten eigens zum Anzapfen von Unterseeleitungen U-Boote entwickelt haben. Es ist auch kein Geheimnis, dass Sicherheitsorgane bestimmter Staaten ihre Abhörsysteme auch für Industriespionage zugunsten der eigenen Volkswirtschaft einsetzen. Aber hinsichtlich der Angriffe auf die TDM-basierende Sprachkommunikation herrscht eine große Asymmetrie. Es gehört zum Allgemeinwissen, dass Staaten in Sachen „Lauschangriffe“ auf ihrem Hoheitsgebiet fast alles können, dass aber ein Abhören gegen den Willen des Staates sehr aufwändig und riskant ist. Nur selten gelingt es anderen als staatlichen Organen, fremde Informationen in bisherigen TK-Netzen anzuzapfen.

Dieses „Allgemeinwissen“ bildet zusammen mit anderen Erkenntnissen über die Sicherheit der klassischen Telekommunikation die weit verbreitete Erwartungshaltung diesbezüglich. Informationssicherheit besteht vor allem darin, dass man keine „Überraschungen“ erlebt. Nach einer gängigen Definition gilt ein System als sicher, wenn es sich so verhält wie er-

wartet. Die klassische Telekommunikation ist eine etablierte Technologie, deren Nutzungsrisiken wohl bekannt sind. Nutzer und Service Provider kennen zum Beispiel die Risiken bezüglich des betrügerischen Missbrauchs von TK-Diensten. Ab und zu verhalten sich die TK-Netze doch nicht so wie erwartet, aber im Großen und Ganzen ist das Sicherheitsniveau dieser Netze bekannt. Die Unternehmen meinen zu wissen, wie sie ihre über die TK-Netze übertragenen Informationen vor Mitbewerbern oder der Öffentlichkeit schützen müssen. Staaten wissen die o.g. Asymmetrie zwischen ihren Möglichkeiten und den Möglichkeiten anderer zu ihrem eigenen Gunsten zu nutzen und bringen tendenziell immer mehr Informationen über natürliche und Rechtspersonen in Erfahrung. Bürger der Staaten kennen die Möglichkeiten und die Bestrebungen ihrer Regierungen. Es handelt sich bei der klassischen Telekommunikation um ein System, das wenig Überraschungen aufweist. Das System verhält sich so wie Staaten, Unternehmen und Individuen erwarten, und gilt daher als relativ sicher.

Diese subjektiv empfundene Sicherheit bedeutet trotzdem nicht, dass es keine gravierenden Angriffe auf konventionelle TK gibt. Mit physikalischem Zugang zur Infrastruktur lässt sich im Prinzip alles machen: Man kann ein analoges Telefon als Abhörmikrofon missbrauchen, man kann sich als Mithörer unauffällig einem Gespräch anschließen, wenn man physikalischen Zugriff auf die Infrastruktur erlangt, man kann mit genügend krimineller Energie auf Kosten anderer telefonieren, Verbindungsdaten durch Diebstahl von Daten auslesen, auf mit schwachen Passwörtern abgesicherte Telefonanlagen zugreifen etc. Aber all dies passiert relativ selten.

Wie ist diese Situation mit der Situation in IP-Netzen zu vergleichen? IP-Netze unterscheiden sich in einigen grundlegenden Merkmalen von TDM-Netzen (siehe Abbildung 2):

- IP-Netze arbeiten verbindungslos. Jedes an ein IP-Netz angeschlossene Gerät kann an jedes andere an das selbe IP-Netz angeschlossene Netz Pakete senden, ohne dass vorher explizit eine Verbindung aufgebaut werden muss. Sicherheitsmechanismen während der Verbindungsaufbauphase können nur bei verbindungsorientierten Protokollen wie z.B. TCP (Transmission Control Protocol) angewandt werden, nicht jedoch bei der IP-Übertragung selbst, die keinen expliziten Verbindungsaufbau kennt.
- IP-Netze nutzen Inband-Signalisierung. Nutzdaten und Steuerungsdaten werden über den gleichen Kanal übertragen. Folglich haben alle Nutzer auch Zugang zu dem Kanal, über den Steuerungsinformationen übertragen werden. Diese können daher durch Zugriff auf den einzigen vorhandenen Übertragungskanal manipuliert werden.
- In IP-Netzen werden Broadcast-Mechanismen genutzt, zum Beispiel um zu einer bekannten IP-Adresse die zugehörige Hardware-Adresse zu finden. Local Area Networks (LANs) mit eingebauten Broadcast. Mechanismen werden in Unternehmensnetzen und bei Service Providern genutzt. In diesen Netzen ist das Mithören wesentlich einfacher als in klassischen TK-Netzen.
- IP-Netze nutzen Multicast-Mechanismen, die „Verzweigungen“ von Informationsströmen erfordern. Folglich sind solche „Verzweigungen“ einfach zu steuern, und das „Kopieren“ von Informationsströmen ist relativ einfach möglich, weil die Netzkomponenten dies unterstützen müssen.
- In IP-Netzen werden einfache, standardisierte Management-Mechanismen genutzt. Die Remote-Steuerung von Netzkomponenten ist relativ einfach. Die erforderlichen Werkzeuge dafür sind im

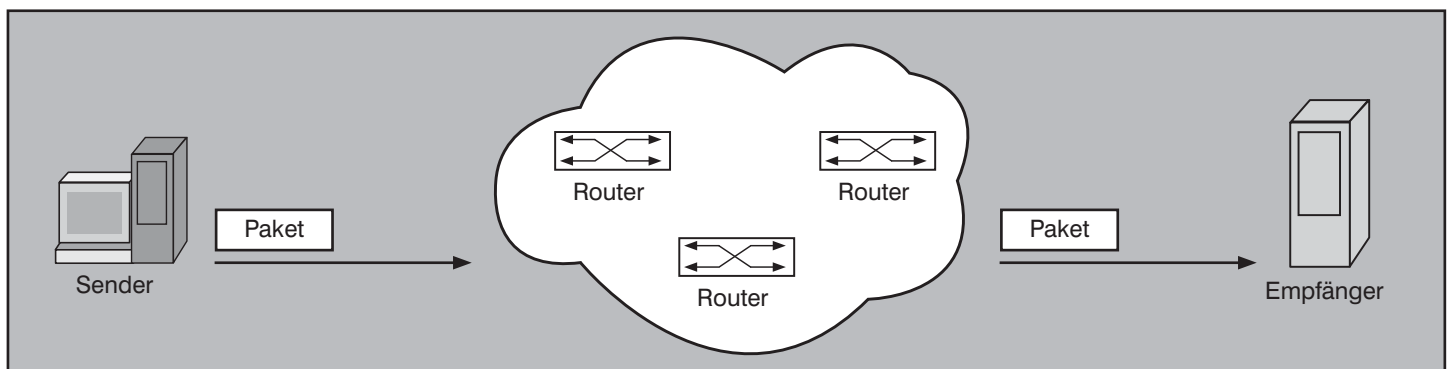


Abbildung 2: Prinzip der Paketvermittlung in IP-Netzen

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

Internet frei erhältlich, und deren Nutzung erfordert kein Spezialwissen.

Nehmen wir das Beispiel von unternehmensinternen Kommunikationsinfrastrukturen: Während bei den bisherigen TK-Anlagen die Möglichkeiten eines Benutzers, mittels klassischer Telefonendgeräte auf eine TK-Anlage zuzugreifen, äußerst eingeschränkt sind, ist die Situation bei VoIP völlig anders: IP-Netze sind universal nutzbare Kommunikationsmedien, die auch für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen auf vielfältige Weise missbraucht werden können. Jede an das IP-Netz angeschlossene VoIP-Komponente (Server, Gateway, Endgerät) kann über das IP-Netz angegriffen werden.

VoIP hebt bei Abhörangriffen die bisher herrschende Asymmetrie auf. Während bisher Staaten auf ihrem Hoheitsgebiet oder in „befreundeten“ Ländern sehr leicht abhören, dafür aber zum Beispiel die organisierte Kriminalität gegen die Abgehörten und gegen den Staat nur schwer abhören konnte, ist bei VoIP zum Abhören keine örtliche Nähe zu den Kommunikationsendpunkten mehr notwendig. Abhören ist bei VoIP auch über Entfernungen von Tausenden Kilometern möglich.

Es sind diese neuen, noch nie da gewesen Angriffsszenarien, welche im Zusammenhang mit VoIP neue Sorgen um die Sicherheit entstehen lassen. Diese Sorgen sind ernst zu nehmen. Sie sind nicht unbegründet. Diesen Sorgen muss mit geeigneten Sicherheitsmaßnahmen für VoIP begegnet werden.

Angriff auf VoIP - ein Schreckgespenst?

Sind die auf den aufgeführten sicherheitsrelevanten Unterschieden zwischen TDM und VoIP basierenden Sorgen nur theoretische Überlegungen? Die im Folgenden exemplarisch dargestellten Angriffsszenarien zeigen, dass es sich bei den denkbaren Angriffen auf VoIP um mehr handelt als ein Schreckgespenst.

Angriffe auf IP-Telefonie können von innen oder von außen initiiert werden. Während interne Angriffe aufgrund der weitaus größeren technischen Möglichkeiten des Angreifers für die Kompromittierung von Systemen und Informationen wesentlich gravierendere Folgen für die Informationssicherheit haben können, ist im Zusammenhang mit externen Angriffe eine weitaus größere Häufigkeit zu befürchten, da der zu solchen Angriffe fähige Täterkreis viel größer ist.

VoIP wird in Unternehmensnetzen über lokale Netze, in der Regel Ethernet, übertragen. Einmal an ein LAN angeschlossen, hat ein Endgerät vielfältige Möglichkeiten, um über das LAN auf Daten und Systeme zuzugreifen. In einem LAN auf der Basis von Komponenten des Typs MAC Layer Switch (MAC steht für Medium Access Control) kann jede Station alle Pakete aufzeichnen, zu denen die Station physikalischen Zugriff hat. Die Kontrolle darüber, zu welchen Ports die Pakete übertragen werden, obliegt zwar dem Switch, aber die Kontrollmechanismen können von einem Angreifer manipuliert werden.

Ein Sicherheitsrisiko wird am Beispiel ARP Poisoning deutlich. Das Address Resolution Protocol (ARP) ist ein Protokoll, das vor allem dazu verwendet wird, zu einer bekannten IP-Adresse die passende Hardware-Adresse (MAC-Adresse bzw. Layer-2-Adresse) festzustellen. In der Regel sendet die suchende Station ein ARP Broadcast an alle Stationen in der selben Broadcast-Domäne. In diesem Paket wird die IP-Adresse der gesuchten Station angegeben und gefragt, welche Station (mit welcher Hardware-, d.h. MAC-Adresse) zum Ansprechen der IP-Adresse Pakete erhalten soll.

In der Regel arbeitet ARP statuslos, d.h. ARP Responses mit einer Zuordnung zwischen einer IP- und einer MAC-Adresse werden von Endgeräten angenommen, auch wenn diese Endgeräte vorher keine Suche initiiert haben. Unaufgefordert gesendete ARP Responses werden Gratuitous oder Unsolicited ARP Responses genannt. Solche Pakete können missbraucht werden, um die ARP Cache des als Angriffsziel ins Visier genommenen Gerätes zu manipulieren, d.h. in die Tabelle eines Endgerätes oder Routers, das die Zuord-

nungen zwischen IP- und MAC-Adressen enthält, Einträge vorzunehmen. Das nachfolgend dargestellte Szenario soll ein Beispiel für einen solchen Angriff wiedergeben (siehe Abbildung 3).

In diesem Szenario kommunizieren zwei IP-Telefone mittels einer LAN-Infrastruktur miteinander. Ein angreifendes Endgerät, das an das selbe LAN angeschlossen ist, sendet in den Schritten 1 und 2 an die beiden IP-Telefone ein Paket mit einer Gratuitous ARP Response. Damit täuscht das angreifende Endgerät den beiden IP-Telefonen die Identität des jeweils anderen Kommunikationspartners vor. Im Schritt 3 sendet das linke IP-Telefon die für das rechte Telefon bestimmten Pakete statt an die Hardware-Adresse des rechten IP-Telefons an das Endgerät des Angreifers. Dieses Gerät leitet im Schritt 4 die Pakete an das rechte IP-Telefon weiter, jedoch nachdem es sie aufgezeichnet hat. Gleiches passiert in den Schritten 5 und 6 mit den Paketen vom rechten zu linken IP-Telefon (hier sind wir zur Vereinfachung davon ausgegangen, dass sich alle dargestellten Geräte in der selben Broadcast-Domäne befinden).

In Folge eines solchen Angriffs kann der Angreifer alle zwischen den beiden IP-Telefonen ausgetauschten Pakete aufzeichnen und zu einer Audiodatei zusammenfügen. Ein solcher Angriff benötigt kein Spezialwissen seitens des Angreifers. Im Internet sind Werkzeuge frei verfügbar, die heruntergeladen werden können und bei Ausführung auf einem handelsüblichen PC das oben genannten Szenario automatisiert umsetzen. Alles, was der Bediener des Programms tun muss, ist es, das Endgerät an das Netz anzuschließen und das Programm aufzurufen.

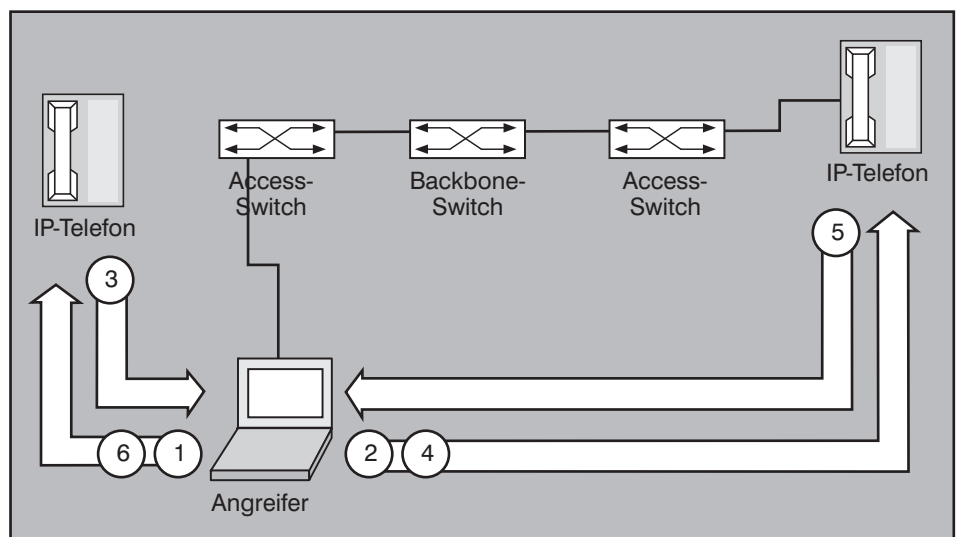


Abbildung 3: Manipulation mittels Gratuitous ARP

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

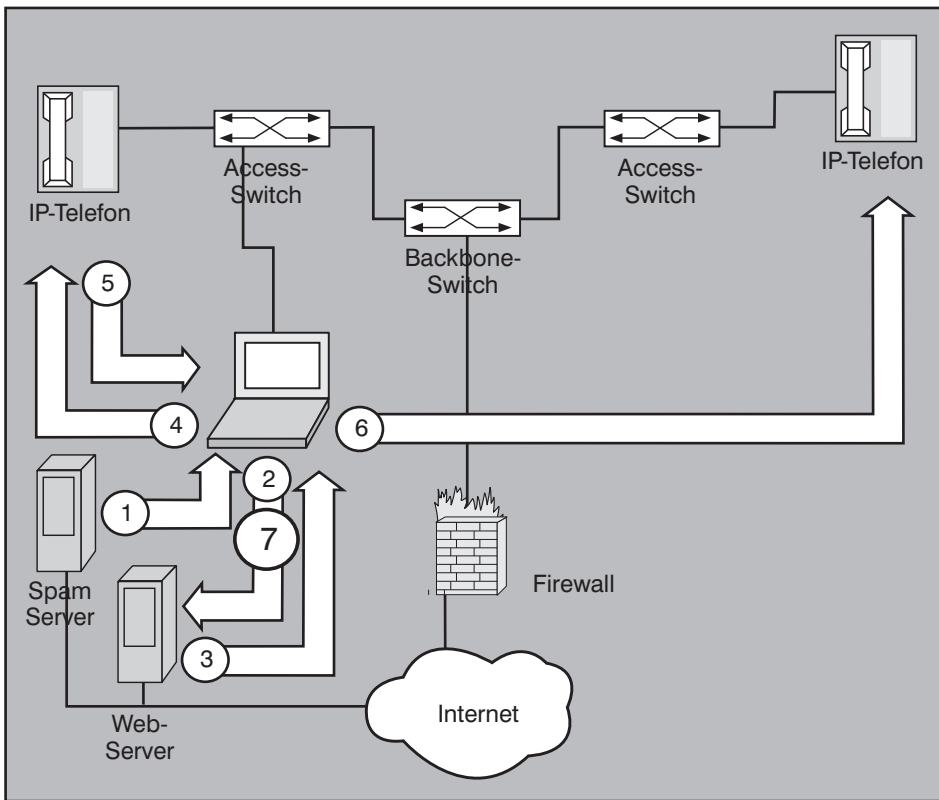


Abbildung 4: Abhörangriff von außen

Der dargestellte Angriff kann auch von außen erfolgen. Hierzu ist ein weiteres Szenario in der Abbildung 4 dargestellt.

Für einen solchen Angriff von außen können E-Mail-Nachrichten an die Benutzer gesendet werden (Schritt 1), die mittels ihrer an das interne Netz angeschlossenen Endgeräte auf E-Mails zugreifen. Wenn eine solche E-Mail-Nachricht einen Link zu einem Webserver enthält und der Benutzer den Link anklickt, greift der PC des Benutzers im Schritt 2 auf den vom Angreifer betriebenen Web-Server zu. Ist die Browsersicherheit auf dem Client-PC nicht stark genug, kann der Webserver mittels Mobile Code (zum Beispiel ActiveX, JScript etc.) ein ausführbares Programm auf den PC übertragen (Schritt 3). Dieses ausführbare Programm kann eine so genannte Spyware sein, d.h. ein Programm, das genau die Schritte auf dem PC ausführt, die mithilfe von ARP Poisoning zum Ausspionieren eines Paketstroms im internen Netz erforderlich sind (Schritte 4 bis 6). Zum Schluss (Schritt 7) wird die vom PC assemblierte Audiodatei, die den Voice-Stream zwischen zwei internen IP-Telefonen beinhaltet, zum feindlichen Webserver übertragen. Die Zusammensetzung mitgeschnittener Pakete zu einer Audiodatei ist sehr einfach möglich und in der Abbildung 5 am Beispiel eines Screenshots des Programms Wireshark dargestellt.

Die Sicherheitsschwachstellen, die der interne oder externe Angreifer für solche Angriffe nutzen kann, ergeben in ihrer Gesamtheit ein lückenhaftes Schutzkonzept:

- Frei zugängliche aktivierte LAN-Dose ohne Schutzmechanismus: Mittels solcher Anschlusspunkte können in-

terne Angreifer Endgeräte ohne Autorisierung mit den LANs verbinden und für Angriffe auf die Vertraulichkeit der über das LAN übertragenen Informationsströme, zum Beispiel des VoIP-Verkehrs, nutzen.

- Frei zugängliches Datenendgerät ohne Schutzmechanismus: Auch wenn nicht autorisierte Endgeräte technisch am Anschluss an das LAN gehindert werden, können Angreifer bereits autorisierte Datenendgeräte für ihre Angriffe missbrauchen.
- Die unverschlüsselte Informationsübertragung ist mit dem Risiko verbunden, dass passives Mithören des Verkehrs möglich wird.
- Ungesicherte Protokolle ohne Sicherheitsmechanismen wie zum Beispiel ARP bergen das Risiko, dass die Steuerung der Kommunikation und der Paketströme manipuliert werden kann.
- Fehlende Authentifizierung und Rechteprofilverwaltung: Endgeräte werden häufig an das Netz angeschlossen, ohne dass mittels einer Authentifizierung bestimmt wird, welche Rechte die Endgeräte im Netz haben. So entstehen diverse Möglichkeiten zum Ausschmuggeln von Daten aus dem Netz.
- Unsichere Browserkonfigurationen führen oft dazu, dass schadensstiftende Software sich in PCs einnisten und Unheil anrichten kann.

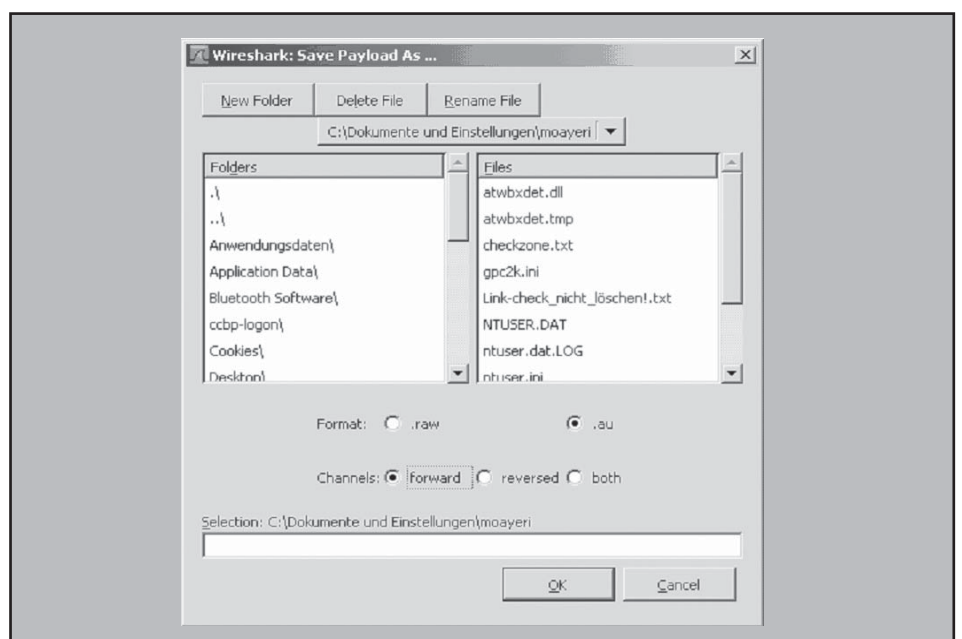


Abbildung 5: Zusammensetzung aufgezeichneter Pakete zu einer Audiodatei

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

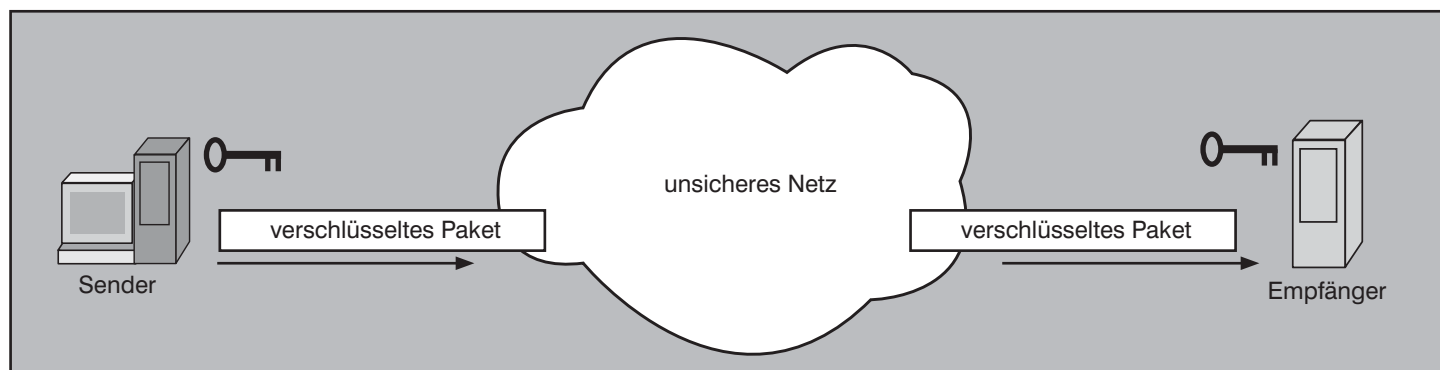


Abbildung 6: Ende-zu-Ende-Verschlüsselung

- Nicht sensibilisierte Benutzer folgen häufig den Aufforderungen in kriminell motivierten E-Mails und klicken die dort enthaltenen Links an.

Schnurlose lokale Netze (Wireless Local Area Networks, WLANs) weisen teilweise sogar noch mehr Sicherheitslücken auf. Allgemein bekannt wurden die Schwächen von „Wired Equivalent Privacy“ (WEP), einem Verfahren, welches in den ersten WLAN-Installationen eingesetzt wurde (und in vielen WLAN-Installationen weiterhin als ausschließlicher Sicherheitsmechanismus verwendet wird) und von frei verfügbaren Programmen kompromittiert werden kann, so dass mittels WEP verschlüsselte WLAN-Kommunikation ohne größeren Aufwand oder Know-how abgehört werden kann.

Obwohl mittlerweile sichere Verfahren statt WEP für WLAN-Verschlüsselung eingesetzt werden können, unterstützen einige WLAN-Endgeräte wie viele VoIP over WLAN Handsets keine Mechanismen, die den ausreichenden Schutz von WLAN-Paketströmen vor Abhörangriffen sicherstellen.

Sicheres Netz oder sichere Anwendungen?

Nun kann der Leser einwenden, dass

- die Kombination der Sicherheitsschwächen, welche die dargestellten Szenarien ermöglichen, nicht nur für VoIP, sondern auch für alle LAN-Anwendungen bedenklich ist, weshalb die Sicherheitsproblematik nicht besonders im Zusammenhang mit VoIP, sondern allgemein für alle IT-Anwendungen betrachtet werden muss, und
- Maßnahmen für die Erhöhung der Sicherheit von Netzen dafür sorgen können, dass keine besondere Betrachtung von VoIP-Sicherheit erforderlich ist.

Sofern über Anwendungen in Netzen diskutiert wird, die das Unternehmen selbst kontrollieren und konfigurieren kann, leuchten die o.g. Einwände zunächst ein. Jedes Unternehmen kann dafür sorgen, dass die eigenen internen Netze sicher konfiguriert werden. Zum Beispiel kann jedes Unternehmen das eigene LAN so konfigurieren, dass keine Fremdgeräte an dieses LAN angeschlossen werden können. Außerdem kann jedes Unternehmen die eigenen Endgeräte und die auf diesen Endgeräten eingesetzten Web-Browser so sicher konfigurieren, dass sich keine von außen kommende Software auf den Endgeräten installieren kann. Auch Angreifern aus den eigenen Reihen (sofern sie nicht Administrationsrechte erlangen) kann man das Handwerk legen, indem man verhindert, dass jeder Benutzer auf den firmeneigenen Endgeräten Software installiert und zur Ausführung bringt.

Mit solchen Maßnahmen wird nicht nur die Sicherheit von VoIP verbessert, sondern auch für einen sichereren Betrieb anderer IT-Applikationen gesorgt.

Trotzdem reicht ein Katalog von Sicherheitsmaßnahmen, der sich auf Maßnahmen im Netz und auf der Ebene der Betriebssysteme beschränkt, nicht aus. Nicht von ungefähr arbeiten viele IT-Anwendungen heute schon mit einer (optionalen oder ständig aktiven) Ende-zu-Ende-Verschlüsselung. Man denke an E-Mail. Mittels elektronischer Post kommuniziert man nicht nur innerhalb von sicher konfigurierten eigenen Netzen, sondern auch über das Internet. Werden mit externen Partnern sensible Daten über E-Mail ausgetauscht, setzt man heute in der Regel Ende-zu-Ende-Verschlüsselung ein. Verfahren wie Pretty Good Privacy (PGP) sorgen für die Vertraulichkeit und Authentizität der E-Mail-Kommunikation unabhängig davon, wie sicher oder unsicher das für die Kommunikation genutzte Netz ist. Auch Web-Anwendungen können so konfiguriert sein, dass Client und Ser-

ver gegenseitig authentifizieren können und dass die ausgetauschten Daten verschlüsselt werden. Bei allen Anwendungen, die potenziell oder aktuell auch mit der Übertragung von sensiblen Informationsströmen über unsichere Netze verbunden sind, entscheidet man sich für eine Sicherheitsarchitektur, die für eine Authentifizierung und Verschlüsselung möglichst von Ende zu Ende sorgt. Dafür muss die Anwendung sorgen und nicht das Netz (siehe Abbildung 6).

Ist die Einführung von IP-Telefonie in Unternehmen mit der Übertragung sensibler Informationen über unsichere Netze verbunden? Zunächst scheinbar nicht. Die interne Telefonie ist mit der Übertragung von Voice über folgende Netze verbunden:

- LAN: Wie bereits erwähnt, kann man das Local Area Network so konfigurieren, dass es als sicher eingestuft wird.
- WAN: Wide Area Networks werden in der Regel als Virtual Private Networks (VPN) entweder auf der Basis von Provider-Plattformen wie Multi-Protocol Label Switching (MPLS) oder basierend auf IP Security (IPsec) aufgebaut, die auch als sicher eingestuft werden.
- Wireless LAN: WLAN können mittels Verfahren wie WiFi Protected Access (WPA) sicher konfiguriert werden.

Somit sorgt man bei der internen Telefonie mit Maßnahmen auf der Ebene des Netzes für die Sicherheit, wie man dies auch für alle anderen Anwendungen tut.

Und was externe Telefonie betrifft, ändert sich ja mit VoIP (zunächst) nichts. Das Public Switched Telephone Network (PSTN) wird nach wie vor für die externe Telefonie genutzt, unabhängig davon, ob man intern klassische Telefonanlagen oder VoIP einsetzt, oder? Moment, war da nicht etwas? Haben die British Telecom und die Deutsche Telekom nicht angekündigt, dass sie

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

in ein paar Jahren das klassische Telefonnetz vollständig durch das Next Generation Network (NGN) abgelöst haben wollen? Und ist das NGN nicht IP-basierend?

Doch, das NGN ist IP-basierend, und für die Provider gibt es keinen Grund, das leitungsvermittelnde Netz ewig am Leben zu halten. Die Argumentation, dass TDM-Netze bestimmten bei IP denkbaren Angriffsszenarien gar nicht ausgesetzt sind, wird die Provider wohl kaum daran hindern, ihre NGN-Vorhaben umzusetzen. Die Kommunikation von morgen ist durchgängig IP-basierend, ob intern oder extern, ob sie mit der Übertragung von Daten, Sprache oder Video verbunden ist. Interne Netze hat man (hoffentlich) in Griff. Aber was ist mit externen Netzen? Soll man auch externen IP-Netzen Vertrauen entgegenbringen? Besser nicht, denn externe IP-Kommunikation ist nichts anderes als Internet-Kommunikation. Es wird kein anderes globales IP-Netz geben außer dem Internet. Das Internet wird in seiner Leistungsfähigkeit ständig verbessert, es mag hier und da auch zusätzliche Funktionen des Netzes geben, aber die Grundarchitektur des Netzes wird sich auf absehbare Zeit nicht ändern, auch nicht mit dem Internet Protocol der Version 6 (IPv6). Das Internet wird auf absehbare Zeit im Großen und Ganzen so sicher oder unsicher bleiben wie es heute ist. Wird das Internet als so unsicher eingestuft, dass man darüber ohne Authentifizierung und Verschlüsselung von Ende zu Ende keine sensiblen E-Mails austauscht oder keine sensiblen Web-Anwendungen betreibt, darf das Internet auch nicht für unverschlüsselte sensible Telefongespräche genutzt werden.

Hat man es mit Kommunikationspartnern zu tun, mit denen man vorher zwecks Verschlüsselung Keys ausgetauscht hat, könnte man verschlüsselte Kommunikation zum Beispiel mittels IPsec durchführen. Aber diese Methode ist bei Telefonie kaum anwendbar. Am Beispiel ComConsult soll die Problematik verdeutlicht werden: Möchte ein Unternehmen bei ComConsult die Mitwirkung an einem sensiblen Projekt (zum Beispiel im Bereich Informationssicherheit) anfragen, nimmt es lieber telefonischen Kontakt auf. Das wird häufig als sicher genug eingestuft und funktioniert auf Anhieb. Jetzt stelle man sich vor, ComConsult sei nur noch über das Internet erreichbar und nicht mehr über das PSTN (weil es dieses nicht mehr gibt). Egal ob man ComConsult anruft oder eine E-Mail schickt, man kann nie sicher sein, wer sonst im Internet die Kommunikation mitbekommt.

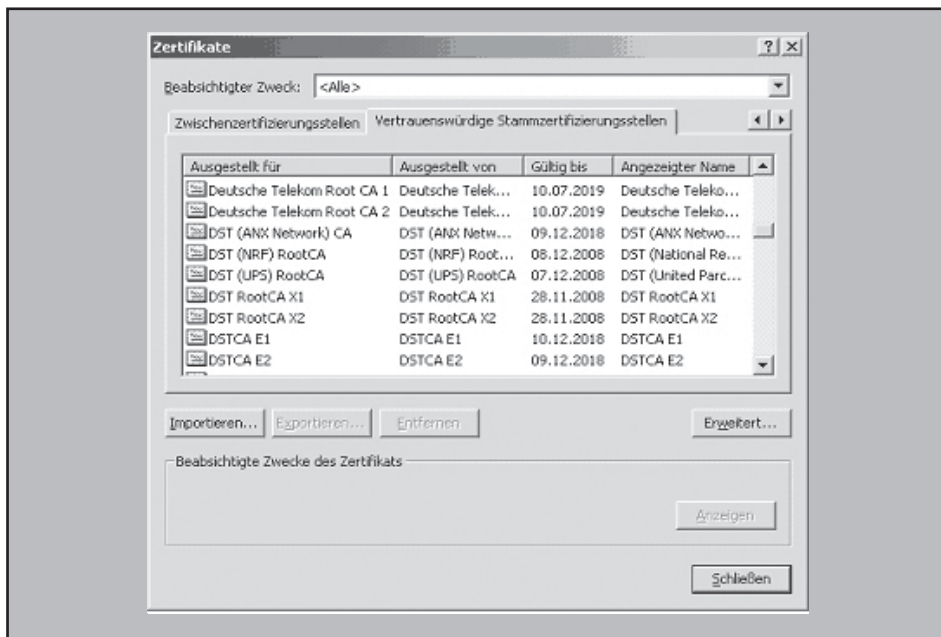


Abbildung 7: Mit Windows mitgelieferte Zertifikate öffentlicher CA

Im Bereich E-Business wird dieses Problem mittels einer Public Key Infrastructure (PKI) gelöst. Nehmen wir das Beispiel Internet Banking: Sie möchten über das Internet Ihre Bank mit einer Überweisung beauftragen. Zugleich legen Sie großen Wert darauf, dass die Kommunikation von Ihrem PC bis zum Server der Bank verschlüsselt ist, dass Sie sicher davon ausgehen können, beim angeklickten Webserver handelt es sich um den Server Ihrer Bank, und dass die Bank Ihr Konto dadurch schützt, dass Zugriffe auf dieses

Konto sicher authentifiziert werden. Normalerweise wird dafür als Sicherheitsarchitektur Transport Layer Security (TLS) bzw. Secure Socket Layer (SSL) eingesetzt. Ihr Browser greift auf den Server der Bank zu, der das Zertifikat der Bank Ihrem Browser übermittelt. Das Zertifikat der Bank ist von einer Certificate Authority (CA) signiert. Der öffentliche Schlüssel der CA ist Ihrem Browser bekannt (in der Regel bereits mit dem Browser oder dem PC-Betriebssystem mitgeliefert, siehe Abbildung 7).

Seminar



Sicherheitsmechanismen für Voice over IP

10.09. - 11.09.07 in Berlin

In diesem Seminar wird vermittelt: was sich in Bezug auf Informationssicherheit mit der Umstellung auf VoIP ändert, welche Gefahrenpotenziale berücksichtigt werden müssen, welche Standards für VoIP-Sicherheit relevant sind, wie die Vertraulichkeit der Sprachkommunikation in IP-Netzen geschützt werden kann, worauf beim Design von VoIP-Umgebungen hinsichtlich Verfügbarkeit zu achten ist, wie die IP-Telefonie in vorhandene Sicherheitsstrukturen in Netzen einzubinden ist, welche Probleme bei VoIP über Vertrauensgrenzen hinweg entstehen und wie sie zu lösen sind, welche rechtlichen Aspekte bei VoIP-Sicherheit relevant sind.

Referent: Dr.-Ing. Behrooz Moayeri
€ 1.390,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.de

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

So kann der Browser die digitale Signatur des Zertifikats der Bank überprüfen und feststellen, dass eine vertrauenswürdige Instanz das Zertifikat signiert hat und die Inhalte des Zertifikats nach der Signatur nicht verändert wurden. Es handelt sich um eine Vertrauenskette: Sie vertrauen der Software auf Ihrem PC, diese vertraut einer öffentlichen CA, und diese der Bank. Im Endeffekt kommt eine Vertrauensbeziehung zwischen Ihrem PC und dem Server der Bank zustande. Sie können somit sicher sein, dass alles, was Ihr PC mit dem im Zertifikat der Bank enthaltenen öffentlichen Key der Bank verschlüsselt, nur durch den Einsatz des privaten Schlüssels der Bank zu entziffern ist (siehe Abbildung 8).

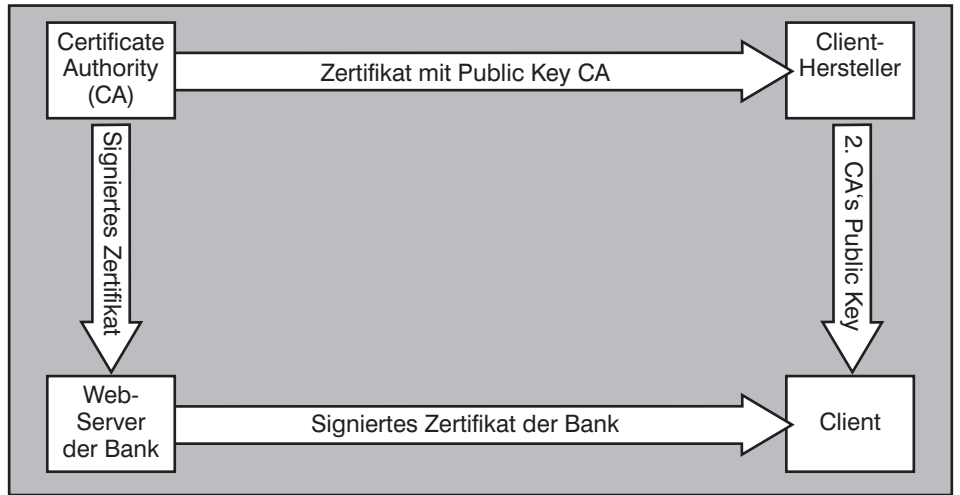


Abbildung 8: Prinzip der Vertrauenskette

In den Anfängen von E-Business herrschten noch große Bedenken und Sorgen darüber, ob das SSL-Verfahren sicher genug ist. Nach jahrelanger Nutzung von E-Business sind TLS- bzw. SSL-basierende Verfahren aus unserem Leben nicht wegzudenken. Allein in Deutschland nutzen Millionen von Menschen Internet Banking. Millionen von Menschen übermitteln mittels SSL/TLS (Grundlage von https) Ihre Kreditkartennummern. Dem Verfahren wird vertraut, obwohl es auch Missbrauch und Angriffe auf das Verfahren gibt. Transport Layer Security im Internet ist sicher in dem Sinne, dass sich das Verfahren so verhält wie man es erwartet. Die Zeit großer Überraschungen ist vorbei. Kann sich etwas Ähnliches auch bei der Internet-Telefonie entwickeln?

VoIP kann sicherer als klassische TK sein, aber ...

Die Sorgen um die Sicherheit von TK sind begründet. Gleichzeitig kann VoIP mehr Sicherheit bieten als die klassische TK jemals geboten hat. Schließlich ist es bei

VoIP mit vertretbarem technischen Aufwand möglich, verschlüsselt zu kommunizieren. Damit VoIP den vergleichbaren Sicherheitsstandard der bisherigen TK-Netze erreicht, diesen aber auch übertrifft, kann als Sicherheitsmechanismus Ende-zu-Ende-Verschlüsselung eingesetzt werden. Es ist heute möglich, verschlüsselte Signalisierung, verschlüsselte Sprachübertragung und verschlüsselte Administration von VoIP-Umgebungen einzusetzen. Dies erfordert jedoch, Verschlüsselung als Technologie zu beherrschen, insbesondere das Schlüsselmanagement.

Und das ist im Moment das größte Problem. Wie tauschen VoIP-Endgeräte Schlüssel aus?

Bei E-Mail werden häufig vor dem Austausch sensibler E-Mails auf einem sicheren Weg (zum Beispiel in einer Besprechung auf Datenträgern oder über eine als sicher eingestufte direkte Netzverbindung) Schlüssel ausgetauscht, zum Beispiel

PGP Keys. Dabei wird in der Regel asymmetrische Verschlüsselung angewandt, d.h. zur Verschlüsselung wird ein anderer Schlüssel eingesetzt als für die Entschlüsselung. Der Schlüssel für die Verschlüsselung ist nicht geheim und kann auch veröffentlicht werden. Aber jede Information, die mit diesem Schlüssel verschlüsselt wird, kann nur mit dem zu diesem Schlüssel passenden privaten Schlüssel entziffert werden, der nur dem Besitzer des Schlüsselpaars zugänglich ist. Wenn A die an B zu schickenden Informationen verschlüsseln will, wird der öffentliche Schlüssel von B eingesetzt, und die so verschlüsselten Daten kann nur B mit dem eigenen privaten Schlüssel lesen. Ab dem Zeitpunkt des Austauschs der öffentlichen Schlüssel können sich A und B gegenseitig verschlüsselte E-Mails senden (siehe Abbildung 9).

Kann man das Verfahren auch bei der Telefonie anwenden? Nein, aus zwei Gründen:

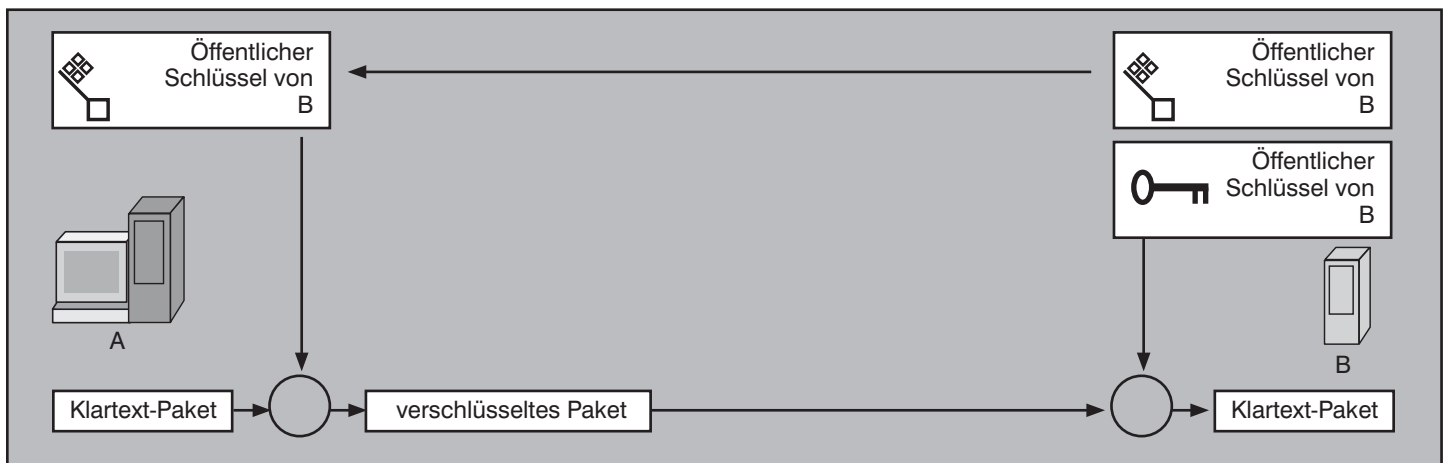


Abbildung 9: Prinzip der asymmetrischen (öffentlichen) Verschlüsselung

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

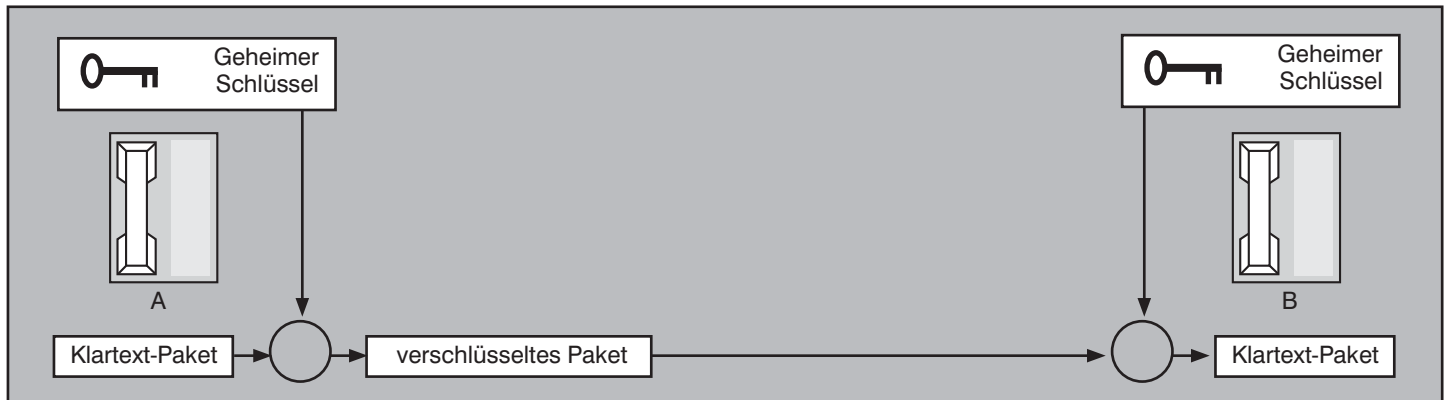


Abbildung 10: Prinzip der symmetrischen (privaten) Verschlüsselung

- Wie sollen zwei Kommunikationspartner Schlüssel austauschen, bevor sie miteinander telefonieren?
- Asymmetrische Verschlüsselung (Public Key Encryption) ist verarbeitungsintensiv. Das kann jeder beobachten, der eine mit PGP verschlüsselte Nachricht öffnet. Der PC braucht dafür wenige Sekunden. Ein Telefon mit einem viel schwächeren Prozessor würde dafür noch länger brauchen. Das ist für die Telefonie zu lang.

Telefonie ist eine höchst interaktive Anwendung. Die Verschlüsselung und die Entschlüsselung müssen binnen Millisekunden durchzuführen sein. Mit den bei Telefonen (Festnetztelefonen, Mobiltelefonen, Smart Phones etc.) üblichen Prozessoren ist dies nur bei Anwendung symmetrischer Verschlüsselung möglich. D.h. die für Verschlüsselung und Entschlüsselung eingesetzten Schlüssel sind identisch, und dürfen zur Wahrung der Vertraulichkeit nur den beiden Kommunikationspartnern bekannt sein (siehe Abbildung 10).

Man spricht dabei von Private Key Encryption. Das Verfahren ist viel weniger verarbeitungsintensiv als Public Key Encryption. Heutige IP-Telefone brauchen für die symmetrische Verschlüsselung bzw. Entschlüsselung nur wenige Millisekunden.

Das setzt aber voraus, dass vor dem Austausch sensibler Audioinformationen der selbe geheime Schlüssel den beiden Kommunikationspartnern mitgeteilt wird. Bei einer überschaubaren Schar von Geräten wären so genannte Pre-Shared Keys (PSK) anwendbar. Man vereinbart über ein sicheres Medium, zum Beispiel im persönlichen Gespräch, den Schlüssel und verwendet ihn immer wieder. Das Verfahren hat aber folgende Probleme:

- Es muss vor der sensiblen Kommunikation über das unsichere Medium ein

sicheres Medium geben, über das man den Schlüssel austauscht. Nicht immer ist das gewährleistet.

- Pro Kommunikationspartner muss jedes Gerät einen geheimen Schlüssel führen. Das Verfahren skaliert nicht.
- Die geheimen Schlüssel sind zu schützen. Man stelle sich vor, ein Angreifer zeichnet die verschlüsselte Information auf und entwendet nachträglich ein Endgerät, auf dem der passende geheime Schlüssel gespeichert ist. Damit kann er nachträglich die aufgezeichneten Gespräche entschlüsseln.

Aus diesen Gründen kann das Schlüsselmanagement für IP-Telefonie in Unternehmen nicht auf PSK basieren. Das Verfahren muss folgende Bedingungen erfüllen:

- Der Schlüsselaustausch muss auch über ein unsicheres Medium durchgeführt werden können, zum Beispiel nach dem Schema, wie bei E-Business Schlüssel ausgetauscht werden.
- Das Endgerät muss mit wenigen dauerhaften Vertrauensbeziehungen auskommen und nicht pro Kommunikationspartner dauerhaft einen Schlüssel verwalten müssen.
- Schlüssel für die Telefonie müssen Session Keys sein, d.h. pro Gespräch vereinbart und dann wieder vernichtet werden, damit eine nachträgliche Entschlüsselung aufgezeichneter Daten nicht möglich ist.

In der Regel wird eine Mischung aus asymmetrischer und symmetrischer Verschlüsselung angewandt. Zum Beispiel

Seminar



Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung in der Praxis

22.10. - 23.10.07 in Aachen

Dieses 2-tägige Seminar beschreibt die Planung, Installation und den Betrieb einer IP-Telefonie-Komplettlösung auf Basis vernetzter Cisco CallManager ergänzt um Zusatzprodukte. In einem Unternehmensnetz wurden bereits 50 der über 100 Standorte mit Systemen und über 15.000 IP-Telefonen ausgestattet. Die im Zusammenhang mit einem VoIP-Projekt stehenden, wesentlichen Aspekte werden in einem Mix aus Erfahrungsberichten und technischen Beiträgen betrachtet.

Referenten: Karl-Heinz Hommen-Menz, Axel Schemberg
Preis: € 1.390,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

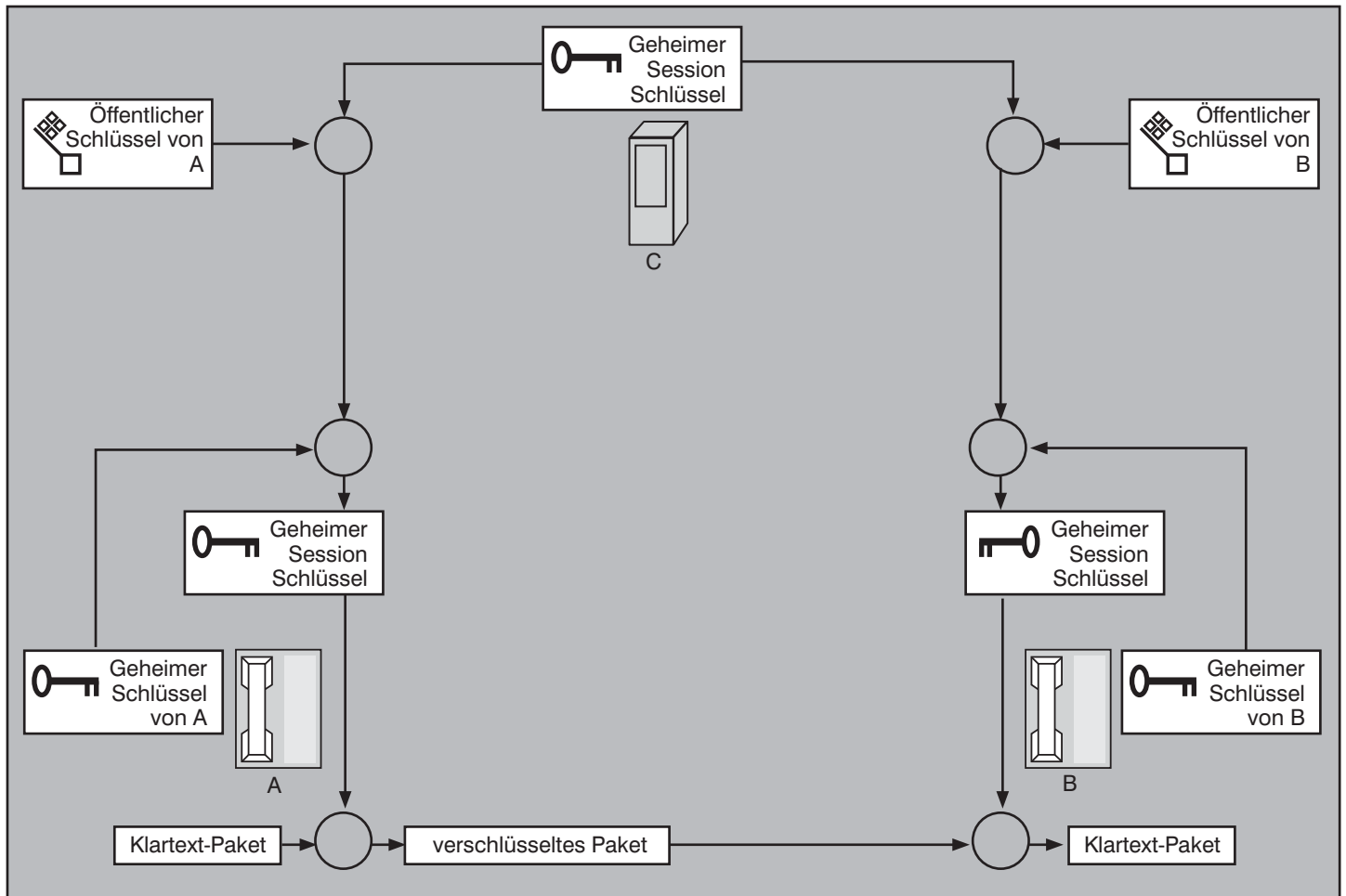


Abbildung 11: Asymmetrische Verschlüsselung des symmetrischen Session-Schlüssels

kann zu Beginn der Session über Public Key Encryption ein geheimer Schlüssel vereinbart werden. Dabei spielt es eine untergeordnete Rolle, dass die asymmetrische Verschlüsselung verarbeitungsintensiv ist, denn wenige Sekunden zusätzliche Verzögerung beim Verbindungsaufbau wird in der Regel toleriert. Ist der geheime Schlüssel vereinbart und beiden Endgeräten bekannt, können die Kommunikationspartner Audiodaten damit verschlüsseln, bevor sie zum Ziel übertragen werden. Am Ende der Session wird der geheime Schlüssel gelöscht.

Das heißt alles, was ein IP-Telefon benötigt, ist der eigene private (geheime) Schlüssel und die öffentlichen Schlüssel der Kommunikationspartner. Können diese öffentlichen Schlüssel als PSK auf alle Geräte verteilt werden? Wohl kaum, denn dann müsste das Telefon eine Vielzahl solcher Schlüssel verwalten und vor allem beim Hinzufügen jedes neuen Telefons dessen öffentlichen Schlüssel auf einem sicheren Weg erhalten. Das PSK-Verfahren skaliert auch in diesem Fall nicht.

Nutzung einer PKI

Das PSK-Verfahren ist nicht praktikabel, aber die Hersteller von IP-Telefonie mussten das Rad nicht neu erfinden. E-Business hat es ja vorgemacht. Man kann zum Schlüsselmanagement eine PKI (Public Key Infrastructure) einsetzen. Konkret kann dies so aussehen: Jedes Telefon unterhält mit einer CA (Certificate Authority) eine Vertrauensbeziehung dadurch, dass dem Telefon der öffentliche Schlüssel der CA und der CA der öffentliche Schlüssel des Telefons bekannt ist. So kann jedes Telefon mit der CA über Public Key Encryption verschlüsselt kommunizieren. Über diesen verschlüsselten Kanal kann der geheime Schlüssel für jede Session mit jedem anderen Telefon vereinbart werden (siehe Abbildung 11). Jedes Telefon benötigt ohnehin für Vermittlungsdienste (zum Beispiel zum Herausfinden der IP-Adresse eines anderen Telefons mit einer bestimmten Telefonnummer) die Hilfe einer zentralen Instanz. Genau diese zentrale Instanz kann auch die Rolle der CA übernehmen. In unternehmensinternen VoIP-Umgebungen handelt es sich dabei

um den Telefonie-Server, den Soft Switch, die IP-PBX-Anlage oder welchen Namen auch immer die zentrale Signalisierungsstelle führt.

Gibt es mehr als eine CA, müssen zwischen den CA Vertrauensbeziehungen aufgebaut werden, damit zum Beispiel A vermittelt von CA1 und CA2 mit B eine verschlüsselte Kommunikation aufbauen kann.

Die Nutzung einer PKI ist das Verfahren, das alle Anbieter von IP-Telefonie für das Schlüsselmanagement in einem Unternehmensnetz anwenden. Damit können alle Teilnehmer miteinander verschlüsselt kommunizieren, die eine Vertrauensbeziehung mit der Signalisierungsinstanz im Unternehmen haben. Dazu zählen in der Regel die unternehmenseigenen Endgeräte sowie Gateways zu anderen Netzen wie zum Beispiel dem PSTN. An der Grenze zum PSTN muss die Verschlüsselung aufgehoben werden, da im PSTN in der Regel ohnehin keine Verschlüsselung möglich ist.

Aber über das Internet kann mit dieser Lösung nicht verschlüsselt telefoniert werden,

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

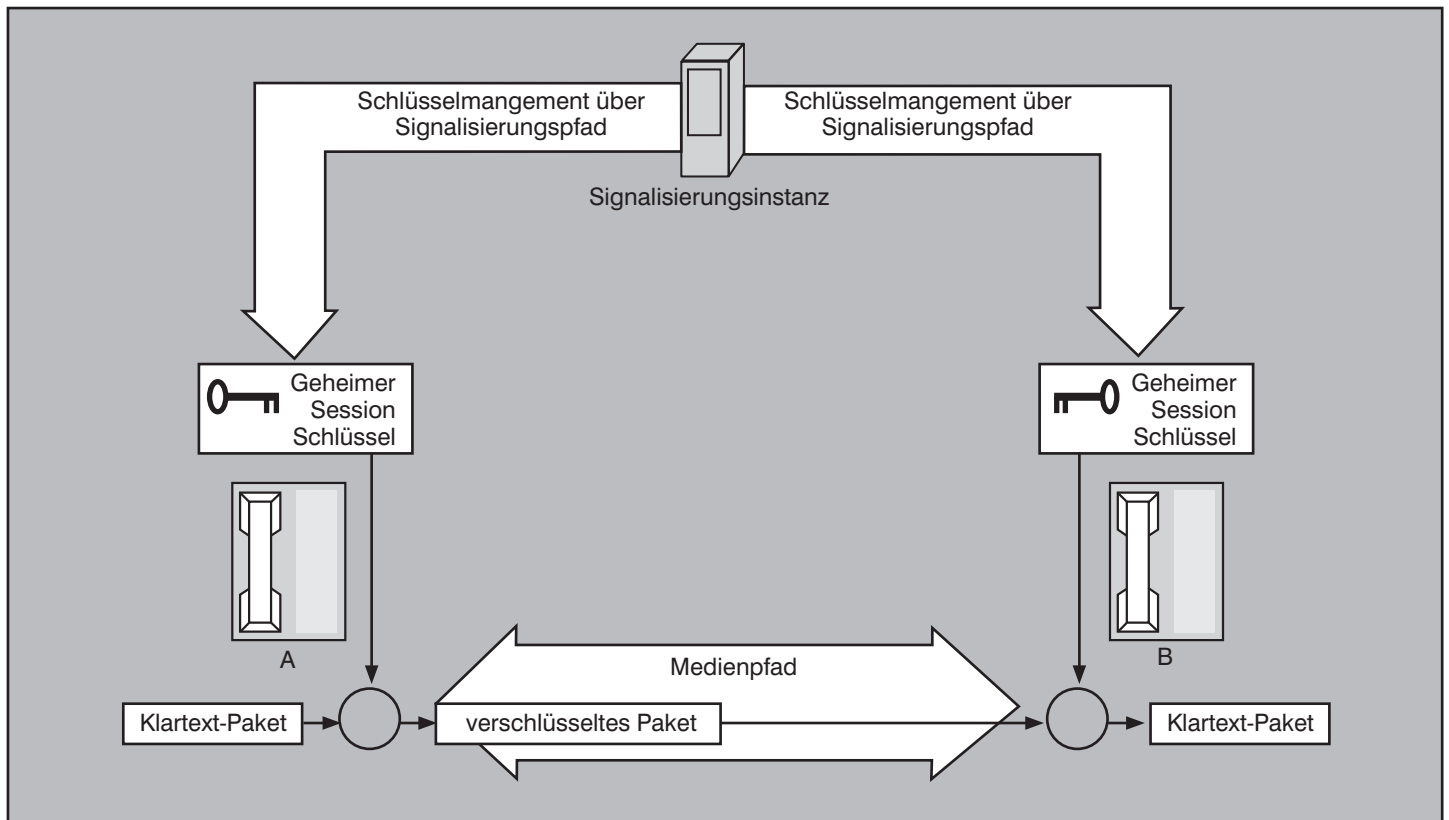


Abbildung 12: Schlüsselmanagement über den Signalisierungspfad

denn die externen Kommunikationspartner unterhalten ja keine Vertrauensbeziehung mit den internen Signalisierungsinstanzen des Unternehmens. Gerade dort, wo die Verschlüsselung mehr als anderswo erforderlich ist, nämlich im Internet, wird Klartext gesprochen. Ist das hinnehmbar? Reicht es, auf die auch heute im PSTN fehlende Verschlüsselung hinzuweisen und mit den Schultern zu zucken?

Offensichtlich nicht, denn sonst würden sich nicht viele Experten und Standardisierungsgremien über verschlüsselte Sprachkommunikation über das Internet den Kopf zerbrechen. Es geht darum, dass VoIP-Verschlüsselung auch unternehmensübergreifend zustande kommt, d.h. herstellerübergreifend und über verschiedene Provider-Infrastrukturen hinweg. Das IP-Telefon A, das in die VoIP-Umgebung 1 im Unternehmen x eingebunden ist, muss mit dem IP-Telefon B, das in die VoIP-Umgebung 2 im Unternehmen y eingebunden ist, verschlüsselt kommunizieren können.

Ist es realistisch zu erwarten, dass verschiedene Signalisierungsinstanzen von verschiedenen Herstellern über eine übergeordnete, globale PKI miteinander verschlüsselt kommunizieren und das Schlüsselmanagement für VoIP regeln können? Darauf setzen diejenigen Exper-

ten, die das Schlüsselmanagement als eine Aufgabe ansehen, die über den so genannten Signalisierungspfad zu erledigen ist. Bei diesem Ansatz wird der Austausch von Schlüsseln über das Signalisierungsprotokoll abgewickelt, das auch für den Verbindungsaufbau erforderlich ist (dazu siehe Abbildung 12).

Das Session Initiation Protocol (SIP) setzt sich als das Signalisierungsprotokoll für VoIP durch. Es ist denkbar, mittels SIP oder genauer mithilfe des zusammen mit SIP eingesetzten Session Description Protocol (SDP) Schlüssel auszutauschen, vorausgesetzt, die entsprechenden Felder in SIP und SDP werden selbst verschlüsselt. Dies kann wiederum analog zu HTTP mittels TLS durchgeführt werden. Damit TLS unternehmensübergreifend kommuniziert, braucht man eine globale PKI. Dies vorauszusetzen, sehen viele Experten als realistisch an. Schließlich hat es ja bei HTTP auch geklappt.

Aber eine PKI und TLS allein reichen nicht aus, um die unternehmensübergreifende Sprachkommunikation zu verschlüsseln. Es muss darüber hinaus auch die Methode vereinheitlicht werden, mit der die per TLS verschlüsselten Signalisierungspfade für das Management der VoIP Session Keys genutzt werden. Zum Beispiel ist

festzulegen, welche Instanz die Session Key bestimmt (Endgerät? Wenn ja, welches? Oder eine der involvierten Signalisierungsinstanzen? Wenn ja, welche?).

Konkurrierende Ansätze

Und genau hier sind wir noch von einer einvernehmlichen Lösung entfernt. Es gibt verschiedene Standardisierungsansätze. Seit Jahren existiert bereits ein Ansatz, der unter dem Stichwort Multimedia Internet Keying (MIKEY) bekannt ist. Dieser Ansatz dient dem Schlüsselaustausch für das Secure Real-Time Transport Protocol (SRTP). Zum Glück besteht schon Einigkeit darüber, wie ein Paket mit verschlüsselter Voice-Payload-Information aussieht. Das etablierte Real-Time Transport Protocol (RTP) bekommt einfach Profile für verschlüsselte Kommunikation, genauso wie es verschiedene Profile für verschiedene Audiokodierungen gibt. Auch der Verschlüsselungsalgorithmus für Audiodaten ist festgelegt. Es ist der Advanced Encryption Standard (AES). Aber es fehlt noch die Komponente des Schlüsselmanagements.

MIKEY ist eine Methode, mit der diese Lücke gefüllt werden kann. Das Verfahren sieht vor, dass ein Traffic Encryption Key (TEK, das ist der Session Key) mittels ei-

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

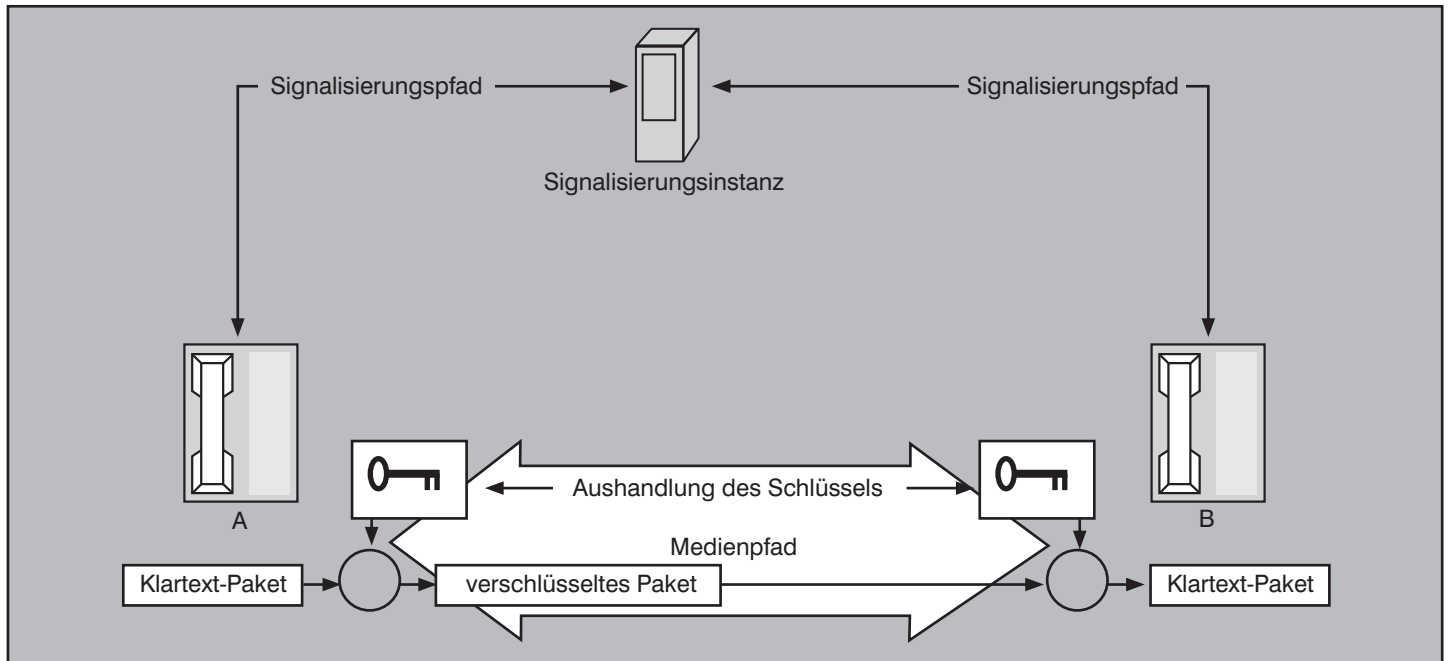


Abbildung 13: Aushandlung des Schlüssels über den Medienpfad

nes TGK (TEK Generation Key) ausgehandelt wird. Diese Zweistufigkeit ist zum Beispiel dafür vorgesehen, dass der Session Key auch mitten in der Session ausgetauscht werden kann. Für die Aushandlung des TGK sieht MIKEY drei alternative Methoden vor:

- Pre-Shared Key (PSK)
- Public Key Infrastructure (PKI)
- Diffie-Hellman (DH)

Wie PSK und PKI funktionieren, wurde bereits erläutert. Auf das dritte o.g. Verfahren wird später eingegangen.

Aber MIKEY ist nicht der einzige existierende Ansatz. Ein weiterer Ansatz, der den Signalisierungspfad für das Schlüsselmanagement nutzt, heißt Session Description Protocol Security Descriptions for Media Streams (kurz SDescriptions). Dieser Ansatz wurde ursprünglich von Cisco Systems vorgeschlagen und nutzt SDP für die Aushandlung der Schlüssel für SRTP.

Ein anderer Ansatz ist unter dem Titel Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP) bekannt. DTLS ist eine Adaption von TLS für verbindungslose Kommunikation, d.h. für das User Datagram Protocol (UDP). DTLS kann auch eingesetzt werden, um Schlüssel für SRTP auszuhandeln. Dieser Ansatz ist nicht mit irgendeinem Signalisierungsprotokoll gekoppelt, kann aber zusammen mit SIP und SDP realisiert werden.

DTLS für SRTP verwendet eine Art Zertifikate für das Schlüsselmanagement. Das Verfahren ist für den Benutzer transparent; Schlüssel und Zertifikate werden automatisch von den Endgeräten selbst generiert. Der Kommunikationspartner braucht die Zertifikate nicht zu überprüfen, denn ein „Fingerprint“ des Zertifikats wurde in der Signalisierung bereits überprüft.

Für den Fall, dass die Signalisierung nicht immer sicher ist, unterstützt DTLS eine „key continuity feature“ wie bei SSH, d.h. ein Shared Secret kann für die Authentifizierung in weiteren Gesprächen auf beiden Endgeräten gespeichert werden. Die Endgeräte müssen dafür sorgen, dass eine Warnung bei Abweichung der beiden Shared Secrets an die Benutzer signalisiert wird.

Schlüsselmanagement über den Medienpfad

Neben den Ansätzen, die den Signalisierungspfad für das Schlüsselmanagement nutzen, gibt es auch Ansätze, die das Schlüsselmanagement statt über den Signalisierungspfad entlang des Medienpfades durchführen, also entlang des selben Pfades, der für die Übertragung der Audioinformationen genutzt wird (siehe Abbildung 13).

Weder auf irgendein spezifisches Signalisierungsprotokoll noch auf eine PKI ist das ZRTP angewiesen. ZRTP steht für Extensions to RTP for Diffie-Hellman Key Agreement for SRTP. Die Autoren des ers-

ten Drafts vom Oktober letzten Jahres sind P. Zimmermann (Zfone Project), A. Johnston (Avaya) und J. Callas (PGP Corporation). Phil Zimmermann ist der Erfinder von Pretty Good Privacy (PGP), der bereits erwähnten weit verbreiteten Methode für die Verschlüsselung von E-Mail. Zimmermann hat mit dem Zfone ein Open-Source-Projekt gestartet, das der möglichst leichten und möglichst weit verbreiteten Verschlüsselung von Voice dienen soll.

Bei ZRTP wird ein Feld in einem Real-Time Transport Protocol Header erweitert, um einen Schlüsselaustausch mittels des Diffie-Hellman-Algorithmus zu ermöglichen. Somit erfolgt der Schlüsselaustausch „inband“ mittels RTP. Nach dem Schlüsselaustausch wird aus der RTP eine SRTP-Kommunikation, wie der SRTP-Standard es vorsieht. Der vereinbarte Sitzungsschlüssel wird nach jeder Sitzung zerstört, damit keine Entschlüsselung aufgezeichneter Daten durch die nachträgliche Kompromittierung des Schlüssels möglich ist.

Der dynamische Schlüssel-Austausch mittels des Verfahrens Diffie-Hellman (DH) ist in der Informationssicherheit weit verbreitet (siehe Abbildung 14).

Das Verfahren basiert auf mathematischen Gesetzen und nutzt die Modulo-Funktion (Bildung des Divisionsrests), welche eine größere Zahlengruppe auf eine kleinere Zahlengruppe abbildet. Die zu Beginn ausgetauschten Zahlen a und

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

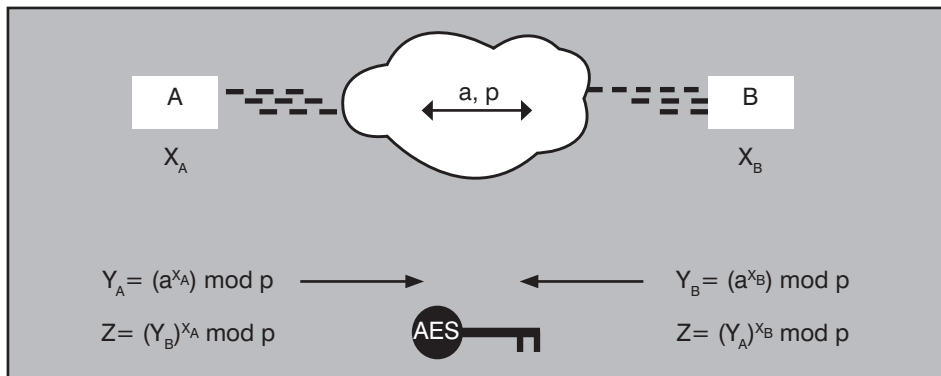


Abbildung 14: Schlüsselaustausch mit dem Diffie-Hellman-Verfahren

p und die Divisionsreste Y_A und Y_B können auch Angreifern bekannt sein, ohne dass die Angreifer daraus die geheimen Zahlen X_A und X_B ableiten können. Angreifer können damit auch nicht den resultierenden Schlüssel Z ausrechnen, denn ihnen fehlen die X -Werte. Die beiden Kommunikationspartner A und B kommen jedoch (auf zwei verschiedenen Berechnungswegen) zum selben Wert Z , der als geheimer Schlüssel genutzt werden kann.

Problematisch bei DH ist, dass dieses Verfahren keinen Schutz vor dem so genannten Man-in-the-Middle(MitM)-Angriff bietet. Ein Angreifer könnte sich von Beginn an in die Kommunikation einschalten und mit jedem der beiden Kommunikationspartner A und B einen Schlüssel vereinbaren, ohne dass A und B auffällt, dass sie jeweils nicht miteinander, sondern mit dem Angreifer (dem MitM) einen Schlüssel vereinbart haben. Der MitM ist somit in die verschlüsselte Kommunikation eingebunden.

ZRTP bietet eine Abhilfe gegen MitM-Angriffe. Die Abhilfe heißt Short Authentication String (SAS). Der SAS ist ein Hash-Wert, der aus dem vereinbarten Schlüssel abgeleitet wird. Zwei verschiedene Schlüssel ergeben zwei verschiedene SAS. Der SAS ist kurz und somit auch auf kleinen Telefondisplays darstellbar und kann von den beiden involvierten Kommunikationspartnern im Gespräch verglichen werden. Zum Beispiel zeigt das von Zimmermann und seinen Kollegen entwickelte, ZRTP nutzende Programm Zfone den SAS an (siehe Abbildung 15).

Nun kann es ja lästig sein, bei jedem Telefongespräch eine solche Zeichenkette vergleichen zu müssen. Deshalb ist bei ZRTP die Zwischenspeicherung eines gemeinsamen Geheimnisses (Shared Secret) möglich, welches bis zur nächsten Sitzung von den Kommunikationspartnern aufbewahrt und bei der nächsten Sitzung durch die Endgeräte verglichen wird. Die Endgeräte können dann anzeigen, seit

wann die sichere Kommunikation mit einem anderen Endgerät möglich ist (siehe Abbildung 15).

So ist es möglich, dass der Short Authentication String (SAS) in einer Sitzung vorgelesen wird, und alle weiteren Sitzungen werden damit authentifiziert. Alternativ kann die erste Sitzung als sicher angenommen werden (weil zum Beispiel die genutzte Verbindung als sicher gilt), und sämtliche weiteren Sessions gelten dann auch als sicher (ein ähnliches Modell wird bei Secure Shell - SSH - angewandt).

Der ZRTP ist bereits im frei verfügbaren Programm Zfone implementiert. Zfone ist als Software für PCs mit den Betriebssystemen Windows XP, Mac OS und Linux verfügbar und kann mit zusammen mit einem Softphone eingesetzt werden. Die Wahl des Softphones ist im Prinzip beliebig. Eine Ausnahme ist Skype, weil Sky-



Abbildung 15: Darstellung des Short Authentication String (SAS) durch Zfone

pe nicht offengelegte Mechanismen verwendet. Somit sind Zfone und Skype nicht kombinierbar.

Mittels Zfone kann somit bereits heute die Kommunikation zwischen zwei Softphones verschlüsselt werden. Die einzige Voraussetzung besteht darin, dass beide Seiten ZRTP unterstützen.

Das Programm Zfone wurde bei ComConsult bereits erfolgreich getestet und ließ

Seminar



IP-Telefonie: Vorbereitung, Migration, Management

15.10. - 17.10.07 in Aachen

Der Referent dieses 3-tägigen Seminars vermittelt seine jahrelange Projekt-Erfahrung bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld.

Referent: Dr.-Ing. Behrooz Moayeri
Preis: € 1.690,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.de

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

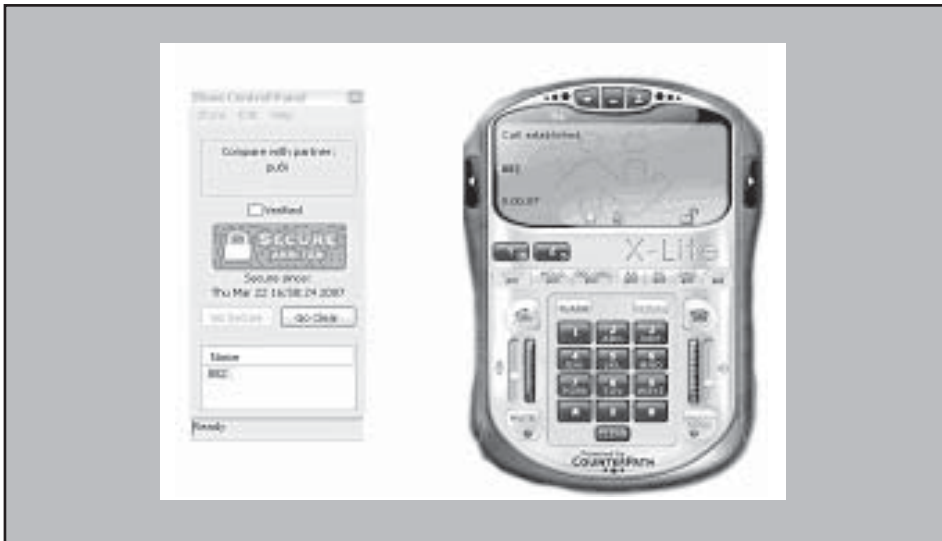


Abbildung 16: Zfone-Benutzeroberfläche neben dem Softphone

sich problemlos mit Softphones kombinieren. Auffällig war lediglich die lange Verbindungsaufbauzeit bei der ersten Verbindung. Eine kleine, vom Softphone selbst getrennte eigene grafische Benutzeroberfläche von Zfone teilt dem Benutzer mit, ob die Session sicher (verschlüsselt und authentifiziert) ist (siehe Abbildung 16).

Das Ziel der Initiator von ZRTP ist, dass dieses Protokoll auch in IP-Telefonen und möglicherweise Gateways wie zum Beispiel Analog Telephony Adapter (ATA) integriert wird.

Argumente gegen ZRTP

Die von einigen Experten vorgebrachten Argumente gegen ZRTP sind wie folgt:

- Latenzzeit durch den Schlüsselaustausch vor einem Gespräch (bedingt durch den hohen Verarbeitungsaufwand des DH-Algorithmus)
- Umständliches Vorlesen und Vergleichen des Short Authentication String durch die Benutzer
- Gefahr von MITM-Angriffen: Es ist prinzipiell denkbar, dass ein Angreifer mit Cut & Paste den Sound für jedes Symbol des Short Authentication String in das Gespräch einfügt und so jedem der beiden Kommunikationspartner eine sichere Verbindung vortäuscht. Dazu muss der Angreifer den Sound aller 32 möglichen Symbole des SAS mit der Stimme beider Kommunikationspartner verfügbar haben.
- Der Short Authentication String bietet keine Lösung für PSTN Gateways und

andere Peers, die eine Authentifizierung mittels SAS nicht unterstützen.

- ZRTP bietet keine Lösung für die Authentifizierung von Gesprächspartnern und überlässt diese Aufgabe vollständig den menschlichen Benutzern. Insbesondere bei Interactive Voice Response (IVR), häufig sensiblen Gesprächen wie zum Beispiel bei Telefon-Banking vorgeschaltet, kann ein Angreifer die Identität eines Sprachportals vortäuschen. Auch gegen dieses Szenario würde ZRTP keine Abhilfe leisten.
- ZRTP schützt nur RTP und damit nur Voice bzw. Video, jedoch keine Daten, zum Beispiel keine Instant Messages.

Trotz dieser Argumente gibt es einige Verfechter des ZRTP-Ansatzes. So möchten zum Beispiel einige von ZRTP überzeugten Entwickler der Open-Source-Lösung

SIP Express Router (SER) ZRTP in den SER-Media-Routern dieser Lösung implementieren.

Rückwärtskompatibilität

Entscheidend für den Erfolg aller kryptografischen Ansätze für den Schutz von VoIP ist die Rückwärtskompatibilität zu Lösungen und Endgeräten, die noch keine Kryptografie unterstützen, und die Signalerhebung zum Benutzer, ob es sich um eine gesicherte oder ungesicherte Verbindung handelt.

Daher muss die Verschlüsselung als eine Art „Capability“ bzw. Session-Merkmal am Anfang der Session ausgehandelt werden. Kann keine sichere Verbindung zustande kommen, muss eine nicht verschlüsselte Kommunikation möglich sein.

Die VoIP-Kommunikationspartner müssen in der Lage sein zu erfahren, ob es sich bei einer Session um eine sichere oder unsichere Session handelt. Dies muss mittels eines schnell erkennbaren Symbols auf dem Telefondisplay zu überprüfen sein, vergleichbar mit dem Schlosssymbol bei Webbrowsern (siehe Abbildung 17).

Vergleichbare Symbole werden von einigen IP-Telefonen bereits unterstützt, zum Beispiel von den Cisco-Telefonen, die SRTP unterstützen.

Rolle von Open Source

Ein kryptografischer Algorithmus entwickelt seine Stärke am meisten, wenn auch der Algorithmus und der Source Code offengelegt sind, damit ausgeschlossen ist, dass „back doors“ eingebaut werden. Deshalb kommt den Open-Source-Projekten bei der Entwicklung der Sicherheitsarchitektur für VoIP eine entscheidende Rolle zu.

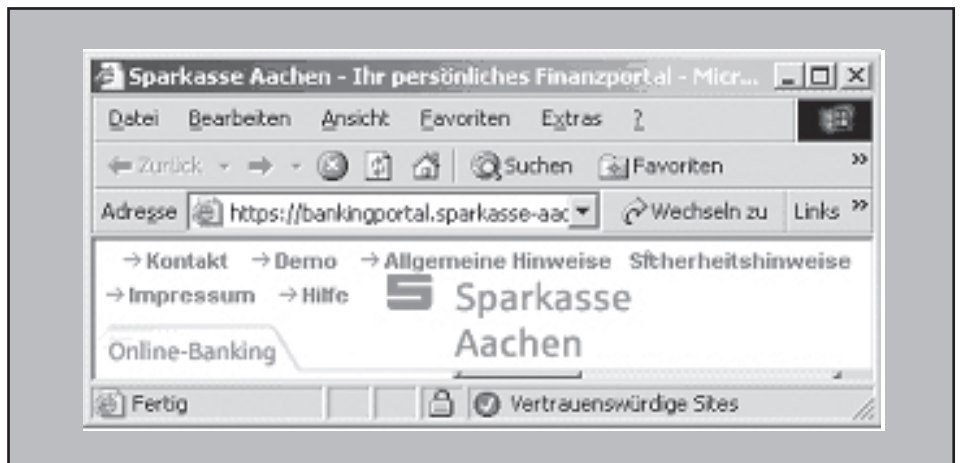


Abbildung 17: Symbol für eine sichere Verbindung muss schnell erkennbar sein

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

le zu. In Open-Source-Projekten sind nicht nur die Protokolle, sondern auch die Implementierungen offen zugänglich und auf Herz und Niere überprüfbar.

Es ist verständlich, wenn Anbieter von Lösungen bestrebt sind, den Wunsch von VoIP-Nutzern nach mehr Sicherheit für ihre eigenen kommerziellen Interessen zu nutzen. Dies muss auch nicht unbedingt in einen Zielkonflikt mit Open-Source-Projekten geraten. Es ist durchaus denkbar, auch Open-Source-Lösungen mit kommerziellen Angeboten zu verknüpfen, indem zum Beispiel ein bestimmter Mehrwert in Bereichen wie Management der Open-Source-Lösung hinzugefügt wird.

Aber rein kommerzielle oder gar proprietäre Lösungen werden nicht imstande sein, das Vertrauen in die Sicherheit von VoIP so zu stärken, dass künftig die Benutzer von VoIP ihre Gespräche mindestens mit dem selben Gefühl von Sicherheit den IP-Netzen anvertrauen wie bisher dem PSTN.

Verstößt VoIP-Verschlüsselung gegen das Gesetz?

Fast alle Staaten haben Gesetze und Verordnungen verabschiedet, mit denen eine Überwachung des Telefon- und Internet-Verkehrs erzwungen werden soll. Im englischen Sprachraum werden diese Regelungen Lawful Interception genannt. In Deutschland gelten seit den 1990er Jahren entsprechende Gesetze und Verordnungen für die Telekommunikationsüberwachung (damals als „Großer Lausangriff“ bezeichnet). In den USA gibt es das Gesetz mit dem Titel Communications Assistance for Law Enforcement Act (CALEA).

Ist es also nach diesen Gesetzen und Verordnungen verboten, Telefongespräche zu verschlüsseln?

Diese Gesetze und Verordnungen beinhalten Verpflichtungen für Service Provider und nicht für Endbenutzer, d.h. der Staat kann die Endbenutzer nicht daran hindern, die Kommunikation zu verschlüsseln. Tauschen zwei Benutzer mit PGP verschlüsselte E-Mails aus, können ohne weitere Vorkehrungen nur die beiden Benutzer die E-Mails entschlüsseln. Entsprechendes gilt für die Telefonie. Sprechen zwei Personen verschlüsselt miteinander, kann niemand im Netz das Gespräch abhören.

Natürlich müssen neben der TK-Überwachung auch andere Gesetze beachtet werden. Zum Beispiel unterliegt der Export von Software für starke Verschlüsselung nach den amerikanischen Gesetzen

bestimmten Einschränkungen. Deshalb wird zum Beispiel beim Download von Zfone überprüft, ob der Download-Vorgang von sanktionierten Staaten aus erfolgt. Allerdings ist die dabei erfolgte Prüfung anhand der IP-Adresse nicht gerade als große Hürde für so genannte Schurkenstaaten und Terroristen zu sehen.

Letztendlich können Staaten die Endbenutzer nicht von der Anwendung von Kryptografie abhalten. Der Autor ist der Auffassung, dass gerade die raffiniertesten und damit gefährlichsten Teile der kriminellen Szene (seien es Terroristen oder die organisierte Kriminalität) bereits heute sämtliche Abhörmaßnahmen umgehen können, wenn sie wollen. Somit wurde in den letzten Jahren in vielen Ländern das Recht auf Schutz der Privatsphäre ausgehöhlt, ohne dass damit langfristige wirksame Mittel bei der Bekämpfung der Kriminalität und des Terrorismus geschaffen worden wären.

Die entscheidende Frage für die Unternehmen lautet, wie sie mit Technologien für die Verschlüsselung der Telefonie umgehen. Wenn die Unternehmen aktiv daran arbeiten, VoIP-Verschlüsselung generell einzuführen, können sie möglicherweise in Zukunft mit einer unlösbaren Aufgabe konfrontiert werden, wenn der Staat die Definition der Service Provider auf Unternehmensnetze ausweiten und wie beim Mobilfunk von den unternehmensinternen Service Provider Abhörschnittstellen verlangen würde. Sollen deshalb die Unternehmen VoIP-Verschlüsselung im ei-

genen Netz verhindern? Auch dies kann sich technisch als eine immer schwierigere Aufgabe erweisen.

Der Autor hegt die Hoffnung, dass irgendwann in der Zukunft die Einsicht, dass moderne Technologien die Abhörung sowohl von Daten- als auch von Sprachkommunikation verhindern können, auch in der Politik ankommt. Angesichts des allgemein verbreiteten Unwissens und der Stimmen, die man in Wahlen mit dem Thema Sicherheit fangen kann, ist diese Hoffnung jedoch nicht sehr groß.

Fazit

Der Stand sicherer IP-Telefonie mittels Verschlüsselung ist also irgendwo auf dem Weg zu einer standardisierten Technik, die analog zu E-Business am Ende nichts anderes als sinnvoll erscheinen lässt als eine von Ende zu Ende verschlüsselte Übertragung, denn nur so kann das Sicherheitsniveau der herkömmlichen Telefonie erreicht und dann auch übertroffen werden. Dass wir noch nicht so weit sind, liegt vor allem an einem fehlenden Baustein: am standardisierten Schlüsselmanagement. Hier gibt es noch verschiedene Ansätze. Welcher Ansatz am Ende sich durchsetzen wird, ist noch nicht absehbar.

Innerhalb der Produktumgebung eines Herstellers funktioniert schon VoIP-Verschlüsselung. In der Regel übernimmt dabei der Telefonieserver neben seinen zentralen Vermittlungsfunktionen auch die zentrale Rolle beim Schlüsselmanage-

Seminar



SIP - Basis-Technologie der IP-Telefonie

10.09. - 12.09.07 in Berlin

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.

Referenten: Dipl.-Inform. Petra Borowka, Dipl.-Ing. Ralf Glörfeld
Preis: € 1.690,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.de

Herausforderung VoIP-Sicherheit - Wie sicher ist die Kommunikation von morgen?

ment. Es reicht, wenn jedes Endgerät eine Vertrauensbeziehung mit dem Telefoneserver unterhält, der dann durch einen verschlüsselten Kanal zu jedem Endgerät den Austausch des symmetrischen Schlüssels für jedes Gespräch sicherstellen kann.

Somit können wir zwar nicht über das Internet ohne größeren Aufwand mit jedem beliebigen Kommunikationspartner telefonieren, aber innerhalb von Unternehmensnetzen, auch wenn sie sich auf mehrere Standorte erstrecken, ist das möglich, vorausgesetzt, es wird für ein zentrales Schlüsselmanagement gesorgt. Diese Voraussetzung ist umso schwieriger zu realisieren, je komplexer die Umgebung ist. Eine homogene Produktumgebung ist natürlich die einfachste Art und Weise, auch für ein funktionierendes Schlüsselmanagement zu sorgen. Wo dies nicht möglich ist, muss man mit Hindernissen und sicherlich mit einem nicht zu unterschätzenden Aufwand für ein Ende-zu-Ende-Schlüsselmanagement rechnen.

Wie lange wird der Weg der IP-Telefonie zum Pendant der von den meisten Benutzern als sicher genug eingestuftes E-Business-Infrastruktur dauern? Wenn man E-Business zum Maßstab nimmt, können wir von einer etwa fünf- bis siebenjährigen Zeitspanne zwischen der Etablierung einer Technologie zunächst ohne sichere Verschlüsselung und der Ergänzung dieser Technologie um die zugehörige Sicherheitskomponente ausgehen (zum Beispiel von der Einführung des World-Wide Web Mitte der 1990er Jahre bis zur Etablierung von https um die Jahrtausendwende). Diese Zeit geht ins Land, weil sich ein Standard als Gewinner durchsetzen muss und dann auch diejenigen der Hersteller und Provider, die diesen Standard nicht favorisiert hatten, ihn im nächsten Produktrelease doch noch unterstützen.

Vom Problem des Schlüsselmanagements abgesehen, ist alles andere für die sichere IP-Telefonie schon standardisiert. Es ist daher nicht mehr sinnvoll, Telefoneserver, Endgeräte und Gateways zu beschaffen, die keine Verschlüsselung unterstützen. Um sicherzustellen, dass diese Unterstützung kein reines Versprechen bleibt, sollte man schon üben und die Sicherheitsfunktionen der Produkte nutzen. Es ist nicht sinnvoll, die Sicherheit der IP-Telefonie auf eine unbestimmte Zukunft zu vertagen. Auch wenn sichere IP-Telefonie zurzeit nur innerhalb der Grenzen des Unternehmensnetzes bleibt und damit scheinbar keinen großen Mehrwert bietet, sollte man sie nicht nur fordern, sondern auch umsetzen. Nur so wird die Technologie beherrschbar.

Kongress



Voice-over-IP-Forum 2007

12.11. - 15.11.07
in Königswinter

Das ComConsult Voice-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2007. Wir greifen die absoluten Top-Themen des Marktes auf und analysieren für Sie den Stand der IP-Telefonie, Security-Lösungsansätze, die Entwicklung des Marktes, Vorteile und Risiken und die Strategien der großen Hersteller.

Moderation: Dr. Jürgen Suppan
Preis: € 2.190,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.de

Aktuelle Veranstaltungen

IP-Telefonie evaluieren, planen, betreiben, 03.09. - 05.09.07 in Bonn

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet.

Preis: € 1.690,- zzgl. MwSt.

SIP - Basis-Technologie der IP-Telefonie, 10.09. - 12.09.07 in Berlin

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.

Preis: € 1.690,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 10.09. - 11.09.07 in Berlin

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

**Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
10.09. - 14.09.07 in Berlin**

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 2.290,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 10.09. - 11.09.07 in Berlin

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,- zzgl. MwSt.

Ethernet-Netzwerke: Techniken, Einsatzgebiete und Betrieb, 10.09. - 12.09.07 in Aachen

Dieses Seminar stellt die aktuellen Ethernet-Themen vor und zeigt, wie etablierte und neue Techniken in bereits wohlbekannten und zukünftigen Anwendungsgebieten eingesetzt werden können. Zu den analysierten Sonderanwendungsgebieten gehören insbesondere VoIP, Gefahrenmeldetechniken, Industrienetze und Rechenzentrumsbereiche. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, Planungsregeln vorgestellt, Möglichkeiten und Grenzen von Quality of Service und Risiken durch Fehlentscheidungen bei der Technikauswahl aufgezeigt. Aufbau von Infrastrukturen, Fehlersuche und das allgegenwärtige Thema Sicherheit werden aus der Praxis moderner Ethernet-Netze beleuchtet.

Preis: € 1.690,- zzgl. MwSt.

IP-Wissen für Voice-over-IP, 17.09. - 18.09.07 in Neuss

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das Sie zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen.

Preis: € 1.390,- zzgl. MwSt.

Trouble Shooting in konvergenten Netzwerken, 17.09. - 21.09.07 in Aachen

Dieses Seminar vermittelt das notwendige Hintergrundwissen über die typischen Fehler, erklärt ihre Erscheinungsformen im laufenden Betrieb und trainiert systematisch ihre Diagnose und Beseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainingsnetzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Preis: € 2.490,- zzgl. MwSt.

**Internetworking: optimales Netzwerk-Design mit Switching und Routing,
17.09. - 21.09.07 in Aachen**

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können.

Preis: € 2.290,- zzgl. MwSt.

**Wireless LANs: Planung, Produktauswahl, Installation, Trouble Shooting,
08.10. - 12.10.07 in Bonn**

Dieses 5-tägige Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. Die letzten beiden Tage sind optional buchbar und liefern vertiefte Kenntnisse zur Planung, Konfiguration und Betrieb von flächendeckenden sicheren WLAN und Hotspots, ergänzt durch praktische Beispiele und Demonstrationen.

Preis: € 2.290,- zzgl. MwSt.