ComConsult Research

Der Netzwerk Insider

Juli/August 2007

Systematische Weiterbildung für Netzwerk- und IT-Professionals

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 Kundendaten 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. Vollendet 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

auf Seite 4

Geleit

ComConsult Certified Voice Engineer

auf Seite 2

Report des Monats

Session Initiation Protocol

auf Seite 13

Zum Geleit

ComConsult Certified Voice Engineer

Wer in die Umsetzung von IP-Telefonie-Projekten einsteigt, bewegt sich schnell in zwei Welten. Nach wie vor ist klassisches TK-Wissen notwendig. Das beginnt bei den bekannten Leistungsmerkmalen, geht über die Gateways zum PSTN, über Rufnummernpläne, Voice-Anwendungen bis hin zu Spezialanwendungen. Gleichzeitig erfordert die Umsetzung von IP-Telefonie erhebliches IP-Wissen:

- IP-Adressen müssen vergeben werden, TFTP-Server eingerichtet und DHCP-Server konfiguriert werden
- Das zentrale Element jeder IP-Telefonie-Lösung ist der Voice-Router, egal ob der als Registar, Call Manager oder wie auch immer bezeichnet wird. Dieser setzt immer mehr auf offenen Betriebssystemen auf und seine Architektur verschmilzt mit der des Betriebssystems. Speziell im Bereich ausfallsicherer und skalierbarer Architekturen ist das eindeutig. Der Trend geht weg von den herstellerspezifischen Spezialtechnologien und hin zur Nutzung offener Betriebssystem-Funktionen
- Die Nutzung von Skripten und XML-Parameter-Dateien ist unvermeidbar
- Die Integration ins Netzwerk erfordert detailliertes Wissen über VLAN´s, PoE, Switching, Layer2/3-Strukturen, Quality of Services
- Die Schaffung einer sicheren Voice-Lösung geht nur in einem integrierten IT-Gesamtkonzept, der Artikel von Dr. Moayeri in diesem Insider macht dies deutlich
- Immer mehr Applikationen gehen in Richtung Kollaboration, die Integration des zugehörigen Softclients ins Betriebssystem führt zu einer Verschmelzung von IT und TK. Nicht macht dies mehr deutlich als der Ansatz von Microsoft mit dem Office Communication Server und der Client-Integration in Office-Anwendungen

Die Entwicklung der technischen Architektur von Sprach-Lösungen entspricht genau diesem Bild. Die herstellerspezifischen und geschlossenen Architekturen öffnen sich in Form von Funktionsblöcken, die zunehmend aus einer Mischung aus offenen und geschlossenen Funktionen bestehen:

- IP-optimierte Infrastrukturen im Kern (Netzwerke, IP-Dienste, Verzeichnisdienste, ...)
- Voice-Routing und Call-Management als zunehmend offener Funktionsblock, Gestaltung von Ausfallsicherheit und Skalierbarkeit mit einer Mischung aus offenen und spezifischen Funktionen
- Leistungsmerkmale als applikationsartiger Aufsatz auf das Basis-Call-Routing in einer Mischung aus genormten und herstellerspezifischen Modulen
- Applikationen, zunehmend neutral von der darunter liegenden Sprach-Lösung

Die Beherrschung dieser Architektur, dieses Wandels weg von einer rein herstellerspezifischen und hin zu einer gemischt offenen/geschlossenen Architektur erfordert ein neues Wissensprofil für Planer und Betreiber.

Ohne tiefer in die Details einzusteigen, wird doch schnell deutlich, dass hier ein neues Berufsbild entsteht. Die Planung und auch der Betrieb einer IP-Telefonie-Lösung erfordert ein Spezialwissen, das in dieser Form bisher nicht vorhanden ist. Dem bisherigen IT-Spezialisten fehlt das TK-Wissen, dem TK-Spezialisten das IT-Wissen.

Nachdem wir nun über die letzten 2 Jahre unsere Basiskurse zur IP-Telefonie aufgebaut haben, hat sich mit dem neuen Kursen der letzten Monate das Mosaikbild geschlossen. Systematisch haben wir die Bausteine aufgebaut, die zu einer soliden Ausbildung zum Voice-Spezialisten erforderlich sind.

Deshalb freuen wir uns, Ihnen heute die Einführung des ComConsult Certified Voice-Engineers ankündigen zu können.

Im Einzelen besteht die Ausbildung aus folgenden Modulen:

- Optional: IP-Wissen für Telekommunikations-Mitarbeiter: was Sie über IP Wissen müssen, um IP-Telefonie umsetzen zu können
- Optional: Voice-over-IP für Telekommunikations-Mitarbeiter, wird aufgrund der an den Kunden angepassten Inhalte zur Zeit nur als Inhaus-Kurs angeboten
- Alternative 1: IP-Telefonie evaluieren, planen und betreiben
- Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
- Session Initiation Protocol SIP
- Voice-Security

Alternative 1 oder 2 müssen wahlweise besucht werden. Aufgrund der beabsichtigten inhaltlichen Überlappung der beiden Kurse reicht es aus, einen der beiden zu besuchen. Wer als Zertifizierungsteilnehmer beide Kurse besuchen will, kann dies zu einem sehr attraktiven Sonderpreis machen.

Die Zertifizierung ist mit einem Abschlusstest verbunden, der elementares Wissen über IP-Telefonie abfragt.

Basierend auf der Projekterfahrung der letzten Monate und Jahre wurde diese Zertifizierung so angelegt, dass sie ein maximales und Praxis-erprobtes Hersteller-neutrales Wissen optimal vermittelt. Sie liefert das optimale Fundament für erfolgreiche Projekte und stellt einen wesentlichen Baustein der beruflichen Weiterentwicklung da.

Sollten Sie Fragen zur Zertifizierung haben, so stehen wir Ihnen gerne beratend zur Seite.

Viel Erfolg
Ihr
Dr. Jürgen Suppan

Neue Zertifizierung

ComConsult Certified Voice Engineer

Die neue Zertifizierung der ComConsult Akademie „ComConsult Certfied Voice Engineer“ besteht aus folgenden Seminaren:

SIP (Session Initiation Protocol)-Basis-Technologie der IP-Telefonie

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.

Sicherheitsmechanismen für Voice over IP

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.

IP-Telefonie
evaluieren, planen, betreiben

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.

IP-Telefonie:
Vorbereitung, Migration, Management

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.

IP-Wissen für TK-Mitarbeiter

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

Voice over IP für TK-Ler

Dieses Seminar richtet sich ausschließlich an Mitarbeiter von Unternehmen und Behörden, die bisher mit dem Betrieb konventioneller TK-Lösungen befasst waren und jetzt auf VoIP umsteigen wollen. Dabei wird nicht so sehr auf die tiefgründige technische Details der neuen Technologie eingegangen, sondern auf die täglichen Anforderungen - bei der Einführung und beim laufenden Betrieb.

Die detaillierten Informationen entnehmen Sie bitte der Seite 2 oder besuchen Sie uns auf unserer Homepage www.comconsult-akademie.de. Unter der Rubrik „Zertifizierungen“ finden Sie dann alle Informationen. Gerne senden wir Ihnen auch Informationen per EMail zu. Füllen Sie dazu bitte nur das untenstehende Formular aus und schicken es uns per Fax unter 02408-955 399 zurück.

Fax-Antwort an ComConsult 02408/955-399

ComConsult Certified Voice Engineer

☐ Ich interessiere mich für die Ausbildung zum ComConsult Certfied Voice Engineer. Bitte schicken Sie mir detailierte Informationen zu.

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

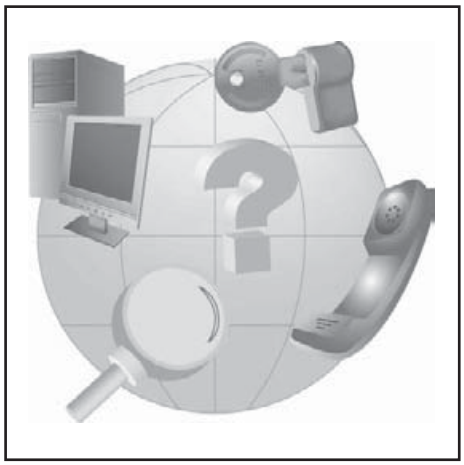
Aktueller Kongress

Voice-over-IP-Forum 2007

Die ComConsult Akademie veranstaltet vom 12. - 15.11.07 ihr diesjähriges Voice-over-IP-Forum in Königswinter.

Das ComConsult Voice-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2007. Wir analysieren die technische Entwicklung der IP-Telefonie hin zu neuen Architektur-Formen, bewerten die Strategien der führenden Hersteller und geben einen tiefen Einblick hinter die Kulissen von Markt und Produkten. Auch in diesem Jahr wird das ComConsult-Voice-Forum von exklusiven Untersuchungen von ComConsult-Research begleitet, die nur den Teilnehmern dieses Forums zugänglich sind.

- Wo steht IP-Telefonie?
  - Funktionsumfang
  - Offenheit
  - Betriebsaufwand
  - Kostenentwicklung
- ComConsult-Research Analyse: Voice-Architektur im Wandel
  - Wohin tendieren Anlagen-Architekturen
  - Ausfallsicherheit und Skalierbarkeit: Kampf der Konzepte
  - Die zukünftige Rolle der Applikation: Auswirkung auf die Kaufentscheidung
- ComConsult-Research Analyse: Marktentwicklung
  - Wohin entwickelt sich der Markt in den nächsten 3 bis 5 Jahren?
  - Positionierung von Produkten und Herstellern: Alcatel, Avaya, Cisco, Nortel, Siemens
  - Wer wird gewinnen, wer verlieren?



- ComConsult-Research: Produkte im Technologie-Test
  - Microsoft OCS: Leistung, Nutzbarkeit, Integrierbarbeit
  - Siemens HiPath 8000: besser als die HiPath 4000? besser als Call Manager 6?
  - Cisco Call Manager 6: Positionierung und Leistung, wie weit geht SIP?
- ComConsult-Research Analyse: SIP, der neue Standard für Sprach- und Multimedia-Kommunikation
  - Die SIP-Vision: eine neue Form von Kommunikation im und zwischen Unternehmen
  - SIP-Architektur
  - Rolle der Hersteller
- Einzelne Detail-Studien
  - Die zukünftige Rolle des Clients: Hard- kontra Softphone, Einfluss der Multimedia-Kommunikation, SIP, Microsoft
  - SIP-Trunking: wo steht der Markt, welche Leistungen beinhaltet das Angebot der Provider
- ComConsult-Research Analyse: Voice-Security
  - Warum ein Sicherheitskonzept vorhanden sein muss
  - Alternative Lösungen
  - Verschlüsselung ja, aber woher kommt der Schlüssel?
  - Hersteller gegen oder mit welchen Standards: Perspektiven einer offenen Lösung

Das Forum bietet in der optimalen und interaktiven Mischung aus

- Exklusiven Analysen von ComConsult-Research
- Erfahrungsberichte aus aktuellen Projekten
- Produkt- und Markt-Diskussionen
- Podiumsdiskussion mit kritischen Fragen an die Hersteller
- einer begleitenden Ausstellung

ein herausragendes Programm.

Zögern Sie nicht, sich einen Platz in dieser wichtigen Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-phase bis 15.09.2007

Anmeldung
Voice-over-IP-Forum 2007

Frühbucher-phase bis 15.09.2007

☐ Ich buche den Kongress
Voice-over-IP-Forum 2007
12.11. - 15.11.07 in Königswinter
zum Preis von € 1.990,-* zzgl. MwSt.
* gültig bis zum 15.09.07

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____07

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

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Zweitthema

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

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

Dies wirft sofort eine Reihe von Fragen auf, auf die dieser Artikel im folgenden eingeht:

- drohen unseren Netzwerken mit dem neuen Microsoft TCP-Stack deutlich höhere Spitzenlasten?
- Können dadurch Überlasten oder Instabilitäten zum Beispiel durch einen Pufferüberlauf in Switch-Systemen entstehen? Müssen die so genannten Buchungsfaktoren für die Planung von Netzwerken angepasst werden (diese beschreiben die theoretische Überlastbarkeit von Switchen unter der Annahme typischer Spitzenlasten)?
- Können dadurch stärker schwankende Betriebssituationen entstehen?
- Erfordern mögliche Überlasten ein Umdenken im Einsatz von Quality of Service? Bisher ist QoS in 100/1000-Netzwerken nicht erforderlich, es steigert nur den Betriebsaufwand. Ändert sich das nun?

1. Warum (Artikel zu Vista's) Verbesserungen für TCP?

Vista ist da, an Longhorn wird fleißig gearbeitet - natürlich werden die damit verbundenen Neuerungen in der Fachpresse beschrieben und diskutiert. Diesmal stürzt man sich dabei nicht ausschließlich auf Aspekte wie Aussehen und Handhabung der Oberfläche, neue Dienstangebote u.Ä.: vermehrt findet man auch Artikel über die Veränderungen an der mitgelieferten TCP/IP-Software. Diese hat Microsoft schon eine Weile als „Next Generation IP-Stack" angekündigt, ja angepriesen.

„Next Generation" - das klingt nach dem Versuch eines großen, neuen Wurfs. Oder wurde diese Bezeichnung gewählt, weil Microsoft mit Vista / Longhorn verstärkt mit der Unterstützung von IPv6 „Ernst macht" (IPv6 wurde anfänglich auch als „IP next generation" bezeichnet)?! Ja, das Thema IPv6 wurde tatsächlich stärker in den Blickpunkt genommen, was auch erklärlich ist, da in 2005/2006 eine deutliche neue Lage hinsichtlich stabiler RFC-Dokumente zu diesem Thema entstanden ist. Insofern könnte man sich an dieser Stelle mit Vista und IPv6 beschäftigen.

Nicht die neue Situation bzgl. IPv6 soll hier aber näher betrachtet werden (gerne ein anderes Mal), sondern ein anderer Themenkreis, bei dem Vista mit Neuerungen aufwartet, und zwar mit potenzieller Wirksamkeit unabhängig von der IP-Version: Flusskontrolle unter TCP. Vista wirbt hier gleich mit mehreren Modifikationen, und diverse Artikel (nicht nur von Microsoft) sagen spürbare Auswirkungen in Netzwerken voraus. TCP-Flusskontrolle, was war das gleich wieder? Im Prinzip wird hier versucht, auf automatischem Wege einen guten Kompromiss zu finden zwischen möglichst guter „Performance" bei der Übertragung von Nutzdaten via TCP und der Vermeidung von Engpässen durch Überlastung der Ressourcen, Ressourcen im Netzwerk bzw. Empfänger-Kapazität. Devise dabei: vorsichtig einsteigen (slow start), bei Übertragungserfolg zunächst kräftig nachlegen, dann wieder vorsichtiger werden (congestion avoidance, also „Engpassvermeidung"); sollte dennoch etwas schiefgehen (timeout, retransmission nötig) - Luft rausnehmen aus der Senderaktivität. (s. Abbildung 1)

Klingt doch überzeugend, also warum zum Thema machen? Der Grund: die Art und Weise, in der dieser Ansatz im Detail ursprünglich umgesetzt wurde, hatte Netzwerk-Kapazitäten vor Augen, die im Vergleich zu heute lächerlich sind. Ent-

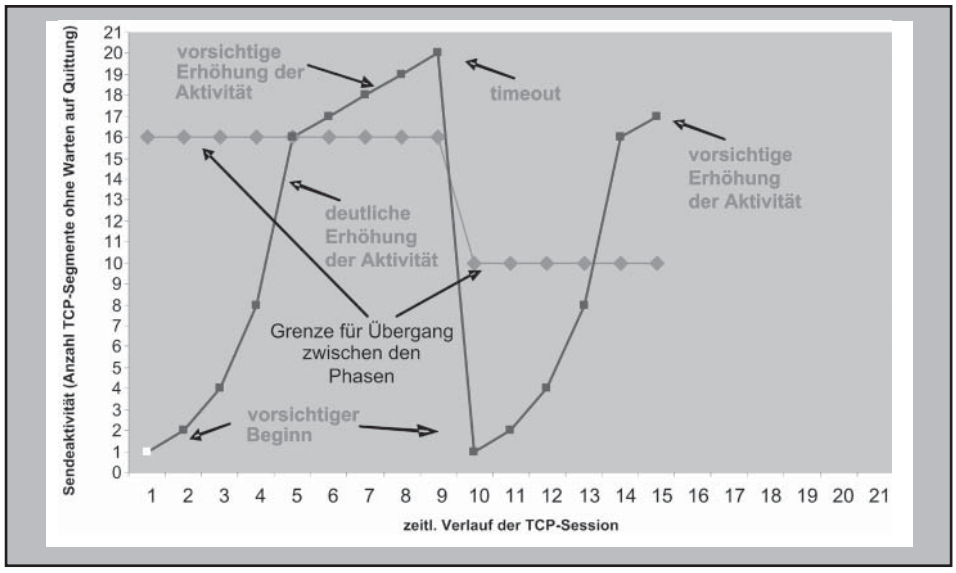


Abbildung 1: Regelung der Sendeaktivität (klassisches TCP)

sprechend wirkt die in TCP von alters her eingebaute Vorsicht in modernen Hochgeschwindigkeitsnetzen eher wie ein „Angstprinzip“. Bloß weil man einmal bremsen musste, ab jetzt ängstlicher weiterfahren? Die Geschwindigkeit auf die Fahrbahnqualität von Autobahnen der 80er Jahre auslegen? Klingt übertrieben, gibt aber das Problem gut wieder: Die Grundannahme, ein Timeout ist ein klares Signal für ein grundlegendes Engpassproblem, lässt sich heute in vielen Situationen nicht mehr aufrecht erhalten:

- beim Zellwechsel im WLAN geht vielleicht das eine oder andere Paket verloren und wird entsprechend nicht quittiert; nach diesem Timeout hat man aber im Bereich der neuen Zelle gleich gute Voraussetzungen wie vorher;

- heilt eine dynamische Redundanz im LAN ein Problem (Timeout-Ursache) auf dem bisher genutzten Übertragungsweg, so steht danach typisch ein gleich guter neuer Weg zur Verfügung, auf dem man sich mit der Daten- und Paketmenge nicht zurückhalten braucht.

Und das Bild mit der Geschwindigkeit passend zur Fahrbahnqualität der 80er Jahre? Geregelt wird die TCP-Übertragungsleistung über das „Congestion Window“, das praktisch als Sliding Window über die zu übertragenden Daten geschoben wird und aussagt, wie viel Datenbytes der Sender als Inhalte aufeinanderfolgender Pakete schicken kann, ohne auf eine Quittung (ACK) durch den Empfänger zu warten. Das macht genauer betrachtet die TCP-Flusskontrolle: sie reguliert zwischen den beiden Extremen „jedes Paket muss einzeln quittiert werden, dann erst geht es weiter“ („ping-pong-TCP“, ganz schlechte Performance!) und „der Sender kann alles ungebremst schicken, was die Anwendung dem IP-Stack an Nutzdaten abgeliefert hat“ (Optimum aus Anwendungssicht). Dabei gibt es von vorneherein eine zulässige „Höchstgeschwindigkeit“, geregelt durch die Aufnahmekapazität, gemeldet vom Empfänger - und für diese Meldung wird vom Empfänger ein bestimmter Wert nie überschritten. Leider ist diese Obergrenze auf ältere Netze ausgelegt: ein Empfänger nach klassischer TCP-Spezifikation meldet niemals eine größere mögliche Window-Größe als 65536 Byte: Nach 64 KB gesendeten Daten muss der Sender bereits warten, bis Quittungen kommen. Angesichts von Netzwerk-Kapazitäten von 100 MBit/s an jedem Endgerät ist das natürlich eine drastische Beschränkung, sobald die Quittungen nicht rasend schnell vom Empfänger zurück kommen: Ist die Round Trip Time (RTT) zwischen Sender und Empfänger nur ein bisschen länger, als der Sender für das Versenden von 64 KB als TCP-Daten benötigt, so ist hier zwangsläufige eine Performance-Bremse gegeben. Selbst im Weitverkehrsbereich ist es heute durchaus möglich, im Rahmen des Bandbreitenangebots mehr als 64 KB unmittelbar auf die Leitung zu bringen …

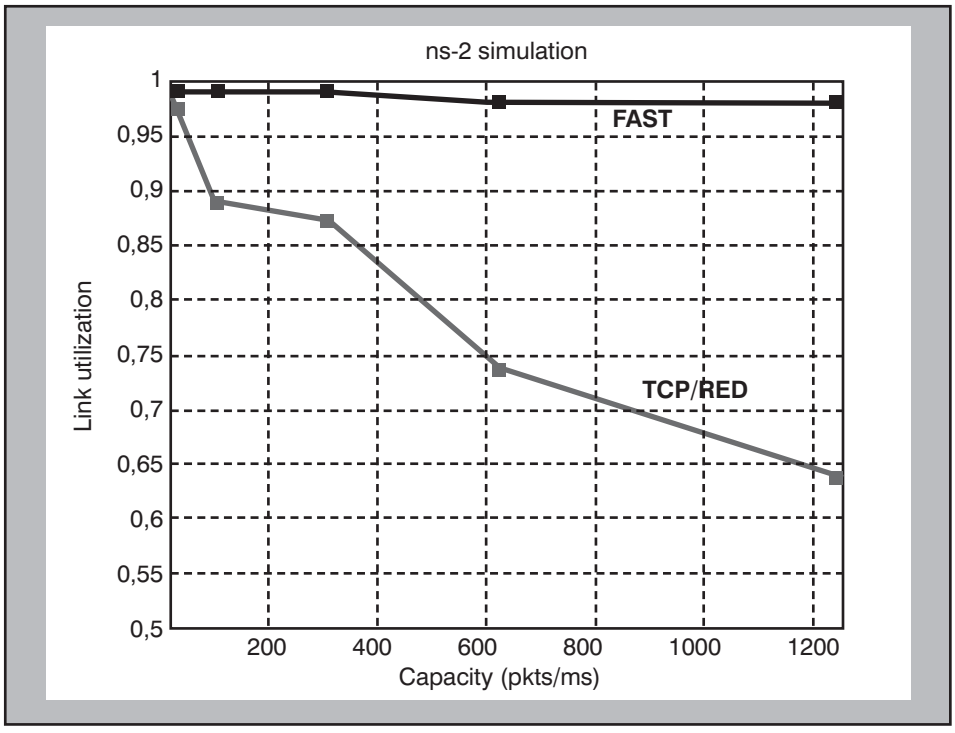


Abbildung 2: Messpunkte bei 155Mbps, 622Mbps, 2.5bps, 5 Gbps, 10 Gbps; 100 ms round trip latency; 100 Flows

Also: jawohl, TCP-Flusskontrolle bzw. eine Anpassung an die Gegebenheiten heutiger Netze ist ein wichtiges Thema und ja, Microsoft hat da ein durchaus aktuelles Thema aufgegriffen. Neueste RFCs (z.B. RFC 4653 aus August 2006) beschäftigen sich mit dem Thema der Optimierung von TCP, und auch andere IP-Stack-Lösungen bieten immer wieder Neuerungen in diesem Bereich an: z.B. wird ein Westwood+ genannter spezieller Ansatz unter diversen Linux- und UNIX-Versionen verfolgt, und es wurden gezielt Tests damit auf 10 GBit/s -Verbindungen durchgeführt. Apple kündigt mit OS 10.5 („Leopard“, vorgesehen für Oktober 2007) ebenfalls ein „self-tuning TCP“ an, das flexibler auf die Gegebenheiten im Netzwerk eingehen soll.

Warum aber überhaupt soviel Anstrengungen an diesem Punkt? Es ist absehbar, dass TCP ohne geeignete Optimierungen Investitionen in immer höhere Bandbreiten umso mehr entwerten kann, je größer die Bandbreitenzuwächse sind. Studien und Experimente kommen immer wieder zu dem Ergebnis, dass ohne gezielte Optimierungen am Verhalten von TCP ein deutliches Missverhältnis zwischen Netzwerk-Kapazitäten und erzieltem Nutzen entstehen kann.

Das in Abbilung 2 exemplarisch wiedergegebene Ergebnis einer Untersuchung mit einer Lösung zur Simulation von Netzwerk-Umgebungen zeigt, dass ohne Nutzung optimierender TCP-Optionen (rote Kurve) die Schere zwischen Bandbreitenangebot und mit 100 parallelen TCP-Datenströmen erreichbarer Auslastung immer deutlicher auseinanderklafft. Auf einem 10 GBit/s-uplink schaffen diese 100 Datenströme bei einer RTT von 100 ms lediglich eine Netzauslastung von unter 65%.

In der Praxis kann dies heißen: viel Geld in höhere Bandbreiten investieren – und keiner merkt einen angemessenen Unterschied! Insofern ist es sicher mehr als nur „nett“, wenn ein Hersteller wie Microsoft, der über sein Betriebssystem einen hohen Anteil der IP-Software in heutigen Umgebungen beisteuert, hier Brauchbares anbietet.

Allerdings - jedes Ding hat zwei Seiten. So auch hier: Artikel, die sich auf die entsprechenden Informationen zum neuen Vista-IP-Stack beziehen, warnen zum Teil, man müsse bei Einführung von Vista unbedingt auch Quality of Service einsetzen. Was denn nun: TCP-Tuning als Mittel, um

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

moderne Netzwerke geeignet ausnutzen zu können, oder als mögliche Störungsursache?

Beides kann richtig sein! Völlig dumm war der klassische Ansatz ja nicht. Findet man Bedingungen vor, auf die er zugeschnitten war, d.h. hohe Engpass-Wahrscheinlichkeit, so ist das darin geübte Vorsichtsprinzip nach wie vor goldrichtig. In eine ohnehin schon am Rande der Kapazitätsgrenze belastete Netzwerk-Strecke noch erhöhte Sendeaktivität einströmen zu lassen, kann wohl kaum zu guten Ergebnissen führen. Wer würde versuchen, sich mit 180 km/h in zähfließenden Verkehr einzufädeln?

Je weiter die Situation jedoch von einem solchen Engpass-Zustand entfernt ist, umso wertvoller ist jede Möglichkeit, dem Fahrzeug die Handbremse weiter zu lösen. Insofern stellen sich typische Fragen:

- Welche TCP-Tuning-Optionen habe ich zur Verfügung?
- Wo setzen diese an, unter welchen Bedingungen werden sie spürbar Wirkung zeigen können?
- Kann eine bestimmte Option durch ungünstig erhöhte Netzlast gefährlich werden, und wenn ja, unter welchen Rahmenbedingungen?

Folgerungen:

- Was passt in meine Umgebung?
- Welche Defaults kann ich bestehen lassen (schaden zumindest nichts), welche ändere ich gezielt ab, um mehr aus meiner Technik herauszuholen oder aber, um Schaden zu verhindern?
- Hat es Sinn, pauschal mit QoS als Hilfsmittel zu reagieren?

Je nach Antworten in der Zielumgebung ergeben sich eventuell gezielte Konfigurationsänderungen, an den Kommunikationsteilnehmern und/ oder an den Netzwerk-Komponenten.

2. Vista-Feature: „Receive Window Auto Tuning“

Ein gutes Beispiel, um solche Überlegungen einmal gezielt anzustellen und dabei ein Gespür für die Tücken der Vorhersage von Wirkungen eines Eingriffs in Flusskontrollautomatismen zu entwickeln, ist eines der Features des neuen Vista-IP-Stacks.

Von der Grundidee her handelt es sich um einen alten Hut, nämlich die Aufhebung der vorhin erläuterten Beschränkung der gemeldeten Empfänger-Kapazität auf ein „receive window“ von 64 KB. Ein alter Hut ist dies aus zwei Gründen:

- Die hierfür vorgesehene Basis ist bereits in RFC 1323 „TCP extensions for high performance“ als „Window Scaling“ (auch: „Large Windows“) spezifiziert, im Vergleich zu den aktuellen 4000er RFCs wahrlich ein Methusalem-Dokument, aus dem Jahre 1992.

- Microsoft unterstützt den RFC 1323 bereits seit Windows 2000, mit geringfügiger Abwandlung der Implementierung / Konfiguration beim Übergang auf Windows XP/ Windows 2003 übernommen.

Sofern für einen IP-Stack RFC 1323-Unterstützung aktiviert ist, signalisiert dieser dies beim Verbindungsaufbau (und nur da) über einen optionalen TCP-Header. Dieser Rückgriff auf einen optionalen Header ist notwendig, denn das „window“-Feld im TCP-Header umfasst nur 16 Bit, mit denen man genau die 65535, also 64 KB, als größte Empfangskapazität angeben kann. Wollte man nicht den TCP-Header modifizieren (und damit sofort eine Änderung aller (!) IP-Stacks notwendig machen, damit diese noch kompatibel bleiben), so musste ein Trick her, der im optionalen Header untergebracht ist. Dieser optionale Header nennt als Parameter „Window scale“ eine Zahl x. Die Window-Angabe in den Folgepaketen dieses IP-Stacks im Rahmen der so begonnenen TCP-Session ist dann stets mit 2x zu multiplizieren, so dass man einen größeren Wert als 65535 signalisieren kann. (siehe Abbildung 3)

Nachteil der bisherigen Lösung unter Windows: die Unterstützung von Window Scaling ist bis Windows XP/ Windows 2003 einschließlich per default deaktiviert, und die Aktivierung erfordert das Setzen von Registry-Variablen (Aktivierung über „TCP1323Opts, Setzen des neuen, größeren maximalen Receive Window-Werts, „TcpWindowSize“ bei Windows XP). (siehe Abbildung 4)

Mit Windows Vista/ dem „Next Generation TCP/IP Stack“ ist dies anders: Window Scaling ist per default aktiviert und erlaubt zunächst eine Window Size von 16 MB. Während der TCP-session wird dann die Receive Window Size an das Produkt aus Bandbreite und Delay sowie die beobachtete Sendeaktivität des Kommunikationspartners angepasst, um eine optimalen Durchsatz zu erreichen (die fest konfigurierte Obergrenze „TCPWindowSize“ von Windows XP/ 2003 fällt weg).

Die Handbremse ist also gelöst, es darf Gas gegeben werden. Wird man einen Unterschied merken? Ein kleiner Test im ComConsult-Labor zeigt: nicht unbedingt!

Probiert wurde mit Hilfe einer ca. 27 MB großen Datei, die per Windows-Explorer zwischen einem Windows XP-Client und einem Vista-Rechner bzw. einem Windows 2003-Server hin- und herkopiert wurde. Das Netzwerk: ein kleines Ethernet-LAN mit 100 MBit/s bis zum Endgerät, der Server mit 1 GBit/s direkt am Core angeschlossen. Die RTT zwischen den Testgeräten spielte sich im kleinen Millisekunden-Bereich ab, war also zu vernachlässigen. Durchgespielt wurden folgende Kopiervorgänge:

- vom Vista-Rechner zum Windows XP-Client (RFC 1323 unter XP aktiviert, mit Maximalwert für TCPWindowSize),
- vom Windows XP-Client zum Vista-Rechner (Receive Window Auto Tuning),

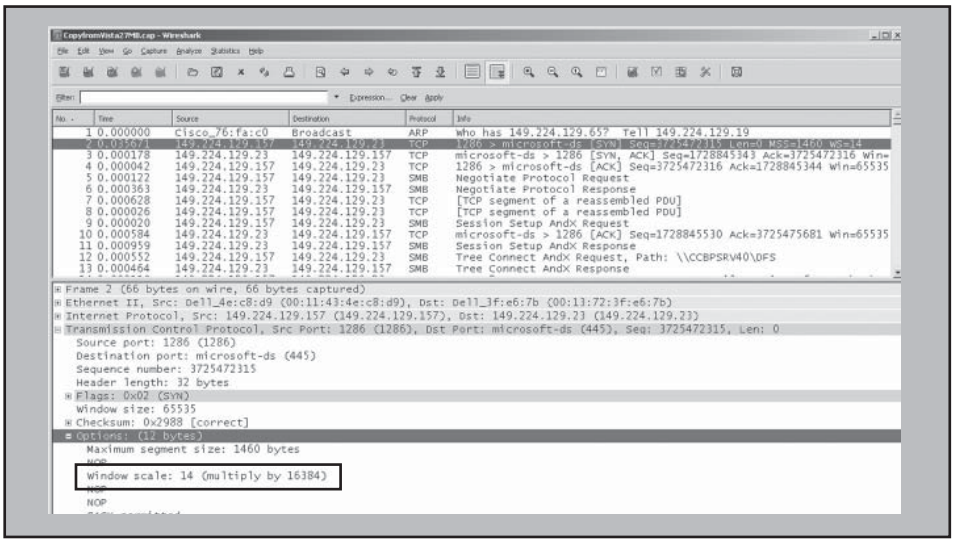


Abbildung 3: Signalisierung von Window Scaling beim Verbindungsaufbau

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

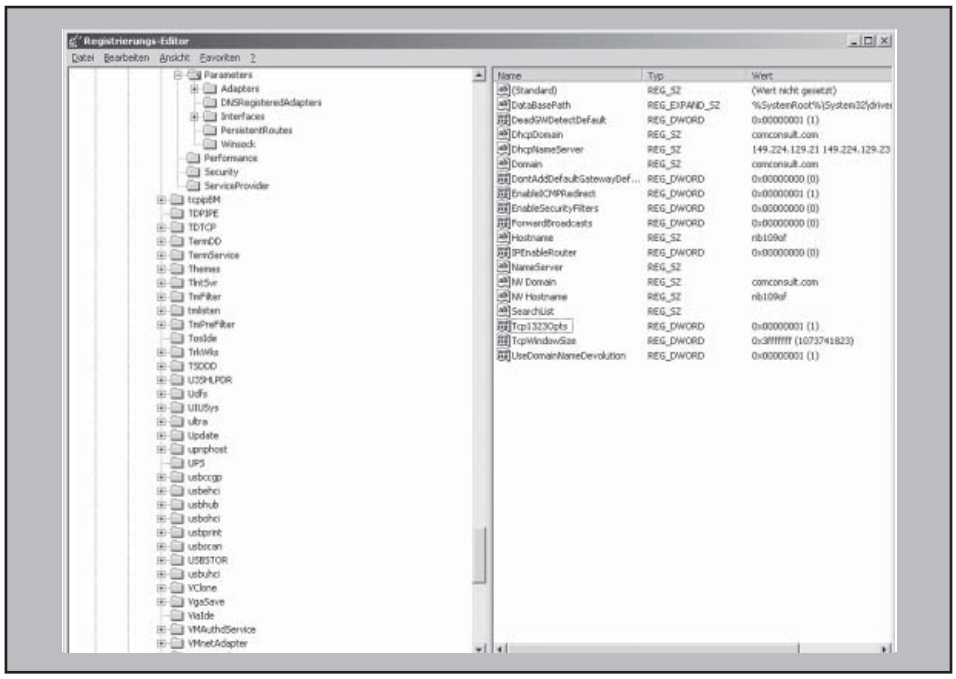


Abbildung 4: Aktivierung von Window Scaling am Beispiel Windows XP

- und zum Vergleich: vom Windows XP-Client zum Windows 2003-Server, auf dem Server die default-Obergrenze von 64 KB Receive Window aktiviert.

Um einigermaßen realistische Rahmenbedingungen zu haben, wurden Server und Vista-Rechner parallel wie im Tagesgeschäft für übliche „Büroarbeiten“ genutzt, der Windows 2003-File-Server dabei gleich durch mehrere Anwender. Auf Vista- und Windows XP-Client waren zudem E-Mail-Client und weitere Programme geöffnet, wie dies im Tagesgeschäft auch der Fall ist, also kein nackter Laborversuch unter Konzentration auf den File-Transfer.

Das Ergebnis der durchgeführten Versuche zeigt Tabelle 1.

So richtig überzeugend ist das nicht, um einen klaren Performance-Vorteil auszumachen. Zwar sind Dauer des Vorgangs und mittlerer Durchsatz vom XP-Rechner zum Vista-Client besser als umgekehrt, allerdings nicht wirklich dramatisch. Sieger ist jedoch die Übertragung vom XP-Client auf den Windows 2003-Server, und bei diesem Fall arbeitet der Empfänger ohne RFC 1323-basierende Optimierung!

Wie kann das denn sein? Taugt der Optimierungsansatz nichts, unter XP gar nicht und die Vista-Verbesserung durch dynamische Anpassung ist nur Schadensbegrenzung? Schaut man sich die mit einem Analysator (Wireshark) begleiteten Vorgänge einmal genauer an, so stellt man etwas anderes fest: es wird offenbar nicht einmal die default-Window-Größe von 64 KB ausgeschöpft. (siehe Tabelle 2)

Das maximale „gesehene Window“ ergab sich dabei durch die Beobachtung, wie viele Pakete jeweils vom Sender aufeinanderfolgend in der Messung enthalten waren, ehe vom Empfänger das nächste ACK-Paket zu sehen war. Na gut, nächster Deutungsversuch: die max. gesehene Fenstergröße gibt zumindest einen Anhaltspunkt darauf, wie gut der Durchsatz im Mittel ausfällt?! Auch nicht: dann hätten alle Kopiervorgänge von Vista zum RFC 1323-aktiven XP einen gleichartigen Durchsatz haben müssen, und dies außerdem im Vergleich zu den anderen Versuchen mit grottenschlechtem Wert. Das stimmt aber auch nicht, trotz des mickrigen gesehenen Window kommen die Kopiervorgänge von Vista zum XP-Rechner noch halbwegs gut davon, jedenfalls nicht viel schlechter als die Gegenrichtung. Wie kann das sein? Die Antwort zeigt eine Betrachtung der Paketabfolgen. (siehe Abbildung 5).

Richtung	Testlauf	Dauer	Mittelwert Durchsatz
XP RFC 1323 ← Vista	1	15,186 s	15,839 MBit/s
	2	18,667 s	11,976 MBit/s
	3	9,358 s	25,078 MBit/s
XP RFC 1323 → Windows 2003	1	6,802 s	35,350 MBit/s
	2	5,375 s	44,731 MBit/s
	3	4,965 s	48,427 MBit/s
XP RFC 1323 → Vista	1	10,645 s	22,363 MBit/s
	2	10,888 s	21,865 MBit/s
	3	13,043 s	18,251 MBit/s
	4	14,327 s	16,616 MBit/s

Tabelle 1: File-Transfer

Richtung	Testlauf	Mittelwert Durchsatz	max. gesehenes Window
XP RFC 1323 ← Vista	1	15,839 MBit/s	2,851563 KB
	2	11,976 MBit/s	2,851563 KB
	3	25,078 MBit/s	2,851563 KB
XP RFC 1323 → Windows 2003	1	35,350 MBit/s	25,515625 KB
	2	44,731 MBit/s	39,921875 KB
	3	48,427 MBit/s	38,496094 KB
XP RFC 1323 → Vista	1	22,363 MBit/s	58,457031 KB
	2	21,865 MBit/s	61,308594 KB
	3	18,251 MBit/s	59,882813 KB
	4	16,616 MBit/s	58,457031 KB

Tabelle 2: Beobachtete Senderaktivität – Eckwerte

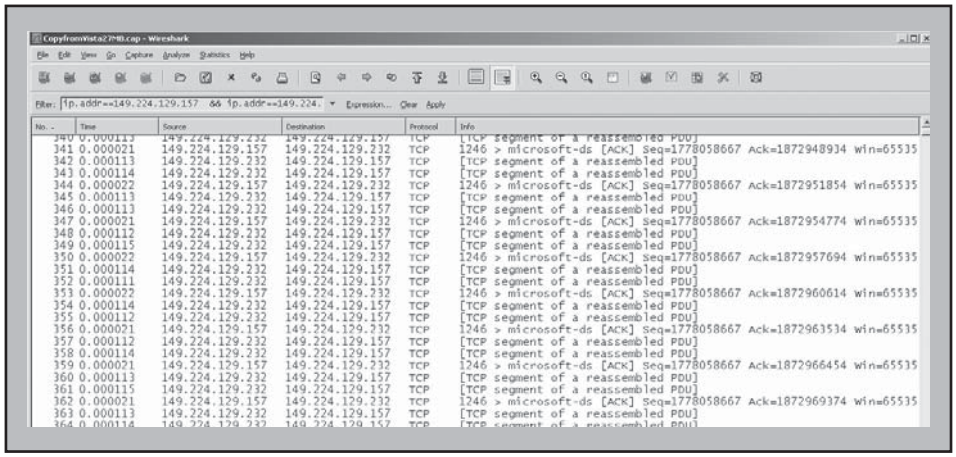


Abbildung 5: Messung Kopiervorgang Vista-Rechner → XP-Test-Rechner (Ausschnitt)

Der XP-Rechner

- trägt konstant 65535 als Window ein, zu multiplizieren mit zu Beginn vereinbarten 214 , also ein Receive Window von 65535*16384 Byte, d.h. ca. 1 GB. Dies ist das voreingestellte Maximum; ein Empfängerengpass als Grund für die nicht berauschende Sitzungsperformance kann wohl ausgeschlossen werden.

- quittiert offenbar schon nach zwei Paketen, und dies innerhalb weniger Millisekunden; der Sender kann also gar nicht durch den Empfänger ausgebremst sein, es liegen längst Quittungen vor, ehe auch nur annähernd die Window-Grenze in Sicht ist.

Wer ist aber dann „schuld“ daran, dass die Empfängerkapazität und die Netzwerk-Bandbreite von 100 MBit/s für den Sender nicht besser genutzt werden? Des Rätsels Lösung liegt beim Sender, genauer der Applikation auf Senderseite und in welcher Menge / welchen Portionen diese Daten zum Transport an den IP-Stack abliefert. Auch ohne detaillierte SMB-Kenntnisse erkennt man am folgenden, auf die Schreibkommandos gefilterten Ausschnitte einer Messung (hier: hin zum als Empfänger optimierten Vista-Client), dass offenbar die Datei vom File-Service-Client „Explorer“ in zu kleine Häppchen zerlegt wird, um die TCP-Window-Erlaubnis auch nur ansatzweise auszunutzen. (siehe Abbildung 6)

Dieser kleine Test zeigt gleich mehrere, für Flusskontroll-Betrachtungen typische Aspekte:

- ein Optimierungsansatz kann nur dann zu besserer Performance führen, wenn er „ungünstige Rahmenbedingungen“ korrigiert, für die er konzipiert ist

  Diese waren hier für den Window Scaling-Ansatz nicht gegeben: eifrig quittierender, engpassfreier Empfänger, und die Quittungen wurden auch nicht durch hohen Delay im Netzwerk „gepuffert“ – der Sender konnte jederzeit auf die Leitung setzen, was immer er zu senden hatte. Also kein Anlass für diese Medizin! Wirksamkeit wäre etwa gegeben bei Verbindungen mit hohem Delay / hoher RTT, so dass die ACKs vom Empfänger nicht so schön frühzeitig eintreffen.

- Wenn nichts zu senden da ist, nützen auch mehr Bandbreite und geringer Delay nichts; oder anders gesagt:

  Netzwerk-Optimierungen und Tuning an Sender/ Empfänger nützen wenig, wenn die Anwendung bremst.

Hier liegt in der Praxis derzeit vielleicht der größte Knackpunkt für die Wirksamkeit höherer Netzbandbreiten und Tuning-Versuche am Kommunikationsverhalten der IP-Software. Spielt die Anwendungsebene den Bremser, d.h. werden Optimierungen im Bereich der TCP-Flusskontrolle nicht zügig genug mit zu versendendem Material beliefert, so wird das Verhältnis aus Netzwerk-Bandbreite und erzieltem Nutzen genauso traurig aussehen wie eingangs für klassisches TCP ohne Optimierungen prognostiziert. Die Performance-Bremse kann dabei in der einzelnen Anwendung enthalten sein, oder aber auch im Betriebssystem: verwaltet dieses die parallelen Prozesse schlecht oder die Daten-Übergabe von Anwendung zu IP-Software schlecht, so entsteht hier der Engpass, der alle Tuning-Bemühungen und alle Investitionen in Netzwerk-Kapazitäten verpuffen lässt. Mit Blick auf Vista/ Longhorn: es kann interessant sein, hier aufmerksam auf Verbesserungen und neuen Konfigurationsoptionen gegenüber XP/ Windows 2003 zu achten; womöglich greifen die TCP/IP-Optionen erst im Paket mit solchen Verbesserungen so richtig spürbar.

3. Vista / Longhorn und weitere TCP-Tuning-Optionen

Apropos Paket: die dynamische Receive Window-Anpassung ist nicht der einzige Pfeil im Köcher des neuen TCP/IP-Stack von Microsoft. Flusskontrolle unter TCP und (das Wegbügeln von) Schwächen des klassischen Vorsichtsprinzips sind komplexer. Ein weiterer unter ungünstigen Umständen empfindlich und unnötig (!) die Performance verschlechternder Aspekt ist das Verhalten in Situationen, in denen der Datenfluss nicht so schön gleichmäßig ist wie im gezeigten Testbeispiel und damit timeouts drohen oder gar gehäuft eintreten. Viele Ansätze zur Optimierung an dieser Achillesferse basieren auf einem Prinzip des vorauseilenden Gehorsams: auf entsprechende Signale des Empfängers erfolgen vorzeitige Retransmissions durch den Sender, um den Timeout und

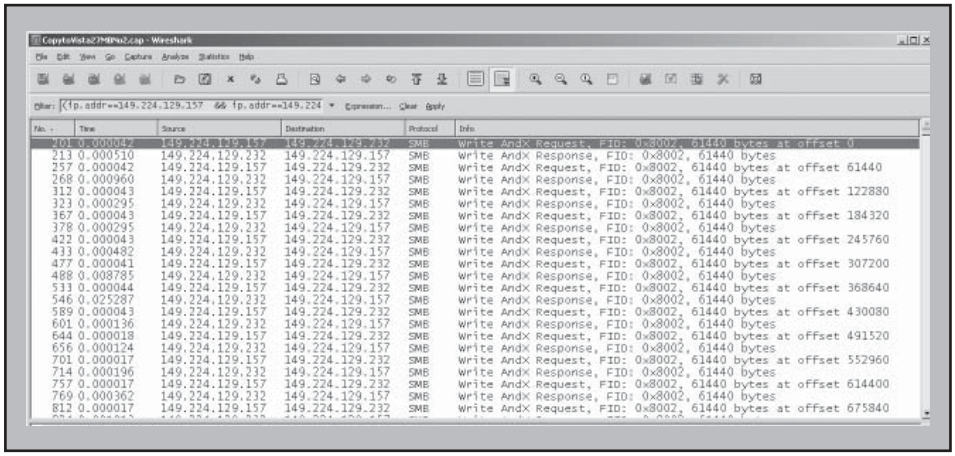


Abbildung 6: „Beispielmessung XP an Vista“ – Verhalten der Anwendung

den damit verbundenen Rückfall in Slowstart / das ab jetzt frühere Einsetzen von „Congestion Avoidance“ zu vermeiden.

Im Zusammenhang mit dieser Thematik gibt es dabei verschiedene Möglichkeiten für Feinschliff: Wie schnell und wie heftig setzt man mit den vorgezogenen Retransmissions ein, wie schickt man möglichst nur die Daten, die wirklich beim Empfänger noch fehlen, damit er nicht durch zu viele Doppler sinnlos belastet wird, …

An dieser Stelle mal ein Sonderlob für Microsoft und seine IP-Stack-Implementierungen: Schon mit dem in Windows 2000 gelieferten und in Windows XP/ 2003 übernommenen Umfang von Features im Bereich TCP-Optimierungen war Microsoft hier durchaus weit vorn, etwa mit der per default gebotenen Unterstützung einer Selective Acknowledgement (SACK) genannten, RFC-spezifizierten Option, die auf „Lücken“ im Datenempfang auf Empfängerende gezielt schlauer reagiert, als einfach ein komplettes Window erneut zu senden. Mit den für Vista / Longhorn erfolgten Ergänzungen wird diese Tradition fortgesetzt: Neben dynamischem Window Scaling werden Ergänzungen im Bereich des durch die SACK-Option behandelten Themenkomplexes integriert, etwa mit Blick auf Umgebungen mit erhöhter Wahrscheinlichkeit auf gelegentliche Paketverluste:

- Unterstützung des New Reno-Ansatzes gemäß RFC 2582 (behutsamere Gestaltung der vorzeitigen Retransmissions zur Vermeidung einer unnötigen und ungünstigen Paketflut)
- Unterstützung eines Fine-Tuning zu SACK, gemäß RFC 2883, zur Rückmeldung von Paketdopplern durch den Empfänger (optimiert nochmals die vorzeitigen Retransmissions); Aufnahme einer weiteren SACK-Optimierung gemäß RFC 3517
- Unterstützung von RFC 4138: Versuch zur Vermeidung unnötiger Retransmissions in Sondersituationen mit sporadischer RTT-Schwankung (kann sonst zur Retransmission eines ganzen, evtl. großen Window führen, obwohl wenige Pakete genügt hätten).

Also schon eine ganze Menge Möglichkeiten, eine Treffer zu landen in dem Sinne, dass eine Sondersituation eintritt, für die eine entschärfende Option gezielt greift.

4. Tipps für die (Vista/ Longhorn-) Praxis

Vielleicht stellen sich aber die eingangs aufgeworfenen Fragen in besonderem Maße: kann so viel geballtes Tuning gefährlich werden, muss man etwa reflexartig zu QoS greifen, gar zu aufwändigeren Formen davon, um Netzwerk und Teilnehmer durch diese geballte Offensive zur Optimierung der Sendereffizienz vor Problemen zu schützen?

Pauschal ist das sicherlich Unsinn. Bei Veröffentlichungen, die scheinbar diese Aussage treffen, kann man nur hoffen, dass diese missverständlich formuliert sind und sich eigentlich auf bestimmte Konstellationen beziehen, dies aber leider nicht deutlich genug zum Ausdruck bringen.

Gerade im LAN wird man etwa viele der Tuning-Optionen lange Zeit gar nicht in Aktion erleben, solange die Datenflüsse gleichmäßig beim Empfänger ankommen und LAN-typisch geringe RTT-Werte die Regel darstellen. Der bei aus Empfängersicht gleichmäßigem Datenstrom am ehesten interessante Parameter „Window Scaling“ bleibt wegen der RTT-Situation mit hoher Wahrscheinlichkeit zunächst auch wirkungslos.

Anders herum betrachtet: wo kann es denn spannend werden? Eine gute Faustregel ist hier: je näher man an einen Zustand kommt, für den der klassische TCP-Ansatz mit all seinen Vorsichtselementen gezielt gedacht war – wenn Ressourcen-Knappheit und resultierende hohe Engpasswahrscheinlichkeit gegeben sind. Kandidaten sind z.B.

- Drahtlosverbindungen mit ungünstigen Rahmenbedingungen
- WAN-Verbindungen, bei denen sich signifikanter Delay / resultierende längere RTT mit im Mittel knapper Bandbreite kombinieren (also nicht unbedingt Hochgeschwindigkeits-WAN-Lösungen)
- Konstellationen mit hohem Bandbreitengefälle an einzelnen Übergangspunkten, die zum Bottleneck wegen Ausschöpfung der Pufferkapazitäten werden können.

Hier hilft natürlich das Prinzip des sich vorsichtig Herantastens an eine „erträgliche“ Sendeaktivität und – im Zweifel lieber auf jeden Fehlschlag (Timeout) noch vorsichtigeren Weitermachens.

Solche Situationen benötigen allerdings keinen besonders intensives TCP-Tuning a la Vista, um problemschwanger zu sein. Hier reichen bereits die heute noch vorherrschenden Versionen von IP-Stacks aus – sofern sie in Verbindung mit entsprechend kräftigen Datenströmen von der Anwendungsschicht beliefert werden.

Also: Vista / Longhorn sind nicht per se gefährlich für das Netzwerk, eventuell können sie zukünftig sogar helfen, lange Gesichter bei der Einführung höherer Bandbreiten zu vermeiden.

Es lohnt sich aber, sich mit den Neuerungen genauer zu beschäftigen: nämlich dann, wenn man Engpass-Konstellationen vorhersieht bzw. in solchen konkret Pro-

bleme beobachtet. Hier wird Detailwissen nützlich:

- Wo setzt welche Tuning-Option an, kann diese in meiner speziellen Situation zum Bumerang werden?

  (Es wäre schade, auf Verdacht Optionen auszuschalten, die an anderer Stelle für die gleichen Clients echte Vorteile bringen können.)

- Was kann man überhaupt ein- bzw. ausschalten bzw. hinsichtlich wichtiger Werte verändern, d.h. feiner einstellen?

  Hier wäre eine Verbesserung wünschenswert, die der Autor mit Sonderapplaus quittieren würde: wenn für solche Themen durchgängig etwas Handlicheres und Selbsterklärenderes angeboten würde, als das Ändern an Registry-Variablen, die im Default noch nicht einmal angezeigt werden.

Eine für Tuning-Aufgaben praxisbewährte Strategie ist in jedem Fall:

- Defaults lassen, wie sie sind, solange keine spürbaren Probleme auftreten
- erst wenn in bestimmten Konstellationen Probleme auftreten, gezielt nach möglichen Zusammenhängen zu abschaltbaren / konfigurierbaren Aspekten suchen, hier im Bereich TCP-Tuning
- wenn der eingangs beschriebene Effekt „schnelleres Netz – keine Verbesserungen“ eintritt: zunächst mal nach Hinweisen auf Bremseffekte auf Anwendungsseite suchen – hier hilft kein mühsames Tuning an Netz oder IP-Stack, und beim Ändern an Defaults drohen immer unerwünschte Seiteneffekte!

Und zuletzt: QoS als präventive Wunderwaffe? Bitte nicht! QoS, insbesondere in mit erträglichem Aufwand verwaltbarer Form, ist gut, um ausgewählte besonders wichtige bzw. „empfindliche“ Datenströme oder solche mit besonderen Anforderungen vor sporadischen Engpass-Situationen zu schützen. QoS benötigen, um überhaupt arbeitsfähig zu sein: das erinnert an „elektronische Hilfen benötigen, damit das Auto grundsätzlich stabil auf der Straße bleiben kann“ – wer will so etwas? Das wäre ein Design-Fehler der Gesamt-Lösung, also ein Planungsfehler – aber kein Vista-, Longhorn-, Linux-, UNIX-, …- Problem.

Fazit

Der neue TCP-Protokollstack in Vista ist ein großer Schritt vorwärts. Microsoft zeigt damit dem Markt, wie eine aktuelle TCP-Implementierung aussehen sollte. Zur Zeit wird das damit geschaffene Potenzial aber nicht genutzt, da die auf TCP aufsetzenden Applikationen (SMB) nach wie vor in der alten Welt leben (andere Abteilung bei Microsoft?).

Trotzdem ist Vorsicht geboten. Mit Longhorn und dem bereits sich abzeichnenden ersten Service Pack kann sich das auch schnell ändern. Auch besteht die Welt nicht nur aus Microsoft. Die Tatsache, dass auch Apple mit der nächsten Version von OS X (Leopard) in die gleiche Richtung geht, zeigt, dass wir hier einen Trend haben. Im Prinzip wurde das auch langsam Zeit, werden doch mit den neuen Protokoll-Stacks Funktionen in die Fläche gebracht, die z.T. bereits seit 15 Jahren genormt sind. Auch ist zu beachten, dass zur Übertragung von Dateien nicht nur SMB zum Einsatz kommt. Spezialisierte Backup-Pakete könnten durchaus die neuen Möglichkeiten ausnutzen und somit zu einer deutlich verbesserten Backup-/Restore-Leistung kommen.

Daraus ist abzuleiten, dass diese Entwicklung weiter beobachtet werden muss. Auf jeden Fall sollten Buchungsfaktoren in der Netzwerk-Planung angepasst werden. Im Klartext heißt das, dass die Kapazität der Uplinks zwischen Hauptverteiler und Etage ggf. ausgeweitet werden muss. Auch könnten einzelne Gigabit-Strecken im Backbone zum Engpass werden. Besonders die Anbindungen im Bereich von RZs und Server-Farmen sind mit Aufmerksamkeit zu beobachten: Hier kommen die Datenströme zusammen, hier können neue Netzbandbreiten gezielter ausgereizt werden, wenn TCP/IP mitspielt.Da dies aber in einem gut aufgebauten Netzwerk-Betrieb sowieso Gegenstand des Monitoring und Reportings ist, sollten die Betreiber entsprechende Entwicklungen in diese Richtung frühzeitig erkennen können.

Seminar des Monats

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie

Die ComConsult Akademie veranstaltet vom 10.09. - 12.09.07 ihr Seminar „SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie “ 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.

Der größte Nachteil der bisher überwiegend verkauften Produkte für IP-Telefonie ist, dass sie mit Hersteller-spezifischen Protokollen arbeiten. Doch dies ist ein reiner Übergangs-Zustand. Mit dem Session Initiation Protocol hat sich ein Standard etabliert, der die Zukunft der IP-Telefonie ausmachen wird. Schon jetzt sind signifikante Anbieter auf diesen Standard umgeschwenkt, die verbleibenden Anbieter werden das kurz- bis mittelfristig nachholen.

Für Jeden, der sich mit IP-Telefonie auseinander setzt, sind elementare Kenntnisse von SIP unverzichtbar. Dies liegt auch darin begründet, dass der Standard in ständiger Weiterentwicklung ist und zurzeit nicht alle Funktionsbereiche abdeckt, so dass die Hersteller fehlende Funktionen basierend auf SIP ergänzen (was der Standard gestattet).

In diesem Seminar lernen Sie:

- was SIP leistet
- was SIP nicht leistet
- was SIP wann leisten wird
- wo die Vor- und Nachteile gegenüber den bisherigen Lösungen liegen
- wie wichtige Hersteller zu SIP stehen
- wie Sie eine SIP-Lösung aufbauen und erfolgreich zum Laufen bringen
- wie Sie mit NAT-Firewalls umgehen

Dieses Seminar bietet Ihnen genau die Information, die Sie zur Umsetzung von SIP-Lösungen benötigen.

Durch das Seminar führen Sie die Referenten Dipl.-Inform. Petra Borowka und Dipl.-Ing. Ralf Glörfeld.

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Ralf Glörfeld ist Diplom Ingenieur Nachrichtentechnik und seit 14 Jahren bei den Stadtwerken Düsseldorf AG im Bereich IS/Kommunikationstechnik tätig. Seit 2005 beschäftigt er sich mit der Konzeption und Implementierung Multimediaapplikationen in die Netzwerkinfrastruktur. Ein Schwerpunkt liegt in der Implementierung von SIP als Kommunikationsplattform. Nebenberuflich ist er seit 2007 als Dozent und Berater tätig.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie

☐ Ich buche das Seminar
SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie
10.09. - 12.09.07 in Berlin
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____07

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

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Report des Monats

Session Initiation Protocol:
Funktionsweise, Einsatzszenarien, Vorteile und Defizite

Ihr Unternehmen wird seine TK-Lösungen in Zukunft auf SIP basieren lassen. Dies ist keine Frage des „Ob“ sondern des „Wann“ und „Wie“. SIP ist der offene, internationale Standard für Sprach- und Multimedia-Kommunikation. SIP wird die bisher noch dominierenden Hersteller-Spezifischen Signalisierungen und Telefon-Lösungen in sehr kurzer Zeit ablösen.

Soeben ist die brandaktuelle SIP-Studie von ComConsult Research erschienen.

Der Report analysiert für Sie:
- Was leisten SIP-Basisdienste
- Was leisten SIP-Mehrwertdienste
- Wie sehen Architekturen aus
- Wie sind Skalierbarkeit und Ausfallsicherheit zu bewerten
- Was bedeutet Offenheit und Interoperabilität
- Welchen Gestaltungsspielraum haben sie
- Im Vergleich zu typischen traditionellen TK-Lösungen: was kann SIP auch, was besser, was nicht
- Wann ist eine Lösung wirklich „SIP-Compliant“, welche nachprüfbaren Kriterien müssen dafür erfüllt sein

Im Anschluss haben wir für Sie eine kurze Leseprobe zusammengestellt:

5 SIP: Erweiterungen und Mehrwertdienste

In den vorhergehenden Kapiteln wurden die Basisfunktionen von SIP dargestellt und Designmöglichkeiten für hochverfügbare Lösungen diskutiert. Damit allein wäre es kaum möglich klassische Telefonanlagen abzulösen.

Gegner führen gerne an, dass mit VoIP im Allgemeinen und SIP im Speziellen nicht alle Leistungsmerkmale abgedeckt werden könnten, die es bisher gab. Befürworter bestreiten das. Umgekehrt führen die Verfechter von VoIP an, dass durch die Verschmelzung der IT- und der TK-Welten ein erhebliches Potential zur Schaffung von Mehrwertapplikationen entstehen. Die Kritiker halten dage-gen, dass das mit CTI schon lange möglich war.

Sicher ist, eine VoIP-TK-Lösung muss mindestens die Anforderungen erfüllen, die die bisherige PBX erbracht hat. Im Folgenden wird darum zunächst gezeigt, wie sich mit SIP klassische Leistungsmerkmale umsetzen lassen. In den weiteren Unterkapiteln werden die Standarderweiterungen, existierende Mehrwertdienste und typische TK-Anwendungen vorgestellt und wie sie sich mit SIP realisieren lassen. Dabei wird darauf verzichtet, die mittlerweile über 100 Standards rund um SIP detailliert vorzustellen. Auch wird nicht auf jede Erweiterung und Anwendung eingegangen, die es mittlerweile gibt. Stattdessen haben die Autoren eine Auswahl getroffen, von der sie meinen, dass sie für die Praxis besonders relevant sind. Das Augenmerk liegt dabei auf der grundsätzlichen Funktionsbeschreibung, der Anwendbarkeit und der Umsetzung in der Praxis. Zusätzlich werden die vorgestellten Funktionen und Mehrwertdienste wenn nötig bewertet und auf Stolpersteine im Praxiseinsatz wird hingewiesen.

Ein separates Unterkapitel ist den Schnittstellen gewidmet, da diese der Dreh- und Angelpunkt für das Zusammenwachsen von IT- und TK-Anwendungen ist.

5.1 Weiterführende Standards

Die Basis-Standards von SIP spezifizieren eine Reihe von Meldungen und Verfahren, die notwendig sind um eine Verbindung aufzubauen, zu beenden und ggf. die Parameter zu ändern. Sie definieren also, wie eine Verbindung gema-ged werden kann (Verfahren) und was dafür notwendig ist (Protokoll). Was sie jedoch nur in wenigen Ausnahmen abdecken ist das, was in der TK-Welt als Leistungsmerkmale bezeichnet wird.

Das heißt aber umgekehrt nicht, dass die klassischen Leistungsmerkmale mit den Mitteln von SIP nicht abgedeckt werden könnten. Zum Teil muss das SIP- oder das SDP-Protokoll dazu ergänzt werden. Jedoch ist es nicht notwendig, für jedes Leistungsmerkmal eigene Protokollparameter einzuführen.

Es ist gute Tradition bei der IETF Protokolle so generisch anzulegen, dass sie unterschiedlichste Aufgaben erfüllen können, ohne dafür modifiziert werden zu müssen. Es liegt dann an der Implementierung, was für Leistungsmerkmale möglich sind. Wie mit Standardbordmitteln von SIP Leistungsmerkmale realisiert werden können, wird später detailliert am Beispiel der „Umleitung bei Besetzt“ vorgestellt.

Der Vorteil dieses Vorgehens ist es, dass Anwendungen sehr modular programmiert werden können: bereits geschriebene Subroutinen können immer wieder verwandt werden, so reicht es beispielsweise eine Routine für das SIP INVITE nur einmal zu programmieren. Diese kann dann sowohl für einen Gesprächsaufbau wie auch für eine Konferenzschaltung genutzt werden. Ein weiterer Vorteil ist, dass den Herstellern so viele Freiheiten gelassen werden, standardkonforme Leistungsmerkmale zu entwickeln, ohne dass dafür der oft langwierige Prozess der Standardisierung abgewartet werden muss.

Der Nachteil ist jedoch, dass viele Leistungsmerkmale zwar keine neuen SIP-Parameter oder -Pakete benötigen jedoch ein gemeinsames Vorgehen der Kommunikationspartner. Insbesondere bei Produkten unterschiedlicher Hersteller können sich sonst schnell Inkompatibilitäten ergeben. Ein Beispiel dafür wäre das Weiterleiten eines Telefonates: alle drei Clients müssen in der Abfolge und im Inhalt der SIP-Pakete übereinstimmen, wenn die Weiterleitung funktionieren soll.

Das Dilemma zwischen möglichst vielen Freiheiten bei der Implementierung und der Interoperabilität wird bei der IETF durch die BCPs gelöst. In ihnen werden erprobte Verfahren vorgestellt, ein Problem mittels bestehender Standards zu lösen.

Die Aufteilung zwischen Vorgehensweisen und Protokoll schlägt sich auch in der Teilung der Arbeiten in verschiedene SIP-Arbeitsgruppen nieder.

Im folgenden werden die relevanten Arbeitsgruppen kurz beschrieben und anschließend praxisrelevante Standarderweiterungen vorgestellt.

5.1.1 Arbeitsgruppen

5.1.1.1 SIP-Arbeitsgruppe

Die SIP-Arbeitsgruppe ist für die Entwicklung der Kernelemente von SIP zuständig. D.h. sie standardisiert alle Dienste, Protokolle, Erweiterungen und Vorgehensweisen, die zwingend vorgeschrieben sein müssen, damit ein Signalisierungsprotokoll interoperabel funktionieren kann.

Sie ist erklärter Weise nicht für die Entwicklung von Anwendungen auf der Basis dieser Signalisierungen zuständig. Tauchen jedoch in anderen Arbeitsgruppen Anforderungen an das SIP-Protokoll auf, so werden diese umgesetzt. Primär kommen diese Anforderungen von den Arbeitsgruppen SIPPING, SIMPLE und XCON.

Die vier Dogmen der Arbeitsgruppe lauten:

1. Dienste und Features werden wenn immer möglich Ende-zu-Ende realisiert.
2. Lösungen müssen generisch angelegt sein und dürfen sich nicht an speziellen Anwendungen ausrichten.
3. Jede Lösung muss so einfach wie möglich sein.
4. Nutzung von und Interoperabilität mit bestehenden Internetprotokollen hat oberste Priorität.

5.1.1.2 SIPPING-Arbeitsgruppe

Die SIPPING-Gruppe beschäftigt sich mit der praktischen Umsetzung des SIP-Standards, dazu hat sie sich fünf Ziele auf die Fahne geschrieben:

5. Evaluierung und Dokumentation von Anforderungen des Marktes
6. Dokumentation der SIP-Nutzung, um Anforderungen (Leistungsmerkmale) standardisiert zu implementieren
7. Beschreibung von Anforderungen notwendiger SIP-Erweiterungen
8. Zusammenführung der Gemeinsamkeiten verschiedener Task Groups
9. Beschreibung der Anforderungen und notwendigen Prozeduren für Entwicklung von Benutzerprofile

5.1.1.3 SIMPLE-Arbeitsgruppe

Die beiden Themen der dritten SIP-Arbeitsgruppe sind Instant Messaging und Präsenz. Wie die SIPPING-Gruppe spezifiziert sie selbst keine neuen Protokolle oder Protokollerweiterungen, bereitet sie im Bedarfsfall jedoch vor und übergibt sie an die SIP-WG. Die drei primären Ziele der Arbeitsgruppe sind:

10. Entwicklung eines Verfahrens, das SIP als Transportprotokoll für IM nutzt.
11. Weiterentwicklung von SIP, um Präsenz-Informationen auszutauschen.
12. Beschreibung einer Architektur, die es erlaubt, IM und Präsenz mittels Buddy-Listen zu implementieren.

5.1.1.4 P2PSIP-Arbeitsgruppe

Die jüngste Arbeitsgruppe zum Thema SIP hat sich im Februar 2007 konstituiert und beschäftigt sich mit SIP als Peer-to-Peer-Anwendung. Da es in einem P2P-Netzwerk keine „ausgezeichneten“ Geräte gibt, die a priori eine besondere Bedeutung besitzen, wie SIP-Server, muss jedes teilnehmende Gerät Dienste und Ressourcen zur Verfügung stellen, die für gewöhnlich von Servern erfüllt werden.

Erklärtes Ziel der Arbeitsgruppe ist es, eine möglichst einfache Technik für solche P2P Netze auf der Basis von SIP zu entwickeln, die zudem mit minimalen Konfigurationseinstellungen an den Clients auskommt.

Nähere Informationen zum Thema P2PSIP gibt es im Insider Artikel „P2P SIP – Das Ende von Skype?“ von Markus Schaub im Netzwerk Insider vom Mai 2006.

5.1.1.5 Nicht-SIP-spezifische VoIP-Arbeitsgruppen

Insgesamt beschäftigen sich aktuell 15 Arbeitsgruppen bei der IETF mit Themen Echtzeit-Anwendungen. Davon haben nur die vier bisher vorgestellten SIP als Schwerpunkt. Allerdings sind auch andere Gruppen für die SIP-Implementierung relevant. Die drei wichtigsten Gruppen sind:

13. XCON-Arbeitsgruppe
    XCON steht für Centralized Conferencing. Konferenzen stellen zwar auch Anforderungen an die Signalisierung, jedoch liegen die besonderen Schwierigkeiten in anderen Bereichen, wie Rollendefinitionen (Besitzer, Moderator, Sprecher, etc.), Authentifizierung und Verschlüsselung. Die Umsetzung dieser Anforderungen ist nur zum Teil Aufgabe des Signalisie-rungsprotokolls.

    Die XCON-Arbeitsgruppe beschäftigt sich ausschließlich mit einem zentralistischen Konferenzmodel, bei dem alle Teilnehmer mit einem Fokus und einem Mixer verbunden sind, die die Konferenz steuern (Fokus) und die Datenströme mixen und verteilen (Mixer).

14. MMUSIC-Arbeitsgruppe
    Schwerpunkt der Multiparty Multimedia Session Control (MMUSIC) Gruppe ist heute die Weiterentwicklung von SDP.

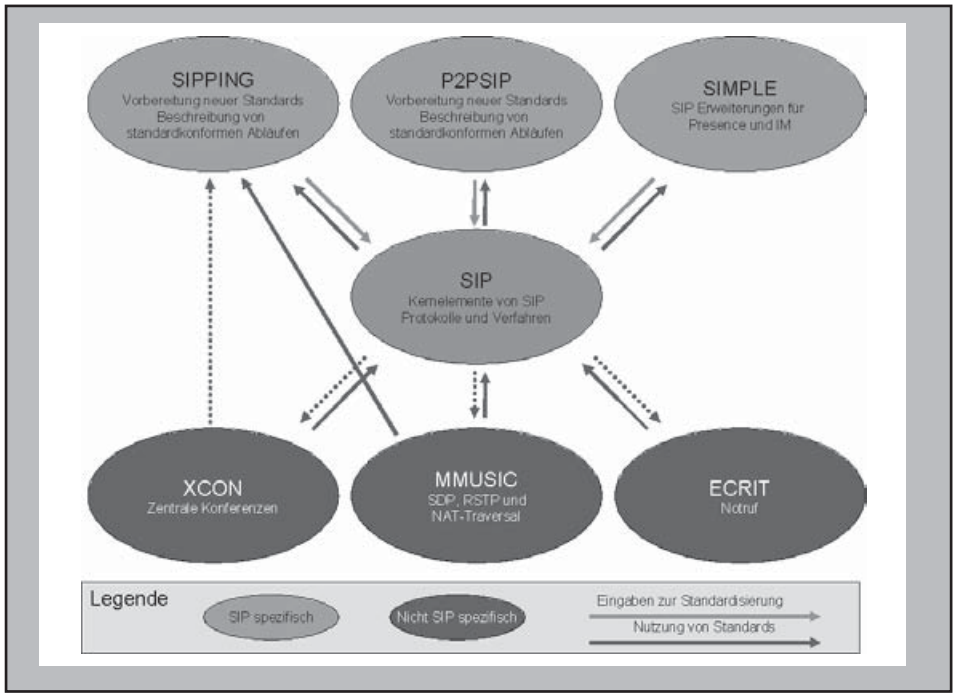


Abbildung 5.1: Verflechtung der Arbeitsgruppen

Neben SDP werden von der Gruppe aktuell nur zwei weitere Themen vorangetrieben: RSTPv2 und NAT-Traversal.

15. ECRIT-Arbeitsgruppe
    Die ECRIT-Gruppe beschäftigt sich mit dem Thema Notruf. Die Schwierigkeit von VoIP bzgl. Notrufen liegt darin, dass im Unterschied zur klassischen, kabelgebundenen Telefonie IP-Geräte nicht ohne weiteres lokalisiert werden können.

    Ziel der Arbeitsgruppe ist es, so weit als möglich bestehende Techniken zu nutzen, um den Aufenthaltsort eines Anrufers bei einem Notfallanruf bestimmen zu können.

5.1.2 DTMF-Töne

DTMF steht für Dual Tone Multiple Frequency, im Deutschen auch MFV, Mehrfrequenzwahlverfahren, genannt. MFV löste mit dem Einzug digitaler Vermittlungsstellen das ältere Impulswahlverfahren, IWV, ab. Beim IWV wurden Nummern durch elektrische Impulse übertragen, die durch die Wählscheibe erzeugt werden konnten.

Für DTMF hingegen ist ein Nummernblock notwendig. Den Zeilen und Spalten werden feste Frequenzen zugeordnet

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Tabelle 5.1 DTMF: Zusammenhang Tastenbelegung und Frequenzen

und eine Ziffer wird durch die Überlagerung der Zeilen- und Spaltenfrequenz bei der Übertragung repräsentiert. Bei der Festlegung der Frequenzen hat man für die Zeilen niedrigere und für die Spalten höhere Frequenzen gewählt. Ferner hat man versucht, die Frequenzen so festzulegen, dass sie bei der Überlagerung eine Disharmonie erzeugen, um zu verhindern, dass zufällige Hintergrundgeräusche mit denselben Harmonien zu unvorhergesehenen Störungen führen.

Neben der Anwahl werden DTMF-Töne heute auch zur interaktiven Steuerung und Eingabe während eines Gespräches genutzt, um beispielsweise Anrufbeantworter abzufragen, Passwörter, Konto- oder Kundennummern einzugeben.

Für die Signalisierung von Telefonnummern und die Steuerung/Konfiguration von Telefonanlagen, wofür DTMF ursprünglich entwickelt wurde, gibt es bei SIP keine Anwendung mehr. Anders verhält es sich jedoch für die Eingabe von Nummern nach dem Verbindungsaufbau. In einer reinen SIP-Welt könnte grundsätzlich auf DTMF verzichtet werden und alle Befehle und Eingaben über entsprechende SIP-Nachrichten übertragen. Liegt zwischen Sender und Empfänger jedoch ein PSTN-Netz, so kann Stand heute nicht auf die Funktion verzichtet werden.

Für die Übertragung bieten sich zwei Varianten an:

16. DTMF wird als Ton kodiert und über RTP übertragen.
17. Die Information, dass und welche Taste gedrückt wurde, wird vom SIP-Client als SIP- oder RTP-Nachricht gesendet.

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. Dies 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), dass 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-

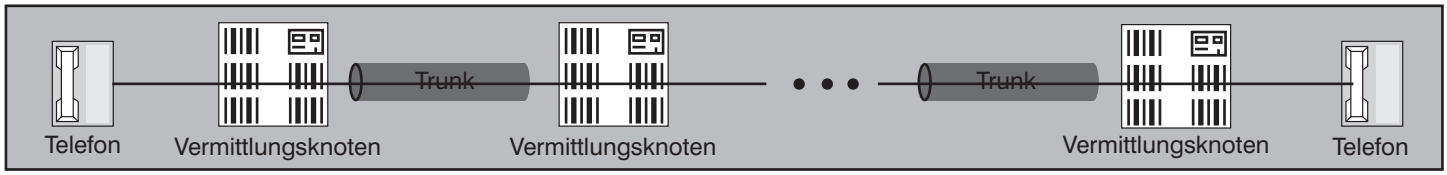


Abbildung 1: Prinzip der Leitungsvermittlung

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 verbreitetet 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 erwartet. 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

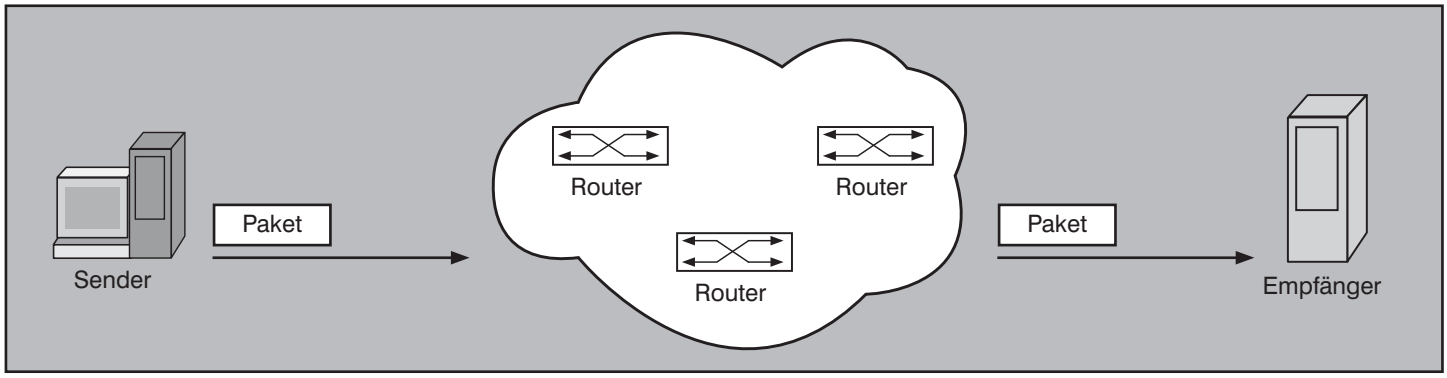


Abbildung 2: Prinzip der Paketvermittlung in IP-Netzen

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 gewesenen 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 Zuordnungen 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.

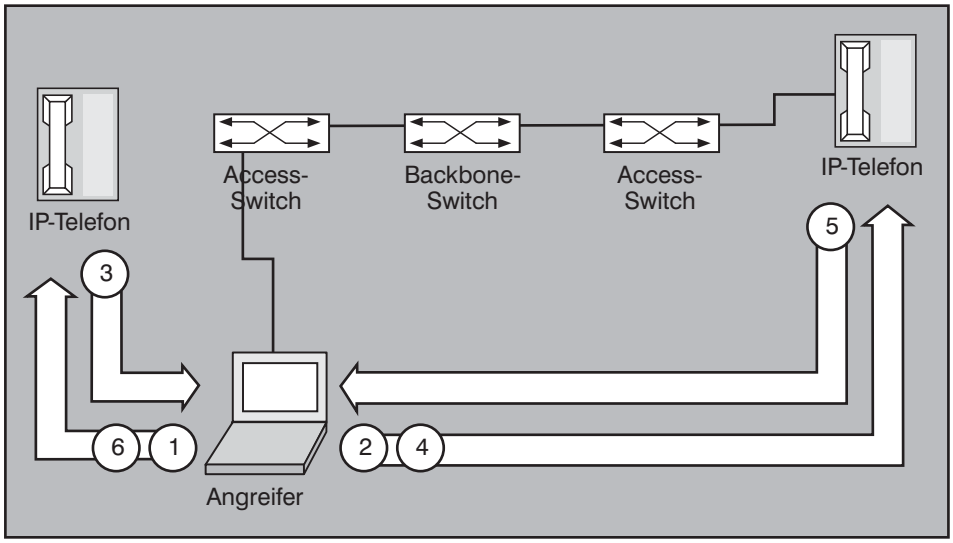


Abbildung 3: Manipulation mittels Gratuitous ARP

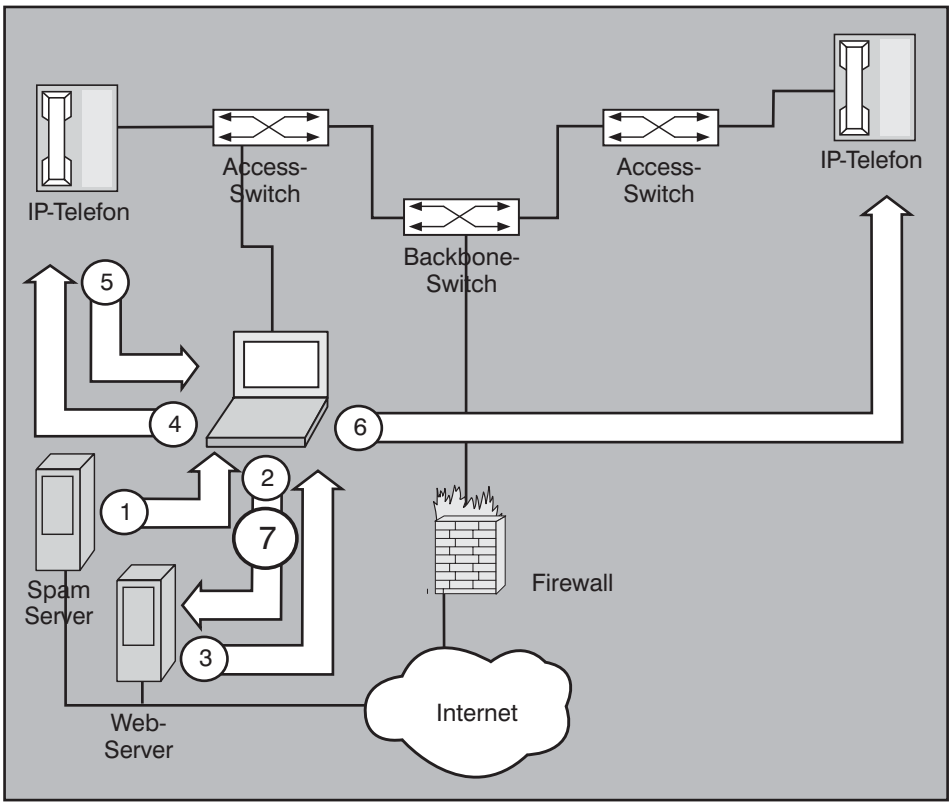


Abbildung 4: Abhörangriff von außen

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 ausführende 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 interne 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.

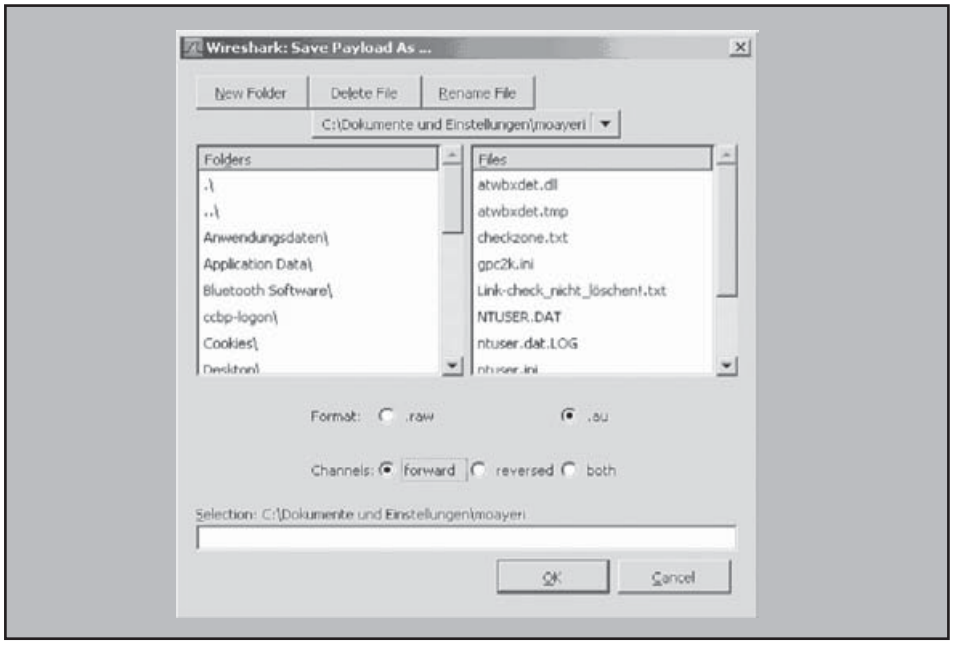


Abbildung 5: Zusammensetzung aufgezeichneter Pakete zu einer Audiodatei

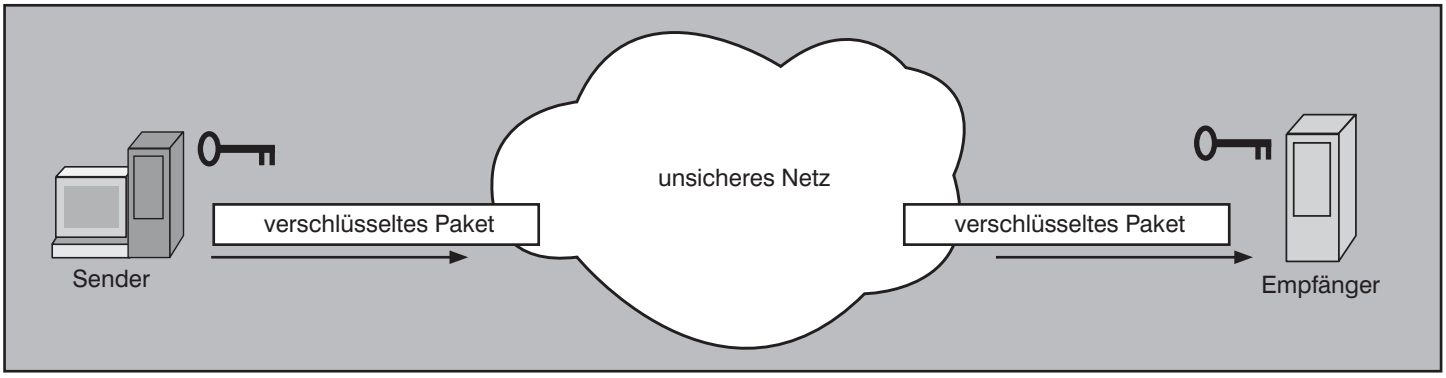


Abbildung 6: Ende-zu-Ende-Verschlüsselung

- 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 Server 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

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.

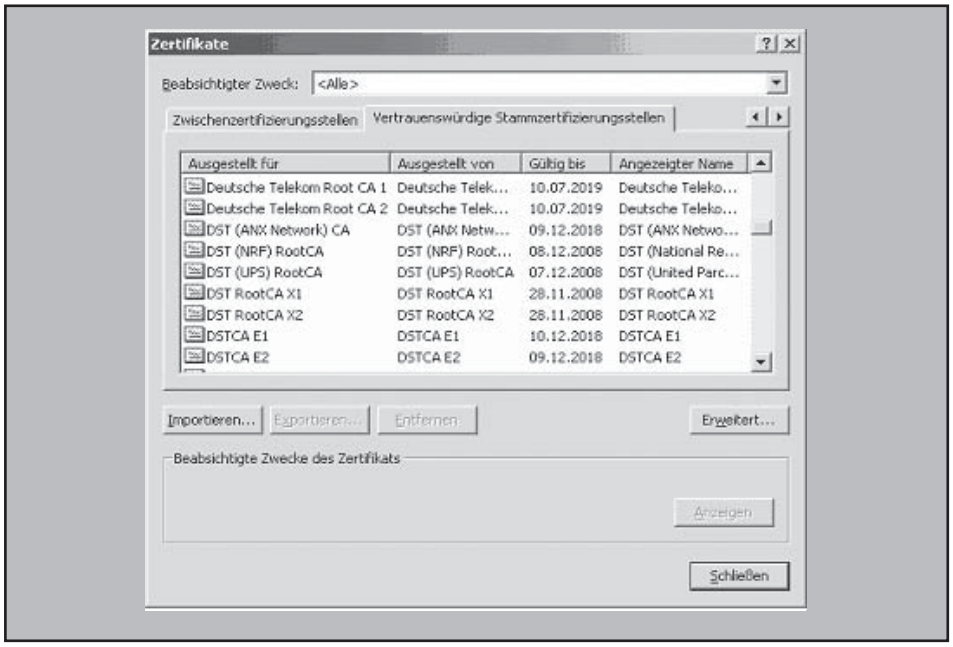


Abbildung 7: Mit Windows mitgelieferte Zertifikate öffentlicher CA

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).

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).

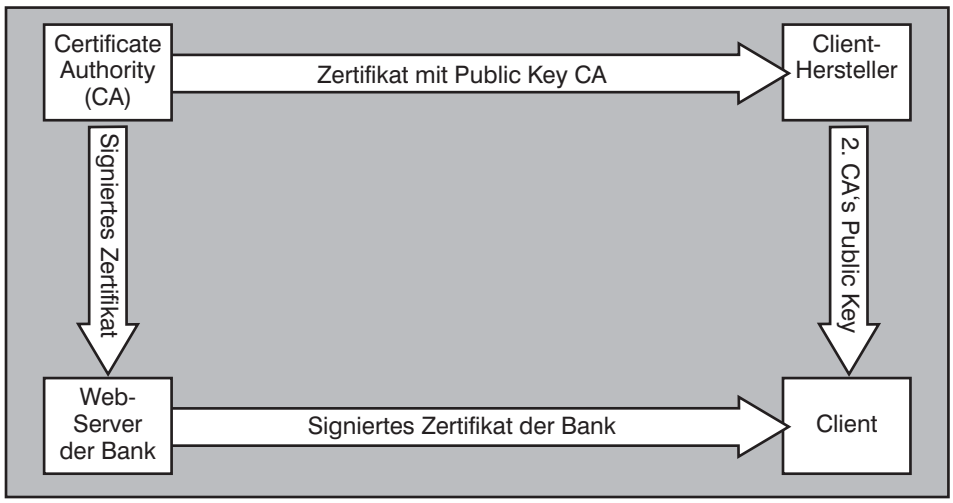


Abbildung 8: Prinzip der Vertrauenskette

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:

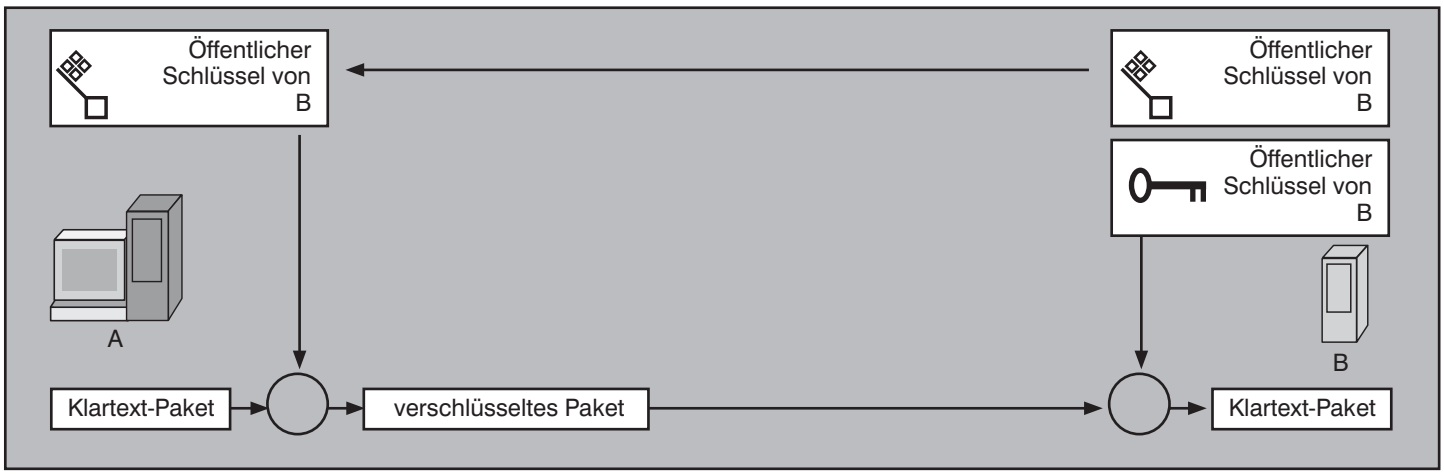


Abbildung 9: Prinzip der asymmetrischen (öffentlichen) Verschlüsselung

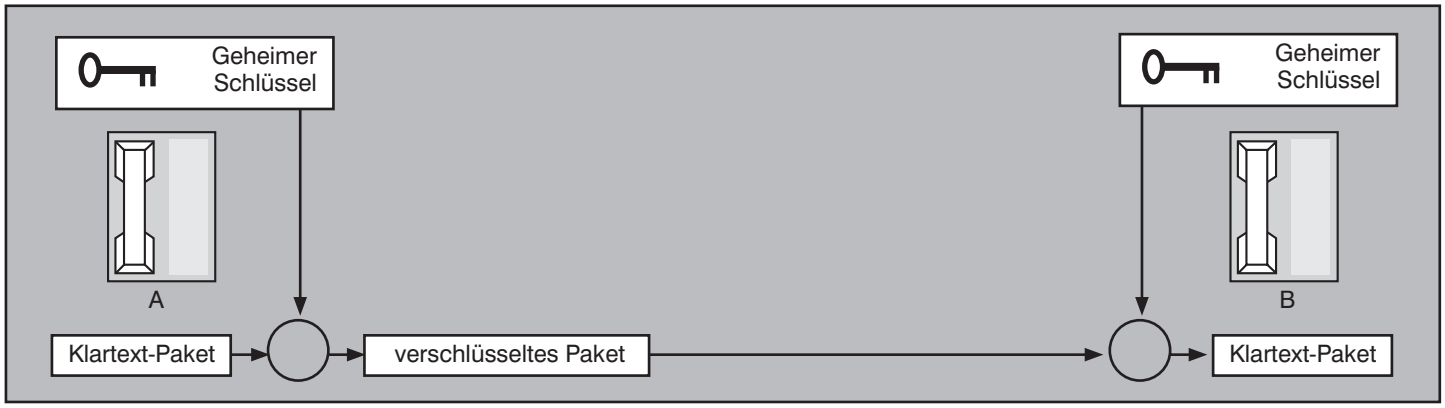


Abbildung 10: Prinzip der symmetrischen (privaten) Verschlüsselung

- 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

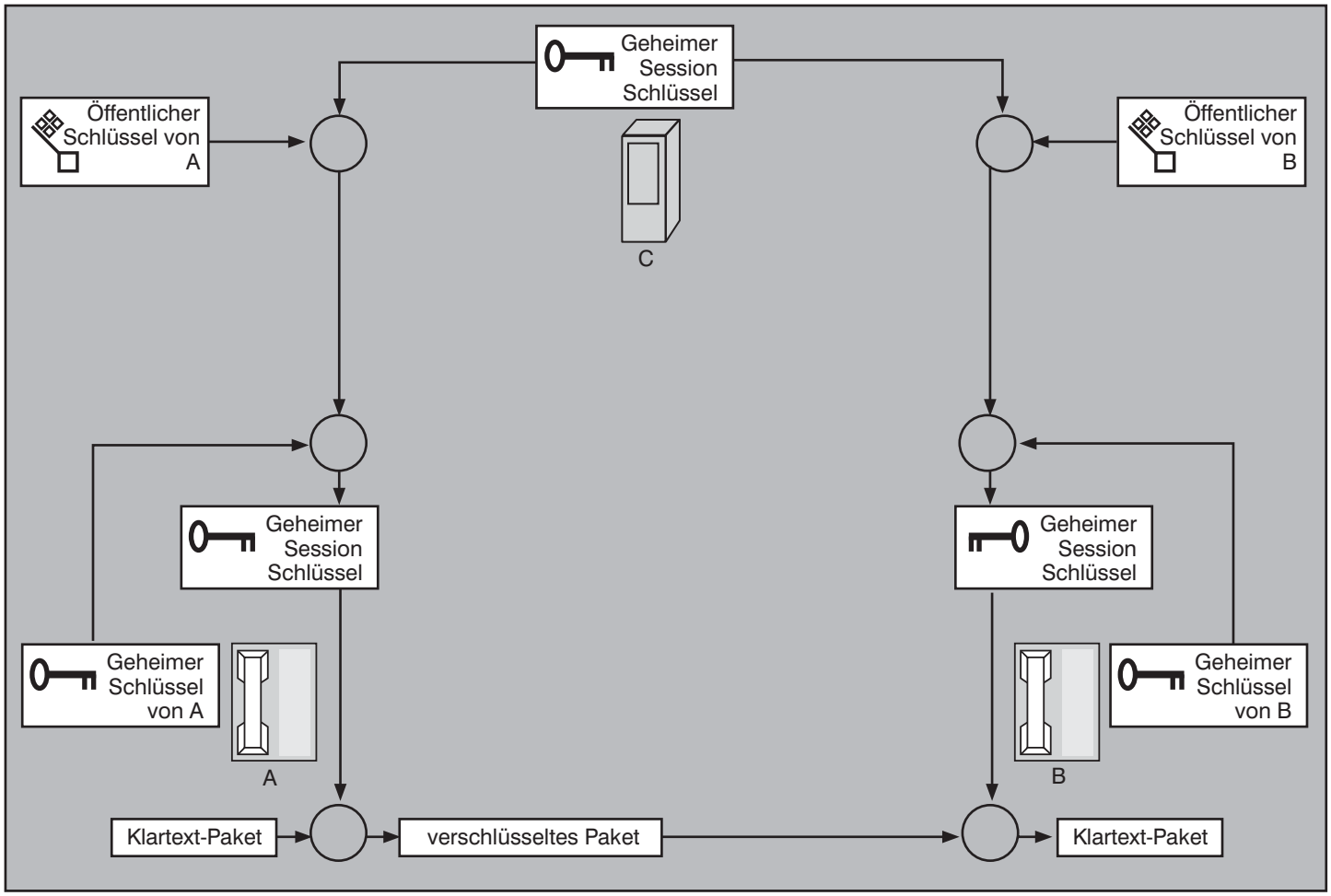


Abbildung 11: Asymmetrische Verschlüsselung des symmetrischen Session-Schlüssels

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,

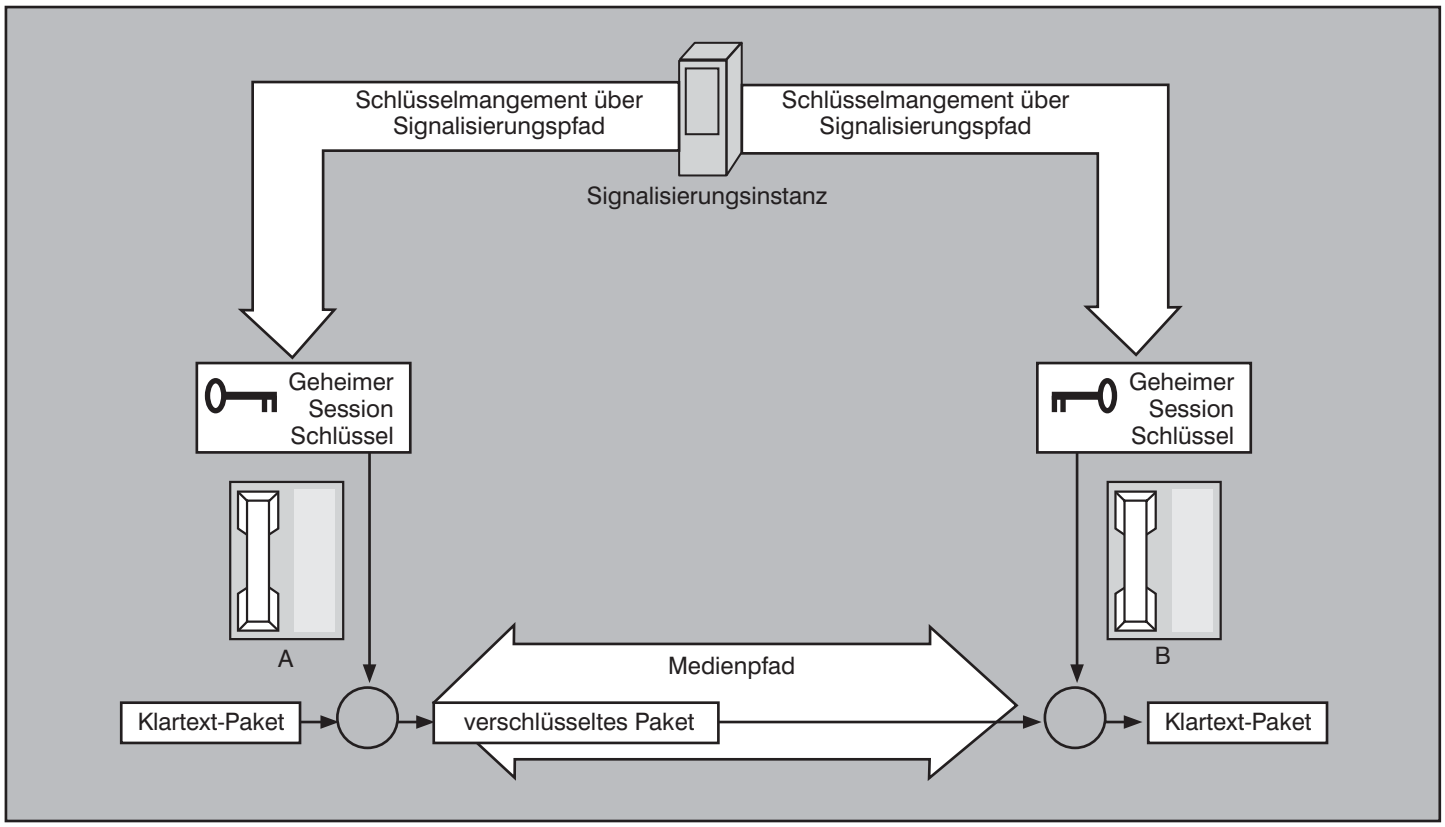


Abbildung 12: Schlüsselmanagement über den Signalisierungspfad

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 Experten, 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-

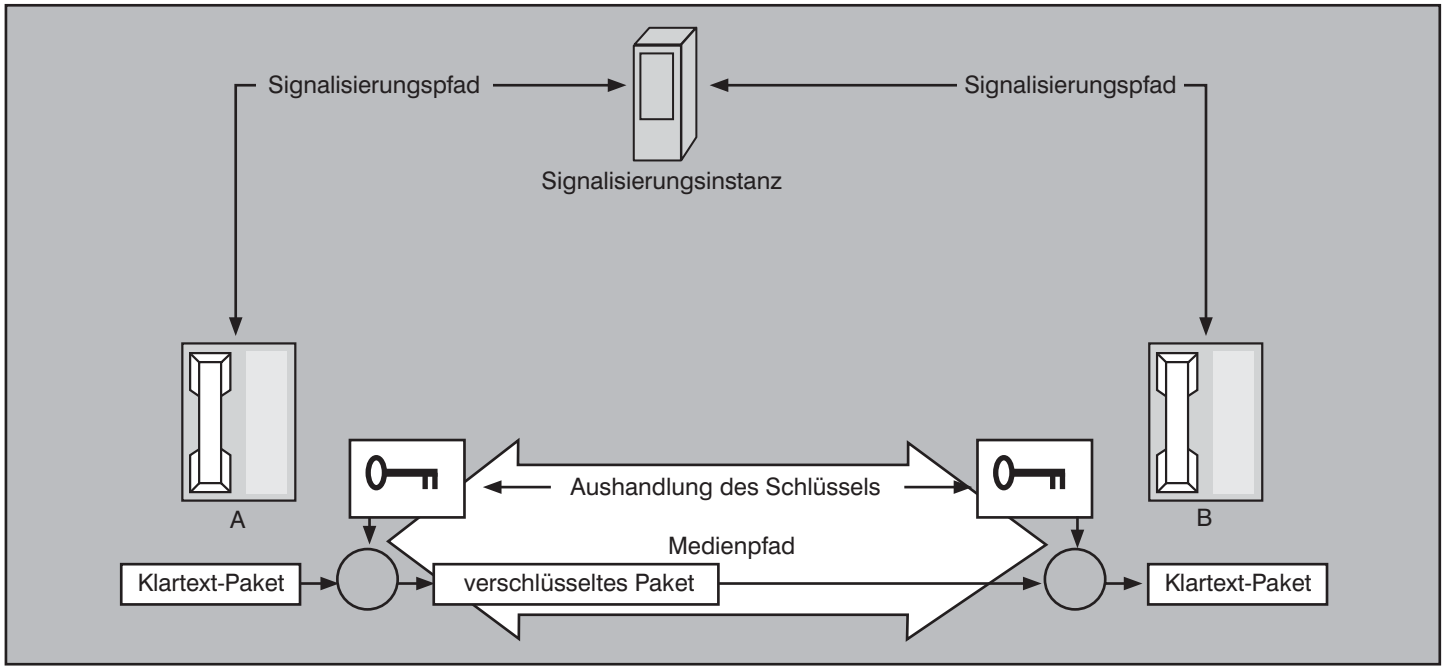


Abbildung 13: Aushandlung des Schlüssels über den Medienpfad

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-Helman (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 Gespräche 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 Medienpfads 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 ersten 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

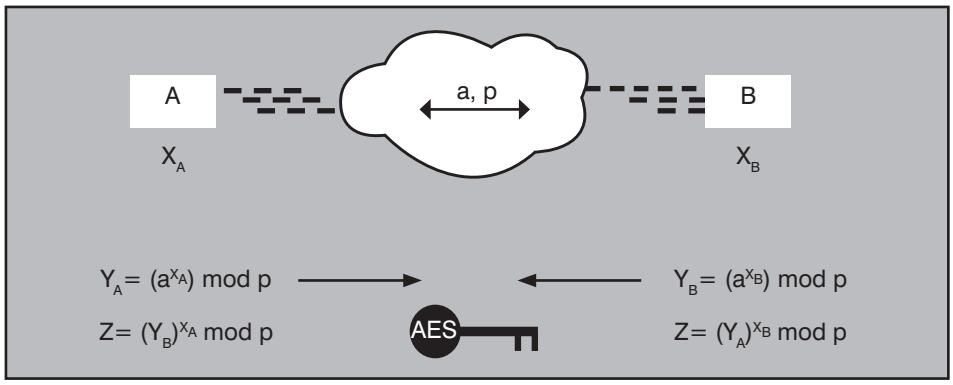


Abbildung 14: Schlüsselaustausch mit dem Diffie-Hellman-Verfahren

p und die Divisionsreste YA und YB können auch Angreifern bekannt sein, ohne dass die Angreifer daraus die geheimen Zahlen XA und XB 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 Skype nicht offengelegte Mechanismen verwendet. Somit sind Zfone und Skype nicht kombinierbar.

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

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

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 Benutzerfläche von Zfone teilt dem Benutzer mit, ob die Session sicher (verschlüsselt und authentifiziert) ist (siehe Abbildung 16).

Das Ziel der Initiatoren von ZRTP ist, dass dieses Protokoll auch in IP-Telefone 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 Signalisierung 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 Rol-

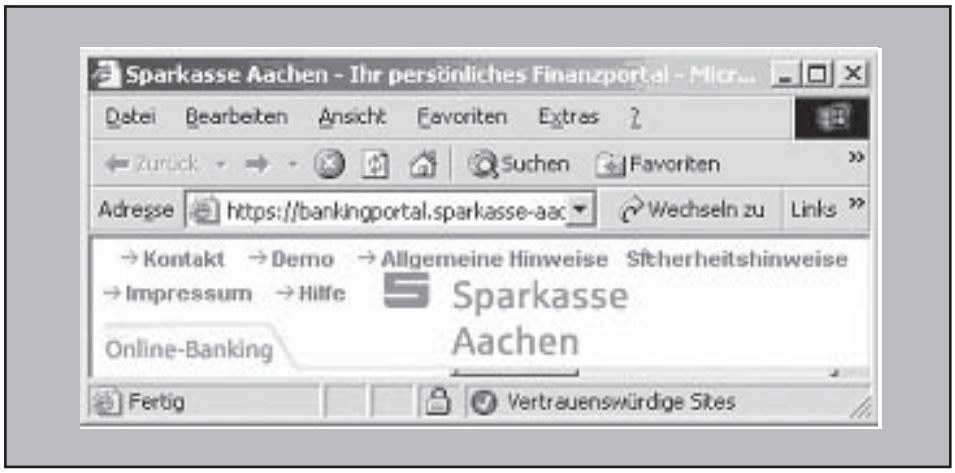


Abbildung 17: Symbol für eine sichere Verbindung muss schnell erkennbar sein

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 Lauschangriff“ 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 langfristig 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 eigenen 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-

ment. Es reicht, wenn jedes Endgerät eine Vertrauensbeziehung mit dem Telefonieserver 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-Businness-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, Telefonieserver, 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.

ComConsult Veranstaltungskalender

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 optinonal 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.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
15.10. - 19.10.07 in Aachen
03.12. - 07.12.07 in Aachen
11.02. - 15.02.08 in Aachen
09.06. - 13.06.08 in Aachen
15.09. - 19.09.08 in Aachen
24.11. - 28.11.08 in Aachen

Internetworking
10.12. - 14.12.07 in Aachen
10.03. - 14.03.08 in Aachen
02.06. - 06.06.08 in Aachen
13.10. - 17.10.08 in Aachen

TCP/IP und SNMP
15.10. - 19.10.07 in Berlin
25.02. - 29.02.08 in Stuttgart
26.05. - 30.05.08 in Aachen
20.10. - 24.10.08 in Berlin

Ethernet Netzwerke
26.11. - 28.11.07 in Aachen
05.05. - 07.05.08 in Aachen
27.10. - 29.10.08 in Bonn

Paketpreis für alle vier Seminare € 7.704.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--, Ethernet Netzwerke: € 1.690.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
03.09. - 07.09.07 in Aachen
12.11. - 16.11.07 in Aachen
03.03. - 07.03.08 in Aachen
16.06. - 20.06.08 in Aachen
01.09. - 05.09.08 in Aachen

Trouble Shooting in konvergenten Netzwerken
17.09. - 21.09.07 in Aachen
19.11. - 23.11.07 in Aachen
31.03. - 04.04.08 in Aachen
23.06. - 27.06.08 in Aachen
08.09. - 12.09.08 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
22.10. - 26.10.07 in Aachen
28.01. - 01.02.08 in Aachen
02.06. - 06.06.08 in Aachen
13.10. - 17.10.08 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
10.09. - 14.09.07 in Berlin
18.02. - 22.02.08 in Aachen
05.05. - 09.05.08 in Bonn
22.09. - 26.09.08 in Bonn

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheits-konzepten
15.10. - 19.10.07 in Aachen
10.03. - 14.03.08 in Frankfurt a.M.
23.06. - 27.06.08 in Bonn
03.11. - 07.11.08 in Bonn

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
03.12. - 07.12.07 in Aachen
07.04. - 11.04.08 in Aachen
25.08. - 29.08.08 in Aachen
01.12. - 05.12.08 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und und „Sicherheit in Wireless LANs“.
€ 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie