



IBM Global Services

Sicherheitsaspekte beim Zusammenwachsen konvergenter Anwendungen

Sicherheitsaspekte bei der paketvermittelnden Sprachübertragung

Antonius Klein, Senior IT Architect Infrastructure

14.09.2006

IBM / Köln – IT Verlag – Security Days

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Einleitung

- Mit dem Vortrag „Sicherheitsaspekte beim Zusammenwachsen konvergenter Anwendungen“ möchte ich eine Diskussionsgrundlage zur Verbesserung der Sicherheit in paketvermittelnden Sprachübertragungssystemen liefern.
- Dieser Vortrag kann nur einige wenige Themengebiete ansprechen und erhebt keinen Anspruch auf Vollständigkeit.
- Dieser Vortrag wird mehr Fragen bei den Zuhörern entstehen lassen, als er selber tatsächlich beantworten kann.
- Mit diesem Vortrag verfolge ich keineswegs die Absicht, und er soll auch keinesfalls dazu beitragen, den Erfolg und die unbestritten bewiesene Praxistauglichkeit von IP basierenden Sprachkommunikationen in Frage zu stellen. Vielmehr soll er eine konstruktive Diskussionsgrundlage bilden, um die hier angesprochenen Probleme durch eine wechselseitige Zusammenarbeit von Anbietern und Anwendern zu beseitigen zu können.

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

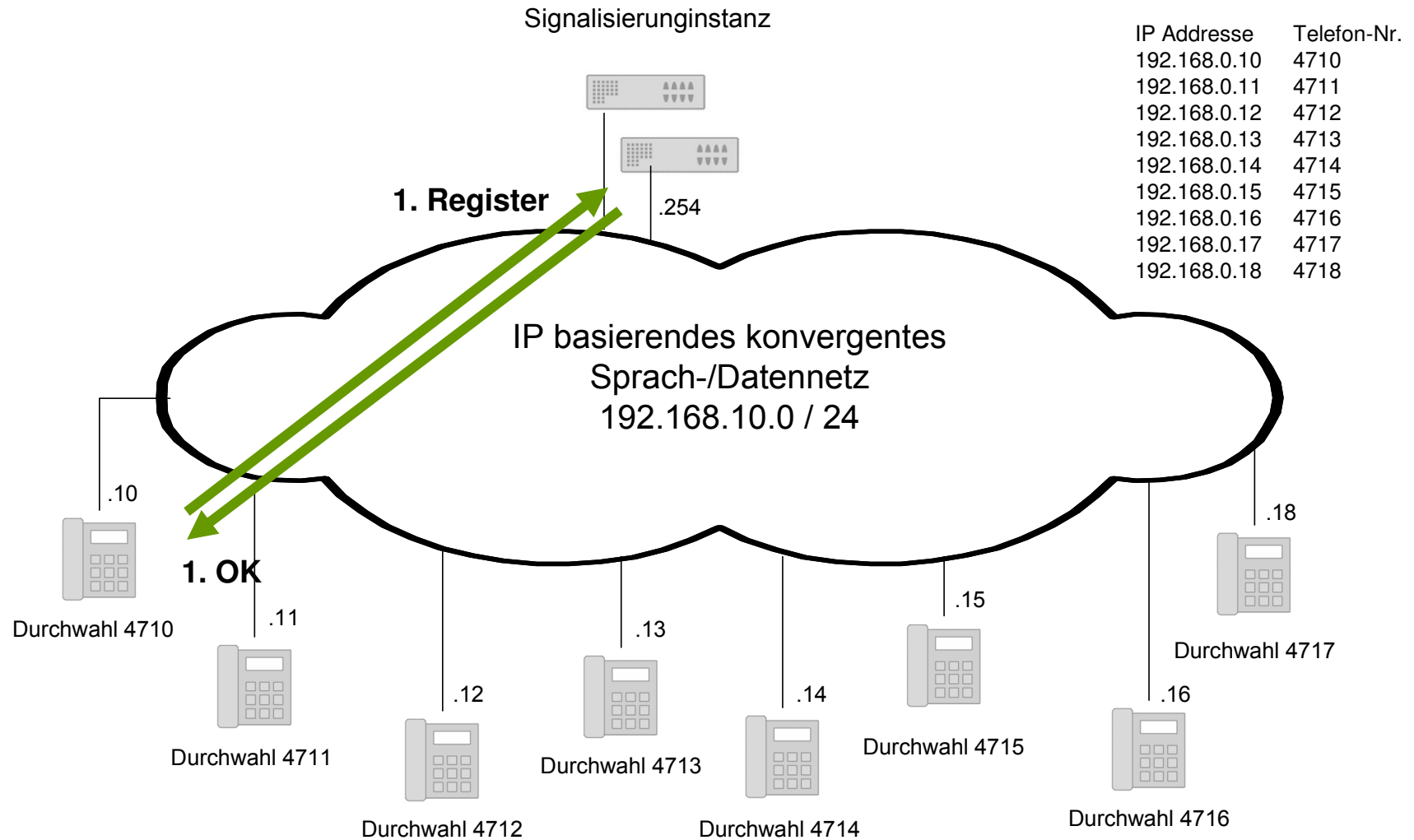
Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

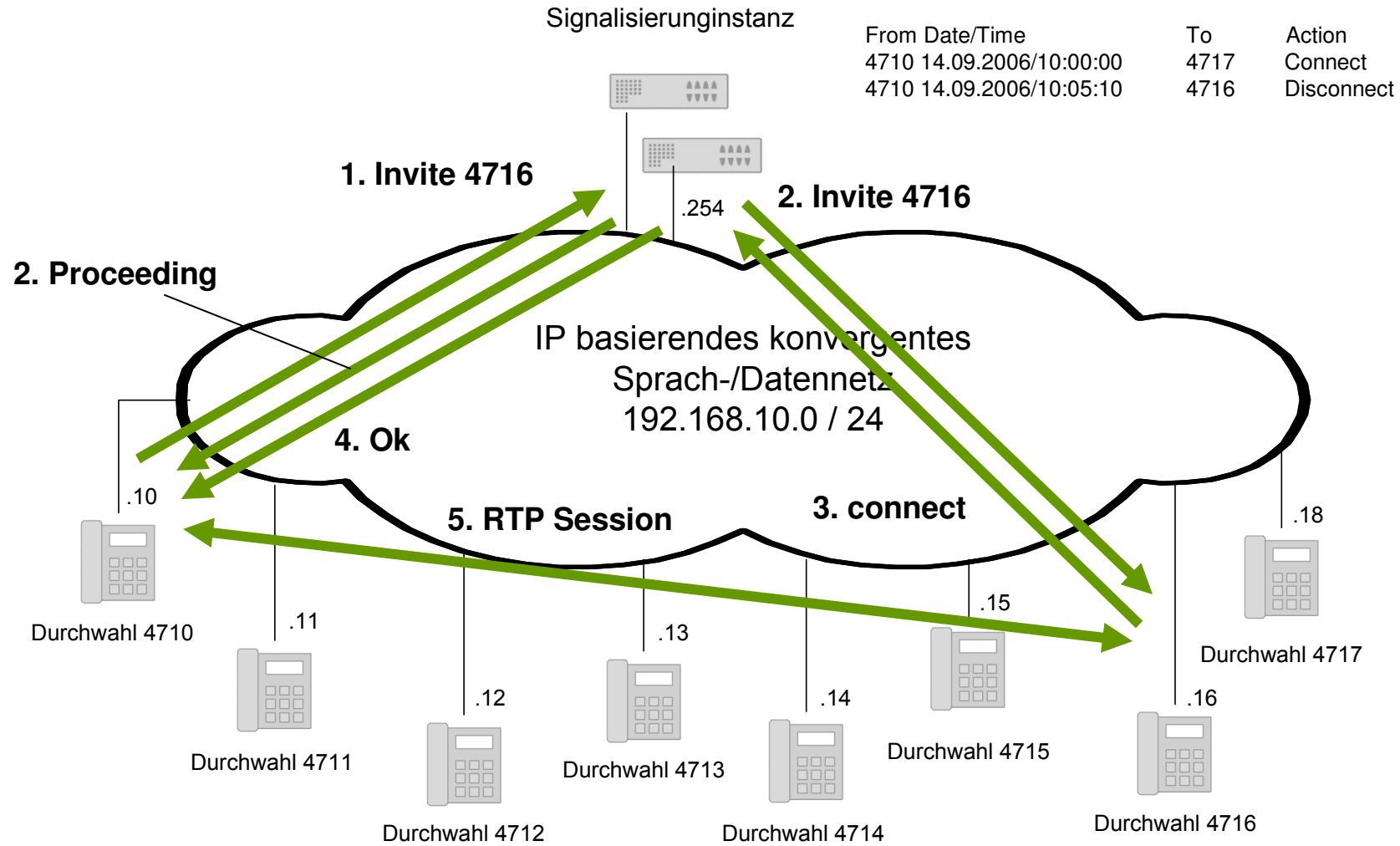
Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Einführung paketvermittelnder Sprachübertragung



Einführung paketvermittelnder Sprachübertragung



Einführung paketvermittelnder Sprachübertragung

Aus den vorhergehenden einfachen Beispielen ergeben sich aus Sicherheitsaspekten bereits einige grundlegende Fragen.

- Ich bin ein Internet Service Provider und möchte sicherstellen, dass sich keine nicht autorisierten Endanwender anmelden können. Wie stelle ich dies sicher?
- Ich bin ein Endanwender und möchte sicherstellen, dass sich kein Hacker mit meinen Anmeldedaten unter meinem Namen anmelden kann. Wie stelle ich dies sicher?
- Ich bin ein Internet Service Provider und betreibe eine VoIP Plattform. Wie kann ich auf Anforderung die Lawfull Interception sicherstellen?
- Ich bin ein VoIP Plattform Betreiber und stelle mir die Frage, wie ich diese Plattform vor Intrusion und Denial of Service Angriffen schützen kann?
- Ich bin ein Endanwender und frage mich, wie ich die Abhörsicherheit meines Telefongesprächs sicherstellen kann?

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Authentifizierungsmechanismus im Session Initiation Protocol (SIP Digest Authentication)

„SIP Digest Authentisierung“ basiert auf der in RFC 2617 HTTP Digest standardisierten Authentisierung und stellt über einen zustandslosen Challenge-Response Authentisierungsmechanismus sicher, dass keine Credentials (Benutzername und Passwort) im Klartext übertragen werden und schützt gleichzeitig vor Replay Attacken.

SIP Digest Authentisierung kann solange als sicher betrachtet werden, als sowohl die Signalisierungsinstanz als auch die Endgeräte vor Intrusion geschützt sind.

Gelingt z.B. über eine Brut Force Attacke ein Zugriff auf ein Endgerät oder die Signalisierungsinstanz, können die Zugangsdaten entweder gestohlen und missbraucht werden, oder aber sogar eigene Benutzerdaten in der Signalisierungsinstanz angelegt werden.

Authentifizierungsmechanismus im Session Initiation Protocol (S/Mime)

Secure Multipurpose Internet Mail Extension (S/MIME) ist ein Kodierstandard, der die Struktur, die Verschlüsselung, die Signatur und den Aufbau von E-Mails und anderer Internetchriften festlegt. Er wurde für die Sicherung des SIP Protokolls in den RFC3261 optional mitintegriert.

Beschrieben ist zum einen die Verschlüsselung des Session Description Protocol (SDP) Bodies, welche die Vertraulichkeit und die Integrität der darin enthaltenen Daten sicherstellen soll. Im Unterschied zum SIP Tunneling wird die gesamte Nachricht mit Header verschlüsselt, in das S/MIME Format kodiert und mit einem identischen SIP Header versehen. Die Gegenstelle kann nun den Header mit dem im S/MIME kodierten Header vergleichen und so Manipulationen auf einfache Weise erkennen.

Als Verschlüsselungsalgorithmen stehen unterschiedliche Verfahren zur Auswahl. Die Mindestanforderungen sind auf DES und SHA-1 spezifiziert. Bedingt durch den optionalen Charakter der S/MIME Spezifikation im RFC3261 sind momentan am Markt kaum Komponenten zu finden, die S/MIME für VoIP unterstützen.

Authentifizierungsmechanismus im Session Initiation Protocol (SIP over TLS)

SIP over TLS verwendet zur Sicherung der Informationen TLS (ehemals SSL), RFC2246. Im Unterschied zu den S/MIME SIP Sicherungsfunktionen stellt SIP over TLS nur eine Sicherheit zwischen den benachbarten Hops her und schützt die Informationen nicht vor kompromittierenden Proxies oder anderen VoIP-Systemen.

Vorteilhaft könnte im Vergleich zu den bereits vorgestellten Sicherungsmechanismen die Verwendung von Zertifikaten bei SIP over TLS sein, wenn zwischen Systemen ohne vorher definierten Vertrauensbeziehung kommuniziert werden muss. Wie auch bei S/MIME sind derzeit kaum Systeme am Markt erhältlich, die SIP over TLS bieten.

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Abhören / Abhörsicherheit aus Sicht der Carrier und des Endanwenders

In letzter Zeit ist eine Vielzahl von Artikeln über die Abhörsicherheit von VoIP erschienen. Gelingt der Zugriff auf den Datenstrom einer RTP Session, so bestehen sehr einfache Möglichkeiten, den RTP Stream wieder mit Hilfe von z.B. Wireshark (www.wireshark.org), ehemals ethereal, zusammenzubauen und in eine Audiodatei umzuwandeln und via PC abzuhören.

Aus technischen Sicht ist damit natürlich eine Abhörmöglichkeit gegeben. Praktikabel ist dies aus meiner Sicht nicht.

Der Lauscher muss den genauen Zeitpunkt, den Zielort, die Ziel IP Adresse und die Rufnummer vorab kennen.

Der Lauscher muss Zugriff auf den RTP Strom bekommen und der RTP Strom muss unverschlüsselt sein.

Nur wenn diese Bedingungen lückenlos erfüllt sind, kann ein sinnvoller Lauschangriff gestartet werden!!!!

Abhören aus der Sicht des Carriers

Das Telekommunikationsgesetz fordert von Unternehmen, welche Telekommunikationsdienstleistungen anbietet in bestimmten Situationen generell eine so genannte Lawfull Interception.

Derzeitig besteht eigentlich für so genannte VoIP Dienste nur die Pflicht der Erfassung der Verbindungsdaten, was aber mit großer Sicherheit in nächster Zeit um die Erfassung des eigentlichen Telefonates erweitert wird. Anders können im Falle einer Ermittlung die Strafbehörden gar keinen Beweis für einen kriminellen Hintergrund liefern. Und genau hier fangen die Probleme für den Carrier an.

Das Abhören eines Telefongespräches sollte dem Endanwender keine Möglichkeit geben, den Abhörvorgang zu erkennen.

Auf der anderen Seite handelt es sich bei IP basierenden Telefonaten um reine Punkt-zu-Punkt Verbindungen. Wie soll und kann ein Carrier hier noch sinnvoll eine Lawfull Interception implementieren?

Wie kann abgehört werden, wenn der Endanwender verschlüsselt?

Abhören aus der Sicht des Carriers

Der Carrier hat derzeitig generell zwei Möglichkeiten.

Möglichkeit 1:

Bei Bedarf führt der Carrier das unverschüsselte Gespräch über einen zentralen unter seiner Kontrolle stehenden RTP-Relay mit Lawful Interception Schnittstelle.

Nachteil: Theoretisch besteht für den Endanwender eine sehr einfache Möglichkeit den Lauschangriff festzustellen. Er muss nur die Ziel IP Adressen analysieren. Gehen die Gespräche immer zur gleichen IP, ist die Gefahr das er abgehört wird sehr wahrscheinlich.

Möglichkeit 2:

Der Carrier führt das VoIP Gespräch immer über einen RTP mit Lawfull Interception Schnittstelle, was einen enormen Aufwand für den Carrier bedeutet.

Abhören aus der Sicht des Carriers

Unabhängig von Möglichkeit 1 und 2 hat der Endanwender in der Regel, bei entsprechender Unterstützung durch die Signalisierungsinstanz, immer die Möglichkeit, durch die Wahl entsprechender Endgeräte sein Gespräch mit seinem Partner zu verschlüsseln. In diesem Fall nützt die Umleitung über einen RTP-Relay gar nichts, da in diesem Fall in der Regel das Gespräch unverschlüsselt aufgebaut wird und dem Endanwender über das Endgerät auch angezeigt wird.

Fazit: Basierend auf der derzeitigen Gesetzgebung kann eine verlässliche Abhörung eines VoIP basierenden Telefonates nicht gewährleistet werden. Dies könnte aus meiner Sicht nur geschehen, wenn via Gesetz zumindest im öffentlichen Bereich die Verschlüsselung des RTP-Stroms verboten wird und auch entsprechend in den Endgeräten umgesetzt wird.

Abhörsicherheit aus der Sicht des Endanwenders

Der Endanwender wird normalerweise ein grundlegendes Interesse daran haben, dass seine Privatsphäre vor Lauschangriffen geschützt ist.

Wie zuvor beschrieben, insofern mir ein Zugriff auf den RTP Stream gelingt, ist ein einfaches Zusammensetzen des Gespräches möglich.

Bei VoIP hat der Endanwender, den richtigen Einsatz vorausgesetzt, erheblich bessere Möglichkeiten, seine Privatsphäre zu schützen, als der Lauscher, der das Gespräch abhören will.

Die sicherste Methode ist, das Gespräch entweder über eine gesicherte IP Verbindung (IPSec) zu führen, oder aber auf Applikationsebene das eigentliche VoIP Gespräche mit Hilfe von SRTP zu verschlüsseln. Sollte dem Lauscher ein Zugriff auf das Netzwerk gelingen, müsste er auch zeitgleich die Schlüsselinformationen von den beiden Endgeräten stehlen, um die Möglichkeit eines Lauschangriffes zu erhalten. Diese Wahrscheinlichkeit halte ich bei solider Security Infrastruktur für ausgeschlossen und auch nicht praktikabel.

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

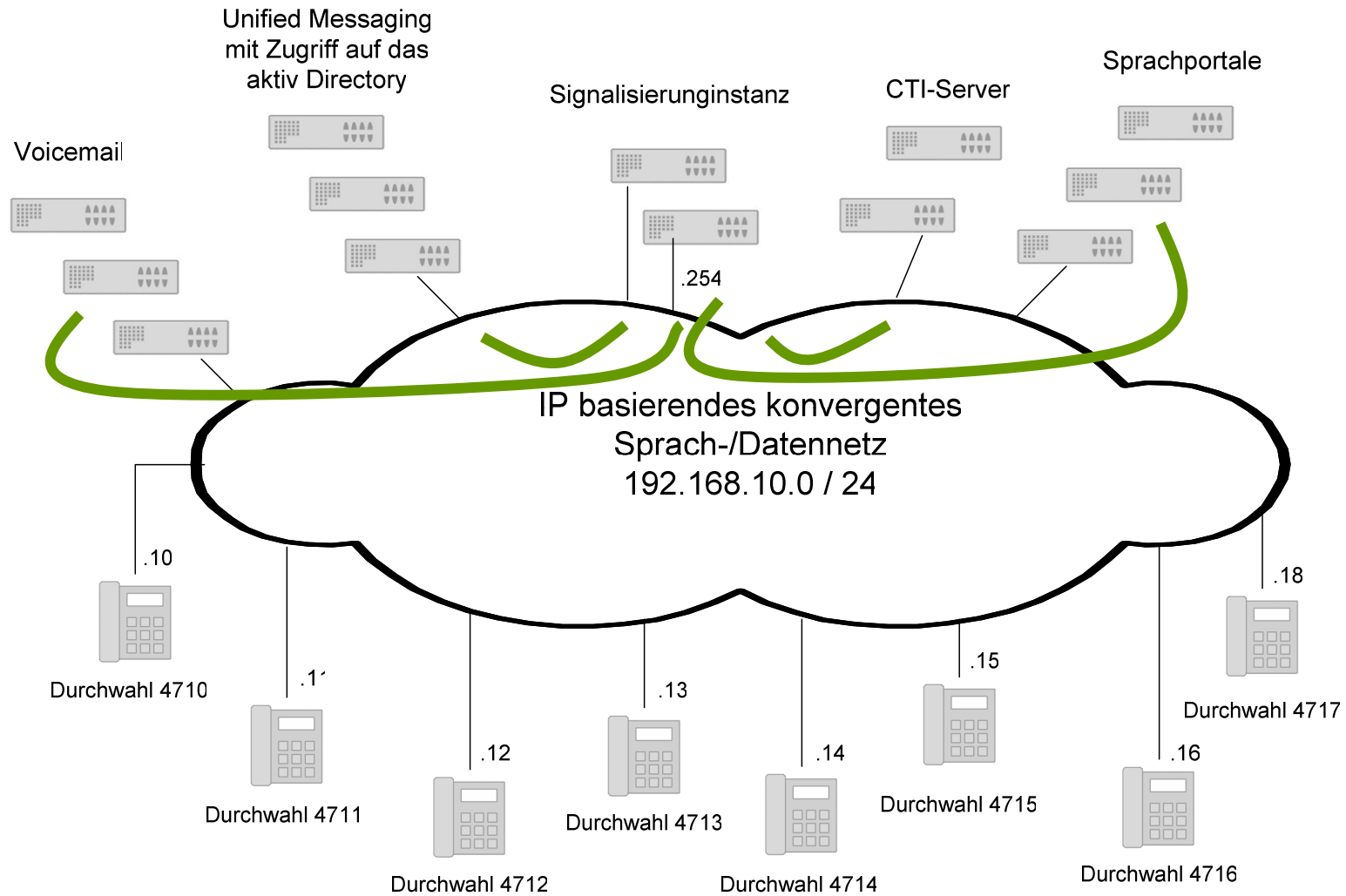
Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit



Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Was passiert sicherheitstechnisch, wenn ich mein IP basierendes Sprachnetz mit sprachkonvergenten Anwendungen (Unified Messaging, Mailbox, CTI, VoicePortal, IP-Contact Center) kombiniere.

Es entstehen ganz neue Sicherheitsrisiken, welche vor Beginn der Planung analysiert und mit berücksichtigt werden müssen, um keine neuen Lücken entstehen zu lassen.

Beispiele:

- Unified Messaging macht unter Umständen ein Andocken an das zentrale Active Directory und Schemata Änderungen erforderlich.
- Zugriff auf Voice Messaging erlaubt bei Nichtschutz unter Umständen die Umgehung von Access Listen im Telefonbereich.
- VoicePortals erlauben den Missbrauch für Voice Phishing und Voice Spam

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

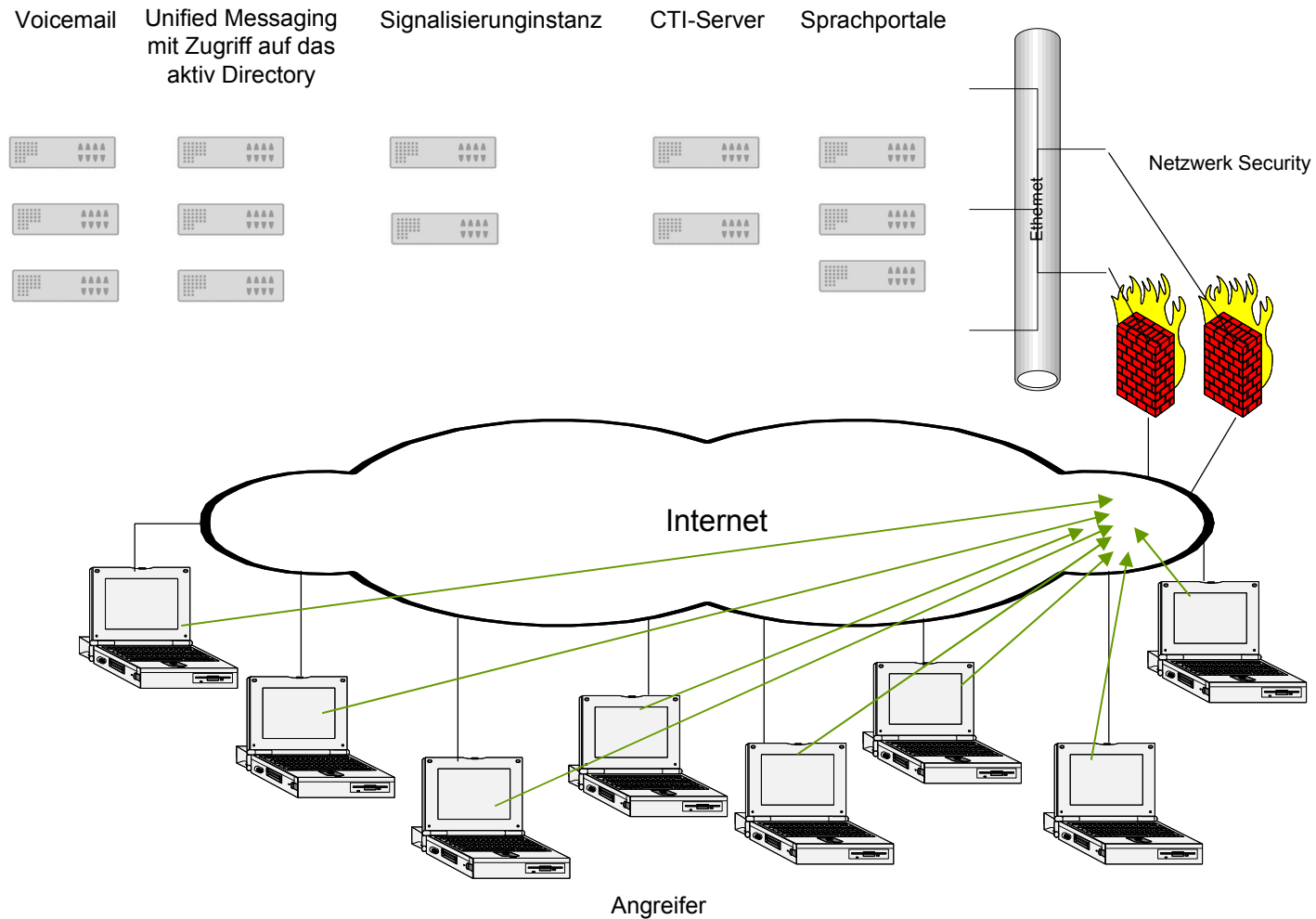
Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Denial of Service Angriffe auf Signalisierungsinstanz und Anwendungen



Denial of Service Angriffe auf Signalisierungsinstanz und Anwendungen

Ein klassischer DoS Angriff ohne entsprechend implementierte Schutzmassnahmen kann zu folgenden Problemen führen:

- Erreichbarkeit von Innen und Außen unmöglich
- Kein Notruf mehr
- Kein Geschäft mehr über IP Contact Center möglich
- Andere Geschäftskritische Anwendungen können für Stunden ausfallen

Folgende Internetseiten enthalten gute Informationen zur Sicherheitsaspekten bei paket vermittelnder Sprachübertragung.

www.bsi.de

www.cert.org

Agenda

Einleitung

Einführung paketvermittelnder Sprachübertragung

Authentifizierungsmechanismus im Session Initiation Protocol

Abhören / Abhörsicherheit aus der Sicht der Carrier und des Endanwenders

Einfluss von konvergenten Sprachanwendungen auf die Sicherheit

Denial of Service Angriffe auf Signalisierungsinstanzen und Anwendungen

Heute zur Verfügung stehende Abwehrmechanismen

Heute zur Verfügung stehenden Abwehrmechanismen

Um sich vor den zuvor geschilderten Angriffsszenarien zu schützen, können selbstverständlich die heute für die Netzwerksicherheit bereits eingesetzten Komponenten verwendet werden.

Darüber hinaus sollte aber schon bei der Konzeption darauf geachtet werden, dass bestimmte Abhängigkeiten zwischen Anwendungen ausgeschlossen sind, dass eine saubere Authentifizierung und Verschlüsselungsinfrastruktur als auch der Einsatz von speziellen Sicherheitslösungen im VoIP Umfeld zur Anwendung kommen:

- VoIP Ready Firewalls
- Session Border Controller
- IntraProtector oder ähnliche Tools
- Gehärtete Signalisierungsplattformen
- Entsprechend geschützte VoIP Endgeräte



IBM Global Services

Sicherheitsaspekte beim Zusammenwachsen konvergenter Anwendungen

Ich bedanke mich für Ihre Aufmerksamkeit !!!

Bei Fragen wenden Sie sich bitte an unsere Presseauftrage
Beate Hoeger-Spiegel (beate.hoeger-spiegel@de.ibm.com)

Antonius Klein, Senior IT Architect Infrastructure

Antklein @de.ibm.com

IBM / Köln – IT Verlag – Security Days