DECOIT

D·A·CH Security 2007

VoIP-Security

Standards, Evaluierung und Konzeptbeispiele anhand von Asterisk

Dr.-Ing. Kai-Oliver Detken
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

© DECOIT GmbH

Inhalt

- Stand der Technik
- Asterisk-Lösung
- Risiken
  - Protokolle
  - Bedrohungen und Attacken
  - Angriffstools
  - Bewertungen und Auswertungen
- Ausblick

© DECOIT GmbH

Voice-over-IP (VoIP)

- Sprachdaten, die über ein IP-basiertes Datennetz transportiert werden
- Dabei sind Echtzeitdaten im Weitverkehrsumfeld gemeint
- VoIP hängt in seiner Qualität stark von den Begebenheiten der Internet-Protokolle ab
- VoIP kann dabei sehr unterschiedlich, stark anhängig vom Hersteller, realisiert werden

© DECOIT GmbH

IP-Telefonie (IPT)

- IP-Telefonie beschränkt sich auf den lokalen Bereich und meint vornehmlich den Einsatz von IP-Endgeräten zur VoIP-Kommunikation
- Mittels VoIP ist die Anbindung an bestehende TK-Netze möglich
- Endgeräte für IP-Telephonie sind mannigfaltig am Markt vorhanden
- Software-basierte Lösungen sind neben Hardware-Geräten verfügbar (u.a. über die TAPI-Schnittstelle)

© DECOIT GmbH

VoIP-Szenarien

- Campus VoIP: es wird eine Nebenstellenanlage auf IP-Basis verwendet, die auch als IP-PBX bezeichnet wird. IP-Telefone und/oder Softphones sind mit dieser IP-PBX verbunden. Der Verbindungsaufbau in das öffentliche Telefonnetz wird über Gateways ermöglicht. Diese Variante ist schwer von außen zu attackieren, da die Telefongespräche nicht über das Internet oder andere unsichere Netze geführt werden.
- IP Centrex / Hosted IP: beinhaltet eine virtuelle, IP-basierte PBX, die von einem Provider zur Verfügung gestellt wird. Der Provider ist hierdurch in der Lage, eigene Sprachdienste anzubieten, ohne dass ein Unternehmen eigene Gateways oder PBX-Systeme anschaffen muss. Aus Sicht des Unternehmens muss nur eine ausreichende Internet-Anbindung vorhanden sein und IP-Telefone und/oder Softphones müssen angeschafft werden. Attacken auf das VoIP-System können über das Intranet oder über das Internet (aus dem Providernetz) erfolgen.
- VoIP-Trunks: VoIP-Trunkverbindungen lösen zunehmend herkömmliche verbindungsorientierte Telefonverbindungen ab. Dabei kann es zu einem höheren Angriffspotenzial kommen, wenn die Übertragung über unsichere Netze realisiert wird.

© DECOIT GmbH

Protokolle und Standards bei VoIP

<table>
<tr><td>Audio-
Applikationen</td><td>Video-
Applikationen</td><td colspan="4">Terminal Kontrolle und Management</td><td>Daten</td></tr>
<tr><td rowspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.261
H.263</td><td rowspan="3">RTCP</td><td rowspan="3">Terminal zu
Gatekeeper
Signalisierung

RAS</td><td rowspan="3">H.255.0
Q.931
Verbindungs-
signalisierung
(Call Setup)</td><td rowspan="3">H.245
Kontroll-
kanal</td><td>T.124</td></tr>
<tr><td rowspan="2">T.125</td></tr>
<tr><td colspan="2">RTP</td><td rowspan="4">T.123</td></tr>
<tr><td colspan="4">Unzuverlässiger Transport (UDP)</td><td colspan="2">Zuverlässiger Transport
(TCP)</td></tr>
<tr><td colspan="6">Netzwerkschicht (IP)</td></tr>
<tr><td colspan="6">Sicherheitsschicht (IEEE 802.3)</td></tr>
<tr><td colspan="7">Bitübertragungsschicht (IEEE 802.3)</td></tr>
</table>

© DECOIT GmbH

Open Source Projekt Asterisk (1)

- Asterisk ist eine Software PBX (Private Branch eXchange) die unter Linux, BSD und OS X läuft
- Dabei ermöglicht Asterisk verschiedene Telefonnetze miteinander zu verbinden.
- Diese Netze können VoIP Netze sein z.B. SIP, IAX oder H.323 oder auch ISDN
- Dazu verwendet Asterisk so genannte Channel Treiber die miteinander kommunizieren können
- Durch die Vielzahl von unterstützten Protokollen und Funktionen, eignet sich Asterisk für Gateways zwischen verschiedenen Netzen, als Konferenzserver sowie als Server für Sprachmenüs und automatisierte Steuerung durch den Anrufer
- Mittels CTI können Desktop Applikationen angebunden werden

© DECOIT GmbH

Open Source Projekt Asterisk (2)

- Leistungsmerkmale
  - Standard Call Features (CLI, Transfer, Parking, DnD …)
  - Konferenzräume mit >3 Teilnehmern (MeetMe)
  - Wartemusik (MoH)/verschiedene Formate u.a. mp3
  - Mischbetrieb Anlagen- und Mehrgeräteanschluss, S2M
  - Message Waiting Indication (MWI)
  - SMS im Festnetz
  - Anrufwarteschlange (ACD, Call-Queue)
  - Gesprächsdatenerfassung
  - Flexible Externgesprächsberechtigungen
  - DISA (Direct Inward System Access)
  - VoiceMail System (Abruf über Telefon mit PW-Schutz, Zustellung per E-Mail, Web-Access)
  - Default- und individuelle Ansagen (verschieden für „nicht erreichbar“ oder „besetzt“)
  - FaxMail System (Fax Mailbox, Zustellung über E-Mail)
  - Sprachdialogsystem (IVR)
  - Telefonbuch zentral und individuell

© DECOIT GmbH

Open Source Projekt Asterisk (3)

- Unterstützte Protokolle & Codecs
  - Protokolle
    - SIP
    - H.323
    - MGCP
    - SCCP/Skinny
    - IAX2
  - Codecs:
    - G.723.1
    - G.711 (μ-Law, A-Law),
    - GSM
    - ADPCM
    - optional G.729

© DECOIT GmbH

Protokoll-Risiken (1)

- H.323
  - Wesentliche Angriffspunkte sind Täuschung der Identität seitens des anrufenden Teilnehmers sowie Manipulation der Nachrichten mit Hilfe von MitM-Attacken.
  - Auch können beim Verbindungsaufbau die Transportadressen der Sprachströme verändert werden, wodurch diese an eine beliebige IP-Adresse umgeleitet, und dort abgehört, aufgezeichnet oder gar verändert weitergeleitet werden können. Diese Bedrohungen betreffen Endgeräte ebenso wie Gateways.

© DECOIT GmbH

Protokoll-Risiken (2)

- SIP
  - bietet eine Sicherung der Nachrichten unter Verwendung kryptographischer Hashes und Verschlüsselungsmechanismen an
  - Dies erlaubt eine zuverlässige Authentifizierung und Absicherung gegen Veränderungen der Signalisierungsnachrichten
  - Allerdings sind nicht alle Header durch Hashing abgedeckt, wodurch eine Manipulation der Absenderkennung möglich ist
  - Wird keine Absicherung der SIP-Nachrichten mit Hashes vorgesehen, so können die im Bereich H.323 beschriebenen Angriffe sogar mit noch einfacheren Mitteln realisiert werden, da die Nachrichten im ASCII-Text kodiert werden
  - Auch hier sind Endgeräte und Gateways betroffen.

© DECOIT GmbH

Protokoll-Risiken (3)

- RTP
  - Mit den RTP-Informationen kann eine Menge von Datenpaketen einer Verbindung in einer korrekten Reihenfolge mit dem passenden Codec decodiert und auf einem Ausgabegerät abgespielt werden, ohne auf die Signalisierung dieser Verbindung zurückgreifen zu müssen
  - Diese einfache Decodierung des Medienstroms versetzt einen Angreifer in die Lage, die Datenpakete eines Sprachstromes abzuhören und zu manipulieren, sobald er auf diese zugreifen kann
  - Dabei ist sogar die Reihenfolge der empfangenen Datenpakete unerheblich
  - Zwar entstehen Lücken bei der Decodierung, wenn bestimmte Datenpakete fehlen, jedoch ist dies nicht mit einem Synchronisationsverlust des Kanals verbunden

© DECOIT GmbH

Protokoll-Risiken (4)

- MGCP und MEGACO
  - Bei den Protokollen MGCP und MEGACO sind Sicherheitsmechanismen nicht direkt vorgesehen
  - Gelingt es einem Angreifer, Datenströme abzuhören und zu manipulieren, so können diese decodiert und beliebig verändert werden
  - Falls die Daten mit ASN.1 oder in ASCII codiert sein sollten, ist für die Offenlegung ein ASN.1-Parser notwendig
  - Diese Protokolle werden nur zwischen VoIP-Servern und Gateways bzw. zwischen Gateways selbst eingesetzt. Somit sind von den Manipulationen der Protokoll-Nachrichten nur Gateways betroffen.

© DECOIT GmbH

Protokoll-Risiken (5)

- Skinny Client Control Protocol (SCCP)
  - Proprietäres Kommunikationsprotokoll, das für die Kommunikationssteuerung zwischen IP-Telefonen und dem Gatekeeper (bei Cisco der Call Manager) verwendet wird. Es ist nicht öffentlich dokumentiert und kann vom Hersteller jederzeit verändert werden.
  - In älteren Protokollversionen, die immer noch in sehr vielen Endgeräten verwendet werden, wird lediglich die MAC-Adresse zur Authentifizierung übertragen. Diese Kommunikation lässt sich relativ einfach abhören.
  - Neuere Versionen von SCCP-basierten IP-Telefonen verwenden SCCPS für die Authentifizierung X.509-Zertifikate und verschlüsseln den TCP-Signalisierungsstrom mit Hilfe von TLS. Damit ist Identity-Spoofing sowie das Decodieren der Kommunikationsdaten zwischen IP-Telefonen und dem Gatekeeper nicht mehr möglich
  - Für die Steuerung unterschiedlicher Leistungsmerkmale der Telefone wird verstärkt HTTP verwendet (ohne Verschlüsselung)

© DECOIT GmbH

Protokoll-Risiken (6)

- InterAsterisk eXchange Protocol (IAX)
  - Proprietär, jedoch offen
  - Signalisierungs- und Medientransport werden über einen einzigen Port (UDP 4569) abgewickelt. Dadurch ist das Protokoll IAX2 einfach über NAT-Umgebungen zu transportieren und die Regeln in Firewalls sind überschaubar.
  - Schlank durch binäre Codierung und geringen Protokoll-Overhead. IAX weist ein Protokoll-Overhead von nur vier Bytes auf, um Sprach- und Videopakete auszutauschen.
  - Die Bündelung mehrerer IAX-Verbindungen zwischen zwei Asterisk-Servern zu einem Trunk ist möglich.
  - Im eigentlichen IAX-Protokoll wurden keine Sicherheitsmechanismen verankert. Dies wurde in der Version IAX2 nachgeholt
  - Hinzu kommt, dass IAX-Endgeräte relativ selten am Markt vorkommen, so dass dieses Protokoll nur in Szenarien mit Asterisk-Servern relevant ist

© DECOIT GmbH

Bedrohungen und Attacken

- Netzwerkattacken
  - Denial-of-Service (DoS)
  - ARP, MAC, IP, UDP, IRDP Spoofing
  - SYN-, PING- oder MAC-Flooding
  - TCP-Session-Hijacking
  - RST-Attack
  - Data Injection through ISN-Guessing
  - Sniffing
  - Replay
- Angriffe gegen die Applikationsschicht
  - Abfangen der Anschlussgebühren
  - Rufmanipulation
  - Nichtautorisierte Nutzung (Phreaking)
  - Dialer
  - Verletzung der Privatsphäre
  - Spam over IP Telephony (SPIT)

© DECOIT GmbH

Angriffstools

- Cain & Abel: bedient sich dem ARP-Spoofing, d.h. es werden ARP-Abfragen vorgetäuscht und MAC-Adressen gefälscht, wodurch der Sprachverkehr umgeleitet und abgehört werden kann.
- Vomit: wandelt ein Cisco-basiertes IP-Telefongespräch in ein WAV-File um, die mit jedem Audio-Player abgespielt werden kann. Vomit erfordert eine tcpdump-Ausgabedatei. Es arbeitet nur mit dem G.711-Codierungsstandard zusammen.
- VoIPong: erkennt und filtert VoIP-Calls in einem Datenstrom heraus. Es legt eine Kopie eines G.711-Gesprächs an und konvertiert dieses in ein WAV-File. Unterstützt werden die Protokolle SIP, H.323, SCCP, RTP und RCTP.
- SIP Vulnerability Scanner (SiVuS): untersucht VoIP-Installationen auf Fehler. Dies wird durch das Initiieren von Attacken vorgenommen. Es können auch eigene SIP-Nachrichten generiert werden.
- SIPcrack: als Protokoll-Login-Cracker enthält es zwei Programme: SIPdump, um die eingelogten SIP-User zu finden und SIPcrack, um die Passwörter der gefundenen SIP-User mittels Bruteforce-Attacks zu ermitteln.
- RingAll: ermöglicht DoS-Attacken auf ungeschützte SIP-Clients

© DECOIT GmbH

Bewertungen und Auswirkungen (1)

- SRTP
  - Es wird eine AES-Verschlüsselung der Medienströme vorgenommen
  - Um eine Verschlüsselung zu gewährleisten, muss zunächst ein Schlüsselaustausch erfolgen
  - Durch die Verwendung von SHA-1 werden die Gesprächsteilnehmer authentifiziert
  - Der Schlüssel, welcher genutzt wird, um die Nutzdaten zu verschlüsseln, wird allerdings über SIP übertragen
  - Somit kann der Schlüssel ausgespäht werden, wenn SIP nicht ausreichend abgesichert ist

© DECOIT GmbH

Bewertungen und Auswirkungen (2)

- SIP
  - Wurde um diverse Sicherheitsmechanismen wie TLS, HTTP Digest, IPsec mit IKE und S/MIME erweitert
  - Es wird Ende-zu-Ende-Sicherheit und Hop-by-Hop-Kommunikation angeboten
  - SIP wird bei Asterisk jedoch nur über UDP realisiert. Das schließt die Absicherung über TLS aus, da dies TCP voraussetzt.
  - Die fehlenden Sicherheitsmechanismen für SIP sollen über die nächste Generation des SIP-Channels (Version 3) nachgeholt werden, die jedoch noch über das Projekt „Pineapple“ in der Entwicklung sind (keine Rückwärtskompatibilität!)
  - Zur Hop-by-Hop-Absicherung gehören TLS und IPsec und zur Ende-zu-Ende-Absicherung zählen SIP-Digest-Authentication und S/MIME
  - S/MIME ist im RFC-3261 allerdings nur optional definiert.
  - Aktuell wird Version 1 eingesetzt. Version 2 hatte nur Patch-Level-Status und wird nicht mehr weiter entwickelt

© DECOIT GmbH

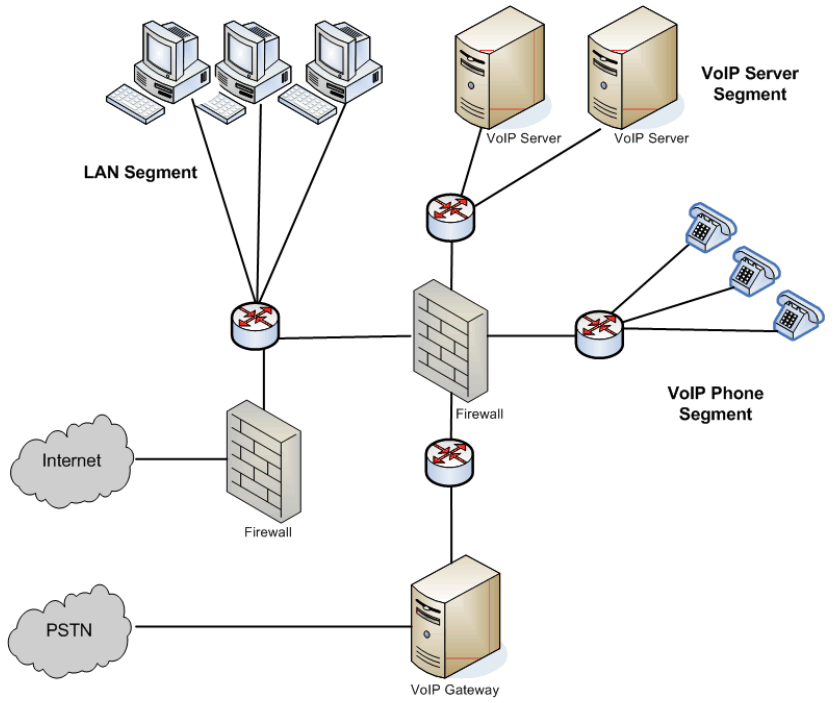
Bewertungen und Auswirkungen (3)

- IAX2
  - Es handelt sich bei IAX2 (im Gegensatz zu SIP) nicht um ein textbasiertes, sondern Binärprotokoll
  - IAX kann zur Kommunikation zwischen Asterisk-Servern eingesetzt werden oder um Gespräche zu initialisieren und Sprachdaten zu übertragen
  - Dafür werden einige Sicherheitsmechanismen zur Verfügung gestellt
  - Asterisk-Server können sich gegenseitig über eine PKI authentifizieren
  - Dazu findet ein RSA- oder alternativ ein Diffie-Hellman-Schlüsselaustausch statt
  - Zur Verschlüsselung der Nachrichten wird hier AES mit 128 Bit verwendet
  - Da IAX2 für den Verbindungsaufbau nur einen UDP Port (4569) benötigt, muss auch nur dieser Port in der Firewall geöffnet werden
  - Da die IP-Endgeräte heute bis auf Ausnahmen kein IAX2 unterstützen, muss auf die Sicherheitsmechanismen in der SIP-Spezifikation und SRTP ebenfalls zurückgegriffen werden

© DECOIT GmbH

Einsatz von Firewalls und VLANs

- IAX2 sollte zwischen Standorten zum Einsatz kommen (Verschlüsselung und Kompression)
- Separation des Daten- und des VoIP-Bereichs über VLANs
- Separate Abtrennung durch Firewalls
- Separate Subnetze für Daten und Sprache
- Einführung von Priorisierung auf den WAN-Strecken (Q-Tag, DiffServ)



© DECOIT GmbH

Risiken und Kompensationsverfahren

Risiken	Praxisansätze
Application Level Attacken	• Application Level Gateways, Firewalls und ISD/IPS
DoS/DDoS	• IDS/IPS • Aktuelle Patch-Levels • Anti-Virus-System • Policy-basierte Sicherheitszonen • VLAN
Abhören	• VPN zum isolieren von VoIP-Datenverkehr • Verschiedene Verschlüsselungen
Attacken gegen die Protokolle	• Application Level Gateways und IDS/IPS
SPIT	• Starke Authentifizierung, Autorisierung und IPsec
Nicht autorisiertes SIP-Monitoring und Spoofing	• Starke Authentifizierung, Autorisierung und IPsec

© DECOIT GmbH

Ausblick

- Das oftmals eingesetzte SIP-Protokoll kann ebenso nicht in allen in der Praxis anzutreffenden Formen als hinreichend sicher betrachtet werden. Es verfügt zwar über Sicherheitsmechanismen (bspw. Call-IDs auf der Basis von Hashes), bietet jedoch Angriffsmöglichkeiten für DoS-Attacken. Außerdem könnte das Phreaking mit VoIP sozusagen ein Revival erleben.
- Ein anderer sicherheitsrelevanter Bereich ist zwar nicht ausschließlich auf diese Technik begrenzt, wird jedoch durch die geringen Kosten, die für die Gespräche anfallen, begünstigt. So besteht die Möglichkeit einer Art von „VoIP-Spam“, auch SPIT („Spam over Internet Telephony“) genannt.
- Für sicheres VoIP muss daher momentan ein Campus-Szenario betrieben werden, aus dem heraus über ISDN kommuniziert wird.
- VoIP sollte hier als zusätzlicher IP-Dienst begriffen werden, der vom restlichen Netz separiert operiert.
- Zukünftig kann dann eine Anbindung an öffentliche VoIP-Provider vorgenommen werden, wenn die Signalisierungsstandards ein hohes Sicherheitsniveau übergreifend erreicht haben sowie Authentifizierung und Verschlüsselung auch von Providern angeboten werden

© DECOIT GmbH

Danke für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies

© DECOIT GmbH