[ARNWSt00] *Ralf Ackermann, Christoph Rensing, Stephan Noll-Husong, Lars Wolf, Ralf Steinmetz;* **SSS4it - Secure Session Setup für Internet-Telefonie;** Systemsicherheit 2000, Bremen, März 2000

SSS4it – Secure Session Setup für Internet–Telefonie

Ralf Ackermann[1], Christoph Rensing[1], Stephan Noll–Hussong[1], Lars Wolf[1], Ralf Steinmetz[1,2]

[1]Industrielle Prozeß– und Systemkommunikation
Fachbereich Elektrotechnik und Informationstechnik
Technische Universität Darmstadt
Merckstr. 25 • D–64283 Darmstadt
{Ralf.Ackermann, Christoph.Rensing, Stephan.Noll,
Lars.Wolf, Ralf.Steinmetz}
@KOM.tu–darmstadt.de

[2]GMD IPSI
Forschungszentrum Informationstechnik GmbH
Dolivostr. 15 • D–64293 Darmstadt

Zusammenfassung

Die Telefonie und Multimedia Konferenzen über das Internet befinden sich aktuell in einer Übergangsphase von einem eher experimentellen Betrieb hin zu einem regulär angebotenen Dienst. Mit diesem Übergang in eine kommerzielle Nutzung entsprechender Angebote wird die Gewährleistung sicherheitsrelevanter Funktionen immer bedeutsamer und zu einem in vielen Anwendungsbereichen unverzichtbaren Qualitätsmerkmal. Die notwendigen kryptographische Algorithmen existieren und entsprechende Sicherheitsinfrastrukturen befinden sich im Aufbau bzw. sind teilweise bereits etabliert. Zwar sehen einige vorhandene bzw. sich entwickelnde Standards für die Kommunikation in IP–basierten Netzen die Nutzung verschiedener kryptographischer Verfahren vor, jedoch sind diese für Internet–Telefonie–Anwendungen bisher kaum im Einsatz.

In diesem Beitrag stellen wir zunächst die Anforderungen an Sicherheitsmechanismen vor und zeigen auf, wie diese mit den bestehenden kryptographischen Verfahren erbracht werden können. Die Authentifizierung der Teilnehmer eines Gespräches während des Verbindungsaufbaues und die zur Sicherung der Vertraulichkeit des Gesprächsinhaltes notwendige Aushandlung eines nachfolgend gemeinsam genutzten symmetrischen Schlüssels kann dabei mittels eines asymmetrischen Verfahrens und unter Nutzung der Dienste einer Sicherheitsinfrastruktur erfolgen.

Als „leichtgewichtige" Umsetzung und Ergänzung zu den in der Standardisierung vorgeschlagenen meist komplexen Protokollen für den Verbindungsaufbau stellen wir das von uns entworfene und umgesetzte System Secure Session Setup für Internet–Telefonie (SSS4it) vor. Dieses wurde mit dem ausdrücklichen Ziel der Einbettung in einen flexiblen und erweiterbaren Rahmen verschiedener Sicherheits–Infrastrukturen konzipiert und realisiert.

Im Rahmen der prototypischen Umsetzung in einer Beispiel–Implementierung bildet es die Grundlage von weiteren Arbeiten zur Gewinnung von Anwendungserfahrungen und zum Vergleich der bei Einsatz unterschiedlicher Konzepte erreichbaren Signalisierungs–Verzögerungen und System–Performance. Nach einer Beschreibung des Protokolls und seiner Implementierung werden abschließend Einsatz–Implikationen sowie Anwendungs–Umgebungen und –Szenarien aufgezeigt.

1 Problemstellung

Internet–Telefonie und Multimedia Konferenzen über das Internet gewinnen zunehmend an Bedeutung. Große Telekommunikationsanbieter stellen mittlerweile in Pilotprojekten aber auch im regulären Angebot eine Vielzahl von entsprechenden Diensten zur Verfügung [DTAG99]. Diese Dienste und die darauf basierenden Anwendungen müssen durch Integration von Sicherheitsmechanismen abgesichert werden, weil sonst kein dem der klassischen Telefonie vergleichbarer Sicherheitsstandard erreicht werden kann.

Eine der wichtigsten Voraussetzungen für einen kommerziellen Einsatz der Internet–Telefonie ist die gegenseitige Authentifizierung der Gesprächsteilnehmer und beteiligten Infrastrukturkomponenten. Diese kann und sollte bereits im Rahmen der Signalisierung zum Gesprächsaufbau eingesetzt werden, ist sie doch unverzichtbare Basis für die verbindliche Abrechnung der Dienste. Heute werden in der Praxis vielfach noch Passwort– und PIN–Verfahren eingesetzt, was die Nutzbarkeit auf einen geschlossenen und vorab bekannten Anwenderkreis einschränkt.

Protokollstandards sehen alternativ die Nutzung von Public–Key–Verfahren unter Verwendung von Zertifizierungs–Infrastrukturen vor oder gehen von einem durch Mechanismen auf Netzwerk– (IP Security – IPSec) oder Transport– (Transport Layer Security – TLS) Schicht abgesicherten Übertragungskanal aus. Aufgrund der fehlenden durchgängigen Verbreitung dieser Verfahren ist ein solches Vorgehen jedoch derzeit und auch in absehbarer Zukunft nicht allgemein praktikabel.

Neben der Authentifizierung sind weitere Sicherheitsmechanismen für die verschiedenen Internet–Telefonie Szenarien notwendig. Diese sind ausführlich u. a. in [RAR99a] beschrieben. Zentrale und unmittelbar naheliegende Aufgabe ist die Gewährleistung der Vertraulichkeit der Audio– respektive Video–Inhalte. Diese kann aus Performancegründen bei dem in Echtzeit und mit der Forderung nach minimaler Verzögerung zu behandelnden Datenvolumen nur mittels eines symmetrischen Verfahrens realisiert werden. Der dazu notwendige Session–Schlüssel sollte während des Verbindungsaufbaues zwischen den Gesprächspartnern ausgetauscht oder ausgehandelt werden.

2 Sicherheitsmechanismen für die Internet–Telefonie

2.1 Betrachtete alternative Ansätze

2.1.1 MBone–Anwendungen als Ausgangs– und Vergleichs–Basis

Seit längerem wird das Internet für eine paketbasierte Sprachübertragung in Anwendungen im MBone (Multicast Backbone) genutzt [Kuma95][Paul98]. Typisch sind insbesondere Audiokonferenzen wie z. B. mit dem „Robust Audio Tool“ (rat) [SHK95], Videokonferenzen und zum computerunterstützten kooperativen Bearbeiten (CSCW) von Dokumenten benutzte Whiteboard–Anwendungen. Gemeinsam können diese die Dienste des „Session Directory

Tools" (sdr) [Hand96] zur Ankündigung von Konferenzen, zum Austausch von mittels des Session Description Protocols (SDP) [HJ98] beschriebenen Parametern und zum Programmstart verwenden.

Typische MBone–Anwendungen realisieren und nutzen Funktionen, die man auch in dedizierten Internet–Telefonie–Anwendungen benötigt. MBone–Multimedia–Konferenzen können daher durchaus als ein Spezialfall für die Audio–Kommunikation in paketbasierten Netzen betrachtet werden und somit unmittelbar Komponenten für Telefonie–Lösungen bereitstellen [APW99]. Ein solcher Ansatz wird von uns in der vorgestellten Arbeit benutzt.

2.1.2 Standardisierungsansatz der ITU

Kommerzielle interoperable IP–Telefonie Produkte nutzen heute zumeist die Protokolle der ITU Protokollfamilie H.323 [ITU98a]. H.323 definiert einen Rahmen für die Kommunikation in paketbasierten Netzen und Übergänge zu anderen Netzen. Die Signalisierung eines Gespräches wird im Protokoll H.225.0 beschrieben. H.245 und H.235 behandeln Call Control und sicherheitsrelevante Funktionen und stellen damit das H.323 Vergleichsbeispiel im von uns betrachteten Problembereich dar.

Das Protokoll benutzt mittels einer in Abstract Syntax Notation (ASN.1) beschriebene Protokoll–Daten–Elemente (PDU), die in nach Basic Encoding Rules (BER) kodiert werden. Die H.323 Signalisierung umfasst mehrere Schritte über verschiedene logische Verbindungen. Diese werden auf verschiedene physische Verbindungen abgebildet, deren Parameter nach einer initialen Kommunikation über einen standardisierten Port dynamisch ausgehandelt werden. Daraus ergeben sich zusätzliche Schwierigkeiten bei der Behandlung des Protokolls durch Firewall–Systeme.

In aktuellen Publikationen werden Komplexität, resultierender Kommunikations–Overhead beim Austausch einer Reihe von Ende zu Ende auszutauschenden Nachrichten und die daraus abgeleitete nicht zu vernachlässigende Verzögerung beim Verbindungsaufbau als kritisch betrachtet [DF99]. Insgesamt wird die Nutzung des H.323 Protokolls zum durchgehenden Einsatz für die Internet–Telefonie im globalen Rahmen überaus kontrovers diskutiert.

2.1.3 Standardisierungsansatz der IETF

Innerhalb der IETF beschäftigen sich verschiedene Arbeitsgruppen mit der Standardisierung von Protokollen für die Übertragung von Multimedia–Daten und die Internet–Telefonie. So entstand ein Protokollstack, der umfassend z. B. in [SR98] beschrieben ist.

Für die Signalisierung von Gesprächen wird das Session Initiation Protocol SIP [HSSR99] genutzt. SIP unterstützt den Aufbau, die Steuerung und das Beenden von Multimedia–Sitzungen. Es zeichnet sich durch seine Einfachheit, Textbasiertheit und Erweiterbarkeit aus. Beim Verbindungsaufbau beschränkt es sich, da es unter der Prämisse eines Einsatzes auch in großen, weltweiten Szenarien konzipiert und standardisiert wurde, bewußt auf ein Minimum von Ende–zu–Ende auszutauschenden Protokoll–Nachrichten.

Zur Identifizierung von Benutzern und Infrastruktur–Komponenten unterstützt SIP als Abstraktionsstufe Distinguished Names, die einen einer Email–Adresse ähnlichen Aufbau besitzen. Diese symbolischen Distinguished Names werden unter Nutzung von Verzeichnis–Diensten in eine IP–Adresse übersetzt. Die Lokalisierung von Teilnehmern kann sowohl unter Nutzung von Proxy– als auch von Redirect–Servern erfolgen.

Die Übertragung der Nutzdaten ist nicht Inhalt des die Signalisierung beschreibenden SIP Standards, diese Daten werden analog zum Vorgehen beim H.323 Protokoll unter Nutzung des Realtime Transport Protocols (RTP) [SCFJ96] weitergeleitet.

2.2 Protokoll–Komponenten mit explizitem Sicherheitsbezug

Für die kommerzielle Internet–Telefonie ist die Authentifizierung der Gesprächsteilnehmer im Rahmen des Verbindungsaufbaus eine wesentliche Voraussetzung. Daher betrachten wir diesen Aspekt am Beispiel der drei ausgewählten Bereiche MBone–Anwendungen, H.323 und SIP an dieser Stelle detaillierter.

In MBone–Szenarien erfolgt die Ankündigung von Konferenzen i. d. R. mittels des Session Directory Tools sdr. Dieses diente ursprünglich nur zur Ankündigung öffentlicher Konferenzen und verfügt daher zunächst über keine Mechanismen zur Gewährleistung von Vertraulichkeit. Seit der Version 2.5 sind allerdings Sicherheitsmechanismen integriert. So können Ankündigungen mittels des Data Encryption Standards (DES) oder der Mechanismen des Programmsystems Pretty Good Privacy (PGP) verschlüsselt werden und eine Authentifizierung ist mit Hilfe von PGP– oder X.509–Zertifikaten möglich. Das Erzeugen von Schlüsselpaaren und die Abfrage bzw. Validierung von öffentlichen Schlüsseln wird von SDR jedoch weiterhin nicht unterstützt und muss unabhängig vom Programm mit Out–of–Band Mechanismen vorab erfolgen.

Innerhalb der H.323 Protokollfamilie existiert der Standard H.235 [ITU98b], der Sicherheitsoptionen für Terminals und Kommunikation in H.323 definiert. H.235 hat primär die Sicherheitsaspekte Authentifizierung der Teilnehmer und Sicherung der Vertraulichkeit der Multimedia–Datenströme zum Gegenstand. Die Verbindlichkeit der Kommunikation wird nicht berücksichtigt. Neben der Sicherung der Multimedia–Datenströme werden auch die Sicherung der Kontrolldaten in H.225 und H.245 behandelt.

H.235 gibt dabei keine Implementierungsrichtlinien an und sieht an vielen Stellen die Verwendung alternativer kryptographischer Verfahren verschiedener Stärke vor. So kann nach H.235 die Gesprächssignalisierung in H.225.0 eine Authentifizierung unter Verwendung von Hash–Funktionen mit einem gemeinsamen Geheimnis und digitale Signaturen enthalten. Ebenso kann während des Verbindungsaufbaues mittels des Diffie–Hellman Verfahrens ein Session–Schlüssel ausgetauscht werden. Soll der gesamte Verbindungsaufbau vertraulich erfolgen, sieht H.235 auch die Verwendung einer mittels IPSec oder TLS gesicherten Transportverbindung vor.

Beim Session Initiation Protocol SIP erfolgt die Signalisierung über den Austausch von Request– und Response–Nachrichten. Der Standard definiert als Basismechanismus für die Gewährleistung der Vertraulichkeit dieser Nachrichten eine PGP basierte Verschlüsselung ausgewählter Felder des Nachrichten–Kopfes (Header) und des gesamten Nachrichten–Körpers (Body). Dazu müssen die PGP–Mechanismen von SIP basierten Implementierungen unterstützt werden.

Zur Authentifizierung der Nachrichten sieht das Protokoll die in HTTP verwendeten Mechanismen vor [FHHL98]. Alternativ kann in einem Header Feld eine digitale Signatur der Nachricht eingefügt werden. Damit kann zusätzlich zur Authentifizierung die Integrität der Nachricht gewährleistet werden. SIP definiert bisher nicht verbindlich, welches Schema für die Digitale Signatur genutzt werden soll, beschreibt aber den genauen Ablauf bei der Verwendung von PGP Mechanismen.

2.3 Beurteilung der betrachteten Mechanismen, Standards und Implementierungen

Die von uns im Vorfeld der eigenen Entwicklungen betrachteten Mechanismen, Standards und Anwendungen sind mit einer Reihe von Nachteilen oder zu hinterfragenden Eigenschaften behaftet.

So sind sie im Fall der MBone–Szenarien nicht erschöpfend und in den vorhandenen Implementierungen nur marginal umgesetzt. Die H.323 Protokollfamilie ist komplex und mit einem nicht zu unterschätzenden und in vielen Szenarien nicht benötigten Overhead behaftet. Für SIP existieren trotz eines zunehmenden Engagements nicht nur von Forschungsinstitutionen, sondern auch von potenten Industriepartnern [Nels99] bisher nur sehr begrenzt praktische und allgemein nutzbare Implementierungen, mit denen weitere Erfahrungen gewonnen werden können.

Die Sicherheitsmechanismen sind in den Standards nur optional verankert und beeinträchtigen bei ihrem Fehlen nicht unmittelbar den primären Einsatzzweck zur Audio–Kommunikation, was dazu führt, dass sie in bisherigen praktischen Realisierungen kaum unterstützt werden. Diese Optionalität führt zu zusätzlichen Interoperabilitäts–Problemen. Nicht zuletzt ist eine fehlende Integration in Sicherheitsinfrastrukturen als Nachteil festzustellen. Wünschenswert und gerade im Fall von H.323 nicht gegeben, ist weiterhin die Möglichkeit, vorhandene Applikationen zum Transfer der Audiodaten in ein entsprechendes Signalisierungs–Framework einzufügen und diese damit für die IP–Telefonie nutzbar zu machen, auch wenn sie zunächst nicht für diese vorgesehen waren.

Aus der Erfahrung heraus, dass einfache Lösungen – die zunächst durchaus nicht alle Probleme gleichzeitig zu behandeln versuchen – vielfach sehr leistungsfähige und evolutionäre Anwendungen ermöglichen, entwarfen und untersuchten wir als Alternative das Secure Session Setup Protokoll. Dieses erfolgte insbesondere mit dem Ziel der Schaffung einer Basis für vergleichende Untersuchungen der Anbindung alternativer Sicherheitsinfrastrukturen, kryptographischer und Zugriffs–Verfahren. Die Spezifika der vorhandenen Protokolle wurden dabei in unserer Entwicklung explizit beachtet und übernommen, wo dies sinnvoll war.

3 SSS4it – Secure Session Setup

SSS4it ist ein System, dass zum Aufbau einer vertraulichen Kommunikation dient. Es kombiniert einen Schlüsselaustausch nach einem Hybrid–Verfahren mit einer in einer wahlweise zu startenden Kommunikationsanwendung vorhandenen und genutzen symmetrischen Verschlüsselungsfunktion.

Das System bildet ein Framework, welches die Einbettung unterschiedlicher Anwendungen für den Versand der Audio–Nutzdaten und die Anbindung unterschiedlicher Mechanismen zum Zugriff auf öffentliche Schlüssel und Zertifikate gestattet. Dabei kam in der erfolgten Referenz–Implementierung Secude [Secu99] als Public–Key–Infrastruktur zum Einsatz.

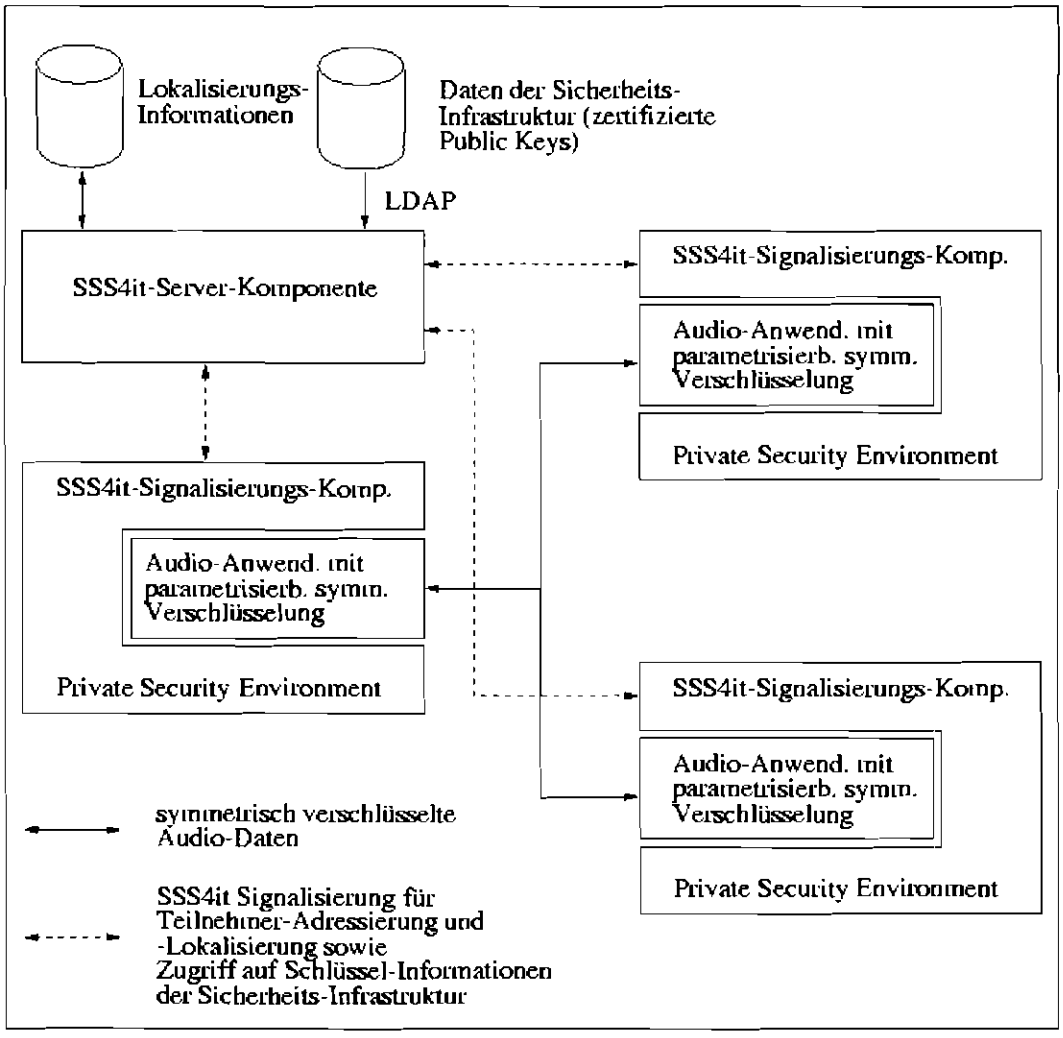

Abb. 1: Systemarchitektur und Zusammenwirken der Systemkomponenten

Protokollelemente und Ablauf des Secure Session Setup Protokolls für Internet–Telefonie (SSS4it) orientieren sich am Session Initiation Protokoll SIP. Es wurde jedoch nur eine Untermenge der dortigen Protokollsemantik realisiert. Zusätzlich erfolgte eine Erweiterung zur – bei SIP nicht vorgesehenen – Unterstützung von IP–Multicast zum Austausch von Nachrichten zwischen den Kommunikationspartnern.

Die Signalisierung im Unicast–Fall erfolgt mit aktionsbeschreibenden (INVITE–, REGISTER, QUERY), OK– und ACK–Nachrichten, die zwischen den Kommunikations–Endpunkten nach dem Client–Server–Prinzip ausgetauscht werden. Kommunikations–Endpunkte können dabei sowohl den Audio–Anwendungen unmittelbar zugeordnete als auch zentrale zur Namens– und Lokalisierungs–Auflösung bzw. zur mittelbaren Kommunikation mit der Sicherheits–Infrastruktur genutzte SSS4it–Komponenten sein.

Alternativ zu einer Unicast–Kommunikation ist auch der Versand von Signalisierungs–Meldungen innerhalb einer zu diesem Zweck vordefinierten und reservierten Multicast–Gruppe möglich. Dieses Vorgehen erlaubt in lokalen Umgebungen einen einfachen und von zentralen Instanzen unabhängigen Verbindungsaufbau sowie die Initiierung von Multiparty–Konferenzen.

3.1 Format der Signalisierungs–Nachrichten

Das im Rahmen unserer Implementierung verwendete Nachrichten–Format ist nachfolgend gezeigt. Dieses wird als Nutzdaten–Anteil eines Unicast– bzw. Multicast UDP–Paketes transportiert.

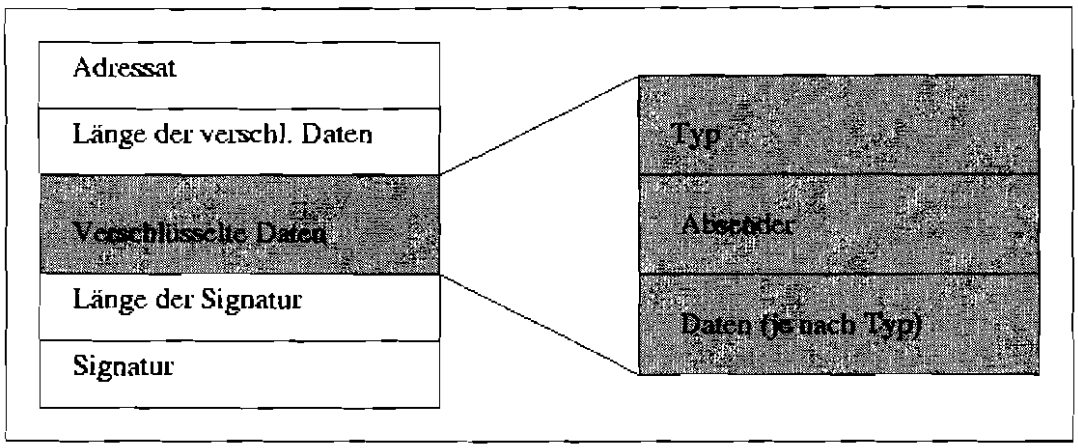

Abb. 2: Aufbau eines SSS4it–Packets

Im Adressat–Feld steht der DName des Benutzers, für den die Nachricht bestimmt ist, im ASCII–Format. Anhand dieses Feldes kann jeder Empfänger der Nachricht feststellen, ob diese an ihn gerichtet ist. Für das Adressat–Feld ist eine konstante Länge vorgesehen. Dadurch kann die genannte Auswertung schnell vollzogen werden.

Im darauffolgenden Feld ist die Länge des unmittelbar anschließenden Blocks verschlüsselter Daten verzeichnet. Die sowohl über den unverschlüsselten als auch den verschlüsselten Teil der Nutzdaten gebildete Signatur des Absenders schließt die Nachricht ab.

Dadurch, dass die für den Verbindungsaufbau relevanten Daten mit dem öffentlichen Schlüssel des Adressaten verschlüsselt sind, wird die Integrität der übertragenen Daten sichergestellt. Mittels der Signatur kann der Adressat die Authentizität des Absenders überprüfen. Damit werden gleichzeitig Veränderungen im Adressat–Feld oder an anderen Stelle der Nachricht durch eine ungültige Signatur erkennbar.

Das Typ–Feld gibt die Art der Nachricht an – dabei sind analog zu SIP alternativ die Typen INVITE, REGISTER, OK oder ACK möglich. Mit einer INVITE–Message teilt ein Sender dem Adressaten seinen Wunsch mit, in einer gemeinsamen Sitzung zu kommunizieren. Gleichzeitig werden die Session–Parameter transportiert. Diese Semantik entspricht der gleichlautenden SIP–Methode. Eine OK–Message entspricht einer SIP–Antwort mit Statuscode 2xx. Damit signalisiert der Angerufene dem Anrufer, dass er bereit und in der Lage ist, die Sitzung mit den angegebenen Parametern anzunehmen. Der Typ ACK dient zur Bestätigung der OK–Message. Nachdem die Kommunikationssequenz in dieser Reihenfolge abgelaufen ist, kann die gesicherte Übertragung der eigentlichen Nutzdaten beginnen. Der Typ QUERY wurde zusätzlich aufgenommen, um den Klienten die Abfrage von Informationen unter Nutzung der zentralen SSS4it–Komponente zu ermöglichen, die dazu das zu realisierende Interface nur einmal für das Gesamtsystem anbieten muss.

Die weiteren Felder in den verschlüsselten Daten beinhalten den DName des Absenders und weitere, vom Nachrichtentyp abhängige Parameter. Im Fall einer INVITE–Message sind das die von der Kommunikationsanwendung zu benutzende Zieladresse bzw. Multicastgruppe und der entsprechende Port. Eine OK–Message erfordert keine weiteren Parameter und mit

der ACK–Message wird schließlich der von den Kommunikationsteilnehmern zu benutzende Session–Schlüssel übertragen.

3.2 Adressierung und Lokalisierung der Gesprächsteilnehmer

Um eine Multimediasitzung zu initiieren oder sich zu einer bestehenden anzumelden, müssen alle Teilnehmer bestimmte Parameter wie z. B. die Adresse des Kommunikationspartners (oder eine gemeinsam genutzte Multicast–Adresse), Portnummern, die Art der zu verwendenden Medien und die Kodierungs–Vorschrift sowie Parameter für diese kennen.

Die Lokalisierung der Anwender erfolgt nicht unmittelbar über Rechneradressen, sondern mittels einer Indirektion über symbolische Namen. Es kommen Distinguished Names (Dnames) zum Einsatz, die eine eindeutige Personenbezeichnung ermöglichen. Durch die Integration der Komponente zur Namensauflösung und Lokalisierung ist ein Anwender in seiner Mobilität ungebunden. Die Verwendung von Distinguished Names erleichtert sowohl die Interaktion mit Verzeichnisdiensten wie X.500 als auch die Einbindung in X.509 basierte Sicherheits–Infrastrukturen.

Die SSS4it Implementierung sieht sowohl das von einem Nutzer mit Protokollmitteln (REGISTER–Nachricht) selbst ausgelöste Registrieren bei der Namens– und Lokalisierungs–Datenbasis als auch deren Manipulation über ein WWW–Interface sowie die zentrale statische Verwaltung vergleichbar zum Vorgehen bei einer konventionellen Telefon–Vermittlung vor.

3.3 Zugriff auf kryptographische Schlüssel

Zu einer erfolgreichen Telefonie–Gesprächsinitiierung ist es notwendig, dass während des Gesprächsaufbaus der sichere Austausch des für die eigentliche Kommunikation benötigten Session Keys und die eindeutige Identifizierung der Kommunikationspartner erfolgt. Der eine Kommunikationsbeziehung initiierende Partner erzeugt einen Session–Schlüssel für die Verschlüsselung der Audio–Datenströme. Dieser Session–Schlüssel wird innerhalb der Nutzdaten der INVITE–Message vertraulich an den Adressaten oder bei Verwendung von IP–Multicast an die Adressaten versandt.

Zur Verschlüsselung der Daten der Kontrollnachricht benötigt der Sender den öffentlichen Schlüssel des oder der Adressaten. Ist dieser nicht in seinem lokalen Private Security Environment (PSE) gespeichert, nutzt unsere Implementierung den Abruf einer zertifizierten Schlüsselinformation des Adressaten per Lightweight Directory Access Protocol (LDAP). Die Information wird von den Teilnehmern in einer QUERY–Message angefragt.

Der Session–Schlüssel wird nachfolgend als Verschlüsselungs–Parameter beim Start der entsprechenden Kommunikations–Anwendung (z.B. rat) verwendet. Die Einbindung anderer Kommunikations–Anwendungen, die eine Parametrisierung auf Kommandozeilen–Ebene oder durch Setzen und Auslesen von Umgebungsvariablen ermöglichen, ist unmittelbar möglich und durch Eintrag in eine Konfigurationsdatei bei den Klienten steuerbar.

4 Implementierung und Anwendung

4.1 Nutzung einer Sicherheits–Infrastruktur auf Basis von Secude

Im Rahmen der praktischen Umsetzung unseres Ansatzes wurde aus Gründen der freien Verfügbarkeit und des umfassenden Funktionsumfanges das SECUDE (Security Development Environment) Security Toolkit eingesetzt. SECUDE enthält eine in C geschriebene Befehlsbibliothek und ist unter verschiedenen Betriebssystemen lauffähig, wobei in der vorliegenden Realisierung SECUDE 5.1.8c in den Versionen für Linux und Win32 (Windows95, Windows98, Windows NT) zum Einsatz kommt.

SECUDE bietet verschiedene APIs zur Anwendung in speziellen Bereichen der Kryptographie und zur Kompatibilität mit bestehenden Standards. Von besonderer Bedeutung sind für den realisierten Einsatz die Funktionen des Authentication Frameworks.

Diese stellen eine Schnittstelle zum Umgang mit Zertifikaten nach dem X.509 Standard zur Verfügung. Es können sowohl lokale Zertifikate, die in der PSE (Personal Security Environment) gespeichert sind, als auch Zertifikate aus einem Verzeichnisdienst verwendet werden. Auf die Zertifikate können die Teilnehmer mittelbar über eine zentrale SSS4it–Instanz per LDAP oder AF–DB, einem speziellen für verteilte Datenbanken geeigneten Format von Secude für Zertifikate, zugreifen. Es wird also nicht voruasgesetzt, dass diese direkt bei ihnen vorliegen. Damit wird auch der für Internet–Telefonie–Anwendungen als Mehrwertdienst betrachtete Aspekt der persönlichen Mobilität mit Möglichkeit des individuellen und in unserem Szenario auch gesicherten Gesprächsaufbaus von einem beliebigen Endgerät aus unterstützt.

4.2 Anwendungs–Szenario

Das Protokoll wurde in dem in Abbildung 3 gezeigten Anwendungsszenario eingesetzt, bei dem MBone–Konferenz–Anwendungen mit Gateways zur Kopplung von konventionellem und IP–basierten Telefonnetz zu einer Virtuellen PBX kombiniert werden.

Dieses bewusst im lokalen Umfeld angesiedelte Szenario besitzt aufgrund der Nutzung eines in der Regel allgemein zugreifbaren Übertragungsmediums und der für alle Klienten vorhandenen Möglichkeit, sich einer der zur Audio–Daten zugeordneten Multicast–Gruppen zu subscriben, unmittelbar naheliegende Sicherheitsanforderungen.

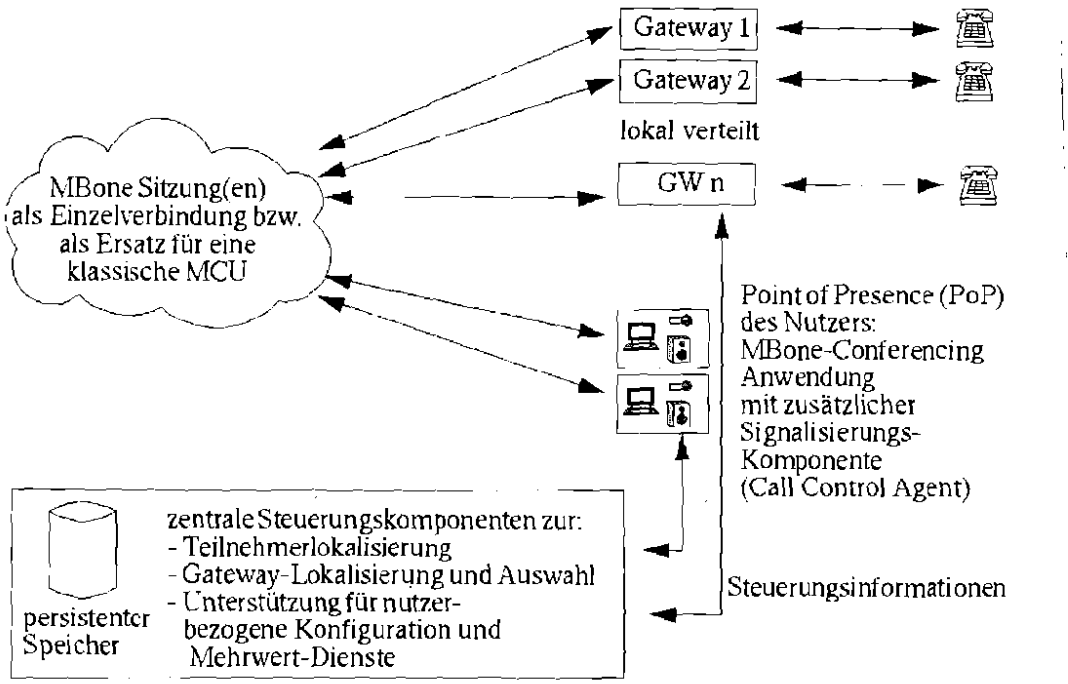

Abb. 3: Einsatz von SSS4it – eine Virtuelle PBX in einer lokalen Umgebung

Ausserdem erlaubt es den durchgängigen Einsatz von IP–Multicast–Mechanismen, die in größeren heterogenen Netzen nicht grundsätzlich vorausgesetzt werden können, und muss sich aufgrund einer limitierten Teilnehmerzahl nicht unmittelbar mit Skalierungsaspekten befassen. Der Einsatz des Protokolls in anderen Szenarien wird von uns aktuell untersucht.

4.3 Ausblick

Das beschriebene System stellt einen exemplarischen Ansatz zur Einbettung der sich mit hoher Dynamik entwickelnden IP–Telefonie–Technologie in Sicherheits–Infrastrukturen dar.

Einen wichtigen Teil der weiteren Untersuchungen bildet die Bewertung des Protokolls hinsichtlich seiner Skalierbarkeit und Eignung in größerem Rahmen. Dazu liegen Messungen hinsichtlich des Kommunikationsaufwandes und der resultierenden Sitzungs–Aufbauzeiten vor [RAR99b]. Die Protokoll–Implementierung und die zur Umsetzung des von uns beschriebenen Einsatzszenarios benötigten weiteren Software–Komponenten stehen für Test und Weiterentwicklung frei zur Verfügung.

Literatur

[APW99] R. Ackermann, J. Pommnitz, L. Wolf, R. Steinmetz: Eine Verteilte PBX, 1. GI–Workshop „Multicast – Protokolle und Anwendungen", Braunschweig, 20.–21. Mai 1999, S. 187–197

[DF99] I. Dalgic, H. Fang: Comparison of H.323 and SIP for IP Telephony Signaling, Proc. of Photonics East, Boston, Massachusetts, September 20–22, 1999

[DTAG99] Deutsche Telekom AG, freecall Online – Telefonieren aus dem Internet, http://www.dtag.de/angebot/freecallOnline/, 1999

[FHHL98] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP authentication: Basic and digest access authentication", Internet Draft, Internet Engineering Task Force, Work in Progress, Sept. 1998

[Hand96] M. Handley: The sdr Session Directory: An MBone Conference Scheduling and Booking System, Department of Computer Science University College London Draft 1.1, 1996, http://www-mice.cs.ucl.ac.uk/mice-nsc/tools/sdr.html

[ITU98a] ITU-T Recommendation H.323 V.2 "Packet-Based Multimedia Communication Systems", Genf, 1998

[ITU98b] ITU-T Draft Recommendation H.235 "Security and Encryption for H. Series (H.323 and other H.245 based) Multimedia Terminals", Genf, 1998

[Kuma95] V. Kumar: MBone: Interactive Multimedia on the Internet, Macimilian Publishing, November 1995

[Nels99] J. Nelson: SIP – Ready to Deploy, FALL Voice on the Net (VON), Atlanta, Georgia, September 28, 1999

[Paul98] S. Paul: Multicasting on the Internet and its Applications, Kluwer Academic Publishers, Boston, 1998

[RAR99a] C. Rensing, R. Ackermann, U. Roedig, L. Wolf, R. Steinmetz: Sicherheitsunterstützung für Internet Telefonie, Sicherheitsinfrastrukturen, Vieweg, Braunschweig, Wiesbaden, 1999, S. 285-296

[RAR99b] C. Rensing, R. Ackermann, U. Roedig, R. Steinmetz: SSS4it – Implementierung und Performance-Messung, TU Darmstadt, Technical Report TR-KOM-1999-05, Industrielle Prozeß- und Systemkommunikation, 1999

[Secu99] SECUDE: http://www.secude.de

[HJ98] M. Handley, V. Jacobson, RFC 2327: SDP: Session Description Protocol.. April 1998

[HSSR99] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, RFC 2543 SIP: Session Initiation Protocol, March 1999

[SCFJ96] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, RFC 1889 RTP: A Transport Protocol for Real-Time Applications, January 1996

[SHK95] A. Sasse, V. Hardman, I. Kouvelas, C. Perkins, O. Hodson, A. Watson, M. Handley, J. Crowcroft, D. Harris, A. Bouch, M. Iken, K. Hasler, S. Varakliotis, D. Miras: Rat, 1995, http://www-mice.cs.ucl.ac.uk/multimedia/software/rat/

[SR98] H. Schulzrinne, J. Rosenberg: Internet Telephony: Architecture and Protocols – an IETF-Perspective, 1998