[Sch07-2] *Johannes Schmitt, Thomas Hecker, Matthias Hollick, Ralf Steinmetz;* **Dynamische Authentifizierung für Provider-übergreifende VoIP-Kommunikation.** In: PIK - Praxis der Informationsverarbeitung und Kommunikation, vol. 04, no. 07, p. 191-198, December 2007. ISSN 0930-5157.

Dynamische Authentifizierung für Provider-übergreifende VoIP-Kommunikation

Johannes Schmitt, Thomas Hecker, Matthias Hollick und Ralf Steinmetz
Fachbereich Multimedia Kommunikation (KOM)
Technische Universität Darmstadt
Merckstr. 25, D-64283 Darmstadt
Telefon: +49 (0) 6151 164451
Fax: +49 (0) 6151 166152
Email: {johannes.schmitt,thomas.hecker,matthias.hollick,ralf.steinmetz}@KOM.tu-darmstadt.de

Zusammenfassung

Voice over IP (VoIP) ermöglicht, dass Netzbetreiber eine einzig auf Internet Technologie basierte, konvergierte Infrastruktur betreiben können. Trotz standardisierter Protokolle ist die Provider-übergreifende VoIP-Kommunikation jedoch bisher nicht weit verbreitet; nicht zuletzt aufgrund offener Sicherheitsfragen. In dieser Arbeit wird ein Ansatz vorgestellt, der es ermöglicht, Anrufe über verschiedene VoIP-Netze hinweg zu authentifizieren. Durch eine Erweiterung des ENUM-Dienstes können dynamische Vertrauensbeziehungen zwischen VoIP-Inseln hergestellt werden, wodurch Interoperabilität ermöglicht wird. Dazu werden innerhalb von ENUM-Domains öffentliche Schlüssel hinterlegt, die über die Telefonnummer mit einem Teilnehmer verknüpft sind. Mit diesem Schlüssel lassen sich Signalisierungs-Nachrichten verifizieren, die der Teilnehmer zuvor mit seinem privaten Schlüssel signiert hat. Somit lassen sich VoIP-Anrufe eindeutig mit einer Festnetznummer verbinden. Der vorgeschlagene Lösungsansatz kann auf Basis existierender Infrastruktur-Komponenten implementiert werden und ist hochskalierbar. Die Machbarkeit wurde im Rahmen einer prototypischen Implementierung auf Basis der VoIP Software Lösung Asterisk gezeigt.

I. Einleitung

Internettelefonie (VoIP) findet zunehmend Verbreitung im privaten und kommerziellen Umfeld. Durch die verschiedenen Einsatzbereiche entstehen unterschiedliche Formen von VoIP-Strukturen. VoIP-Teilnehmer können beispielsweise (wie bei Firmen üblich) über ein separates LAN oder (wie in der Regel bei Privatpersonen) über das Internet mit ihren VoIP-Providern verbunden sein. Da eine Interoperabilität zwischen VoIP-Providern in der Regel nicht möglich ist, bilden sich Inseln von Providern mit ihren Teilnehmern, die zueinander nicht in direkter Verbindung stehen. Die existierende VoIP-Landschaft besteht aus zahlreichen separaten Inseln dieser Art, die von Firmen oder Privatpersonen betrieben werden. Ein Teilnehmer kann damit zwar innerhalb seiner VoIP-Insel über das Internet telefonieren, nicht aber, wenn das Gespräch zwischen Teilnehmern verschiedener Inseln stattfinden soll. Obwohl auch hier eine reine VoIP-Verbindung technisch möglich und vorteilhaft wäre, wird das Gespräch über das Festnetz (Public Switched Telephone Network - PSTN) geleitet.

Eine entscheidende Ursache hierfür liegt im Fehlen von Vertrauensbeziehungen zwischen den VoIP-Inseln. Teilnehmer oder Betreiber eines VoIP-Netzes haben nur eingeschränkte Möglichkeiten, die Identität von Anrufern zu ermitteln, die nicht der gleichen VoIP-Insel angehören. Da davon auszugehen ist, dass diese Anonymität zu unerwünschten Anrufen und „Spam over Internet Telephony" (SPIT) führen wird, werden externe Anrufe aus fremden VoIP-Netzen in der Regel nicht zugelassen.

A. Szenario

Abbildung 1 veranschaulicht ein Beispielszenario zur Motivation unserer Arbeit. Es sind zwei Teilnehmer dargestellt, die per VoIP auf Basis des Session Initiation Protocol (SIP) erreichbar sind. Teilnehmer *A* ist Kunde des VoIP-Anbieters *Provider1* und besitzt die SIP-Adresse *123@provider1.de*. Teilnehmer *B* ist Kunde des VoIP-Anbieters *Provider2* und besitzt die SIP-Adresse *456@provider2.de*; zusätzlich ist Teilnehmer B Kunde eines herkömmlichen Telefonanbieters und somit unter der Rufnummer *+49 6151 16456* an das PSTN angeschlossen. Beide VoIP-Provider betreiben Gateways, die Anrufe ihrer Kunden in das PSTN oder umgekehrt die Erreichbarkeit aus dem PSTN ermöglichen. Möchte Teilnehmer *A* anhand der Rufnummer von Teilnehmer *B* einen Anruf zu diesem aufbauen, wird die Verbindung in der Regel über das Gateway von *Provider1* hergestellt. D.h. der Anruf wird bis zum Gateway über VoIP geführt und anschließend über das gewöhnliche Telefonnetz zu Teilnehmer *B* durchgestellt. Wenn Teilnehmer *A* die SIP-Adresse von *B* kennt oder *Provider1* beim Anrufaufbau mit Hilfe von einem Verzeichnis-Dienst wie ENUM (siehe Abschnitt II) anhand der gewählten Rufnummer eine SIP-Adresse zuordnen kann, ist es sinnvoller, den Anruf über das Internet herzustellen.

Problematisch wird jedoch das Durchstellen des SIP-Anrufs von *Provider1* in das Netz von *Provider2*. SIP-Anrufe von einer unbekannten Herkunft durchzustellen bedeutet nichts anderes als anonyme Anrufe durchzustellen. Um die Kunden vor unerwünschten (Werbe-)Anrufen schützen zu können, werden daher von den VoIP-Providern in der Regel keine externen Verbindungsversuche aus dem Internet zugelassen. Daher ist eine reine VoIP-Verbindung über Provider-Grenzen hinweg meist nicht möglich.

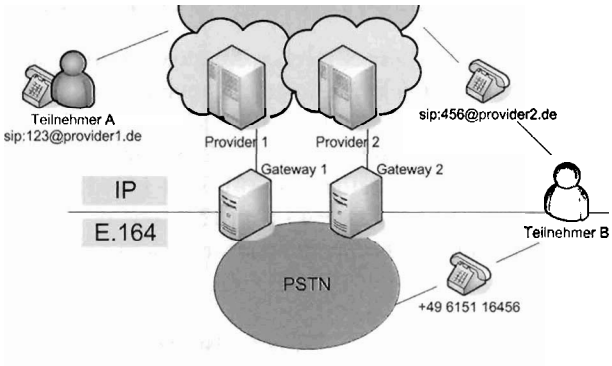

Abb. 1: Beispielszenario

B. Problemstellung

Einige VoIP-Provider ermöglichen ihren Kunden dennoch, untereinander Provider-übergreifend kostenfrei zu telefonieren. Sie identifizieren dazu Gespräche aus dem jeweiligen Partnernetz und stellen diese zum Teilnehmer durch. Dieses Identifizieren der Herkunft eines Anrufs erfordert Vertrauensbeziehungen zwischen den Providern. Unabhängig von Art und Umfang der Vertrauensbeziehungen, sie müssen jeweils zwischen allen VoIP-Inseln separat geschaffen werden. Bei n Inseln muss jede dieser Inseln $n-1$ Vertrauensbeziehungen eingehen. Insgesamt müssen $m = (n^2-n)/2$ Vertrauensbeziehungen geschaffen werden. Diese statischen Vertrauensbeziehungen haben daher drei große Nachteile:

- Hoher Aufwand: Sie müssen auf nicht-technischer Ebene geschaffen werden.
- Schlechte Skalierung: Sie müssen zwischen jedem Kommunikationspartner separat bestehen.
- Schlechte Dynamik: Neue Kommunikationspartner können nicht dynamisch in das System integriert werden.

In Folge dessen sind häufig keine Provider-übergreifenden Gespräche ohne Routing durch das PSTN möglich. Um externe Verbindungsaufforderungen in eine VoIP-Insel durchzustellen, müssen diese in geeigneter Weise identifizierbar sein. Durch Anrufer-Authentifizierung kann eine dynamische Vertrauensbeziehung hergestellt werden und damit die notwendige Sicherheit erreicht werden.

C. Gliederung und eigener Beitrag

In dieser Arbeit werden ein neuer Ansatz und dessen Umsetzung vorgestellt, um die in der Problemstellung erörterten Herausforderungen elegant zu lösen. Da dieser Ansatz auf dem Verzeichnis-Dienst ENUM basiert, wird dessen Funktionsweise zunächst im folgenden Abschnitt erläutert. Wir schlagen eine erweiterte Nutzung des ENUM-Dienstes zur dynamischen Authentifizierung von Anrufen und damit zur Verbindung von VoIP Inseln vor. Die genaue Funktionsweise dieses Ansatzes wird in Abschnitt III beschrieben.

ENUM stellt eine erweiterte Form des DNS Systems dar. Um ENUM als Grundlage für das Keymanagement heranzuziehen, ohne den laufenden Betrieb zu beeinträchtigen, gilt es daher eine Reihe von DNS-spezifischen Aspekten zu berücksichtigenden. Deren Beschreibung, sowie die für die Umsetzung getroffenen Entscheidungen sind in Abschnitt IV aufgezeigt.

Die Umsetzung des Ansatzes hat zum Ziel, ohne Änderungen an bestehender Hardware oder an beteiligen VoIP-Infrastruktur-Elementen (abwärtskompatibel) integrierbar zu sein. Die Beschreibung der durchgeführten Umsetzung zur Evaluation des Ansatzes und deren Ergebnisse folgt in Abschnitt V. Abschließend werden in Abschnitt VI die verwandten Arbeiten zu diesem Thema aufgezeigt und in Abschnitt VII eine Zusammenfassung gegeben.

II. ENUM

Die ITU-T definierte unter E.164 das Format international verwendeter Telefonnummern. Diesen Namensraum, in dem die verschiedenen Teilnehmer des PSTN adressiert werden, bilden eindeutige, max. 15 stellige Nummern. Mit t**E**lephone **NU**mber **M**apping (ENUM [Fal00]) besteht die Möglichkeit, den E.164 Namensraum in den Domain Name System (DNS) Namensraum umzusetzen (in Abbildung 2 ist ein DNS-Eintrag für die Nummer +49615116456 exemplarisch dargestellt).

ENUM ist im Prinzip eine erweiterte Form des bestehenden DNS-Systems; mit der Möglichkeit PSTN Nummern auf DNS-Einträge abzubilden, um dort zusätzliche Adressen (unter denen ein Teilnehmer ebenfalls erreichbar sein möchte - z.B. E-Mail oder SIP-Adressen) zu hinterlegen.

Die ENUM-Zone „e164.arpa" ist eine eigens für ENUM eingerichtete Zone im DNS-Namensraum. Für die E.164-Landeskennzahl +49 wurde die ENUM-Domain 9.4.e164.arpa an die DENIC delegiert, die bereits für die Verwaltung

```
6.5.4.6.1.1.5.1.6.9.4.e164.arpa. 14400 IN NAPTR 3 10 "u" "E2U+tel" "!^.*$!sip:456@provider2.de!".
6.5.4.6.1.1.5.1.6.9.4.e164.arpa. 14400 IN NAPTR 2 10 "u" "E2U+tel" "!^.*$!tel:+496151116456!".
6.5.4.6.1.1.5.1.6.9.4.e164.arpa. 14400 IN NAPTR 1 10 "u" "E2U+mailto" "!^.*$!mailto:456@provider2.de!".
```

Abb. 2: NAPTR Resource-Records zu einer ENUM-Domain

der *.de* Zone verantwortlich ist. Die DENIC läßt die Zuteilung der Nutzungsberechtigungen von ENUM-Domänen durch Delegationsaufträge über Registrare vornehmen [DEN05].

A. Registrierung und Validierung von Adressen

Der Registrar, der im Auftrag des Kunden eine Domain reserviert (in Deutschland ein Mitglied der DENIC eG), ist verpflichtet, die Angaben zur Identität dieses Kunden zu überprüfen. Bei ENUM-Domains ist diese Überprüfung besonders wichtig, da es sich um eindeutige Adressen handelt. Es gibt daher in der Regel nur eine zur Registrierung dieser Domain berechtigte Person - den Anschlussinhaber. Um Missbrauch zu verhindern gibt es verschiedene Systeme, die Identität zu überprüfen:

- Schriftliche Registrierung
- Validierung per Telefonrechnung
- Validierung per Rückruf

Da die Validierung per Rückruf automatisiert in den online Bestellvorgang eingebettet werden kann und dabei im Gegensatz zu den anderen Varianten keine nennenswerten zeitlichen Verzögerungen auftreten, wird diese Variante von der Mehrzahl der Provider eingesetzt. Ist der Teilnehmer registriert, kann er die unter seiner ENUM-Domain hinterlegten Informationen z.B. über ein Webformular des Providers nach eigenen Wünschen anpassen und so seine zusätzlichen Kontaktinformationen zur Verfügung stellen.

B. ENUM Resource-Records

Im ENUM-System werden die Kontaktinformation in Form von DNS-Resource Records (RR) unterhalb der jeweiligen ENUM-Domain abgelegt. Dabei werden RRs vom Typ Naming Authority Pointer (NAPTR) verwendet. NAPTR RRs stellen einen regulären Ausdruck dar, der es ermöglicht, die vom DNS-Server zurückgelieferte Antwort abhängig von der genauen DNS-Anfrage zu machen. Darüber hinaus erlaubt die Verwendung von NAPTR RR eine Abstufung von Prioritäten, um festzulegen, welcher der hinterlegten Kommunikationswege bevorzugt gewählt werden soll. Abbildung 2 zeigt einen typischen Satz von NAPTR-RRs einer ENUM-Domain, passend zum Szenario aus Abschnitt I-A.

C. Anrufaufbau mit ENUM

Ein typischer Anrufaufbau unter Verwendung von ENUM beinhaltet folgende Schritte (vgl. Abb. 3):

1) Der Teilnehmer wählt eine Rufnummer am Endgerät.
2) Die VoIP-Telefonanlage (Private Branch Exchange/PBX) wandelt die Rufnummer in eine ENUM-Domain und stellt eine DNS-Anfrage.
3) Das DNS liefert den Satz von RRs mit Kontaktinformationen.
4) Die PBX wählt eine geeignete Adresse aus und startet den Anruf.

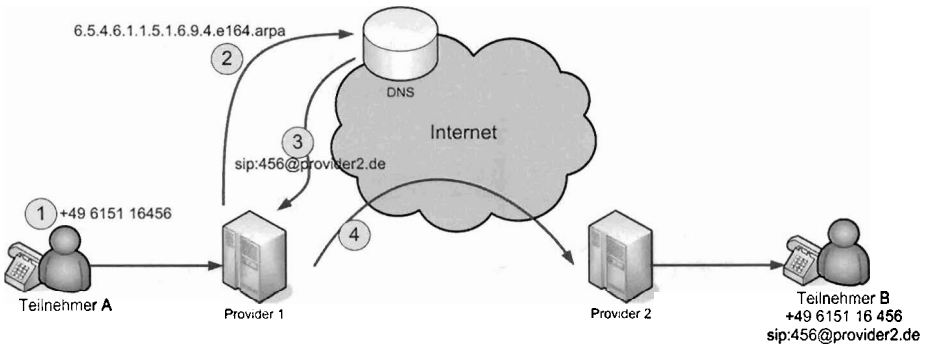

Abb. 3: Anrufaufbau mit ENUM-Abfrage

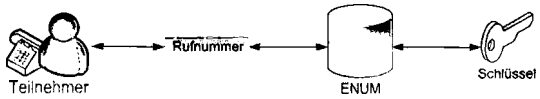

Abb. 4: Kopplung des Teilnehmers an einen Schlüssel

III. ENUM als Authentifizierungsinstanz..

Im Rahmen dieser Arbeit wurde der Ansatz ENUM als Authentifizierungsinstanz zu verwenden ausgearbeitet und umgesetzt. Im folgenden Abschnitt wird erläutert, warum ENUM sich als Authentifizierungsinstanz anbietet und beschrieben, wie das bestehende ENUM-System in erweiterter Form dafür genutzt werden kann.

ENUM bietet sich durch die bereits verfügbaren Funktionen als Authentifizerungsinstanz an:

- ENUM bildet die Grundlage, um VoIP-Infrastrukturen zu verbinden.
- ENUM bietet durch ein Mapping der VoIP-Kennung auf die entsprechende PSTN/E.164 Rufnummer einen einheitlichen Namensraum.
- Durch Kopplung von VoIP-Kennung an eine Rufnummer, können unerwünschte Rufnummern leicht durch Blacklist-Methoden herausgefiltert werden.
- Neue VoIP-Kennungen zu generieren ist für Angreifer einfach. Durch die notwendige Anbindung der VoIP-Kennung an eine bestehende PSTN Rufnummer wird das Generieren von neuen Kennungen extrem erschwert.
- Durch die erweiterte Nutzung von ENUM, kann die gewünschte Funktionalität ohne zusätzliche Infrastruktur-Elemente erreicht werden.
- Ebenso findet bei einer Registrierung einer ENUM-Domain zu eine Rufnummer die notwendige Validierung des Eigentümers statt (siehe Abschnitt II-A).
- ENUM läuft seit 1.4.2006 im Wirkbetrieb und stellt seine Dienste bisher kostenfrei zur Verfügung.

Wie die dabei durchgeführten Erweiterungen genutzt werden können, um Anrufe zwischen Providern dynamisch zu authentifizieren, wird im Folgenden beschrieben.

A. Funktionsweise

Über digitale Signaturen kann ein Anruf an einen kryptographischem Schlüssel gekoppelt werden. Wenn es eine Möglichkeit gibt, die Herkunft dieses Schlüssels zweifelsfrei einem Teilnehmer zuzuordnen, ist eine Verbindung zwischen seiner Identität und dem Anruf hergestellt und dieser authentifiziert. Um die Einrichtung einer dedizierten PKI für VoIP-Infrastrukturen zu vermeiden, wird ENUM als Schlüsselverteiler benutzt. Wenn es gelingt, innerhalb einer ENUM-Domain kryptographische Schlüssel zu hinterlegen, sind diese an die jeweilige Festnetznummer gekoppelt. Der Inhaber einer ENUM-Domain, der mit dem dazugehörigen Rufnummerninhaber identisch ist, ist allein berechtigt, unter einer ENUM-Domain Informationen abzulegen. Daher ist eine Kopplung zwischen diesen kryptographischen Schlüsseln und der Identität des Rufnummerninhabers gewährleistet. In Abbildung 4 ist diese Kopplung dargestellt.

Weiterhin muss die Integrität des öffentlichen Schlüssels auf dem Weg vom DNS zum Verifizierenden geschützt sein. Da das DNS vielseitige Angriffsmöglichkeiten (siehe Abschnitt V-D) bietet, müssen geeignete Abwehrstrategien (z.B. durch DNSSEC oder auf Zertifikaten basierende Methoden) angewendet werden.

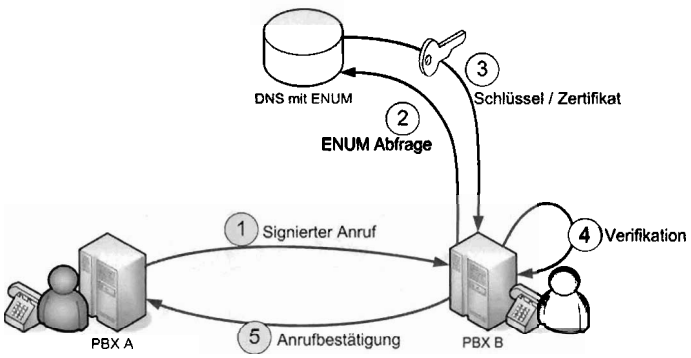

Abb. 5: Verifikation beim Anrufaufbau

Zu Beginn werden bei der ENUM-Registrierung die Schlüssel generiert. Der private Schlüssel verbleibt beim Teilnehmer bzw. dessen PBX-System. Der öffentliche Schlüssel wird im ENUM-Eintrag (dh. unter der jeweiligen PSTN-Kennung) abgelegt. Der Anrufaufbau und der Verifikationsablauf ist in Abbildung 5 dargestellt. Dabei erfolgt der Anrufaufbau in fünf Schritten:

1) PBX A signiert relevante Nachrichten-Inhalte mit privaten Schlüssel und startet die Anruf-Signalisierung.

Nameserver			
TinyDNS / djbdns	ja	ja	ja
MS DNS Server	k.A.	k.A.	ja
MyDNS	nein	nein	128 Zeichen
PowerDNS	ab v.2.9.21	ia	ia

Tabelle I: Unterstützung der RRs von Nameservern

2) PBX B empfängt die Nachricht mit den signierten Inhalten. Anhand der PSTN-Kennung startet es eine ENUM-Abfrage.
3) Als Antwort auf diese ENUM-Abfrage erhält PBX B den öffentlichen Schlüssel zur PSTN-Kennung von Teilnehmer A.
4) PBX B kann nun die Signatur des eingegangenen Anrufs mit dem öffentlichen Schlüssel von Teilnehmer A verifizieren.
5) War die Verifikation erfolgreich, bestätigt PBX B den Anruf und die Verbindung wird hergestellt.
6) Optional kann PBX B seine Antwort ebenfalls signieren. PBX A kann dann durch eine eigene ENUM-Abfrage die Antwort verifizieren und so gegenseitige Authentifikation gewährleisten (nicht in der Abbildung dargestellt).

IV. Keymanagement durch ENUM

Um ENUM als Systemkomponente zur Authentifizierung heranzuziehen, ohne den laufenden Betrieb zu beeinträchtigen, bedarf es einiger grundlegender Überlegungen. Unter anderem gilt es herauszufinden, welche Daten von ENUM bereitgestellt werden müssen und in welcher Form dies innerhalb heutiger Systeme möglich ist.

A. Resource-Record Typen

Die Einsatzmöglichkeiten der verschiedenen RR-Typen sind in den jeweiligen Spezifikationen genau definiert. Um ein Fehlverhalten des sensiblen DNS-Systems zu verhindern, sollte unbedingt davon abgesehen werden, RR-Typen für andere Zwecke zu verwenden, als im Standard definiert sind. Soll in einer DNS-Zone ein kryptographischer Schlüssel oder ein Zertifikat hinterlegt werden, müssen existierende RR-Typen auf deren Eignung analysiert werden:

a) NAPTR RR : Der Naming Authority Pointer (NAPTR) RR wird dazu genutzt, Internet-Domains die zugehörigen Adressen von Servern, Services oder sonstige Informationen zuzuordnen [MD00]. Durch base64 Kodierung von binären Daten lassen sich somit 255 * 6 / 8 Byte = 1530 Bit oder 191 Byte im NAPTR RR einbetten.

b) KEY und DNSKEY RR : Der KEY RR wurde 1999 im ersten Entwurf der DNS-Sicherheitserweiterungen eingeführt (vgl. [Eas99]), um kryptographische Schlüssel mit DNS-Namen zu verbinden. „Dies ermöglicht, das DNS als Public-Key Verteilungssystem zu benutzen, um DNS-Sicherheit oder andere Sicherheitsprotokolle zu unterstützen" [Eas99].

Diese Sicherheitserweiterungen wurden wegen aufgekommener sicherheitskritischer Probleme überarbeitet und im Jahr 2004 durch DNSSEC abgelöst (vgl. Abschnitt VI). Im Rahmen dieser Überarbeitung wurde auch ein zum KEY RR ähnlicher DNSKEY RR eingeführt, der allerdings ausschließlich zur Absicherung von DNS-Infrastruktur verwendet werden darf.

c) CERT RR: Der CERT RR ist in [EG99] definiert, um Zertifikate und ihre Rückruflisten (Certificate Revocation List) im DNS abspeichern zu können. Er unterstützt Zertifikate vom Typ X.509, SPKI und PGP, sowie das Verlinken eines extern gespeicherten Zertifikats über eine URI.

d) TXT RR: Der TXT RR ermöglicht die Verknüpfung des DNS-Namens mit freiem Text [Moc87]. Die maximale Länge des im TXT RR hinterlegten Textes beträgt 255 Zeichen. Sollte diese Zeichenanzahl nicht ausreichen, können mehrere TXT Einträge eingerichtet werden.

B. Softwareunterstützung der Nameserver

Bei der Wahl des verwendeten RR zum Speichern der Daten muss neben der Eignung des Records selbst auch die Kompatibilität mit den Nameserver Produkten beachtet werden. Nicht alle Nameserver unterstützen alle definierten RRs. Tabelle I stellt eine Übersicht dar, welche RRs von den führenden Nameservern unterstützt werden.

C. Öffentliche Schlüssel im DNS

Der öffentliche Schlüssel ist ein zentrales Element in einer asymmetrischen Sicherheitskommunikation. Anhand von ihm wird die Signatur überprüft und damit eine Validierung durchgeführt. Mit der Authentizität des öffentlichen Schlüssels ist unmittelbar das gesamte Sicherheitskonzept verknüpft.

Soll ein öffentlicher Schlüssel im DNS abgelegt werden, bieten sich die oben vorgestellten Resource-Records KEY und TXT an. Der KEY RR ist genau dafür ausgelegt, kryptographische Schlüssel zu repräsentieren. Seine Anwendung kann problematisch werden, da diesen RR nicht alle Nameserver unterstützen oder nur in sehr aktuellen Versionen.

```
IN  TXT "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfwqtxpIfOjFgs6YlGmNjaMUZVC/+C9BMPpQTnAy5IFda5R2ryazLA2hbd
  R7ZSl50eqC2Y2x2djImGT8L5lAE2Zrtyecn33XHn0gg51Y+pXGv85ZqZTQ+ViveKIBT39JbSO2pjdcp+BYuuw2DVZ/TiDSWSy0PdTZX
  rUlmXN4vJJwIDAQAB"
```

Abb. 6: Öffentlicher Schlüssel als TXT Record in einer ENUM-Zone

Der TXT Record gibt keine semantische Bedeutung seines Inhalts vor. Daher können hier in beliebiger Syntax kryptographische Schlüssel abgelegt werden. Da die hier vorgestellte Implementierung der ENUM-basierten Anruferauthentifikation vorgibt, welcher Algorithmus verwendet werden soll, muss diese Information auch nicht zusätzlich im RR integriert sein. Da innerhalb von ENUM-Domains bisher keine Verwendung von TXT Records üblich ist, besteht keine Gefahr von semantischen Überlappungen. Aufgrund dieser gefahrfreien Verwendung benutzt der hier vorgestellte Ansatz TXT Records, um die öffentlichen Schlüssel im DNS abzulegen.

Kryptographische Schlüssel sind binäre Daten. Sollen diese Daten wie hier in einem ASCII-basierten System hinterlegt werden, müssen sie zunächst in eine Zeichenkette umgewandelt werden. Zum Einbetten binärer Daten in ASCII-Umgebungen werden diese gewöhnlich base64 kodiert abgelegt. In der durchgeführten Implementierung können 255 Zeichen eines TXT Records ausgelesen werden. Durch base64 Kodierung stehen effektiv 255 * 6 / 8 Byte = 1530 Bit oder 191 Byte Speicherplatz für den öffentlichen Schlüssel zur Verfügung.

D. Zertifikate im DNS

Um die bei Verwendung von asymmetrischer Kryptographie auftretenden Probleme der Schlüsselauthentizität und Gültigkeitsdauer zu vermeiden, werden Zertifikate eingesetzt. Sie bieten höhere Sicherheit, benötigen aber mehr Speicherplatz. Generell gilt im DNS, dass das System nicht darauf ausgelegt ist, als Datenspeicher zu dienen. Die hinterlegten Datenmengen sollten gering gehalten werden. Zertifikate können im DNS im CERT RR abgelegt werden. Dieser bietet Unterstützung für die gebräuchlichen Zertifikat-Arten.

Wird zur Absicherung des DNS ohnehin bereits DNSSEC eingesetzt, ist das Verwenden von Zertifikaten im vorgestellten Szenario nicht unbedingt notwendig. Kann die Integrität der vom DNS gelieferten Daten sowie die Authentizität des Servers selbst gewährleistet werden, ist sichergestellt, dass sämtliche RRs (auch der öffentliche Schlüssel) vom Domain-Inhaber hinterlegt wurden.

Wird der DNS-Server nicht durch DNSSEC abgesichert, dies sollte eine auf Zertifikaten basierende Authentifikation verwendet werden. Da von einer zukünftigen schrittweisen Einführung von DNSSEC auszugehen ist, wird in dieser Implementierung auf den Einsatz von Zertifikaten verzichtet.

E. DNS über UDP und TCP

Standardmäßig wird eine DNS-Abfrage in einem UDP-Paket versendet, worauf die Antwort ebenfalls per UDP gesendet wird. Um Fragmentierung von UDP-Paketen zu vermeiden, ist in [Moc87] definiert, dass mit einem Paket maximal 512 Byte Nutzdaten übertragen werden dürfen. Für den Fall, dass mehr als 512 Bytes versendet werden sollen, ist zwar vom Standard vorgesehen, die Übertragung vollständig per TCP zu wiederholen, sollte aber wegen des Mehraufwandes vermieden werden.

Im EDNS0 Standard [Vix99] ist ein Verfahren spezifiziert, mit dem Sender und Empfänger aushandeln können, welche maximale Länge das Datenfeld der DNS-/UDP-Antwort haben darf (z.B. 1280 Byte). In der Praxis ist die Grenze von 512 Bytes bei Verwendung von ENUM schnell erreicht. Systeme, die in einer ENUM-Umgebung integriert sind, müssen oft mit großen Sätzen von RRs umgehen, wodurch diese Datenmengen leicht zusammenkommen. Als Optimierung sollten die Systeme den EDNS0-Standard unterstützen, wie in einem Entwurf der IETF gefordert wird [CR06].

V. Evaluation

Um das korrekte Funktionieren des vorgestellten Konzepts zu demonstrieren, wurde die Funktionalität „Signieren" und „Verifizieren" in einer VoIP-PBX integriert. Hierzu wurde die OpenSource Software-PBX Asterisk und das SIP-Protokoll wegen ihrer weiten Verbreitung ausgewählt.

A. Umsetzung in Asterisk

Der Code des SIP-Channels von Asterisk wurde erweitert, um die Authentizität ausgehender Anrufe mittels Signaturen verschiedener Informationen der SIP-Nachrichten-Header zu gewährleisten. Analog zum SIP-Identity-Standard (siehe Abschnitt VI), wird ein Hashwert unter anderem über die Felder FROM, TO, DATE, CALL-ID und CSEQ zum Zeitpunkt des Anrufes mittels SHA1 gebildet, mit dem privaten Schlüssel des Nutzers signiert und anschließend innerhalb der SIP-Nachricht über eine base64 Kodierung eingebettet.

Auf der Seite des angerufenen Teilnehmers gilt es, einen eingehenden Anruf zu verifizieren. Dazu wurde der SIP-Channel, um eine neue Funktionalität erweitert. Bei einem eingehenden Anruf kann nun anhand der CALL-ID eine ENUM-Anfrage gestartet werden, um die Daten aus der SIP-Nachricht über den dabei erhaltenen öffentlichen Schlüssel zu verifizieren.

	Signieren	Verifizieren
RSA 1024	2,75 ms	0,13 ms
RSA 2048	15,18 ms	0,39 ms
RSA 4096	92,48 ms	1,27 ms

Tabelle II: Geschwindigkeitsmessung Signieren und Verifizieren

B. Parameter der Evaluation

Ein Testfeld, bestehend aus zwei Asterisk Installationen und einem DNS-System auf jeweils unterschiedlichen Rechnern, wurde genutzt, um das entstandene System zu evaluieren. Als Schlüssel wurde der noch großflächig eingesetzte RSA-1024 gewählt. Zum Signieren und zur Verifizierung wurde die Asterisk eigene kryptographische API genutzt.

C. Ergebnisse

a) Datenmengen: Bei Verwendung des vorgestellten Konzepts wird durch das zusätzliche Feld im SIP-Header sowie die DNS-Abfrage Datenverkehr generiert. Insgesamt werden der INVITE Nachricht 183 Byte Informationen hinzugefügt. Im Vergleich zu einer standard INVITE Nachricht ohne Signatur (ca. 871 Byte incl. UDP Header und SIP-Body) ist dies ein Zuwachs von ca. 21%.

Auf Empfängerseite erfolgt zusätzlich zum größeren Header noch eine ENUM-Abfrage, die ca. 351 Byte beträgt. Dies setzt sich zusammen aus 61 Byte für die Anfrage (DNS-Query) und 290 Byte für die Antwort (DNS-Response). In der Summe entsteht dem Empfänger und dem DNS-System somit ein zusätzliches Datenvolumen von 351+183=534 Byte pro Gespräch. Durch die Verwendung von DNSSEC wird laut [Age05] das DNS Datenaufkommen um den Faktor 4 bis 4.5 ansteigen.

b) Zeitverzögerungen: Mit dem in OpenSSL integrierten „Speedtest" kann getestet werden, wie viel Zeit ein Signier- oder Verifiziervorgang jeweils benötigt. In Tabelle II sind die Messdaten auch für andere Schlüssellängen zusammengefasst.

Mit dem aufgebauten Szenario wurden zudem verschiedene Tests in Kombination mit realen Anrufsignalisierungen durchgeführt. Die gemessene Zeit zum Signieren beträgt durchschnittlich 5ms. Die Zeit zum Verifizieren beträgt durchschnittlich 6ms, worin die Zeit, die eine DNS-Abfrage zum Ermitteln des öffentlichen Schlüssels benötigt, bereits enthalten ist. Diese beträgt im Testaufbau ca. 5ms. Die verschwindende Differenz bestätigt das mit 0.75ms sehr schnelle Verifizieren der Signatur. Die DNS-Antwortzeit ist in dieser Messung sehr kurz, da die Ergebnisse bereits im Cache des lokalen Nameservers vorhanden sind. In der Regel werden in einer realistischen Umgebung allerdings unbekannte ENUM-Adressen aufgelöst, weshalb hier im Produktiv-Einsatz Werte von ca. 60ms zu erwarten sind.

D. Mögliche Angriffsmethoden

Im Folgenden werden einige mögliche Angriffe auf das System dargestellt. Dies soll keine ausführliche Bedrohungsanalyse ersetzen.

- **Ausfall des ENUM-Systems:** Bei einem Ausfall des ENUM-Systems können beim vorgestellten Konzept keine Signaturen überprüft werden und somit keine Gespräche verifiziert werden.
- **Angriffe auf das DNS:** Durch DNS-Spoofing ist es möglich, dass ein Angreifer eigene Schlüssel hinterlegt. Dadurch kann dieser signierte Anrufe unter einer fremden Absenderkennung führen. Dieser Angriff lässt sich durch den Einsatz von DNSSEC verhindern. Eine Alternative ist die Verwendung von Zertifikaten im DNS.
- **Abhören:** Dieser Ansatz verfolgt nicht das Ziel, Vertraulichkeit zu gewährleisten. Durch Mitschneiden von Anfragen ist es beispielsweise möglich, Kommunikationsprofile zu erstellen oder Anrufe aufzuzeichnen.

Sofern die Übermittlung des Schlüssels sicher durchgeführt werden kann, ist das Hauptziel - die Unversehrtheit der Signalisierungsdaten - erreicht. Sobald ein Angreifer versuchen sollte, Header der INVITE Nachricht zu verändern („Man-in-the-middle Attacke") oder gefälschte Daten zu verwenden, wird die Signatur ungültig und der Anruf kann nicht verifiziert werden bzw. wird abgeblockt.

VI. Verwandte Arbeiten

Aus den Bereichen E-Mail und VoIP gibt es bereits zahlreiche Ansätze, um Sicherheitsziele im Nachrichtenaustausch zu erreichen. Im Folgenden werden die wichtigsten vorgestellt, um Gemeinsamkeiten und Unterschiede zum vorgestellten Konzept zu verdeutlichen.

a) DKIM: DKIM ist ein Ansatz gegen SPAM im E-Mail-Verkehr. Es ist aus dem ursprünglich von Yahoo! Inc. entwickelten DomainKeys Konzept hervorgegangen. DKIM definiert ein Authentifikations-Framework auf Domänen-Ebene für E-Mail auf Basis von Public-Key Kryptographie. Der öffentliche Schlüssel der Domain kann dabei im DNS abgelegt sein, in einem zur Domain gehörenden Eintrag. Somit besteht eine Verknüpfung zwischen Domain und öffentlichem Schlüssel. Der hier vorgestellte Ansatz übernimmt von DKIM das Hinterlegen des öffentlichen Schlüssels im DNS. Außerdem werden bei beiden Ansätzen Signaturen im Protokoll-Header eingefügt.

b) Digest Authentication: Digest Authentication wird eingesetzt, um den SIP-User gegenüber einem SIP-Proxy basierend auf kryptographischen Hashes zu authentifizieren. Diese Authentifizierungsform kann nur gegenüber dem eigenen Provider eingesetzt werden. Sie kann nicht dazu genutzt werden, Provider-übergreifende Sicherheit herzustellen.

c) Secure SIP: Das in [RSC+02] definierte Secure SIP (auch SIPS genannt) ist ein Verfahren, SIP-Nachrichten über eine verschlüsselte TLS Verbindung zu senden. Ursprünglich für HTTP entwickelt, wird TLS eingesetzt, um Integrität und Vertraulichkeit herzustellen. Da TLS auf einer „Hop-by-Hop" Architektur arbeitet, müssen alle Elemente in dem System SIPS unterstützen, um Anrufe gesichert durchzustellen. Secure SIP findet langsam Verbreitung in kommerziellen VoIP-Produkten, viele OpenSource Projekte unterstützen SIPS bisher noch nicht.

d) SIP-Identity: Bei SIP-Identity wird eine Signatur über wichtige SIP-Header angelegt und in den Header integriert. Ebenfalls im Header integriert ist eine URI, die auf das zur Verifizierung der Signatur notwendige Zertifikat verweist. Der Empfänger einer SIP-Nachricht kann über die angegebene URI das Zertifikat beziehen und damit die Signatur verifizieren. Das Protokoll kann lediglich die Integrität der vom Absender verwendeten Kennung gewährleisten. Eine endgültige Authentifizierung kann nur über Inhalte oder Herkunft des Zertifikats erfolgen. Der Standard geht hier von einer Zertifikatverteilung auf Basis von HTTPS aus. SIP-Identity wurde im August 2006 in [PJ06] spezifiziert und wird derzeit noch nicht von verbreiteter SIP-Software unterstützt. Der hier vorgestellte Ansatz übernimmt von SIP-Identity das Signieren von Protokollnachrichten zur Authentifikation des Absenders.

e) DNSSEC: Mit DNSSEC wird das DNS um kryptographische Erweiterungen ergänzt, die parallel zum bisherigen System stehen und daher völlige Abwärtskompatibilität garantieren. DNSSEC bietet Authentisierung, indem eine Vertrauenskette von der DNS Antwort hin zu einem kryptographischen Schlüssel hergestellt wird. In einer sicheren DNS-Zone werden RRs mit einer Signatur ausgeliefert. Diese Signatur lässt sich mit einem Schlüssel überprüfen, der in einer übergeordneten Zone hinterlegt ist. Die Signatur dieses Schlüssels lässt sich wiederum mit der darüber geordneten Zone verifizieren. Dieses Verfahren kann sich über mehrere Zonen erstrecken, bis oben angelangt die vertrauenswürdige root-Zone steht. Um die Einführung von DNSSEC zu begünstigen, ist das Delegation-Signer-Modell (DS) entwickelt worden. Es bietet den Ansatz der „sicheren Inseln", wobei jede Zone als Einstiegspunkt für eine der folgenden DNS-Hierarchien dienen kann [Gud03]. DNSSEC führt eine Reihe neuer RRs ein, um Signaturen über RRs (RRSIG) oder die zu deren Verifikation notwendigen Schlüssel (DNSKEY) zu speichern.

VII. Zusammenfassung und Ausblick

Mit dieser Arbeit konnte gezeigt werden, dass die in der Problemstellung geforderte Provider-übergreifende und dynamische Anrufer-Authentifizierung möglich ist. Auf Basis einer erweiterten Nutzung des existierenden ENUM-Systems kann eine Vertrauensbasis für die Kommunikation zwischen VoIP-Inseln geschaffen werden, ohne zusätzliche Infrastruktur-Komponenten zu erfordern. Die Umsetzung kann in bereits existierende VoIP-Architekturen integriert werden, ohne deren Funktion zu beeinträchtigen. Für das Hinterlegen von TXT RR müssen seitens ENUM bzw. deren Registrare entsprechende Möglichkeiten geschaffen werden oder es muss auf eigene DNS-Server verwiesen werden.

Durch den Einsatz von ENUM als Authentifizierungsinstanz ist eine eindeutige Kopplung zwischen kryptographischem Schlüssel und Rufnummerneigentümer realisiert. Das DNS ist durch seine verteilte Architektur und Verfügbarkeit eine Schlüsselverteilungsinstanz, auf die anonym und ohne vorherige Registrierung zugegriffen werden kann. Somit ist das Ziel des Herstellens von dynamischen Vertrauensbeziehungen erreicht. Das zusätzliche Datenaufkommen vergrößert die SIP-Protokoll Nachrichten. Diese sind aber im Vergleich zum Datenaufkommen des Anrufs selbst verschwindend gering. Die entstehende zeitliche Verzögerung bewegt sich zudem mit ca. 60ms in einem annehmbaren Rahmen.

Die erweiterte Nutzung von ENUM kann schrittweise in existierende Software- bzw. Hardware Komponenten integriert werden. Die in dieser Arbeit durchgeführten Erweiterungen von Asterisk können mit relativ wenig Aufwand in existierende Asterisk-Installationen übernommen werden. Hierzu können weitere Informationen, sowie der Quellcode des erweiterten SIP-Channels von der URL `http://www.kom.tu-darmstadt.de/en/downloads/software/voip-call-auth-with-enum/` bezogen werden.

Literaturverzeichnis

[Age05] Bernhard Ager. Performance Evaluation of DNSSEC, März 2005.

[CR06] Conroy and Reid. ENUM Requirement for EDNS0 Support, September 2006.

[DEN05] DENICeG. Abschlussbericht zum Feldversuch ENUM, September 2005.

[Eas99] Eastlake. RFC 2535: DNS Security Extensions, März 1999.

[EG99] Eastlake and Gudmundsson. RFC 2538: Storing Certificates in the DNS, März 1999.

[Fal00] Faltstrom. RFC 2916: E.164 number and DNS, September 2000.

[Gud03] Gudmundsson. RFC 3658: Delegation Signer (DS) Resource Record (RR), Dezember 2003.

[MD00] M. Mealling and R. Daniel. RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record, September 2000.

[Moc87] P. Mockapetris. RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, November 1987.

[PJ06] Peterson and Jennings. RFC 4474: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), August 2006.

[RSC+02] Rosenberg, Schulzrinne, Camarillo, Johnston, and Peterson. RFC 3261: SIP: Session Initiation Protocol, Juni 2002.

[Vix99] Vixie. RFC 2671: Extension Mechanisms for DNS (EDNS0), August 1999.