[SHKHSt06] *Johannes Schmitt, Oliver Heckmann, André König, Matthias Hollick, Ralf Steinmetz;* **ENUM-Erweiterung zur Sicherung der Kommunikation zwischen VoIP-Infrastrukturen;** Essener Workshop zur Netzwerksicherheit (EWNS) 2006, Essen, Oktober 2006, S. .

ENUM-Erweiterung zur Sicherung der Kommunikation zwischen VoIP Infrastrukturen

Johannes Schmitt, Oliver Heckmann, André König, Matthias Hollick, Ralf Steinmetz
[Johannes.Schmitt;Oliver.Heckmann;Andre.Koenig; Matthias.Hollick;Ralf.Steinmetz]@KOM.tu-darmstadt.de
Multimedia Kommunikation Lab (KOM), Technische Universität Darmstadt, Germany

I. Einleitung und Motivation

Internettelefonie (Voice over IP, VoIP) findet verstärkt Verwendung bei Privat- und Firmenkunden. Viele VoIP Lösungen sind allerdings heute Insellösungen, da eine freie Interoperation zwischen unterschiedlichen VoIP Providern zumeist nicht stattfindet. Vollständig über VoIP kann der Kunde daher zumeist nur mit anderen direkten Kunden seines Providers telefonieren. Gespräche mit Kunden anderer Provider laufen zumeist über das Festnetz – obwohl technisch gesehen auch eine reine IP Verbindung möglich wäre. Ein wichtiger Grund hierfür liegt in der fehlenden Vertrauensbeziehung zwischen Providern. Ein Provider und damit auch seine Kunden haben nur mangelhafte Möglichkeiten, die Identität eines Anrufers, der nicht beim gleichen Provider ist, zu authentifizieren. Dies öffnet die Tür für unautorisierte Anrufe, gefälschte Caller IDs und SPIT (VoIP Spam).

In diesem Paper stellen wir einen Ansatz vor, mit dem diese Gefahr entscheidend verringert werden kann und der es erleichtert, die Authentizität von Anrufern über Providergrenzen zu gewährleisten. Hiermit können die unterschiedlichen Adressräume der Provider vertrauenswürdig gekoppelt werden. Anstatt eine externe Public-Key-Infrastruktur zu nutzen, schlagen wir eine einfache aber effektive Erweiterung des „t*E*lefone *NU*mber *M*apping" (ENUM) Dienstes vor, der heute schon zur Adressauflösung zwischen Adressräumen verwendet wird.

II. Verwandte Arbeiten

Das gleiche, grundsätzlich verwandte Problem der sicheren Sender-Authentifizierung, findet sich bei E-Mail Systemen. Der hier vorgestellte Ansatz greift dabei dort verwendete Mechanismen [1] auf. Existierende Ansätze, Sicherheit in VoIP zu gewährleisten [2][3] finden durch den benötigten organisatorischen und technischen Mehraufwand oder den begrenzten Einsatzmöglichkeiten [3] nur selten Einsatz. Zur Authentifizierung zwischen zuvor unbekannten Systemen spielt die Nutzung zusätzlicher Publik Key Infrastrukturen eine zentrale Rolle. Beim Einsatz einer PKI entsteht das Problem der Abwägung von Sicherheit, Kosten und Aufwand [4][5].

ENUM [6] selbst wird auch kritisch bewertet, da es ebenso als Mittel genutzt werden kann, um Adressen von Teilnehmern z.B. für SPIT zu erfragen [7]. ENUM ist eine Erweiterung von DNS. Bestehende Angriffsmöglichkeiten auf DNS und Vermeidungsstrategien müssen daher auch bei ENUM Beachtung finden [8].

III. Ansatz

Aktuell findet das Session Initiation Protokoll (SIP) [9] verstärkt Einsatz als VoIP Signalisierungsprotokoll, sowohl in Privat- als auch Unternehmensbereichen. ENUM bietet eine sinnvolle Lösung um VoIP Infrastrukturen dynamisch zu verbinden. In Abbildung 1 ist der Ablauf einer Anrufverarbeitung bei SIP Systemen mit ENUM schematisch dargestellt (nur durchgezogene Linien).

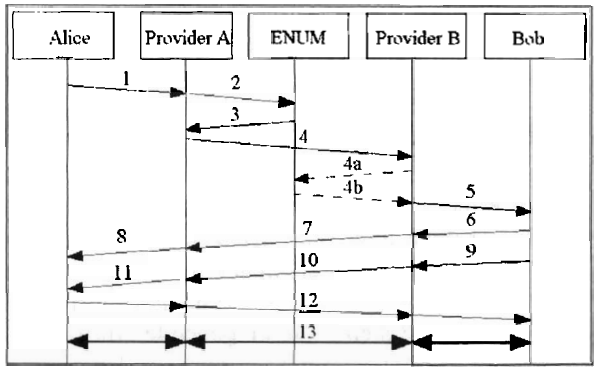

Abbildung 1. SIP Nachrichtenfluss für Anrufaufbau mit ENUM und Erweiterung zur Authentifikation.

Die Nachrichten 1,4,5 stellen die Nachrichten für eine Anfrage zum Kommunikationsaufbau (SIP-INVITE) zwischen Alice und Bob dar. Die Adressanfrage an den ENUM Dienst findet sich in Nachricht 2 und 3 wieder. Die Nachrichten 6 bis 11 sind SIP-Status Nachrichten, welche Informationen über die Eigenschaften und den Status (klingelt, abgehoben) des Endgerätes von Bob zurückreichen. Die Bestätigung in Nachricht 12 und der Mediendatentransfer 13 werden je nach System unterschiedlich gehandhabt. Bei Firmen findet meist ausschließlich eine Kommunikation „nach außen" über ein firmeninternes Gateway (in diesem Fall ist dieses der „Provider") statt. Dagegen kann im offenen/privaten Anwendungsfall eine Kommunikation hier auch direkt zwischen den Endgeräten erfolgen.

Aktuell ist es meist nicht möglich, providerübergreifend Anrufe zu tätigen, da eine Öffnung eines VoIP Netzes für Anrufe von außen meist bedeuten würde unbekannte bzw. unsichere Anrufer zuzulassen. Um diese Schwachstelle zu sichern, sieht unser Ansatz vor, den ENUM Dienst um die Bereitstellung der öffentlichen Schlüssel (S_δ) der jeweiligen Provider zu erweitern:

Der bei der ENUM Registrierung bei ENUM erzeugte S_{δ} wird in Kombination mit der dafür gültigen Festnetznummer bzw. einem Nummernblock von ENUM signiert (Nummernzugehörigkeit wird aktuell bei einer ENUM Registrierung sichergestellt). Diese Daten werden in Form eines von ENUM ausgestellten Zertifikates, gemeinsam mit den Adressen eines Nutzers in ENUM hinterlegt. Bei einer ENUM Anfrage wird das Zertifikat eingebettet innerhalb einer URI [10] eines zusätzlichen ENUM-Service [11] Feldes („cert") in der ENUM Antwort mitgeliefert - wie in Abbildung 2 exemplarisch dargestellt. Der private Schlüssel (S_P) verbleibt beim jeweiligen Provider.

```
$ORIGIN 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa.
    NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:ab@xy.com!" .
    NAPTR 10 101 "u" "E2U+h323" "!^.*$!h323:ab@xy.com!" .
    NAPTR 10 102 "u" "E2U+msg" "!^.*$!mailto:ab@xy.com!" .
    NAPTR 10 103 "u" "E2U+cert" "!^.*$!data:[certifikate]!" .
```

Abbildung 2. ENUM Antwort mit zusätzlichem Feld für den öffentlichen Schlüssel.

Der Ansatz sieht vor, dass Provider A bei einem Anruf die zum eigenen S_{δ} registrierte Festnetznummer (sowie weitere sitzungsrelevante Daten) mit seinem S_p signiert und in Nachricht 4 innerhalb eines SIP-Header Feldes anhängt. Die zusätzlichen Schritte 4a und 4b ermöglichen Provider B, durch eine weitere ENUM Anfrage über die angegebene und signierte Festnetznummer, das Zertifikat von Provider A zu erhalten, um anschließend die Signatur von Provider A zu prüfen und sicher die eingehende Anruferkennung einer Festnetznummer zuordnen zu können. Im Gegenzug kann in Nachricht 7 die angerufene Festnetznummer von Provider B signiert zurückgesendet und mit dem S_p aus der ENUM Antwort 3 verifiziert werden.

Dieser Ansatz bietet eine einfache Möglichkeit der Schlüsselverwaltung und des Schlüsselaustausches, welche genutzt werden kann, um beide Teilnehmer wechselseitig zu authentifizieren und sicher einer Festnetznummer zuzuordnen. Durch die Zuordnung zu einer Festnetznummer können unsichere Provider bzw. unerwünschte Anrufer schnell bestimmt und durch Einsatz von Blacklists aussortiert werden. Die ausgetauschten S_{δ} können zudem genutzt werden, um anschließend eine verschlüsselte Verbindung zwischen den Providern aufzubauen. Sichere Verbindungen zwischen Providern sind in folgenden Szenarien sinnvoll:

- Im Firmenumfeld verläuft die Strecke zwischen den Endgeräten und dem Gateway/Provider über ein gesichertes Intranet.
- Eine Ende-zu-Ende Verschlüsselung steht im Konflikt mit Legal-Interception Vorlagen.
- Endgeräten und Providern benutzen von Beginn an eine symmetrische Verschlüsselung auf Basis des vorher ausgetauschten Account-Passwortes.
- Bekannte Sicherheitsverfahren können auf herkömmliche VoIP Endgeräten nicht eingesetzt werden, da diese sie nicht unterstützen oder technisch nicht die Leistung dafür erbringen.

Der Ansatz erzeugt einen geringen zusätzlichen Aufwand in der Kommunikation bei Nachricht 4a und 4b, welcher mit dem Einsatz von Caching-Techniken minimiert werden kann.

Es entsteht zudem zusätzlicher Rechenaufwand bei der Signaturerzeugung für die Nachricht 4 und 7, sowie der jeweiligen Überprüfung der Signatur auf der Gegenseite. Dieser zusätzliche Rechenaufwand (1x signieren, 2x verifizieren) ist von der Größenordnung wie der Wechsel von http zu https zu sehen und mit heutiger Rechenleistung auch bei vielen Verbindungen unproblematisch, vgl. etwa [12].

Wenn ENUM zum Signieren seiner Zertifikate einen S_{δ} nutzt, welcher durch eine sichere CA ausgestellt wurde, können zudem die Schwachstellen, welche durch DNS entstehen vermieden werden und das System bietet dann eine relativ hohe Sicherheit.

IV. Zusammenfassung und Ausblick

In diesem Paper stellen wir eine einfache Erweiterung des ENUM Dienstes vor, durch die bei einer ENUM Anfrage auch das Zertifikat des Providers mitgeteilt wird. Dies ermöglicht eine einfache und effiziente Authentifizierung des Anrufers, ohne zusätzliche Infrastrukturen zu benötigen.

Sofern die Endgeräte das unterstützen, kann eine Authentifizierung auch durch den Endkunden erfolgen. In zukünftigen Arbeiten evaluieren wir solche Umsetzungsalternativen und weitere Erweiterungen von ENUM.

V. Referenzen

[1] Boelen and Ekkebus, Dealing with spam in the near future – Overview of sender authentication techniques, Distributed e-bussiness techniques, Univesity of Twente, 5/2005

[2] Rosenberg and Jennings. Draft, The Session Initiation Protocol (SIP) and Spam, Internet-Draft 6/2006, draft-ietf-sipping-spam-02

[3] Schmitt and Ackermann, VoIP-Sicherheit – Status Quo und neue Aspekte, D-A-CH Security 06 S. 433-444, 3/2006

[4] Stark, Mehr Unternehmenssicherheit durch Trustcenter?, IT-Sicherheit, WIK – Unternehmen und Sicherheit 4/2001 http://www.secorvo.de/publikationen/trustcenter-stark-2002.pdf

[5] Oppliger, PKI: Eint Tanz um das goldene Kalb?, 3/2001, http://www.fgsec.ch/events/ft2001.03.28/doc/1_PKI-TagungFGSec_Oppliger.pdf

[6] Faltstrom, RFC 3761 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM), 4/2004

[7] Electronic Privacy Information Center (EPIC), Comments on Privacy Issues in ENUM, 11/2002 http://www.epic.org/privacy/enum/enumcomments11.02.html

[8] Arends, RFC 4033-4035, DNS Security (DNSSEC), 3/2005

[9] Rosenberg and Schulzrinne, RFC 3261 SIP: Session Initiation Protokoll, 6/2002

[10] Eastlake, RFC 2538, Storing Certificates in the Domain Name System (DNS), 3/99

[11] Iana.org, Enumservice Registrations, ftp://ftp.iana.org/assignments/enum-services

[12] Goldberg and Buff and Schmitt, A Comparison of HTTP and HTTPS performance, Computer Measurement Group, 12/1998 http://www.cs.nyu.edu/artg/research/comparison/comparison.html