Konvergente Services in der Telefonie

Faxen, Least-Cost Routing,
verschlüsselt telefonieren mit Asterisk

Dr. Ralf Schlatterbeck
Open Source Consulting

Email: office@runtux.com
Web: http://www.runtux.com
Tel. +43/650/621 40 17

Inhalt

FAX mit Asterisk 4
FAX-Empfang 5
FAX-Versenden: existierende Lösungen 6
FAX-Versenden: unsere neue Lösung 7
FAX-Gateway: used Software 8
Least Cost Routing 9
Asterisk Dialplan – Least Cost Routing 10
Least Cost Routing: Poor mans version 11
Least Cost Routing: Extended version 12
Download + Auswerten von Gebühreninfos . . . 14
Gebühreninfos: Quellen im Netz 15

Inhalt

Gebühreninfos: Kleingedrucktes Telekom 17
Zusammenfassung Least-Cost-Routing 18
Standards für verschlüsselte Telefonie 19
Probleme mit verschlüsselter Telefonie 20
Exkurs: Man in the middle 21
VoIP: Exkurs: Skype 22
Existierende Implementierungen 23
Zusammenfassung 24
Literatur 25

FAX mit Asterisk

- Asterisk-Modul spandsp von soft-switch.org
- FAX wird von Host-CPU gerechnet, kein externes Modem
- Freie Software
- Mehrere gleichzeitige Fax-Übertragungen nach Prozessor-Kapazität
- Konvergenz: Gateways
  Email-to-FAX bzw. FAX-to-Email

FAX-Empfang

- Läuft stabil
- Mehrere FAX-Durchwahlen möglich, z.B.: Eigene FAX-Durchwahl für jeden Mitarbeiter
- FAX-to-Email Gateway einfach möglich: AGI-Script konvertiert TIF auf PDF

```
[fax]
exten => s,1,Set(FAXFILE=.../${UNIQUEID}.tif)
exten => s,2,Set(EMAILADDR=fax@example.com)
exten => s,3,rxfax(${FAXFILE})
exten => h,1,deadagi(/usr/local/sbin/mailfax)
```


FAX-Versenden: existierende Lösungen

Spandsp-Problem: Fehlercodes werden nur ins logfile (mit Debug-Option) geschrieben

- „Fire-and-forget“: astfax – keine Fehler-Auswertung
- Seltsame Lizenz von AsterFax: „Rest assured, AsterFax will be Open Source and it will be freely available to user with a single fax line.“
- AsterFax ist in Java implementiert [Gra04]
- Anscheinend nur Java Bytecode verfügbar
- AsterFax: Logfile-Auswertung für Fehlercodes

FAX-Versenden: unsere neue Lösung

- Patch für txfax (und rxfax) von spandsp macht Fehlercodes als Asterisk-Variablen sichtbar
- Serialisiert Email als TIF
- Sendet TIF mit txfax
- Fehlercode von Asterisk an Gateway
- Retries, Bounces handled by Postfix
- Erfolgreiches Versenden erzeugt Rück-Email
- Problem mit mehr als 1 Seite – tiffcp or gs?

FAX-Gateway: used Software

- magicfilter, H. Peter Anvin’s version from Debian
  → convert anything to Postscript, then to TIF
  → uses various other toolkits, e.g., netpbm
- Tools from libtiff: tiffcp, tiff2ps, tiff2pdf
- Postfix for the Email-to-Fax Gateway and for Queue handling
- of course, Ghostscript
- A script in Python to tie it all together

Least Cost Routing

- Hohes Einsparungspotential
- Aber: Derzeit Hohe Kosten für die Wartung der Routing-Information
- Traditionell: Call-by-Call Provider
- Neu: SIP Provider mit Festnetz-Zugang

→ Kostensenkung durch vereinfachte Wartung der Routing-Infos

→ Einbeziehung von Internet (SIP) Anbietern

Asterisk Dialplan – Least Cost Routing

```
[dialout]
exten => _00432243.,1,Macro(lcroute,${EXTEN:8},${CALLERIDNUM})
exten => _02243.,1,Macro(lcroute,${EXTEN:5},${CALLERIDNUM})
exten => _0043.,1,Macro(lcroute,0${EXTEN:4},${CALLERIDNUM})
exten => _X.,1,Macro(lcroute,${EXTEN},${CALLERIDNUM})

[macro-lcroute]
exten => s,1,SetCallerID(${ARG2})
exten => s,2,GotoIfTime(8:00-18:00|mon-fri|*|*?200)
exten => s,3,Noop(Freizeit)
exten => s,4,Goto(10)
exten => s,10,GotoIf($["${ARG1}" : "[1]"]?10010)
exten => s,11,GotoIf($["${ARG1}" : "[2-9]"]?50)
exten => s,12,GotoIf($["${ARG1}" : "0664"]?10010)
exten => s,15,GotoIf($["${ARG1}" : "0650"]?10120)
exten => s,19,GotoIf($["${ARG1}" : "08"]?10010)
exten => s,25,GotoIf($["${ARG1}" : "00491[567]"]?10120)
exten => s,26,GotoIf($["${ARG1}" : "0049"]?10250)
exten => s,50,SetVar(ARG1=100302243${ARG1})
exten => s,51,Goto(10010) ; local call

exten => s,10010,Dial(${TRUNK}/${ARG1}/${OPTIONS})
exten => s,10011,Noop(10011_${DIALSTATUS})
exten => s,10012,GotoIf($["${DIALSTATUS}" = "BUSY"]?10014)
exten => s,10013,Congestion()
exten => s,10014,Busy()
exten => s,10015,Hangup()
```


Least Cost Routing: Poor mans version

- GotoIf-Kaskade
- Schwierige Wartung
- Unübersichtlich
- nur für wenige Anbieter

\+ Mit „Bordmitteln“ realisierbar

\+ Internet-Anbieter (SIP) möglich

– hohe Wartungskosten

Least Cost Routing: Extended version

- Externes Script für Routing-Entscheidungen
- Parameter
  - Gewählte Rufnummer
  - Uhrzeit
  - z. B. Aufbrauchen von Freiminuten bei einem Provider . . .
- Benötigt Gebühreninformation der Provider
- Daten auch für andere Zwecke einsetzbar, z. B. Abrechnung pro Endgerät

Least Cost Routing: Extended version

- (fast) alle Anbieter haben Kostenpläne im Netz
- HTML – einfach automatisch auszuwerten
- . . . oder PDF – schwieriger auszuwerten
- Aber manche Anbieter ändern Webseite häufiger als die Gebühren
  - Telekom (TikTak privat Tarif)
  - UTA
  - Telering

Download + Auswerten von Gebühreninfos

Einfaches Framework benötigt:

- Einfach zu Warten bei Änderung der Webseite
- Modular: Neue Provider einfach dazuzugeben

Entscheidungen:

- Written in Python
- Verwendet ElementTidy ElementTree Interface

Status: Stay tuned but don't hold your breath
Mitarbeit erwünscht!

Gebühreninfos: Quellen im Netz

Framework unterstützt bereits:

- Wikipedia: ISO-3166-1 (2-letter + 3-letter) Ländercodes
- Wikipedia Vorwahl nach Code oder Land
- World Telephone Numbering Guide: Vorwahl nach Code oder Land
- Wikipedia Mobile Rufnummern nach Ländern
- Numberplan.org – frei verfügbare Informationen sind voller (absichtlicher?) Fehler.

Gebühreninfos: Quellen im Netz

- Telekom TikTak Tarif
  - Inland und Mobiltarife als HTML
  - Ausland: PDF-Liste nach Land (nicht Vorwahl)
  - Hotline: Diese Infos gibt es nur im System (!)
  - Auf Email-Nachfrage dann doch ein Link – Geschäftsbedingungen unter „EB" – Entgeltbestimmungen: uralte Liste der Vorwahlen + Gebühreninformation. Natürlich als PDF
- Multikom: auch als PDF

Gebühreninfos: Kleingedrucktes Telekom

. . . Dabei kann allerdings nicht ausgeschlossen werden, dass aufgrund der Rufnummernpläne der einzelnen Länder auch geografische Rufnummern unter diesen Kennzahlen erreicht werden können. In diesem Fall wird dem Kunden das billigere Entgelt für Rufe ins ausländische Festnetz verrechnet.
Weiters kann nicht ausgeschlossen werden, dass aufgrund von kurzfristigen Änderungen der Rufnummerpläne der einzelnen Länder Mobilkennzahlen nicht in dieser Liste aufscheinen. Aktuelle Informationen über Mobilkennzahlen . . . unter 0800 100 100 . . .

Zusammenfassung Least-Cost-Routing

- Viele preiswerte Anbieter
- Gebühreninformation schwierig zu bekommen
- Gebühreninformation schwierig automatisch auszuwerten

Ausblick:

- ENUM: Telefonnummern über DNS
- DUNDi: Distributed Universal Number Discovery
  → Peer-to-peer für Telefonnummern-Suche

Standards für verschlüsselte Telefonie

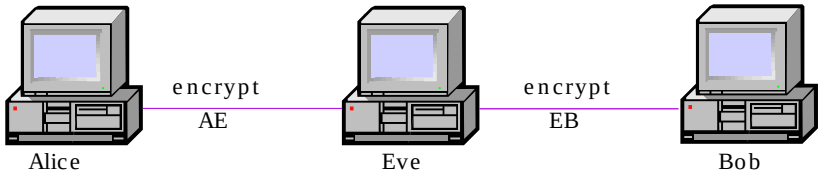
- Verschlüsselungsoption für De-facto Standard IAX mit pre-shared keys
- VoIP kann auch über ein VPN, z. B. OpenVPN geroutet werden
- SRTP/SRTCP: Spezifiziert aber kaum verwendet Master-Key: Telefoniepartner müssen Schlüssel vorher vereinbaren
- Phil Zimmermanns ZRTP: SRTP + Diffie-Helman
  → Telefoniepartner müssen sich nicht kennen!
  → Verwendung existierender SIP-Infrastruktur

Probleme mit verschlüsselter Telefonie

Sicherheit:

- Verkehrsanalyse (Traffic Analysis): „Wer mit wem“
  → fast Vorratsdatenspeicherungskonform :-)
- IAX überträgt Wahlinformation im Klartext
- Selbst bei VPN kann anhand Paketgrößen und -frequenz auf VoIP geschlossen werden
- SRTP ohne ZRTP, IAX und VPN Lösungen: vorherige Absprache der Telefoniepartner!
- ZRTP MITM-Protection: Vorlesen des Key-Hash

Exkurs: Man in the middle



- Eve – die Frau in der Mitte – führt Key Discovery mit Alice und Bob durch
- Es gibt zwei Schlüssel, AE und EB
- Aber: Alice und Bob können ihre Schlüssel vergleichen und sich diese vorlesen
  → Authentifizierung über Sprache!

VoIP: Exkurs: Skype

- „It just works“, keine Probleme mit Firewalls
- Skype-Hersteller bekannt durch Spyware-verseuchte Filesharing Software (KazaA)
- Eingebaute Software-Update Funktion in Skype
- Hält sich an keine Standards – keine Drittanbieter
- Closed Source – Open Source Skype wäre nice

→ Wem vertraut man seine Telefongespräche an?

→ Verschlüsselung???

Existierende Implementierungen

Allgemein:

- IAX Verschlüsselung: Keine Erfahrungen
- OpenVPN + Asterisk IAX (or SIP/RTP) works well

ZRTP:

- SRTP/ZRTP derzeit in Asterisk nicht verfügbar
- Phil Zimmermanns ZFone
- GNU ccRTP unterstützt ZRTP
- GPL-Client Twinkle mit ZRTP

Zusammenfassung

Herkömmliche Telefonie mit neuen „Internet“-Features

- FAX: Gateways from/to Email
- Least-Cost Routing:
  → Routinginfos aus dem Netz
  → Routing mit Einbezug von Internet-Providern
- Verschlüsselte Telefonie mit Standard-Protokollen
  → Unabhängige ZRTP-Implementierungen
  → Frage der Zeit bis es Asterisk auch kann . . .

Literatur

[Gra04] Paul Graham. Revenge of the nerds. In *Hackers & Painters – Big Ideas from the Computer Age*, pages 181–199. O'Reilly Media, Inc., Sebastopol, CA, May 2004.