VoIP-Probleme aus Sicht eines Providers

Hendrik Scholz
<hendrik.scholz@freenet-ag.de>

Freenet Cityline GmbH, Kiel

Sicherheit 2006
20.02.2006, Magdeburg

Wer ist freenet?

- PSTN Carrier und ISP
- 600.000 DSL Kunden
- Hohe VoIP Akzeptanz
- 95% Hardware-Endgeräte
  - AVM Fritz!, Siemens SX541, Cisco, Grandstream
- VoIP als PSTN-Ersatz
  - sehr großes pro Kopf Call Volumen

Agenda / Probleme

- Administration
  - Features
  - Angriffe
  - Endgeräte, Infrastruktur
- Regulierung
  - Endbündelung
  - Enum
  - Notruf
- Zukunft

Rufnummernanzeige

- CLIP, CLIR, COLP, COLR
  - elementare Features
- Vereinheitlichung schwer
  - Intercarrier Konfiguration
  - PSTN-Übergänge
- Probleme
  - Fehlkonfiguration
  - Angriffe möglich
    - fremde Mailboxen abhören
    - SPIT

Rufnummernanzeige

- Unterschiedliche Standards
  - From header Feld (RFC 2354, 3261)
  - Remote-Party-ID (draft-ietf-sip-privacy-04)
  - P-Asserted-Identity (RFC 3323, 3325)
  - Propritäre Erweiterungen
- fortlaufende Entwicklung
  - unterschiedlicher Stand der Geräte
  - fortlaufend neue Probleme

SPIT

- SPIT = Spam over IP Telephony
- Das gibt es?
- Anruf (INVITE) erfordert Authentisierung
  - Challenge Authentication (CHAP)
  - Schwer spoofbar
  - Vertrauen zu Peeringpartnern
- MCID (Malicious Call Identification)
  - Noch nicht ausführlich definiert
  - Muss zwischen Anbietern funktionieren

SPIT: Endgeräte

```
for (;;) {
   DSL Router mit VoIP finden
   INVITE schicken (z.B. mit sipsak)
   Alert-Info:
     http://meinhost.tld/spit.wav
}
```

- stateless, schnell, spoofbar
- Hersteller verantwortlich

DOS-Attacken: Infrastruktur

- SIP Server mit INVITE/REGISTER/SUBSCRIBE überladen
- PSTN-Gateway (call attempts/sec Limitierung)
- PSTN-Leitungen blockieren
- Gegenmaßnahmen:
  - Session Border Controller (Nachteile!)
  - Ratelimiting

DOS-Attacken: Endgeräte

- ungeschützt
- wenig Rechenleistung
- keine Authentisierung für eingehende Pakete
- remote Management
  - Reboot, Configänderung, Call-Aufbau
- Beispiel: limitierte Anzahl physikalische Telefone hinter DSL-Router

Endgeräte

- Monokulturen gefährlich
  - AVM lässt INVITEs von überall zu
- Engeräte angreifbar
  - Webinterface
  - Betriebssystem
  - Seltene Updates
  - SPIT ohne ISP möglich
  - kein bzw. minimales Log

Billing: Rufweiterleitung

- Problem
  - A ruft B an, B leitet auf C weiter
  - A telefoniert mit C
  - B soll bezahlen
- Implementation
  - Diversion-Header
  - REFER
  - komplexe Stateengine
- Angriff? Stack-Unterschiede ausnutzen

Billing: Genauigkeit

- Telekommunikations-Kundenschutz-Verordnung (TKV)
- Problem: Abrechnungsgenauigkeit
  - DSL-Ausfall
  - Kunde sendet kein BYE
- PSTN hat geswitchte Verbindungen
  - Erkennung von Ausfällen einfacher
- Diskussionsbasis von BNetzA gefordert

Richterliches Mithoeren

- Ausleitung von Daten an berechtigte Stellen
  - definiert durch BNetzA
- Mehrstufige Implementation
  - Signalisierung (IRI) jetzt
  - Mediadaten (Content) ab 2007
- Probleme
  - große Kostenstelle, besonders für kleine ITSPs
  - Medienausleitung noch nicht definiert

Rufnummernvergabe

- Vergabe von Ortsbezogenen Rufnummern
- 032er Gasse 'geplant'
  - Nomadische Nutzung erlaubt
  - 01801 Nummern als Übergangslösung
- Stichwort: Wohnortwechsel
- VoIP Anbieter sind oft keine Carrier
  - Sipgate hat keine eigenen Telefonnummern
  - Zuführung aufwendig

ENUM 1/2

- ENUM bietet
  - 'Telefonbuch', Nummernaustausch
  - Routinginstanz
- Vorteile
  - Keine Peeringabkommen, einfach Konfiguration
  - Mehr kostenlose Calls
- Nachteile
  - Routing basierend auf Informationen im Netz
  - Vertrauensbasis fehlt

ENUM 2/2

- Umgebung heute
  - Insel-ENUM-Lösungen
  - Nummernaustausch von ISP zu ISP (1:1, nicht 1:n)
  - Kunde bezahlt ggf. für ENUM-Eintrag
- Vergleich: Local Number Portability (LNP) im PSTN
- einheitliche Lösung nötig

Notruf

- VoIP muss Notruf bieten (§108 TKG)
  - Notruf muss an lokale Notrufstelle geroutet werden
  - Rufnummernübermittlung
  - Lokalisierung des Kunden nötig
- aktuell: PSTN-Backupleitung für Notruf
- nomadische VoIP-Nutzung mit Notruf?

Zukunft

- Lawful Interception
  - Aufwand?
  - Tod fuer kleinere ITSPs?
- VoIP-Umfeld unsicher
  - PSTN ist IP-enabled
- VoIP in World of Warcraft?
- Vorratsdatenspeicherung

Entscheidungen müssen 2006 kommen!

Fragen?

<hendrik.scholz@freenet-ag.de>

http://www.wormulon.net/