Spam goes VoIP
Number Harvesting for Fun and Profit

Hack in The Box 2007 - Dubai
Hendrik Scholz
hs@123.org
Agenda

• VoIP Threads
• Difference between Spam and SPIT
• Use Cases for VoIP numbers
• Number Harvesting
• Attack Examples (the fun part)
• Conclusions
VoIP Threads
VoIP Attacks: What's possible?

Social Threads
- Theft of Services
- Unwanted Contact (i.e. SPIT)

Signalling
- DOS attacks / Blackholing
- Communication Reconstruction
- Call Rerouting

Media
- RTP Injection
- Conversation Degration
VoIP Attack: What's real?

Theft of Services
- Stolen accounts

Misrepresentation
- Faked Caller-ID

ISPs losing money
- Attacker takes over Asterisk box and terminates PSTN calls
- Customer selling subsidized hardware on Ebay
- "creative" ways to get around billing
VoIP-Attacks: What's missing?

How about SPIT?
Ask a VoIP Security Vendor to send you some

- Cebit 2007
- NEC Anti-SPIT Project
- Germany Government Project (spit-abwehr.de)

SPIT hardly exists as of now
Spam vs. SPIT
How does Spam work?

Spammers harvest or buy email addresses
  – Brute force attempts on mailservers, wild guesses
  – Off Usenet, web forums/communities, ...

Spammers send mails through backup MX
  – Get around some Spam filtering

Spam attributes
  – Mass
  – Quality (user actually reads his mails)
  – Auxiliary information (name, country)
Spam vs. SPIT

much harder to filter phone conversations
- Greylisting somehow works
- No Spamassassin (yet)
- Filtering has big impact on Quality of Service
- Legal issues have yet to be properly defined

phone number lifetime: several years?
- Constant use
- Less leftovers
  - people tend to port their phone # to their new carrier
Spam goes Voice over IP
Information we crave for

**Contact address**
- SIP URI == email address

**SIP REGISTRAR**
- VoIP provider
- like the MX for VoIP

**optional**
- Realname
- Country (language!)
- email address to relate to
Number Harvesting
Number Harvesting

is

- a prerequisite to Spaming/SPITing
- gathering valid usernames/addresses

might become

- a market for people to sell numbers
- much like currently done for email

should

- not be too easy
Use Cases

Sell numbers like email addresses

Spit
- sell stuff
- polls / surveys
- viral marketing, slander

Why contact people over the phone?
- more intrusive than Spam, hard to filter
- High success rate (as well to being sued)
- format break: you cannot click on a URL in a conversation
Number Harvesting Sources

Public Directories
- ENUM
- Yellow Pages

ISPs themselves

Government databases

Auxiliary services

Active Probing

Sniffing

Social Engineering
Public Directories

**ENUM**
- DNS based directory
- lookup SIP URI for a phone number

**public ENUM**
- aka "user ENUM"
- open to everybody
- foundation of the P2P SIP and free VoIP movement

"Number Harvesting Success Rating"
- probably not worth it
- could be used to enrich existing data
also known as
- Carrier ENUM
- Infrastructure ENUM

used in bilateral peerings / Federations
- can only be accessed by partners
- contract may prohibit SPIT

HUGE database
- 8+ mio entries (numbers + blocks) for Germany
- currently under development at DENIC(.de)
ITSPs usually buy number blocks

- publish blocks
- number length known (guessable)
- iterate through number space to get numbers in service

Sample ITSPs

- freenet(.de)
- sipgate.(de|net|co.uk)
- sipphone / gizmoproject.com
- Vonage(.com)
## Area Codes Available

### USA - Pacific Standard Time
- 714 Anaheim, CA **Available.**
- 310 Beverley Hills, CA **Available.**
- 702 Las Vegas, NV
- 213 Los Angeles, CA
- 323 Los Angeles, CA **Available.**
- 818 Los Angeles, CA **Available.**
- 626 Pasadena, CA **Available.**
- 503 Portland, OR
- 916 Sacramento, CA **Available.**
- 619 San Diego, CA **Available.**
- 760 San Diego, CA **Available.**
- 858 San Diego, CA
- 415 San Francisco, CA **Available.**
- 206 Seattle, WA **Available.**
- 360 Seattle, WA **Available.**
- 650 Silicon Valley, CA **Available.**
- 408 Sunnyvale, CA **Available.**
- 805 Ventura, CA **Available.**

### USA - Eastern Standard Time
- 706 Athens, GA **Available.**
- 678 Atlanta, GA **Available.**
- 410 Baltimore, MD **Available.**
- 617 Boston, MA **Available.**
- 718 Brooklyn, NY
- 704 Charlotte, NC **Available.**
- 216 Cleveland, OH **Available.**
- 614 Columbus, OH **Available.**
- 954 Ft Lauderdale, FL
- 201 Hackensack, NJ **Available.**
- 860 Hartford, CT **Available.**
- 904 Jacksonville, FL
- 786 Miami, FL **Available.**
- 732 New Brunswick, NJ **Available.**
- 203 New Haven, CT **Available.**
- 347 New York, NY **Available.**
- 973 Newark, NJ **Available.**
- 215 Philadelphia, PA **Available.**
- 610 Philadelphia, PA **Available.**
<table>
<thead>
<tr>
<th>Area Code</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>012 27</td>
<td>Canterbury</td>
</tr>
<tr>
<td>012 28</td>
<td>Carlisle</td>
</tr>
<tr>
<td>012 29 79</td>
<td>Barrow-in-Furness</td>
</tr>
<tr>
<td>012 29 80</td>
<td>Barrow-in-Furness</td>
</tr>
<tr>
<td>012 33</td>
<td>Ashford</td>
</tr>
<tr>
<td>012 34</td>
<td>Bedford</td>
</tr>
<tr>
<td>012 35</td>
<td>Abingdon</td>
</tr>
<tr>
<td>012 36</td>
<td>Coatbridge</td>
</tr>
<tr>
<td>012 37</td>
<td>Bideford</td>
</tr>
<tr>
<td>012 39</td>
<td>Cardigan</td>
</tr>
<tr>
<td>012 41</td>
<td>Arbroath</td>
</tr>
<tr>
<td>012 42</td>
<td>Cheltenham</td>
</tr>
<tr>
<td>012 43</td>
<td>Chichester</td>
</tr>
<tr>
<td>014 92</td>
<td>Colwyn Bay</td>
</tr>
<tr>
<td>014 93</td>
<td>Great Yarmouth</td>
</tr>
<tr>
<td>014 94</td>
<td>High Wycombe</td>
</tr>
<tr>
<td>014 95</td>
<td>Pontypool</td>
</tr>
<tr>
<td>014 96</td>
<td>Port Ellen</td>
</tr>
<tr>
<td>014 97</td>
<td>Hay-on-Wye</td>
</tr>
<tr>
<td>014 99</td>
<td>Inveraray</td>
</tr>
<tr>
<td>015 01</td>
<td>Harthill</td>
</tr>
<tr>
<td>015 02</td>
<td>Lowestoft</td>
</tr>
<tr>
<td>015 03</td>
<td>Looe</td>
</tr>
<tr>
<td>015 05</td>
<td>Johnstone</td>
</tr>
<tr>
<td>015 06</td>
<td>Bathgate</td>
</tr>
<tr>
<td>015 07</td>
<td>Alford</td>
</tr>
<tr>
<td>017 79</td>
<td>Peterhead</td>
</tr>
<tr>
<td>017 80</td>
<td>Stamford</td>
</tr>
<tr>
<td>017 82</td>
<td>Stoke-on-Trent</td>
</tr>
<tr>
<td>017 84</td>
<td>Staines</td>
</tr>
<tr>
<td>017 85</td>
<td>Stafford</td>
</tr>
<tr>
<td>017 86</td>
<td>Stirling</td>
</tr>
<tr>
<td>017 87</td>
<td>Sudbury</td>
</tr>
<tr>
<td>017 88</td>
<td>Rugby</td>
</tr>
<tr>
<td>017 89</td>
<td>Stratford-on-Avon</td>
</tr>
<tr>
<td>017 90</td>
<td>Spilsby</td>
</tr>
<tr>
<td>017 92</td>
<td>Swansea</td>
</tr>
<tr>
<td>017 93</td>
<td>Swindon</td>
</tr>
<tr>
<td>017 94</td>
<td>Romsey</td>
</tr>
</tbody>
</table>
ISP Peering Information

VoIP ISPs need to publish their numbers
- Peering Partner Routing databases

Information available from
- Public ENUM (Sipgate did it)
- Web page
- Email to tech people

Lists leak information
- User movement per ISP per day

"Number Harvesting Success Rating"
- very valuable but hard to come by
Government Databases

Used For

- PSTN routing at DTAG AG (Deutsche Telekom)
- Law Enforcement
  - where to tap the line?

Official Copies available

- Website (i.e. bnetza.de)
- Lookup # blocks assigned to VoIP ISPs

"Number Harvesting Success Rating"

- best place to start
Active Probing

locate VoIP device and ask for registered #
  - hardly works

ask VoIP server about a number
  - “100 Trying”, 180, 183, 200, ...
    • user exists and is logged on
  - “404 Not Found”
    • belongs to ISP but unassigned
  - “480 Temporarily Unavailable”
    • hit but currently not registered

"Number Harvesting Success Rating"
  • best way to increase quality of information
Demo: Server Responses
Demo: Scanning a Number Block
Auxiliary Services

“Sign Up and get a username for email, community ... and VoIP”
- VoIP addresses not limited to numbers

Use email address for VoIP
- or DSL account name
- true for freenet.de

"Number Harvesting Success Rating"
- high hit rate
- false positives: account exists but is unused
Sniffing

Sniff messages off wire

Numbers used in

- Request URI
- To / From
- Diversion
- Caller-ID
- Presence / Instant Messaging

"Number Harvesting Success Rating"

- low density
- redundant information
Enhancing Information

- pull more information from public ENUM
  - or webpage

- subscribe victim in ICQ like Presence service
  - track online activity patterns

- sniff call patterns
  - time of day, length, destination
Social Engineering

Ask ISP

– “I was billed for a call to xxx-xxx-xxx. I thought this was free. Which numbers belong to you in <sometown> or can be reached for free?”
– “What do your numbers in <thattown> start with?”

Ask Someone

– “What's your Vonage number?”
  • obtain number length and common prefix

"Number Harvesting Success Rating"
– anything from worst-case to direct hit
SPIT Examples

Real World Examples
- I have yet to experience large scale real life SPIT

Artifical Examples
- Sure ... demos!

Will SPIT work?
- probably not
- due to media discontinuity
- indirect use of SPIT would work
  - viral marketing, slander
certain Clients support Alert-Info header
- Thomson
  - www.thomsontelecompartner.com/getfile.php?id=3450
- Snom
- Cisco

Alert-Info header part of INVITE
- Alert-Info: <http://123.org/viagra.wav>

send Alert-Info pointing to SPIT message
- make phone play Viagra SPIT as ring tone
Non-SPIT Abuse of Information

use information gathered to attack networks
- get victims IP by calling him
- break into router, resell services
- send low quality SMS spam

televoting fraud
- Eurovision Song Contest / American Idol
- place fake votes using hijacked equipment
Conclusions

- SPIT will happen
- Increased load due to scanning
  - Likely
  - Likely to be pretty low
- Protection against SPIT
  - Problematic legal situation
  - Projects still in the kindergarten days
Questions and Answers

Hendrik Scholz
hs@123.org
http://www.wormulon.net/