freenet

Hacking VoIP Routers

Power Of Community 2007
Hendrik Scholz
hs@123.org

Agenda

- VoIP enabled DSL Routers
- Locating devices
- Fingerprinting
- Attacks
- Conclusions

VoIP enabled devices

Software Clients

- aka "softphones"
- your average Windows client
- often reassembles look and feel of a phone
- features
  - lots of CPU power
  - constant updates

Hardware Phones

- aka "hardphones"
- three major types
  - VoIP enabled (mobile) phones
  - PSTN to VoIP converters (ATAs)
  - (DSL) routers with embedded VoIP capabilities

The usual Suspects

The Suspect

- direct internet connection
  - no NAT issues for VoIP
  - no protection from the outside world
  - direct access to SIP stack
- Linux based

Locating VoIP devices

Locating VoIP Routers

- comparison
  - search for open mailservers / http proxies
  - well known port (25/80, 5060 in this case)
  - nmap is great for this
  - conclusion
- write a SIP aware nmap clone
  - low SIP density, thus has to be fast

smap

- feature-wise mashup of
  - nmap (http://insecure.org/nmap/)
  - sipsak (http://sipsak.org/)
- somewhat stateful SIP test tool
- http://www.wormulon.net/smap/
- NEW: multi-threaded for POC2007
  - 5-100x faster than before
  - can saturate ~~your~~ my local DSL uplink ;)

live demo

single host scanning with smap

smap: testing a single host

```
$ smap router.wormulon.net

smap 0.6.0-ng <hs@123.org> http://www.wormulon.net/

89.53.25.243: ICMP not tested, SIP enabled

1 host scanned, 1 SIP enabled
$
```

scanning networks

- which networks? sources:
  - check DSL/cable ISPs that also have VoIP
  - Dialup Blacklists
    - verified that these IPs belong to customers
  - IRC channels
    - topic related (Linux, VoIP, Asterisk, ...)

live demo

network scanning with smap

smap: scanning a network

```
$ time smap 89.53.25.0/24
89.53.25.72: ICMP not tested, SIP enabled
89.53.25.100: ICMP not tested, SIP enabled
...
89.53.25.254: ICMP not tested, SIP disabled

256 hosts scanned, 180 SIP enabled (70.3%)

real    0m18.880s
user    0m0.004s
sys     0m0.008s
```

network scanning results

- 60-80% success rate on "good" networks
- around 1-5% on random networks
- Best case attack preparation
  - vulnerable device known
  - ISP selling that device is known
  - 1 minute scan time per /24
  - 50% success rate
  - result: ~7500 vulnerable hosts per hour

VoIP related protocols

- helpful protocols to identify VoIP devices
  - ACS - Auto Configuration server
  - MGCP - Media Gateway Control Protocol
  - IAX - Inter-Asterisk eXchange
  - H.323 – ITU-T Q931 based VoIP
- protocols all less used than SIP

Auto Configuration Server

- Thesis: DSL router configuration is too complicated
- Solution: Remote configuration/management
- Implementation: TCP port 8000 open on router
- Features
  - push/pull/replace config
  - remote actions, i.e. reboot

ACS - Scanning / Attacking

- Scanning and Fingerprinting
  - send "GET / HTTP/1.0" to port 8000
  - compare quoted realm against database of known ACS strings
- Attacking
  - SSL all the way
  - Certificates on both client and server
  - another talk next year?

MGCP

- MGCP = Media Gateway Control Protocol
  - RFC 3435 defines MGCP 1.0
- API for media gateways
  - no way to set up calls
  - divert/manage media
- Usage
  - deprecated for clients
  - used on backbones for decomposed Voice switches

Fingerprinting VoIP devices

Fingerprinting

- Three steps
  - send request
  - receive response
  - parse response and compare oddities to database
- Source of differences
  - supported methods, features
  - text representation (SIP is clear text)
  - ability to parse broken messages

Fingerprinting: sample message

```
OPTIONS sip:smap@localhost SIP/2.0

Via: SIP/2.0/UDP 89.53.52.174:12345;branch=z9hG4bK.
   18752;rport;alias

From: <sip:smap@89.53.52.174:12345>;tag=3170f461dc2786

To: <sip:smap@localhost>

Call-ID: 91902014@89.53.52.174

CSeq: 45717 OPTIONS

Contact: <sip:smap@89.53.52.174:12345>

Content-Length: 0

Max-Forwards: 70

User-Agent: smap 0.6.0-ng

Accept: text/plain
```

live demo

fingerprinting a single host

smap: fingerprinting a single host

```
$ smap -o router.wormulon.net

smap 0.6.0-ng <hs@123.org> http://www.wormulon.net/

89.53.52.154: ICMP not tested, SIP enabled
       Guess: AVM FRITZ!Box Fon Series firmware: 14.04.06 (May 18 2006)
  User-Agent: AVM FRITZ!Box Fon WLAN 7170 (fs) 29.04.40 (Aug  3 2007)

1 host scanned, 1 SIP enabled (100.0%)
$
```

live demo

fingerprinting a network

smap: fingerprinting a network

```
$ smap -o 89.53.52.0/24
[...]
89.53.52.0: ICMP not tested, SIP enabled
       Guess: AVM FRITZ!Box Fon Series firmware: 29.04.29 (Dec  8 2006)
  User-Agent: AVM FRITZ!Box Fon WLAN 7050 14.04.31 (Feb  5 2007)
89.53.52.1: ICMP not tested, SIP enabled
       Guess: AVM FRITZ!Box Fon Series firmware: 29.04.29 (Dec  8 2006)
  User-Agent: AVM FRITZ!Box Fon WLAN 7170 29.04.22 (Sep  6 2006)
[...]
89.53.52.4: ICMP not tested, SIP disabled
89.53.52.5: ICMP not tested, SIP disabled
[...]
256 hosts scanned, 177 SIP enabled (69.1%)
$
```

Attacking VoIP routers

Possible Attacks

- Unwanted Contact (SPIT)
- Denial of Service
- Misrepresentation
- Communication Interception
- lots of low level parser stuff

Attack: Unwanted Contact

- Issues
  - need to bypass ISP authentication
  - need to bypass blacklists, firewalls, ...
  - need to know extension/user to contact
- Attack
  - craft message(s) to make phone ring
  - get users attention
  - optional: play V*i*a*g*r*a SPIT message

Samsung Unwanted Contact

- task: bypass ISP
  - directly talk to IAD
- task: bypass "firewall"
  - not implemented on Samsung IAD
- task: find valid extension
  - bug on Samsung IAD
- 0day advisory: Samsung-unwanted-contact.txt

live demo

Samsung IAD
''Unwanted Contact''

SPIT: Alert-Info Abuse 1/2

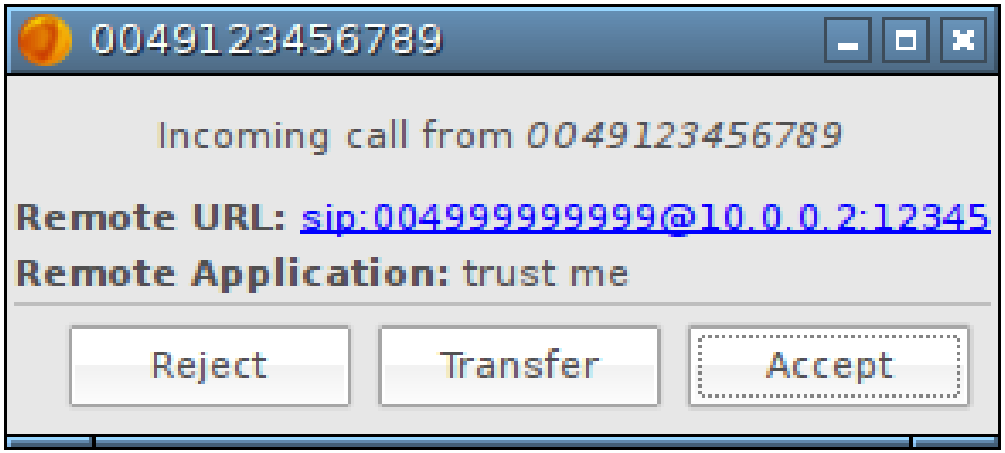
- Alert-Info is a SIP header defined in RFC3960
- set distinct ringtone
  - proprietary/abstract number
  - proprietary/abstract name
  - URI to .wav file
- supported by
  - Asterisk, Grandstream, Thomson, Snom
  - not mandatory (RFC 3960 > 3261)

Unwanted Contact: Ekiga

- comparable to Samsung issue
- published as:
  `Ekiga_INVITE_RURI_advisory.txt`
- adds a new twist:
  - Misrepresentation

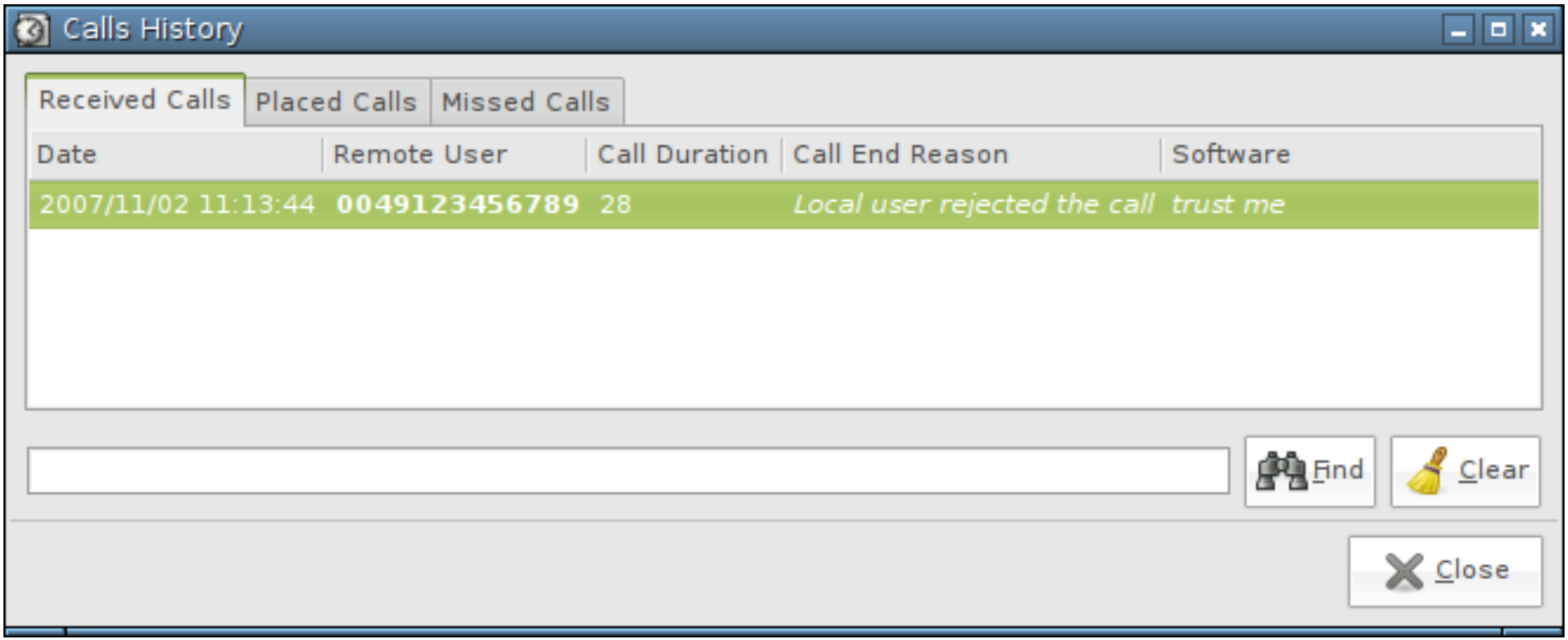
Ekiga Misrepresentation Attack

- INVITE contains From: header
  - `From: "abc" <sip: 123@10.0.0.2:12345>;tag=71a59b73`
  - split into displayname and SIP URI
- popup window on incoming call:



Ekiga Misrepresentation 2/2

- Call History shows displayname field



Misrepresentation Attacks

- Inside Ekiga
  - user clicks on displayname
  - Ekiga calls SIP URI
  - “oh my bank called” “please enter account information”
- Outside Ekiga
  - user copies displayname
  - calls number which wasn't known/trusted inside VoIP network

SPIT: Alert-Info Abuse 2/2

- Preparation
  - put SPIT audio file on hacked webserver
- Attack
  - send modified call setup message to victim
  - phone receives message
    - pulls .wav file off website
    - starts playing "custom" ringtone

AVM 0-Byte UDP bug

- AVM Fritz!Box is series of VoIP/DSL routers
- empty UDP message to SIP port will be forwarded to SIP stack
  - SIP stack crashes
  - no incoming calls possible
- Attack: `hping3 -2 -d 0 -p 5060 <target>`
- first published:
  http://mazzoo.de/blog/security/FritzBox_DoS.writeback
- fixed in early 2007 but still seen in the wild

VoIP Cross Site Scripting

- VoIP devices have web interface with call logs
  - inject malicious content
  - i.e. Javascript
- credits to Radu State
  - “Owning the internal network with SIP (part 1) and a Linksys Phone”
  - http://seclists.org/fulldisclosure/2007/Oct/0174.html

XSS Example

```
INVITE sip:testac.0180.01@freenet.de SIP/2.0
Via: SIP/2.0/UDP 10.0.0.2:12345;branch=z9hG4bK.
  0c430fd8;rport;alias
From: "blafasel" <sip:
  01801411111999@10.0.0.2:12345>;tag=71a59b73
To: sip:testac.0180.01@freenet.de
Call-ID: 190667864 3@10.0.0.2
CSeq: 9 INVITE
Content-Length: 0
Contact: sip:sipsak@10.0.0.2:12345
```

$ sipsak -f <filename> -s sip:freenet.de -p <IP>

Outlook

- VoIP Botnets
- SPIT
- SBC in between all calls?
  - VoIP firewalls
  - breaking them has huge impact

Questions and Answers

Hendrik Scholz

hs@123.org