Just how vulnerable is your phone system?

by Sandro Gauci

$ whoami

- Sandro Gauci (from .mt)
- Security researcher and Pentester
- SIPVicious / VOIPPACK for CANVAS
- VOIPSCANNER.com
- Not just about VoIP
- EnableSecurity

Introducing: security issues

- VoIP attack surface is huge
  - SIP RFC 3261 = 269 pages
  - Referencing a large number of other RFCs
  - Most solutions come with other services
    - Web interface, tftp etc

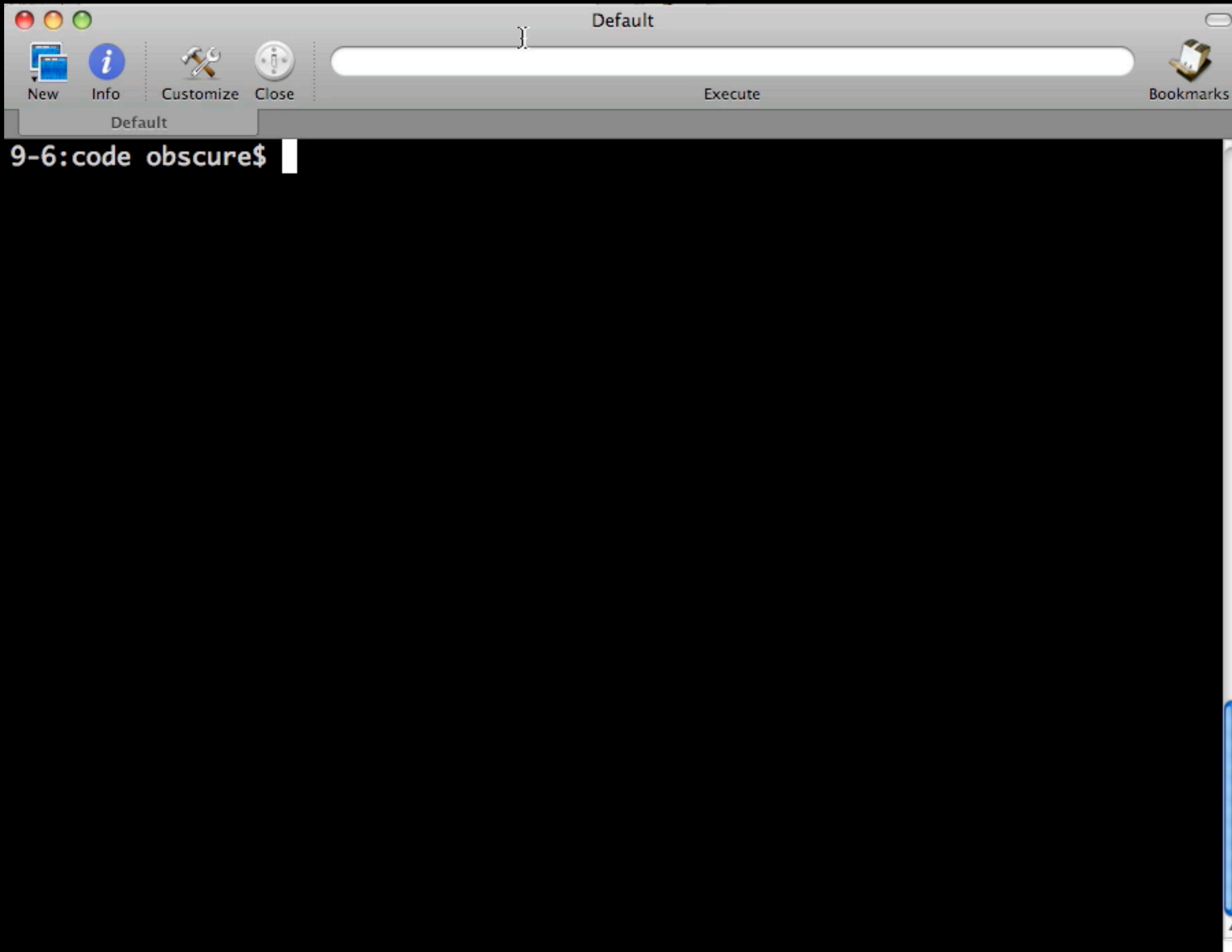
Protocol specific issues

- SIP on UDP is most common
  - also most vulnerable to passive monitoring
  - no encryption used
- The SIP RFC enables user enumeration
- Peer to peer SIP creates some challenges

User enumeration on SIP

- Different responses to REGISTER request
- Returns 404 when ‘user’ is not found
- Returns 200 or 401 when the ‘user’ exists
  - 200 = no password set!
  - 401 = challenge / authenticate

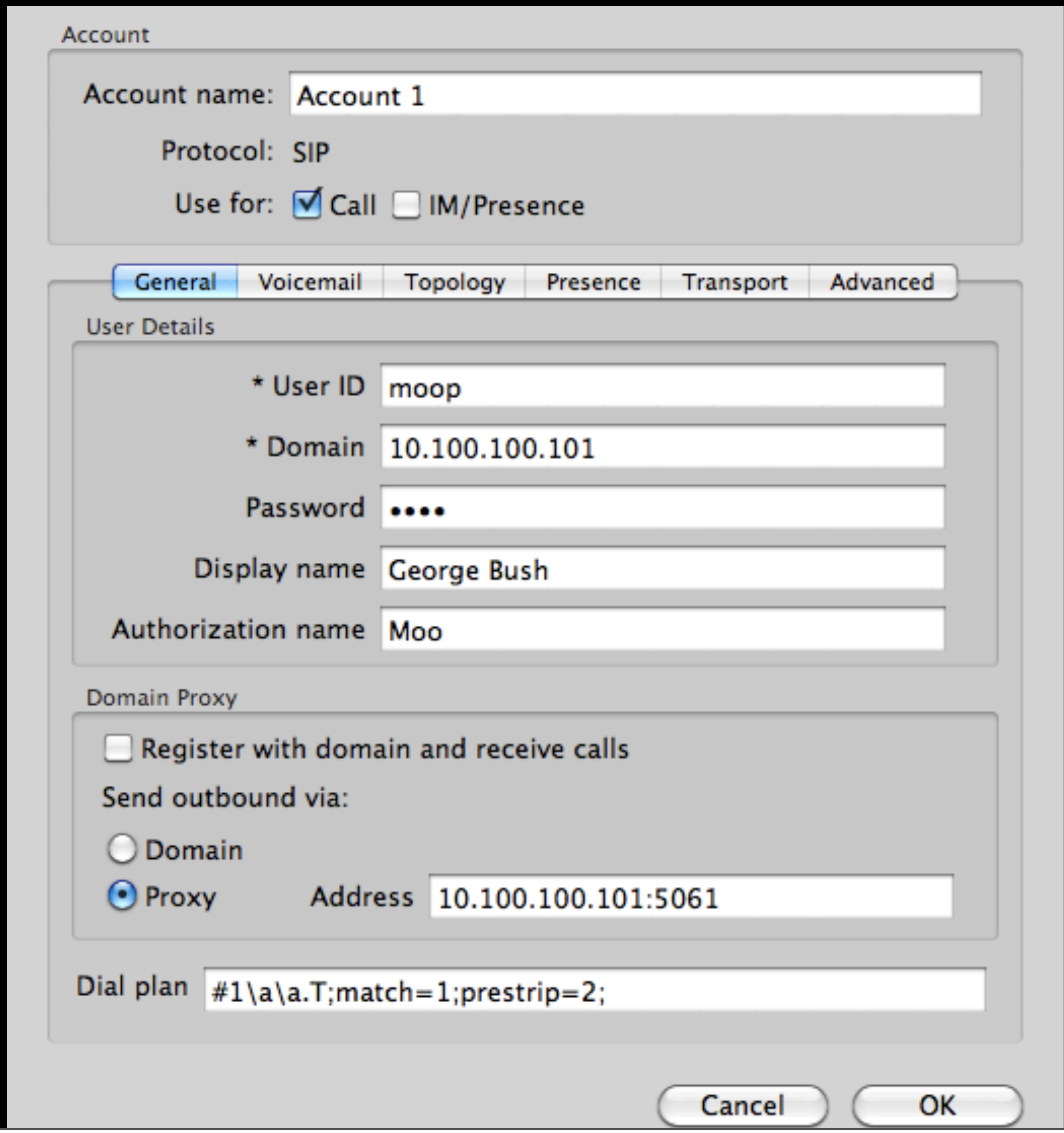
enumeration demo


Default
New
Info
Customize
Close
Execute
Bookmarks
Default
9-6:code obscure$

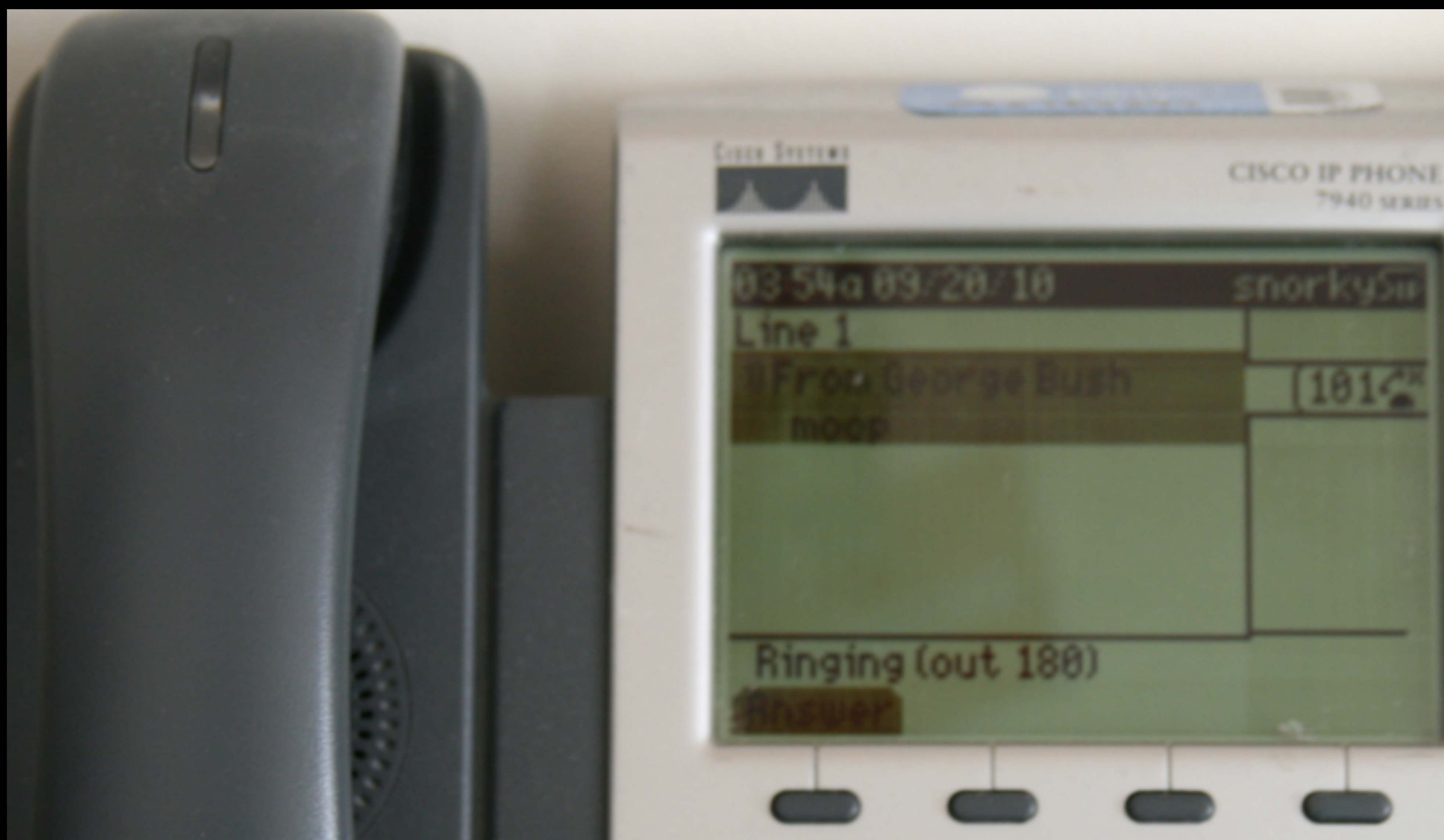
Peer to Peer SIP

- When endpoints can contact each other
    - they can spoof caller ID
    - they can bypass logging
    - exploit some interesting features in SIP

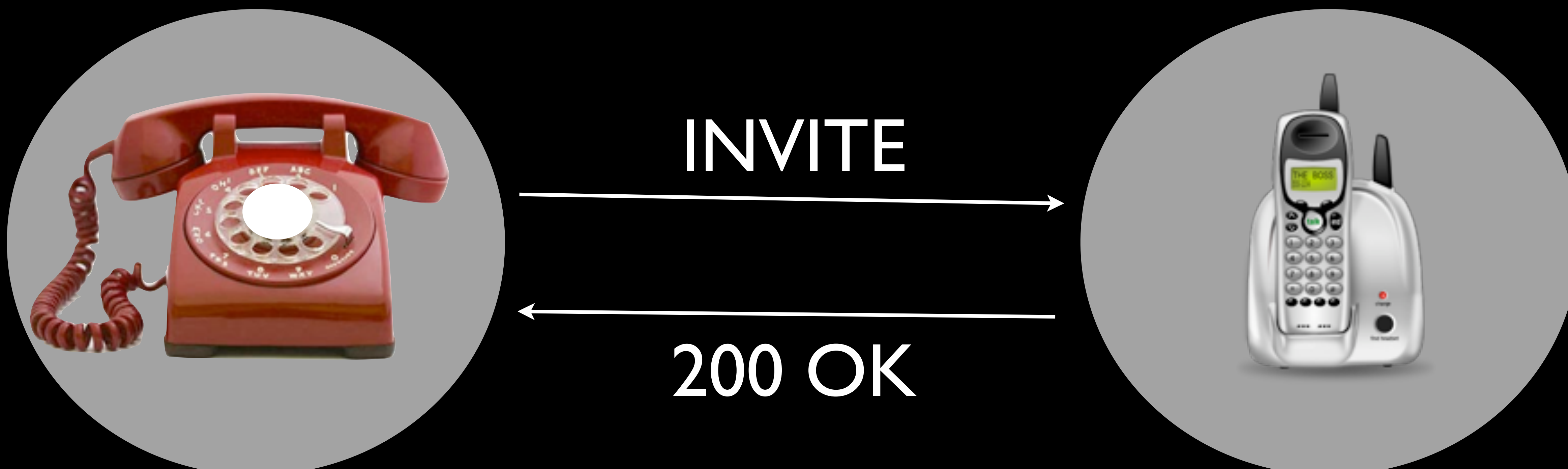
Spoofing caller ID



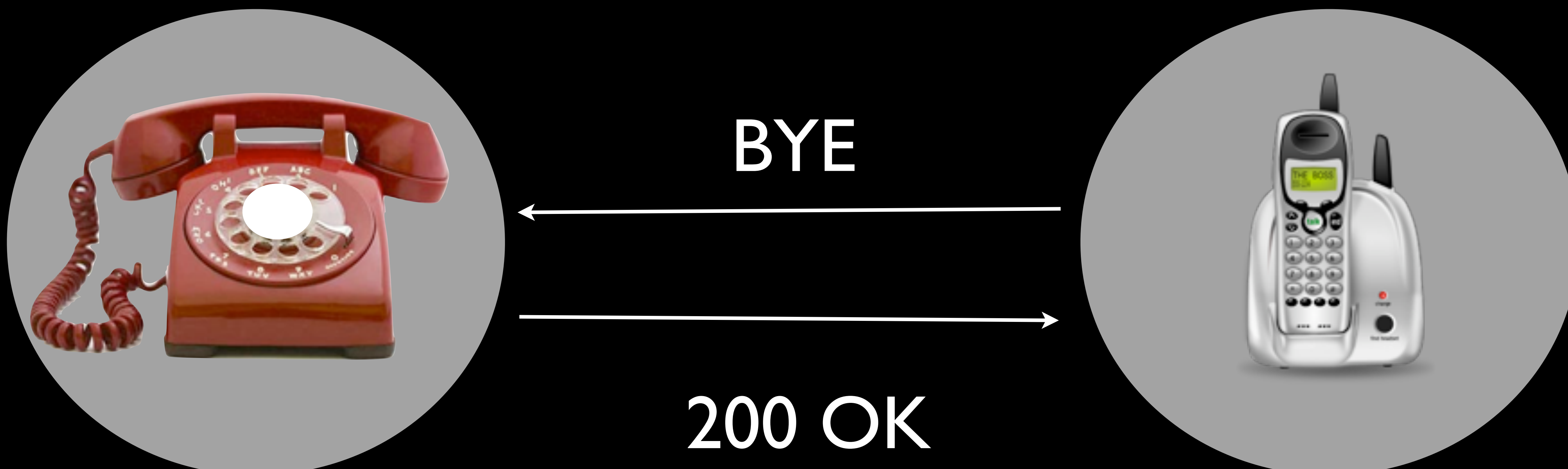
Spoofing caller ID



SIP Digest Leak

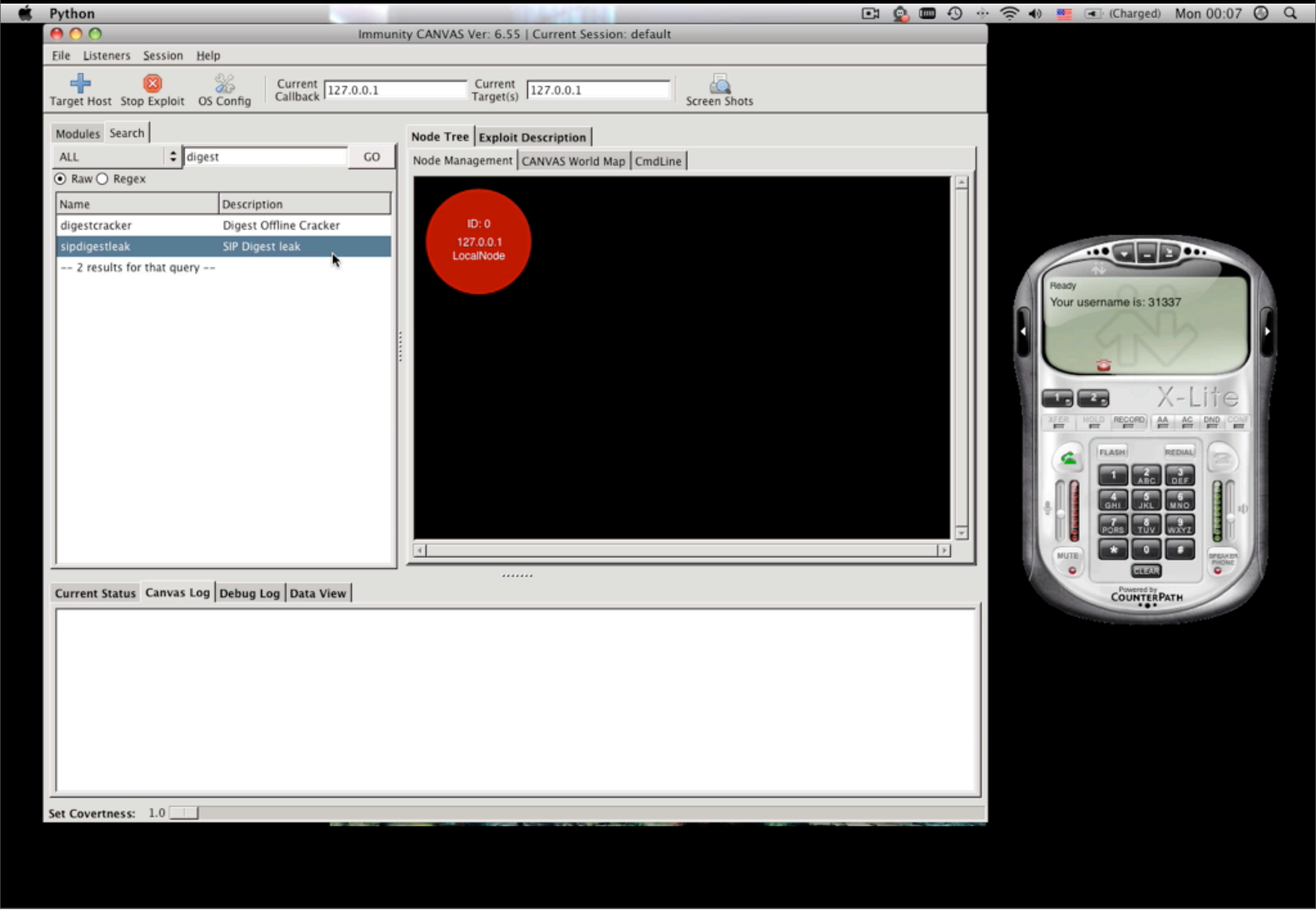


SIP Digest Leak



SIP Digest Leak

Demo of SIP Digest leak



Friday, 29 October 2010

Distro and PBX specific

- Default passwords
- PHP-based web applications
- FreePBX etc: emulation of other systems
- Various other services

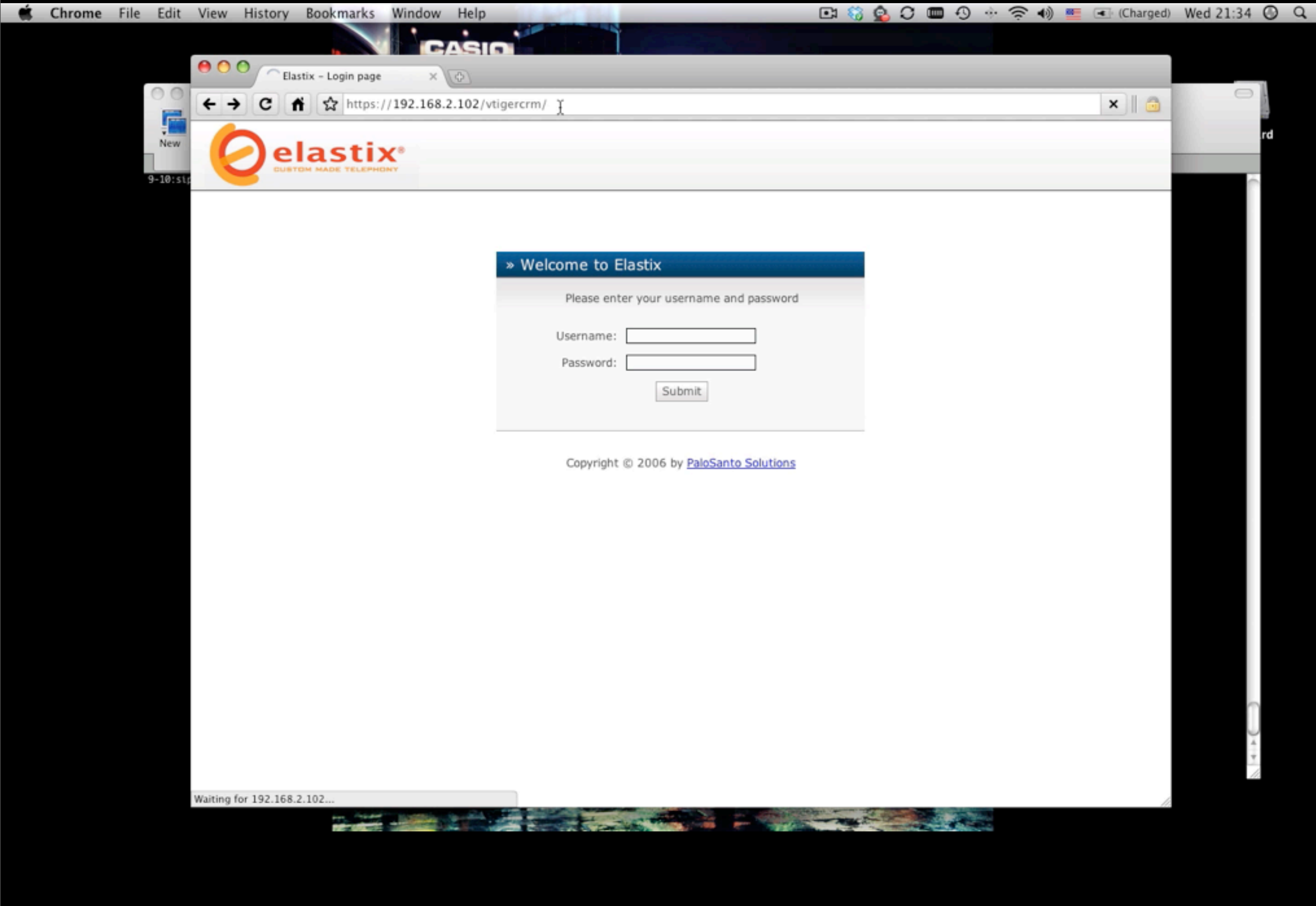
Trixbox defaults

Service	Username	Password
FOP	NA	passw0rd
AMP	admin	amp111
Admin (freepbx)	maint	password
FTP	ftpuser	asteriskftp

Elastix defaults

Service	Username	Password
web interface	admin	palosanto
freePBX	admin	admin
FOP	admin	eLaStIx.2oo7
a2billing	admin	mypassword
sugar crm	admin	admin
vTiger	admin	password

* reference


Chrome File Edit View History Bookmarks Window Help
(Charged) Wed 21:34
Elastix - Login page
https://192.168.2.102/vtigercrm/
New
elastix
» Welcome to Elastix
Please enter your username and password
Username:
Password:
Submit
Copyright © 2006 by PaloSanto Solutions
Waiting for 192.168.2.102...

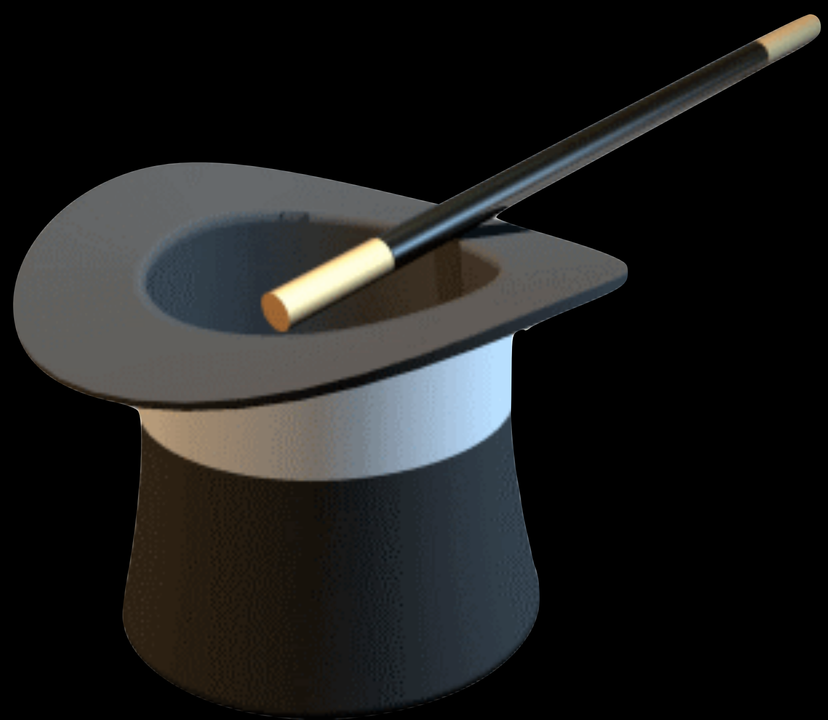
What’s happening?

- Are these vulnerabilities really an issue?
- Which ones are being abused?
- What are their motivations?
- Who are they?

Introducing voiphun

- Short for "voip honeypot" :-)
- A very simple fake SIP registration server
- And fake proxy too (i.e. takes calls)
- Which can be used as a honeypot
- Still limited in functionality

What's in voiphun's hat?



What we're seeing

- Compromised hosts looking for SIP devices
- Attackers trying to make phone calls
- Attackers scanning for extensions with weak passwords

What we’re seeing

- SIPVicious scans
- Custom / unknown scanners
- INVITE scans

INVITE scan example

```
INVITE sip:00423662701946@xx.xx.xx.xx;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 188.27.208.189:62399;branch=z9hG4bK-d8754z-ffab3c4b5a504640-1---
d8754z-
Max-Forwards: 70
Contact: <sip:100@188.27.208.189:62399;transport=UDP>
To: <sip:00423662701946@xx.xx.xx.xx;transport=UDP>
From: "UNKNOWN"<sip:100@xx.xx.xx.xx;transport=UDP>;tag=9a46293c
Call-ID: OGVmNmI1NmU3MTVmYTBmMTliMWZjMzdlYjI2N2U3ZTk.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Content-Type: application/sdp
User-Agent: Zoiper rev.5324
Content-Length: 332

v=0
o=Zoiper_user 0 0 IN IP4 188.27.208.189
s=Zoiper_session
c=IN IP4 188.27.208.189
t=0 0
m=audio 65287 RTP/AVP 3 0 8 110 98 101
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:110 speex/8000
a=rtpmap:98 iLBC/8000
a=fmtp:98 mode=30
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

I <3 Patterns

- INVITE scans bruteforces phone numbers
- Why not extract those numbers?
- Group them by source IP / country

INVITE scan 1

Came from Romania Data Systems network

```
00000447799584555
0000441372456539
00011442086702315
0001440129870903
000441622620388
0011447876617548
001442075828187
00441189780316
011442076339733
01447850294946
0442078375450
1442072425376
900441767677666
9011442082163104
90447973642015
9442074998161
```

INVITE scan 2

Also from China Telecom (Guangdong) network

```
#442076501050
00#442076501050
011#442076501050
01144161660606 5
0442076501050
442076501050
900442076501050
9011442076501050
9442076501050
```

fax number

INVITE scan 3

Came from China Telecom (Shanxi) network

```
00000447799584555
0000441372456539
0000442076297347
00011442086702315
0001440129870903
0001441844208220
000441622620388
000442073878081
0011442076381111
0011447876617548
001442075828187
001447775742174
00441189780316
011442076339733
012441535610840
01447024074657
-- clipped --
```

INVITE scan 4

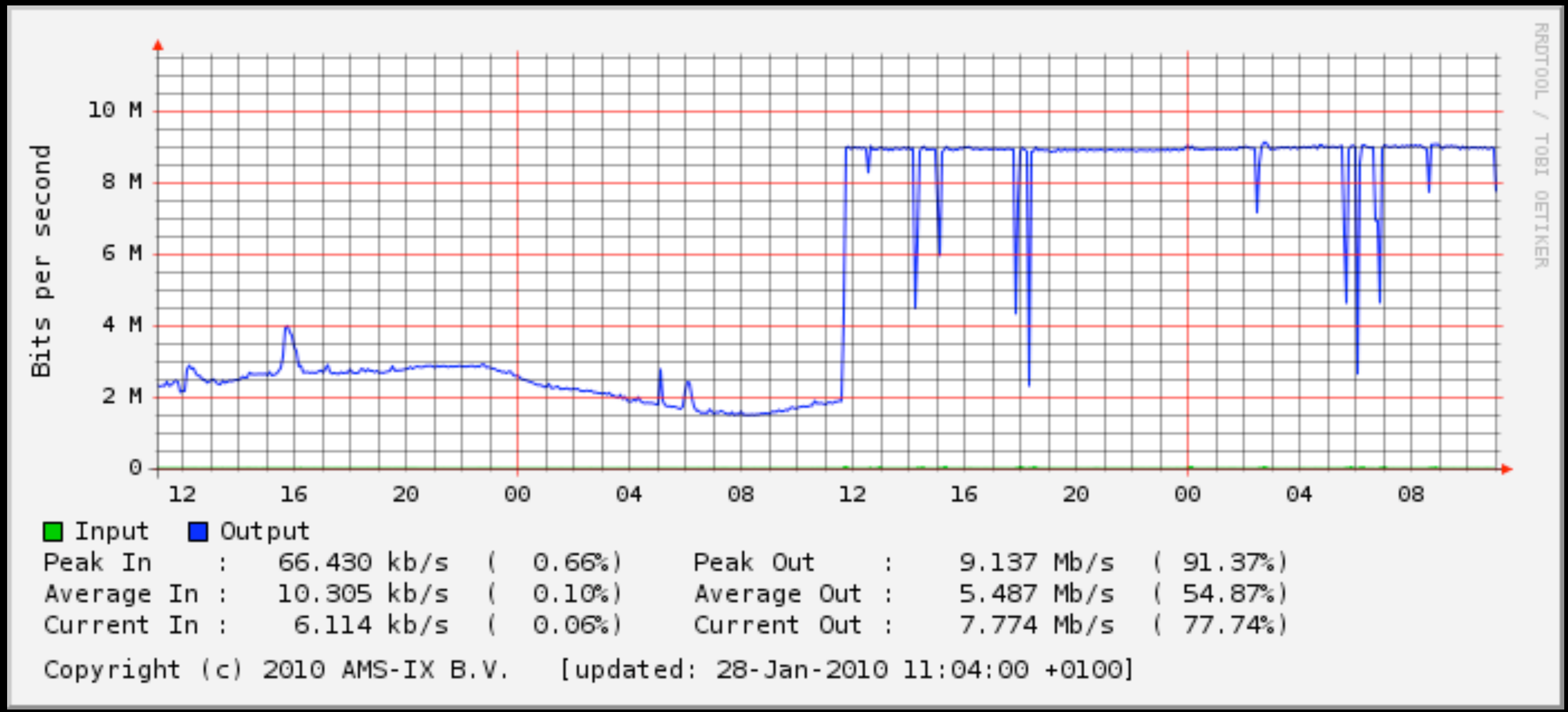
Came from ProXad network

```
33681368319
37322719718
33681368319
37322719718
33681368319
37322719718
33681368319
33681368319
```

The RIPE experiment

- 2010-01-27 they started announcing 1.1.1.0/24
- Only 10 MBit port
- It was maxed out immediately

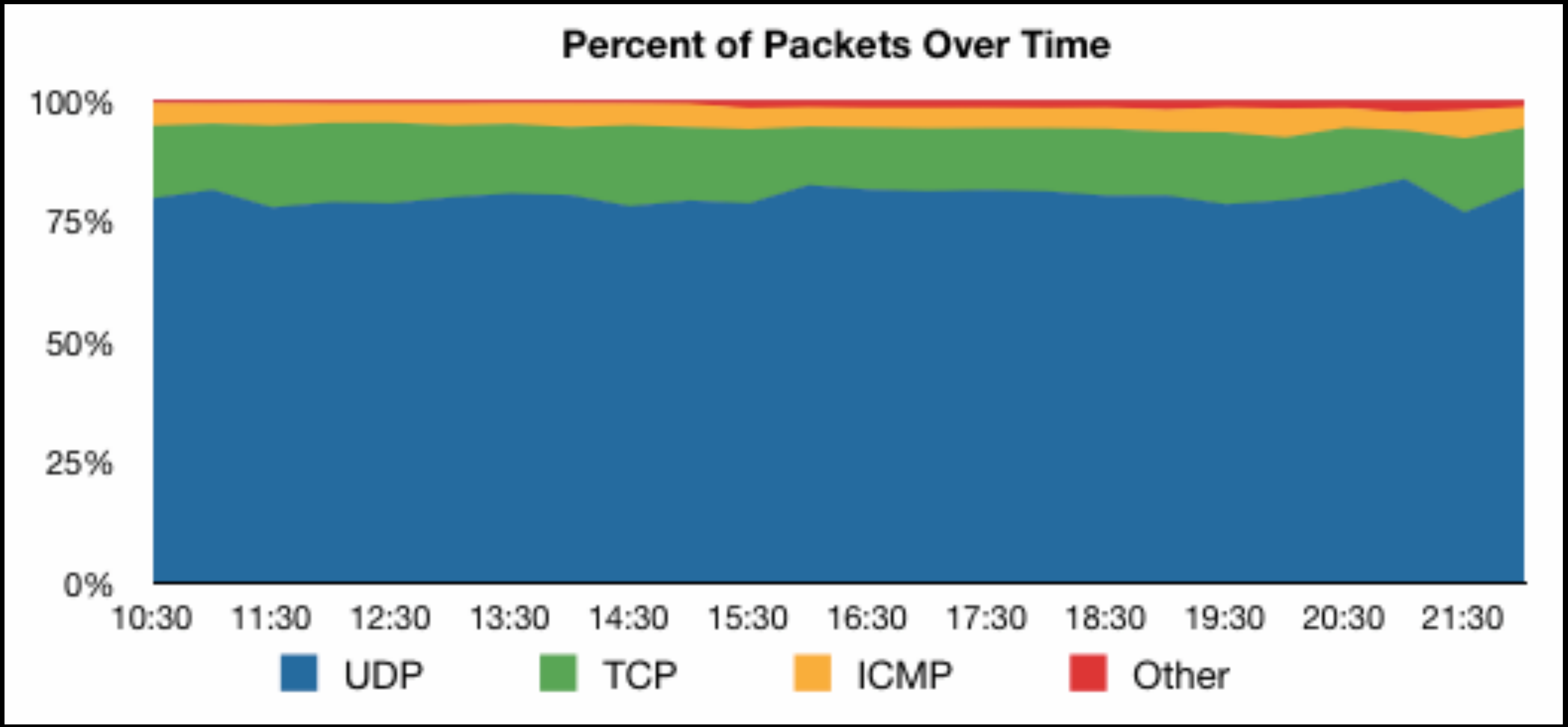
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

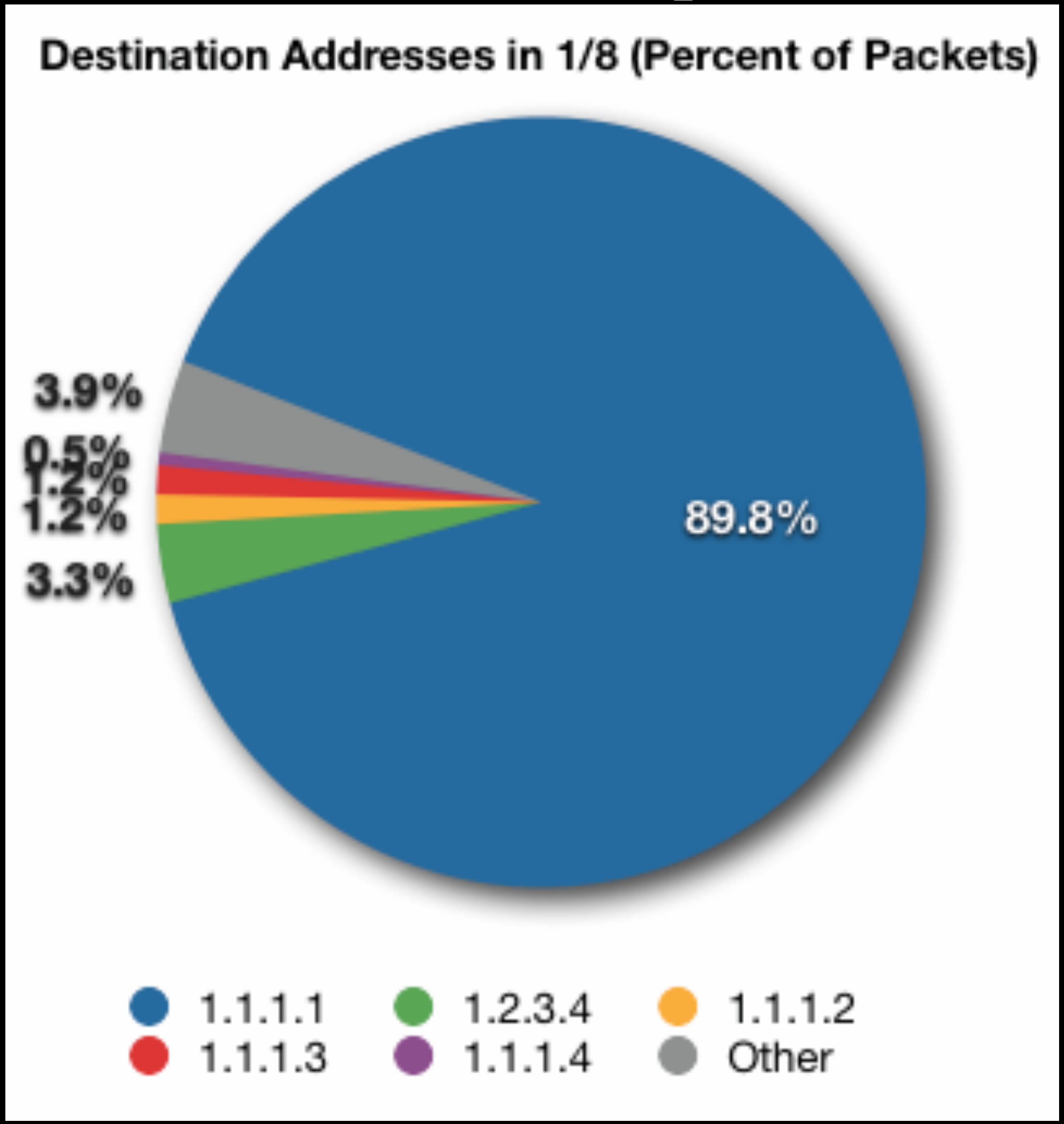
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

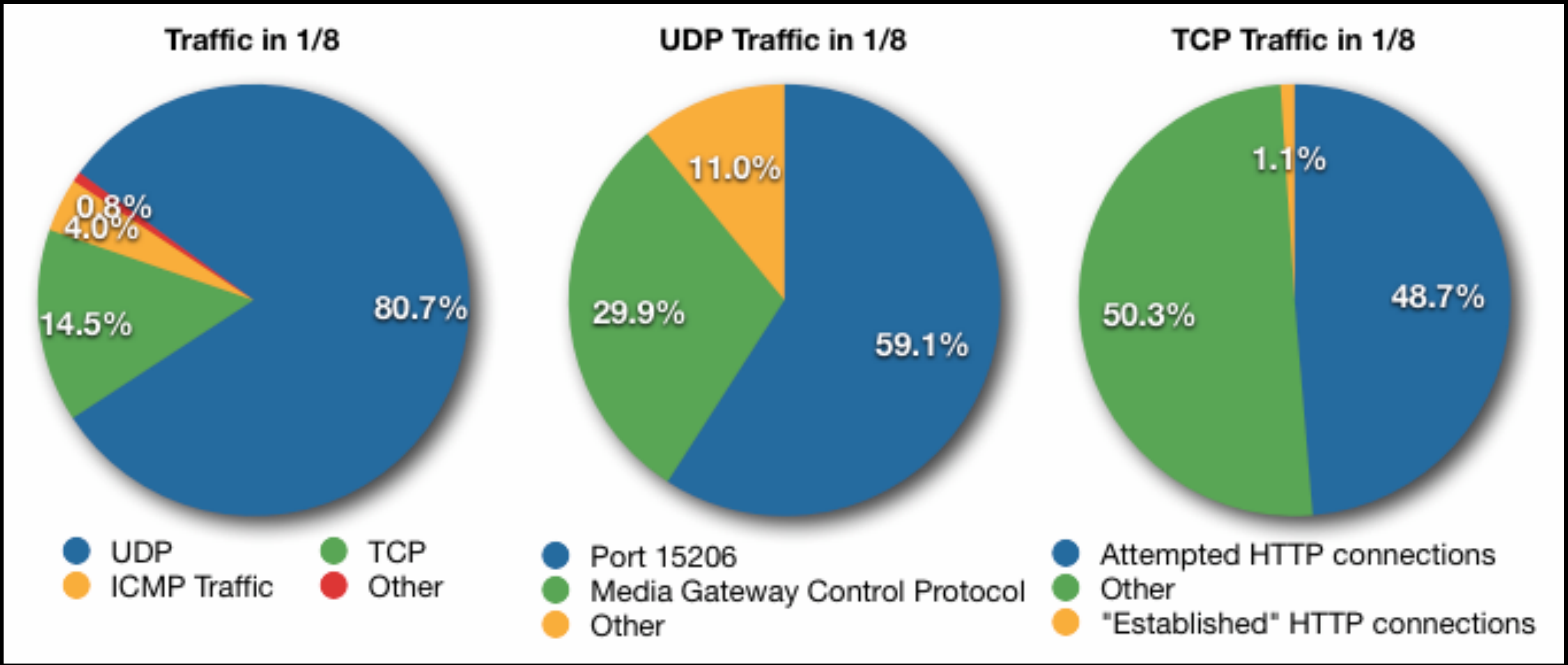
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

The RIPE experiment

the part that i found interesting:

“We found that almost **60%** of the **UDP packets** are sent towards the IP address **1.1.1.1 on port 15206** which makes up the largest amount of packets seen by our RRC. Most of these packets **start their data section with 0x80,** continue with seemingly random data and are padded to 172 bytes with an (again seemingly random) 2 byte value. Some sources (http://www.proxyblind.org/trojan.shtml) list the port as being used by **a trojan called "KiLo"**, however information about it seem sparse.”

quoting the RIPE blog

http://labs.ripe.net/content/pollution-18

back in voiphun land

```
INVITE sip:011442083327467@re.pl.ac.ed SIP/2.0
Via: SIP/2.0/UDP 83.142.202.195:3058;branch=ca4b60ae7ba821fREPLACEDjrgrg;rport
From: <sip:sip@83.142.202.195>;tag=Za4b60aeREPLACED
To: <sip:011442083327467@re.pl.ac.ed>
Contact: <sip:sip@83.142.202.195>
Call-ID: 213948958-00227506489-384748@83.142.202.195
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 503

v=0
o=sip 2147483647 1 IN IP4 1.1.1.1
s=sip
c=IN IP4 1.1.1.1
t=0 0
m=audio 15206 RTP/AVP 10 4 3 0 8 112 5 7 18 111 101
a=rtpmap:10 L16/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:112 AAL2-G726-32/8000
a=rtpmap:5 DVI4/8000
a=rtpmap:7 LPC/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:111 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

RTP Stream goes to IP 1.1.1.1

on port 15206

RTP & SDP

- RTP (almost) always starts with an 0x80
- If an INVITE is accepted the RTP stream is sent to the IP in the SDP

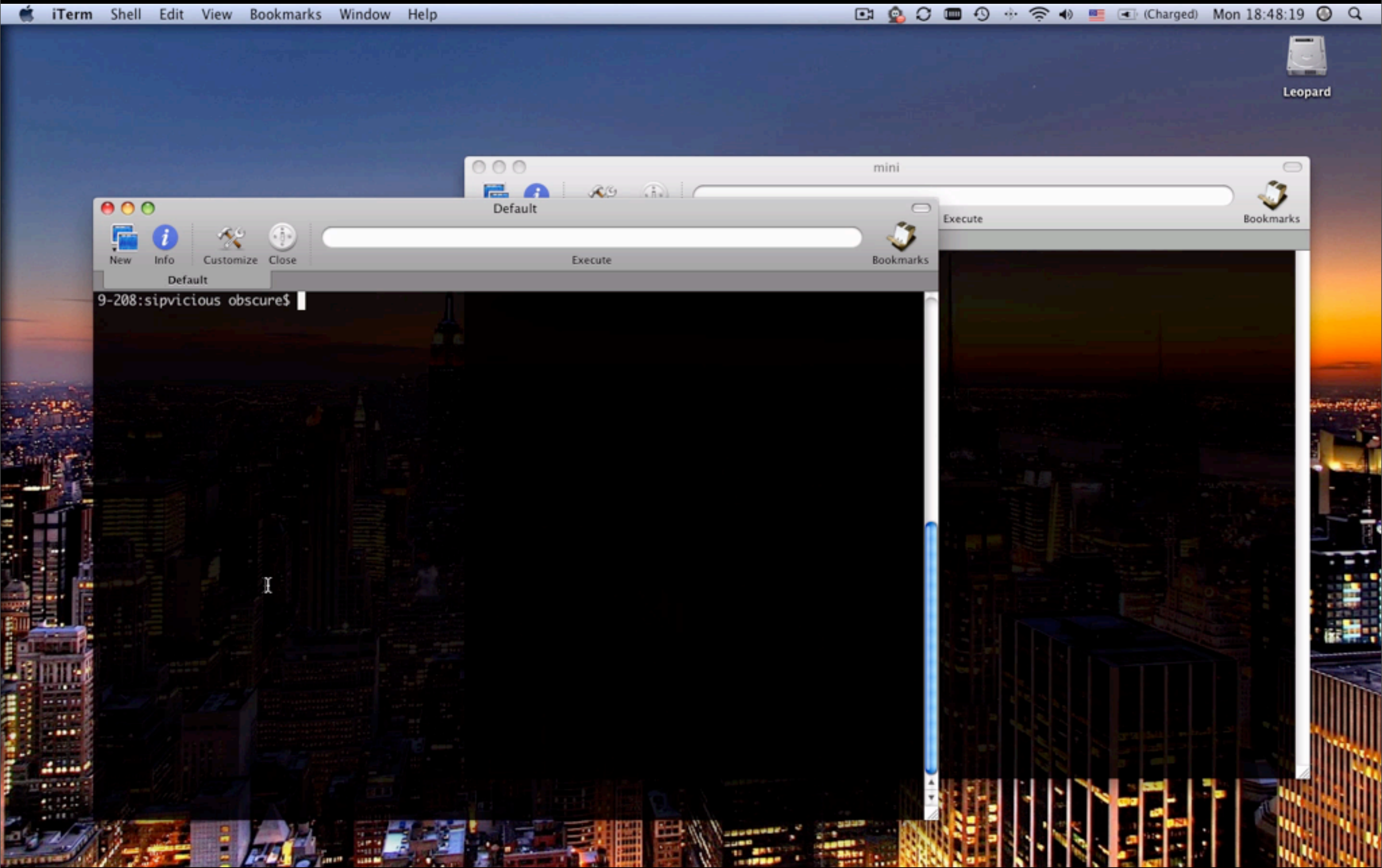
Conclusions and solutions?

- These attacks are all internet borne
- Therefore put your Asterisk on the inside
- But ..

.. this is not always possible

- ✓ Fail2ban + svcrash.py (comes with SIPVicious)
  - create exclusions for your providers!
- ✓ Responsive upstream provider
- ✓ Report to abuse
- ✓ Asterisk specific: enable alwaysauthreject

svcrash demo


iTerm Shell Edit View Bookmarks Window Help
(Charged) Mon 18:48:19
Leopard
mini
Execute
Bookmarks
Default
New Info Customize Close
Execute
Bookmarks
Default
9-208:sipvicious obscure$

Thanks

- John Todd and the Astricon team
- Sn0rky, Sjur & others who helped
- SIPVicious contributors and users

More at..

- EnableSecurity.com/research
- Sipvicious.org
- VOIPSA.org

Q.A

alternatively contact me

sandro@enablesecurity.com