The Honeynet

P R O J E C T

VoIP fraud methods used on the Internet today

Sjur Eivind Usken

Sjur Eivind Usken

Education:
Computer Engineer (University of Stavanger)
Industrial Economy and Technology Management (NTNU)

Work:
Altibox AS
→ Alarm and sensor technologies

Hobby: The Honeynet Project (and of course sailing)

Blog:
www.usken.no
Contact: sjur@usken.no

The Honeynet Project

- Open source computer security research
- Not for profit
- Volunteer
- Goal: "learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned"
- International

C T

Alaskan Chapter
Australian Chapter
Bay Area Chapter
Brazilian Chapter
Canadian Chapter
Chicago Chapter
Chinese Chapter
CyberSecurity Malaysia Chapte
Czech Chapter
French Chapter
German Chapter
Giraffe Chapter
Global Chapter
Hawaiian Chapter
Hong Kong Chapter
Indian Chapter
Iran Honeynet Chapter
Italian Chapter
Malaysian Chapter
Mexican Chapter
New Zealand Chapter
Norwegian Chapter
Orange County Chapter
Pacific Northwest Chapter
Pakistan Chapter
Philippines Chapter
Portuguese Chapter
Rochester Institute of Technolo
Singapore Chapter
Southern California ("SoCal") C
Spanish Chapter
Spartan Devils Chapter
Taiwan Chapter
UK Chapter
UNAM Chapter
UNCC Chapter
United Arab Emirates Chapter
Vietnam Honeynet Chapter
West Point Chapter

Agenda today

Short introduction to SIP

Demo SIP Exploits and vulnerabilities

Successful VoIP attacks in Norway

Does and don'ts

"You know, you can do this just as easily online."

SIP is similar to HTTP

Both are clear text based

Request and response type

Same status codes as HTTP (404 Not Found)

But SIP is different from HTTP;

In SIP - ALL devices are BOTH Server and Client

request method

request URI

caller address
and description

destination
address

content type
of the request body

header

```
INVITE sip:7170@iptel.org SIP/2.0
Via: SIP/2.0/UDP 195.37.77.100:5040;rport
Max-Forwards: 10
From: "jiri" <sip:jiri@iptel.org>;tag=76ff7a07-c091-4192-84a0-d56e91fe104f
To: <sip:jiri@bat.iptel.org>
Call-ID: d10815e0-bf17-4afa-8412-d9130a793d96@213.20.128.35
CSeq: 2 INVITE
Contact: <sip:213.20.128.35:9315>
User-Agent: Windows RTC/1.0
Proxy-Authorization: Digest username="jiri", realm="iptel.org",
 algorithm="MD5", uri="sip:jiri@bat.iptel.org",
 nonce="3cef753900000001771328f5ae1b8b7f0d742da1feb5753c",
 response="53fe98db10e1074
 b03b3e06438bda70f"
Content-Type: application/sdp
Content-Length: 451
```

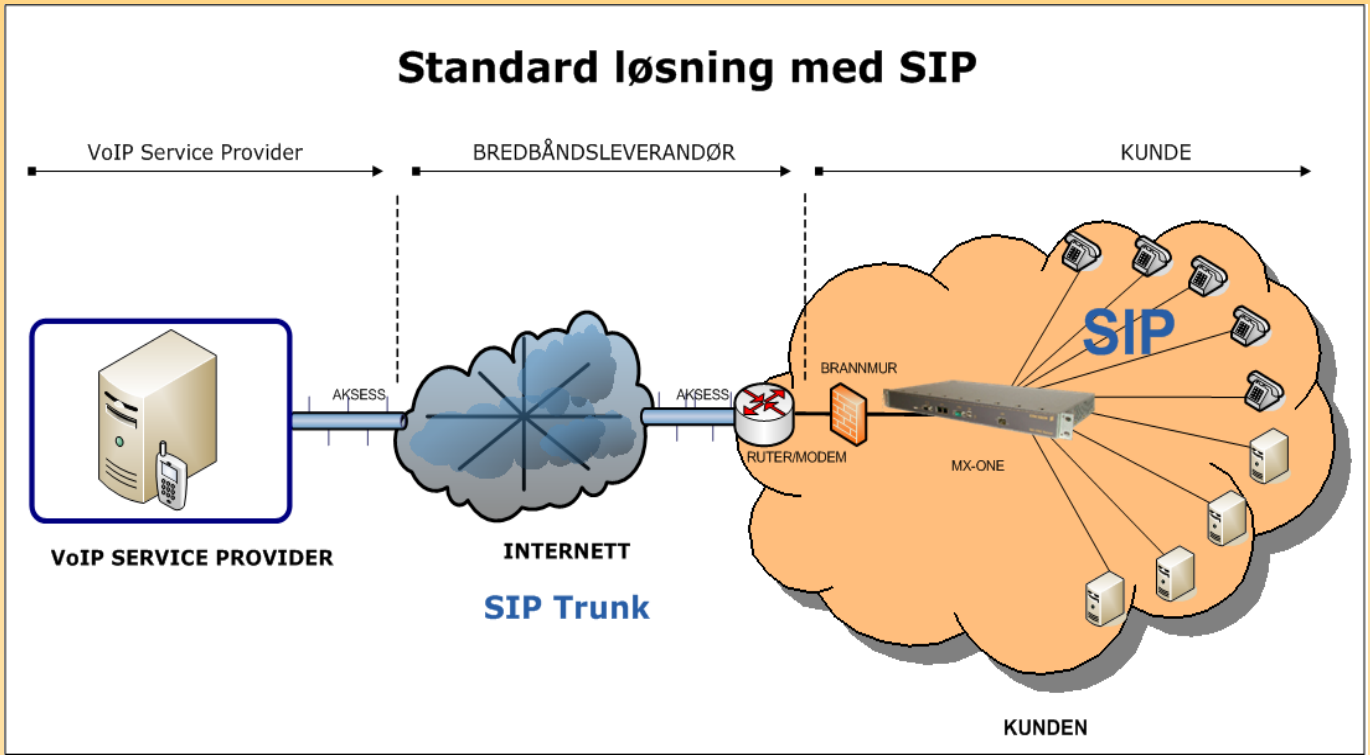
body

```
v=0
o=jku2 0 0 IN IP4 213.20.128.35
s=session
c=IN IP4 213.20.128.35
b=CT:1000
t=0 0
m=audio 54742 RTPi/AVP 97 111 112 6 0 8 4 5 3 101
a=rtpmap:97 red/8000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:6 DVI4/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
```

Where is SIP used today?

Connect to the PSTN network (bylinjer)

- SIP Trunk
  - Static IP authentication
  - SIP REGISTER
- End-devices
  - Desktop phones
  - Soft clients

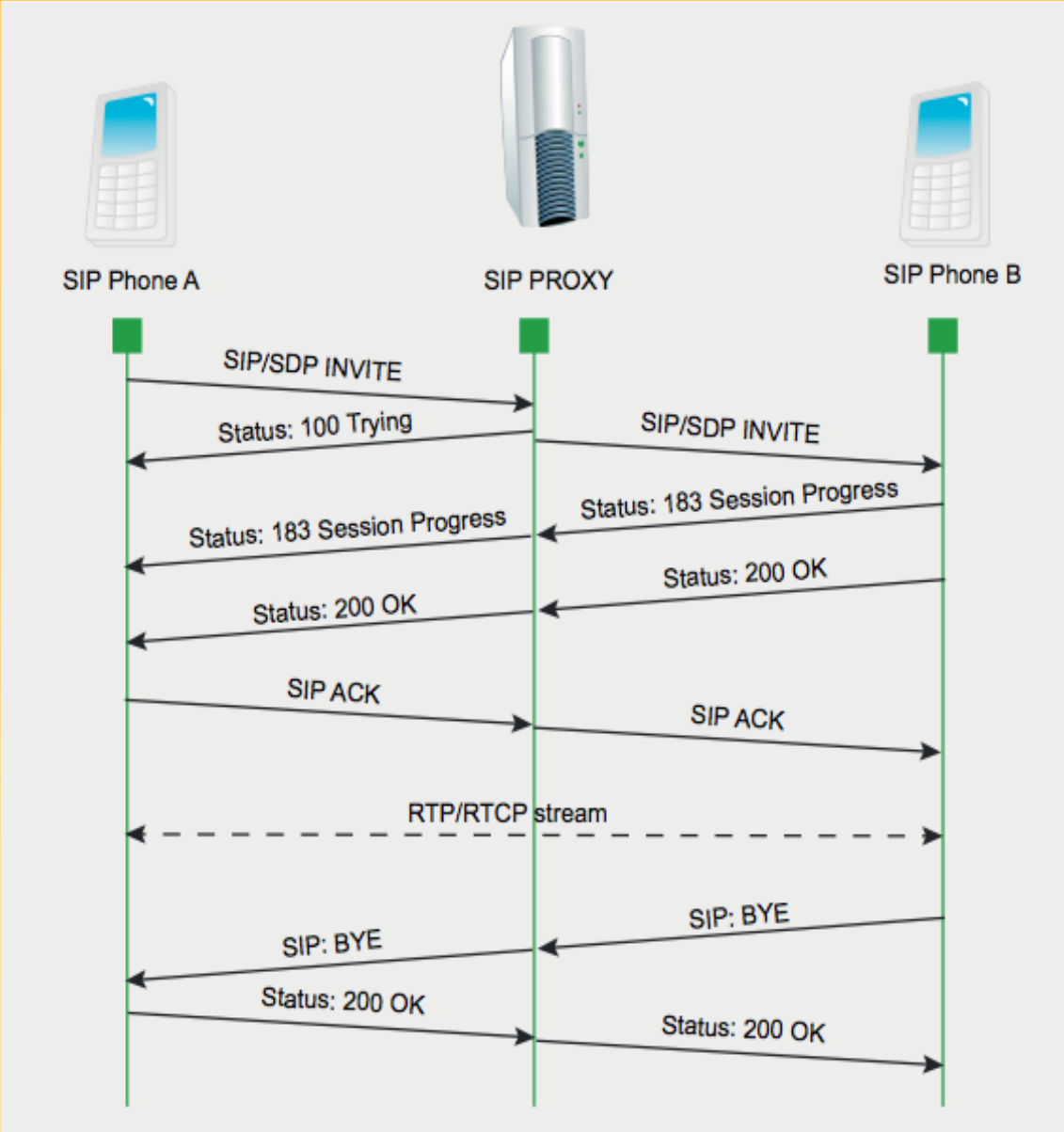


Normally runs over UDP port 5060

SIP TLS (port 5061) secures the SIP session, but does NOT encrypt the RTP stream.

Request and response type, same familiar status codes as HTTP
100 Trying
180 Ringing
200 OK
301 Moved Permanently
403 Forbidden
404 Not Found
etc

Major difference between SIP and HTTP is,
In SIP - ALL devices are BOTH Server and Client



http://enablesecurity.com/resources/

SIP needs several supporting standards

SIP method extensions from other RFCs

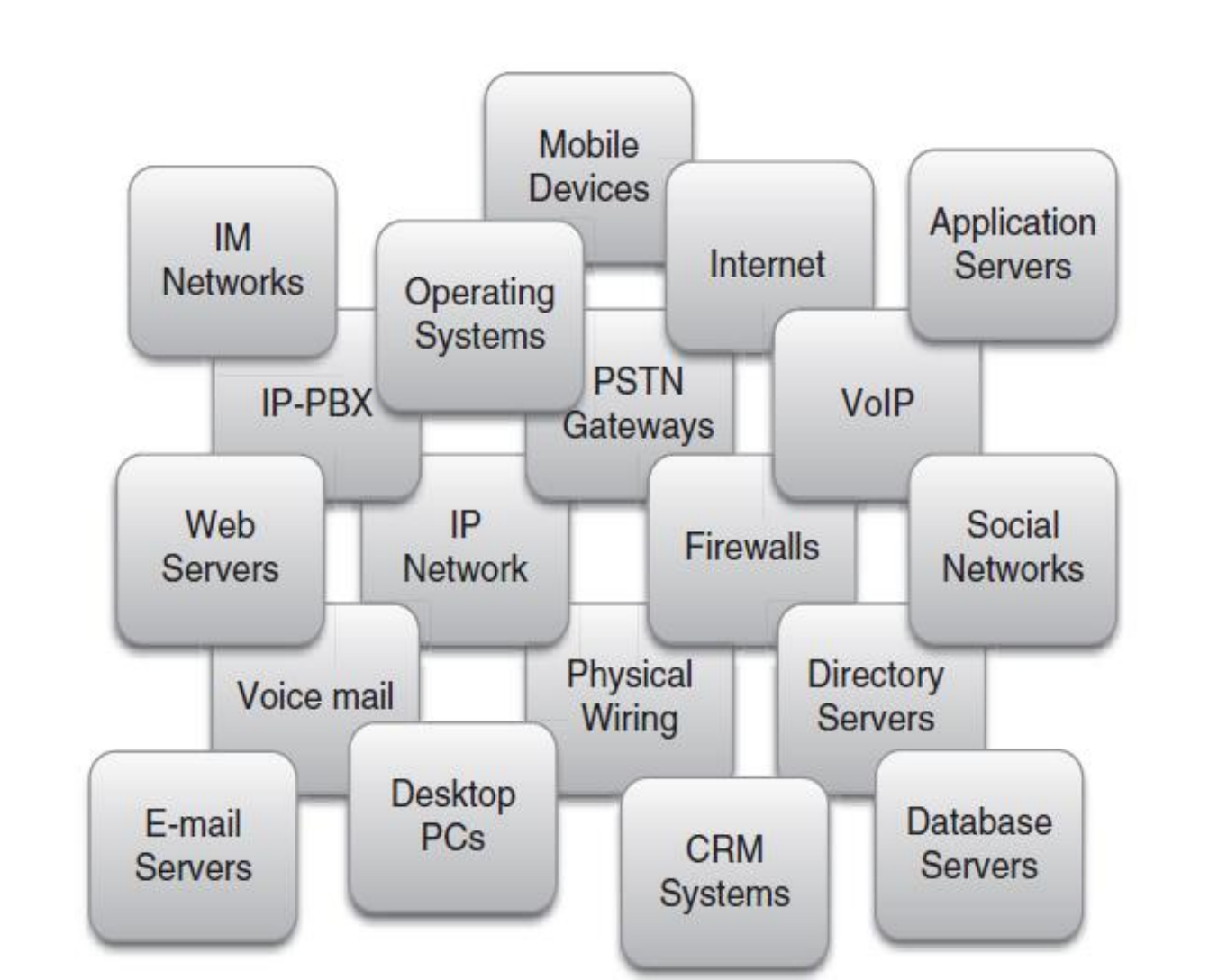
- SIP method info: Extension in RFC 2976
- SIP method notify: Extension in RFC 2848 PINT
- SIP method subscribe: Extension in RFC 2848 PINT
- SIP method unsubscribe: Extension in RFC 2848 PINT
- SIP method update: Extension in RFC 3311
- SIP method message: Extension in RFC 3428
- SIP method refer: Extension in RFC 3515
- SIP method prack: Extension in RFC 3262
- SIP Specific Event Notification: Extension in RFC 3265
- SIP Message Waiting Indication: Extension in RFC 3842
- SIP method PUBLISH: Extension is RFC 3903

and some more....

RFC 3261 Official Main SIP RFC
RFC 4694 - Number Portability Parameters for the "tel" URI
RFC 3966 - The tel URI for Telephone Numbers
RFC 3524 - Mapping of Media Streams to Resource Reservation Flows
RFC 3515 - The Session Initiation Protocol (SIP) Refer Method
RFC 3487 - Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)
RFC 3486 - Compressing the Session Initiation Protocol (SIP)
RFC 3485 - The Session Initiation Protocol (SIP) Static Dictionary for Signaling Compression (SigComp)
RFC 3428 - Session Initiation Protocol (SIP) Extension for Instant Messaging
RFC 3420 - Internet Media Type message/sipfrag
RFC 3388 - Grouping of Media Lines in the Session Description Protocol (SDP)
RFC 3361 - Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers
RFC 3319 - Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC 3327 - Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3324 - Short Term Requirements for Network Asserted Identity
RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3329 - Security Mechanism Agreement for the Session Initiation Protocol (SIP)
RFC 3313 - Private Session Initiation Protocol (SIP) Extensions for Media Authorization
RFC 3312 - Integration of Resource Management and Session Initiation Protocol (SIP)
RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
RFC 3261 - SIP: Session Initiation Protocol (Main SIP RFC)
RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3265 - Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3087 - Control of Service Context using SIP Request-URI
RFC 3050 - Common Gateway Interface for SIP
RFC 2976 - The SIP INFO Method
RFC 2848 - The PINT Service Protocol: xtensions to SIP and SDP for IP Access to Telephone Call Services

Which of these are secure?

UC brings more challenges…



An example of abusing the AUTH

- REGISTER usually gets a 401 Unauthorized
- INVITE gets a 407 Proxy Authentication
- Challenge response mechanism
  - Takes various properties + password
  - Nonce, Method, URI

Normal SIP INVITE

INVITE

200 OK

Normal BYE

BYE

200 OK

Wait, let's add an AUTH to the BYE

BYE

407 Challenge

Challenge Response!

We got the digested pwd, let's crack it!

- Tested tools on a Macbook*
  - sipcrack
    - Passwords tested per second: 494000 c/s
  - john the ripper (with some patches)
    - Passwords test per second: 580000 c/s

Example:

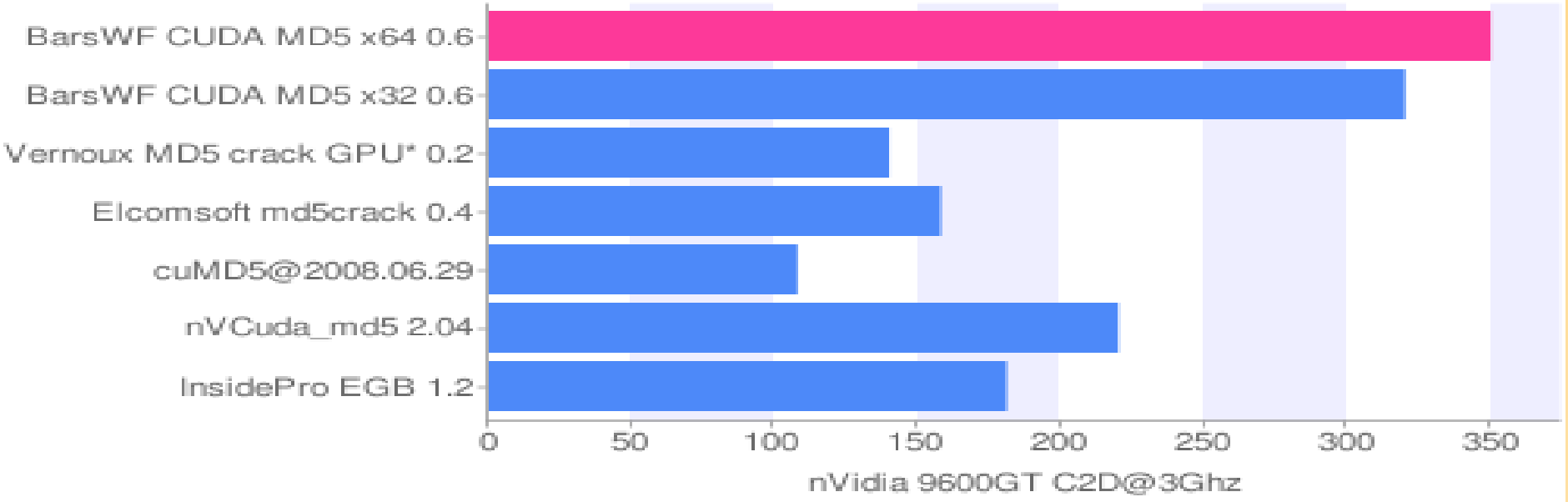
- Six letter password ~ less than 10 minutes (e.g abcdef)

*Macbook is a Intel Core Duo 1.83 GHz

Why not just use my graphic card?

- We can speed this up with GPUs too
  - World Fastest MD5 cracker BarsWF = 350 M keys/sec

~250 times faster with GPU
From days down to minutes.



Statistics from Sweden

- Scanned 1,000,000 ip addresses using svmap
- 2,296 replied with a SIP response
- Around 80 different vendors
  - Linksys (1362)
  - unknown (159)
  - Asterisk (121)
  - sipgt-67 (114)
  - EPC2203-080530 (111)
  - RIX67GW2 (78)
  - SpeedTouch (66)
  - Intertex (27)

And Norway (what are we thinking????)

- Scanned 10,000,000 ip addresses using svmap
- 64,638 replied with a SIP response
- Around 152 different vendors
  - SpeedTouch (25305)
  - Linksys (17828)
  - ARRIS-TM502B (4455)
  - Sipura (3609)
  - ARRIS-TM602B (3267)
  - ARRIS-TM402B (2591)
  - M5T (1812)
  - unknown (1337) <--- good number ;-)
  - WGR613VAL-V2.3_43 (1140)
  - AVM (552)

Pick your targets...

Patton SN4552 2BIS EUI 00A0BA024705 R5.T 2008-09-18 SIP M5T SIP Stack/4.0.26.26

Linksys/SPA1001-3.1.19(SE)

Nortel CS1000 SIP GW release_5.0 version_sse-5.50.12

Polycom HDX 7000 HD (Release - 2.5.0.5-3548)

TANDBERG/512 (TC2.1.1.200802)

Sip EXpress router (2.1.0-dev1 OpenIMSCore (x86_64/linux))

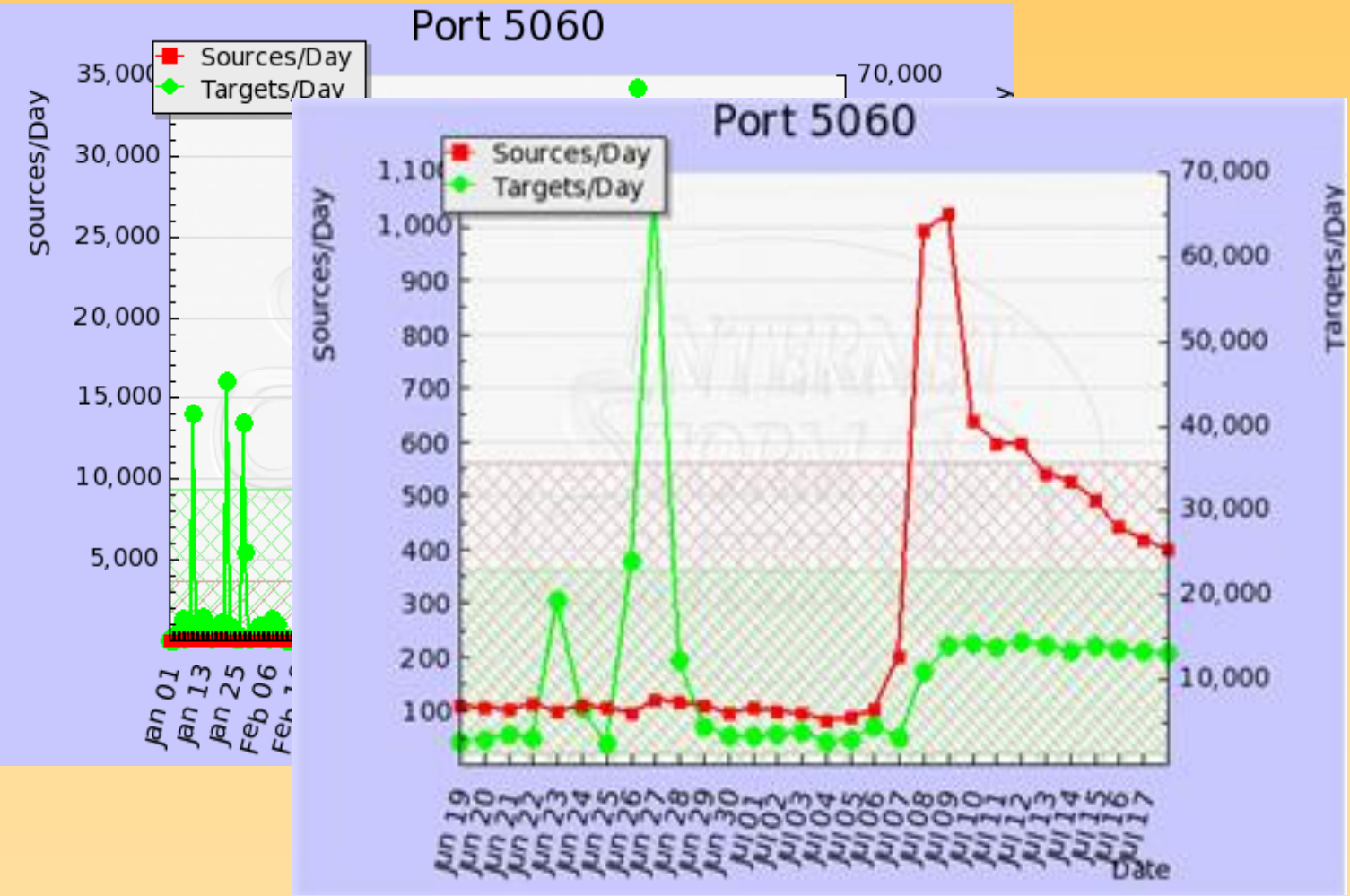
Pick your attack

Tools \ Tests	Scan	Enumerate	Fingerprint	Intercept traffic/ Eavesdrop	UDP flood	INVITE flood	Session teardown	RTP media injection	RTP media mixing	REGISTER attacks
Cain&Abel	X			X						
Inviteflood						X				
Netdiscover	X									
Nmap	X	X	X							
add_registration										X
erase_registration										X
reghighjack										X
rtpinsertsound								X		
rtpmixsound									X	
SIPBomber						X	X			X
SIP_rogue				X			X	X	X	X
SIPSack		X	X		X	X				X
SiVuS		X			X	X	X			X
Udpflood					X					
Teardown							X			
Wireshark				X						

But no one is targeting VoIP, right?

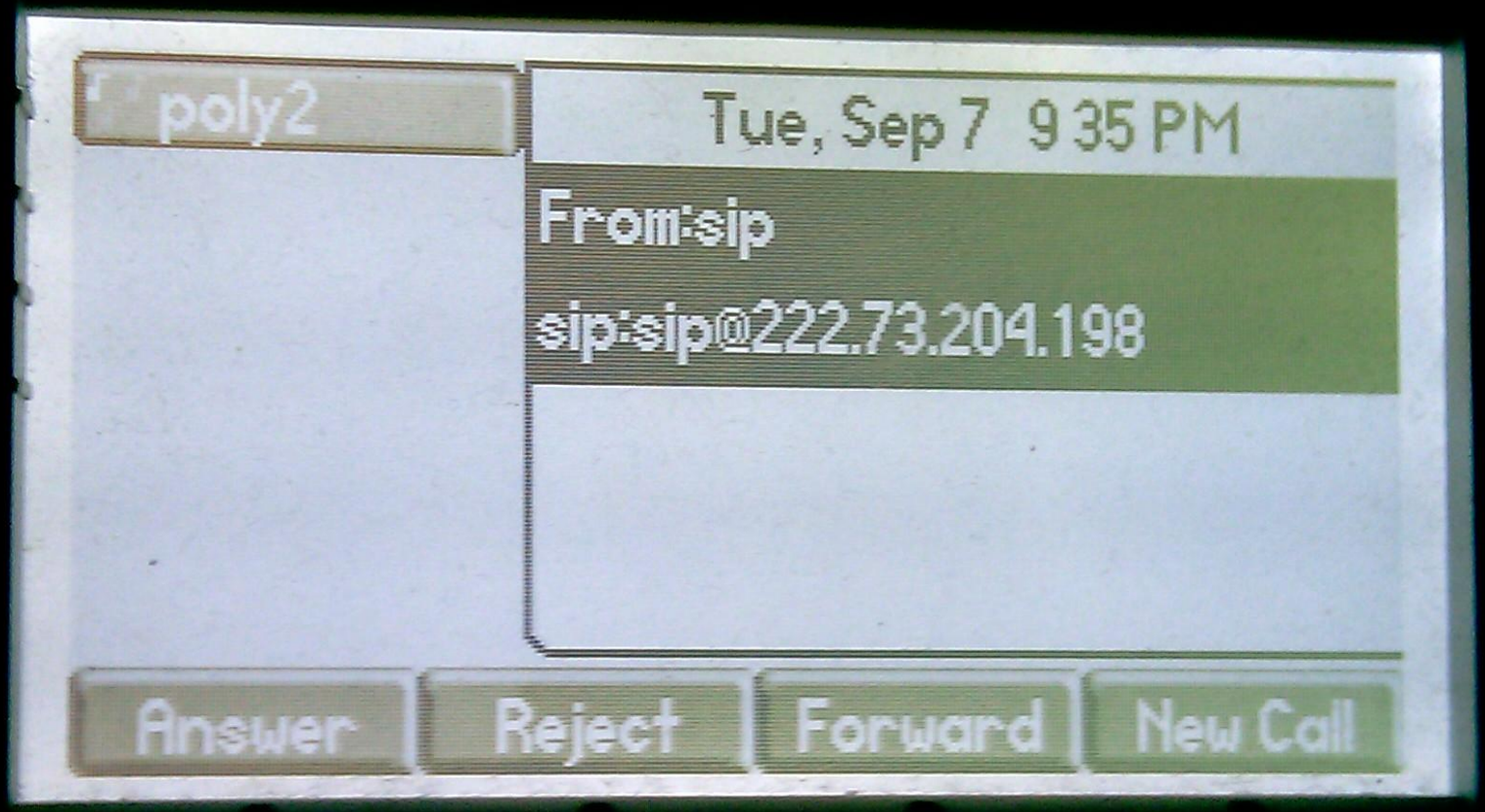
hmm...

Internet Storm Center reports



http://isc.sans.edu/diary.html?storyid=8641

Picture from a Polycom on public IP




POLYCOM
..int IP
Incoming call from:
sipvicious
Answer
Reject
Forward
Directories
Services
Call Lists
Conference
Transfer
Redial
Sel
Del
Menu
Messages
Do Not Disturb
Hold
1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PQRS 7
TUV 8
WXYZ 9
*
OPER 0
#

Search, INVITE, then abuse

1. Search for insecure PBXs or Gateways
2. Methods for getting access
   - Easy way
     - Try to make a call to a landline phone number
     - If that rings, then take note
   - Though way
     - Bruteforce extensions on the PBX
     - Bruteforce passwords for any extensions found
     - Attach the end devices
3. Configure an Asterisk box to use the vulnerable extension
4. Sell cheap access to third parties or call your own premium numbers!

Honeynet VOIP Forensic Challenge

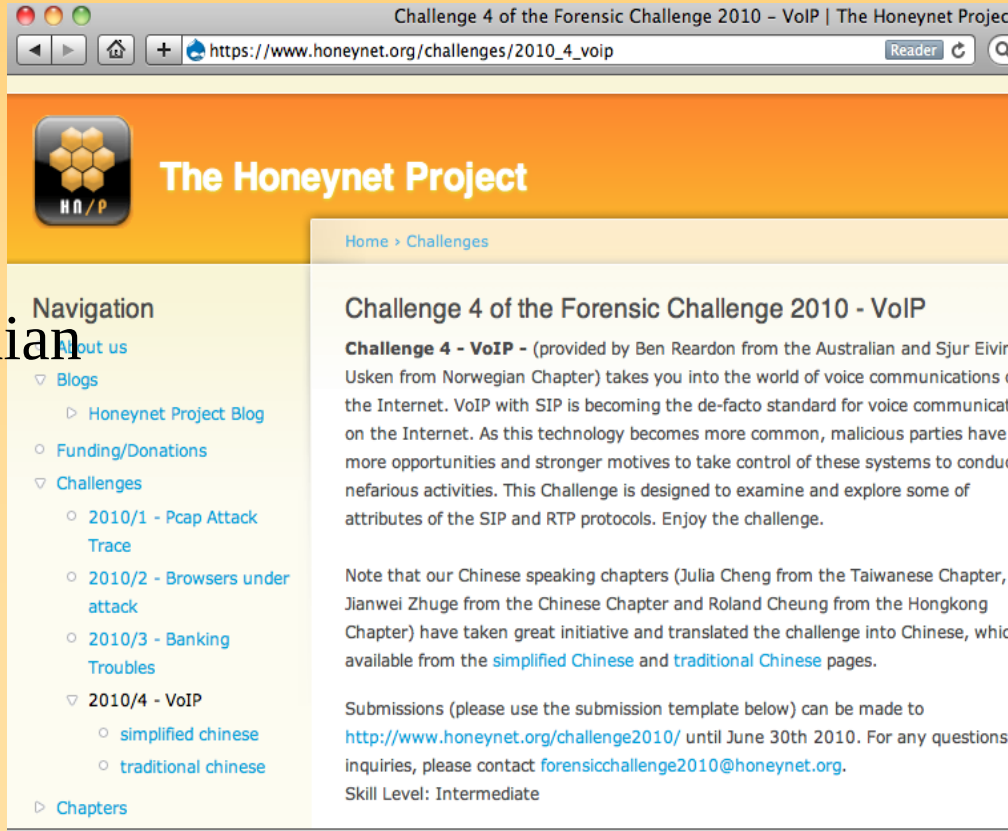
Austria

Somalia

Sierra Leon

Hong Kong IP

Romanian IP



Publicly available tools:

1. SIPVicious

Private tools:

1. Custom scanners
    1. Sundayddr
    2. “Counterpath”
    3. others
2. Asterisk server with scripts

.. To understand the private tools are the reason why the Honeynet project exists.

"To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned."

The sundayddr OPTIONS message

OPTIONS sip:100@X.X.X.X SIP/2.0
Via: SIP/2.0/UDP 192.168.1.9:5060;branch=
z9hG4bK-31055767;rport
Content-Length: 0
From: “sipsscuser”<sip:100@192.168.1.9>;
tag=016690163348628870071031857187851564983857029 49 Accept
application/sdp
User-Agent: **sundayddr**
To: “sipssc”<sip:100@192.168.1.9>
Contact: sip:100@192.168.1.9:5060
CSeq: 1 OPTIONS
Call-ID: 022827170099429274868738305
Max-Forwards: 70

OPTIONS messages are more ”quiet” than INVITE. Doesn’t make the phone ring….

Sundayddr botnet

”Counterpath” INVITE message

INVITE sip:82727117149111@the.honeypot.ip;transport=udp SIP/2.0
Via: SIP/2.0/UDP
202.71.111.5:3916;branch=1101001011101000101010100011 0202.71.11
neypot.ip751302518;rport
Max-Forwards: 70
From:
<sip:73611589670379845 5@the.honeypot.ip>;tag=5475511560139881 9
5115605475511560202.71.111.5
To: <sip:82727117149111@the.honeypot.ip>
Call-ID:
ed6681d6101100111101101001001101110000110100101110100010101
202.71.111.5the.honeypot.ip7513025181c895d98272711714911154755 1
8819959547551156054755115 60202.71.111.51621419374
CSeq: 1 INVITE
Contact: <sip:1c895d9@202.71.111.5:3916;transport=udp>
Content-Type: application/sdp

A custom scanner

```
INVITE sip:8615539868888@X.X.X.X SIP/2.0
Via: SIP/2.0/UDP 68.168.118.2:5060;branch=
z9hG4bK29b4d965;rport
From: "asterisk" <sip:asterisk@68.168.118.2>;tag=as1119ff85
To: <sip:8615539868888@X.X.X.X>
Contact: <sip:asterisk@68.168.118.2>
Call-ID: 431a5b42398d2f1174b4a73269bea904@68.168.118.2
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Date: Tue, 29 Dec 2009 03:53:05 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE,
NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 287

v=0
o=root 24696 24696 IN IP4 68.168.118.2
s=session
..... (truncated)
```

Analysis of one kit

Used the EnergyMech open-source IRC botnet client combinded with SipVicious

Very easy to do…

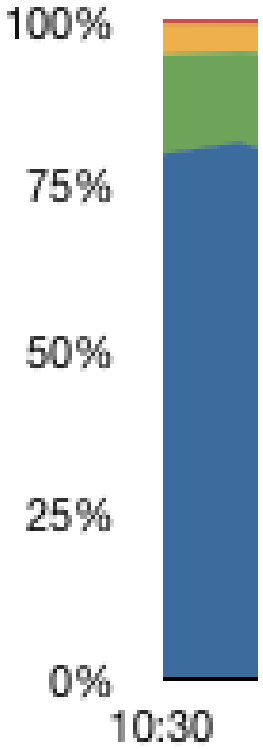
details...

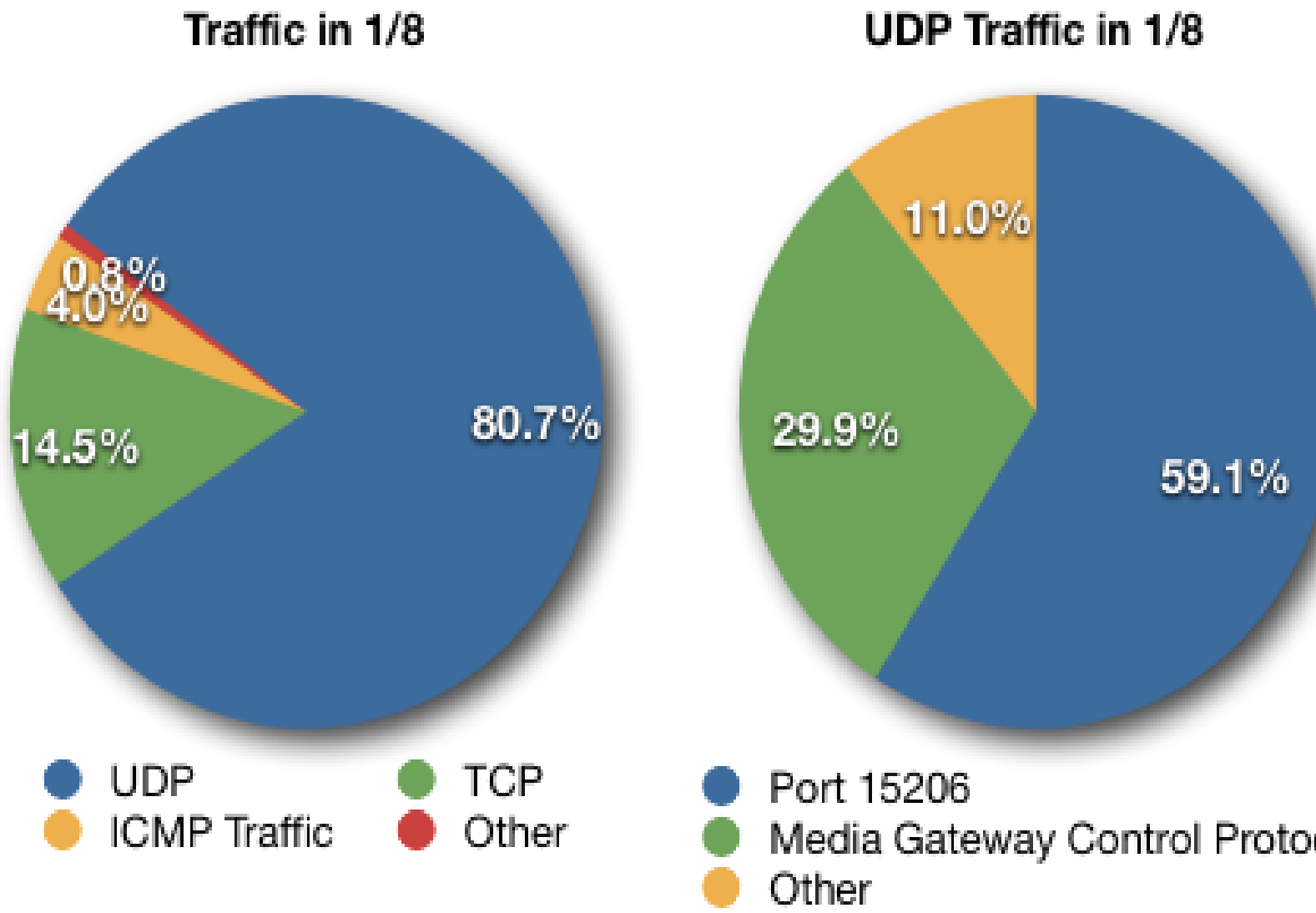
```
INVITE sip:011441442828700@X.X.X.X SIP/2.0
Via: SIP/2.0/UDP
62.220.128.243:3058;branch=ca4b76bc9681679erugroijrgrg;rport
From: <sip:sip@62.220.128.243>;tag=Za4b76bc9681679
To: <sip:011441442828700@X.X.X.X>
Contact: <sip:sip@62.220.128.243>
Call-ID: 213948958-00379064808-384748@62.220.128.243
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIF
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
```

IP to send traffic to: 1.1.1.1

Port to send audio to:

INVITE asks for audio traffic to IP 1.1.1.1





Proves there is a lot of scanning!

Approximately 60mbit of traffic.
80% UDP, of this 60% UDP port 15206.
Use voice codec G711 which is 0,1Mbit/s

=288 concurrent calls

SIP has a timer on INVITE on 20 seconds.

Approximately 900 call per minute with success!

Successful attacks in Norway

"Lawnmover" attack towards a company

All phones ringing randomly with ghost calls

Successful attacks in Norway

"Lawnmover" attack towards a company
All phones ringing randomly with ghost calls

"Bounce attack" on Cisco gateways with insecure configuration
Frauded for approximately 1.2 million NOK in 10 days.

Successful attacks in Norway

“Lawnmover" attack towards a company
All phones ringing randomly with ghost calls

"Bounce attack" on Cisco gateways with insecure configuration
Frauded for approximately 1.2 million NOK.

Test calls to Citibank in England.
Bounces of insecure VoIP servers (Asterisk, Cisco and others)

Successful attacks in Norway

“Lawnmover" attack towards a company
All phones ringing randomly with ghost calls

"Bounce attack" on Cisco gateways with insecure configuration
Frauded for approximately 1.2 million NOK.

Test calls to Citibank in England.
Bounces of insecure VoIP servers (Asterisk, Cisco and others)

Firewall service provider left the PBX wide open (too many rules on the firewall and the technician did not quality check his work)

Successful attacks in Norway

“Lawnmover" attack towards a company
All phones ringing randomly with ghost calls

"Bounce attack" on Cisco gateways with insecure configuration
Frauded for approximately 1.2 million NOK.

Test calls to Citibank in England.
Bounces of insecure VoIP servers (Asterisk, Cisco and others)

Firewall service provider left the PBX wide open (too many rules on the firewall and the technician did not quality check his work)

An Asterisk for test was connected to the main system. Abused!

Do's and don'ts

Do

- Keep long passords (12+ letters and numbers)
- Use VPN for remote phones/softclients
- Use at least access lists on firewalls, minimum!
- Intrusion Detection Systems
- Honeypot

Don't!

- Use phones or PBXes on a public IP without a **stateful** firewall or a good SIP firewall
- Use have standard passwords
- Run unnecessary services on your PBX
- Use VLAN as secure network

Future attacks

- More advance attacks on individual PBXes (buffer overflows, bug exploits etc.)
- Trojans on local PCs doing internal search for PBXes (and can be a ”VoIP” bridge)
- SPiT coming from the PSTN network (because it is so damn cheap to call)
- RTP injections to send commercials etc
- Eavesdropping on unencrypted calls

Are you prepared?

Resources

VoIP (SIP) Honeypot Implementation in Dionaea
http://google-summer-of-code-2010-honeynet-project.googlecode.com/files/Tobias_Wulff.tar.gz

Sandro Gauci
http://blog.sipvicious.org/
http://enablesecurity.com/

The AustralianHoneynet Project
http://honeynet.org.au

Sjur Usken's blog (Honeynet Project, Norwegian Chapter)
http://www.usken.no/

Artemisa SIP honeypot
http://artemisa.sourceforge.net/