Voice Over IP

How technology has taken a step back?

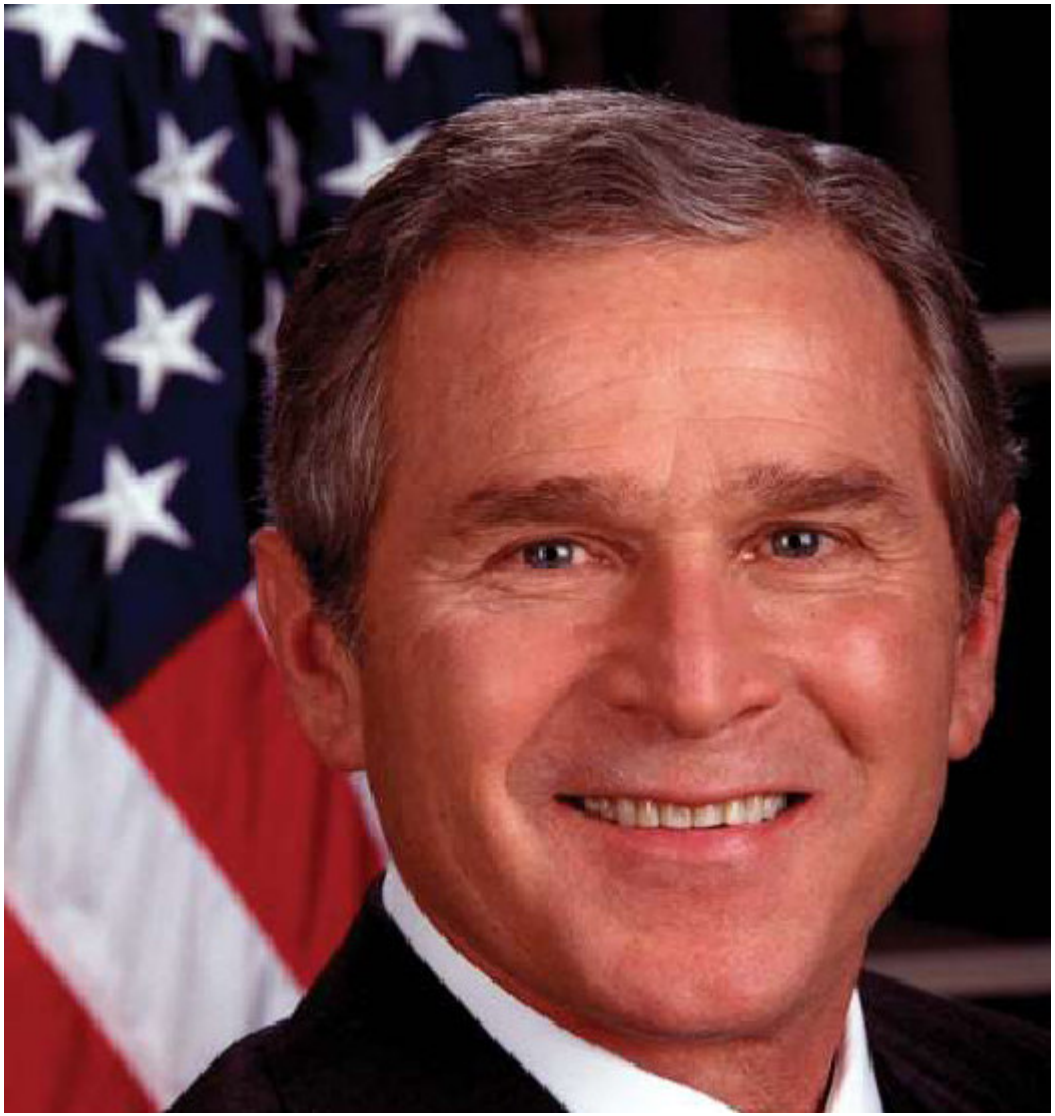
- Today is 22nd December….
- Who I am ? What I do? (next slide)
- What is the “tumult” all about? ☺
- How do I think that technology has taken a step back?

Who am I? A Britisher at heart..It's sad that I don't have HSMP ☺

Few of my inspirations and tributes

No Boo’ing please

I love this guy for ‘Patriot act’



Without him, we would’nt have had CHASE and other prestigious events in the world

This is not my nephew. It’s just a Windows 95 version of me and I love this guy

Agenda

- VoIP (SIP, H.323, MGCP, IAX, proprietary)
- How does SIP work?
- Phreaking
- VoIPhreaking
- Tributes and tools
- VoIPhishing
- Conclusion
- Q&A

SIP it!

- Signaling, media and supporting protocols
- What is signaling? What happens if the signaling is not there?
- SIP is signaling, nothing more
- ASCII text protocol designed by Internet Crunchies (IETF)
  - Bastard child of HTTP and mail
  - Over a decade old (1995) and still considered “emerging”
- Vendors keep on bragging about the SIP

SIP elements

SIP Proxy Server

- relays call signaling, routing, AAA
- rendezvous point for callees and UA's

SIP Redirect Server

- redirects callers to other servers

SIP Registrar

- accept registration requests (REGISTER method) from users
- maintains user's whereabouts at a Location Server (like GSM HLR)

User Agents (RFC 3261)

SIP messages

- Start line
  - Request or Response
- Headers
  - Information about the message
    - Destination
    - Origin
    - Route
- Body
  - Usually media stream location information (Session Description Protocol)

SIP messages (Cont'd)

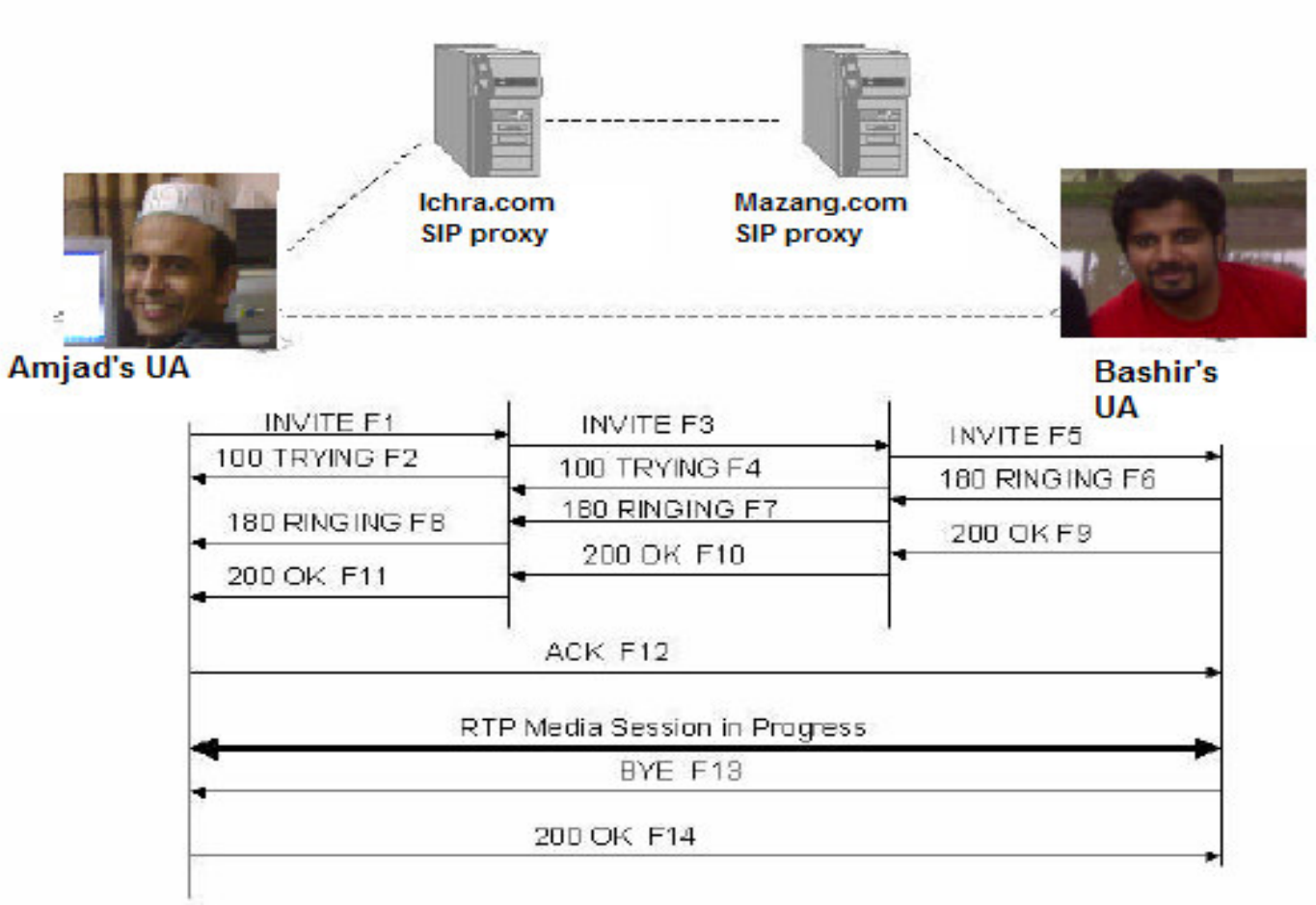
- **Start Line**
  - Request Messages
    - Method based request system (INVITE, BYE, REGISTER, OPTION, ACK,CANCEL)
  - Response Messages
    - Error code + reason (smells like HTTP)
    - 404 Not Found, 403 Forbidden
    - 200 OK Successful response
    - 500 Server failure

What does a SIP message look like (on the wire)?

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via:SIP/2.0/UDP 192.168.22.36:6060
From:UserAgent<sip:6710@192.168.22.36:6060;user=phone>
To:6713<sip:6713@192.168.26.180:6060;user=phone>
Call-ID:96561418925909@192.168.22.36
Cseq:1 INVITE
Subject:VovidaINVITE
Contact:<sip:6710@192.168.22.36:6060;user=phone>
Content-Type:application/sdp
Content-Length:168

v=0
o=-238540244 238540244 IN IP4 192.168.22.36
s=VOVIDA Session
c=IN IP4 192.168.22.36
t=3174844751 0
m=audio 23456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=ptime:20
```

A SIP call


Ichra.com
SIP proxy
Mazang.com
SIP proxy
Amjad's UA
Bashir's UA
INVITE F1
100 TRYING F2
180 RINGING F8
200 OK F11
INVITE F3
100 TRYING F4
180 RINGING F7
200 OK F10
INVITE F5
180 RINGING F6
200 OK F9
ACK F12
RTP Media Session in Progress
BYE F13
200 OK F14

Phreaking

- **History**

Started in the 1960's

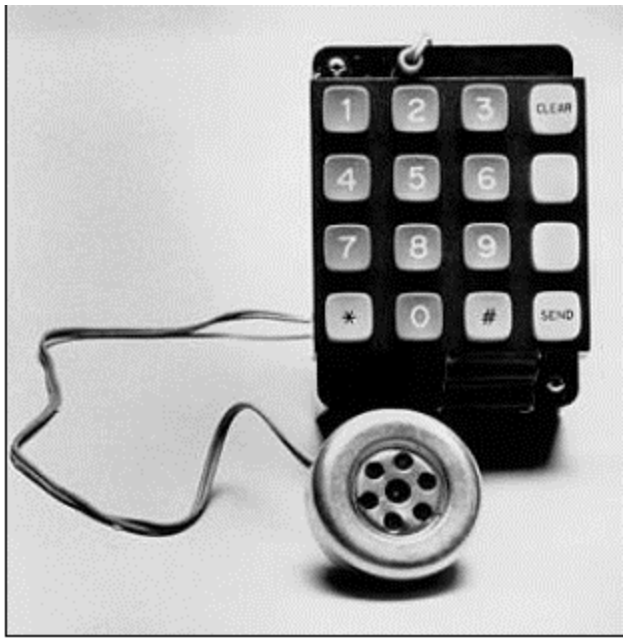
Exploited in-band signaling

Relied heavily on hardware attacks

- Famous Phreaks
  - Steve Jobs
  - Steve Wozniak
  - Cap'n Crunch

Phreaking techniques

- In band signaling @ 2600 Mhz
- Typically used for toll-fraud
- The “colour boxing era”
  - Blue boxing
  - Red boxing



- The grugq’s account

Death of Phreaking

- Out of band signaling
- Aggressive prosecution of phreakers
- Improved fraud analysis complements
- Packet voice is secure?
- Let us all marry VoIP and admit that revolution is in the air…..
- No phreaking possible against VoIP……
- Blaaaa..Blingggg….Blooo…Beeeep…@@@##$$%%%^^&&&****

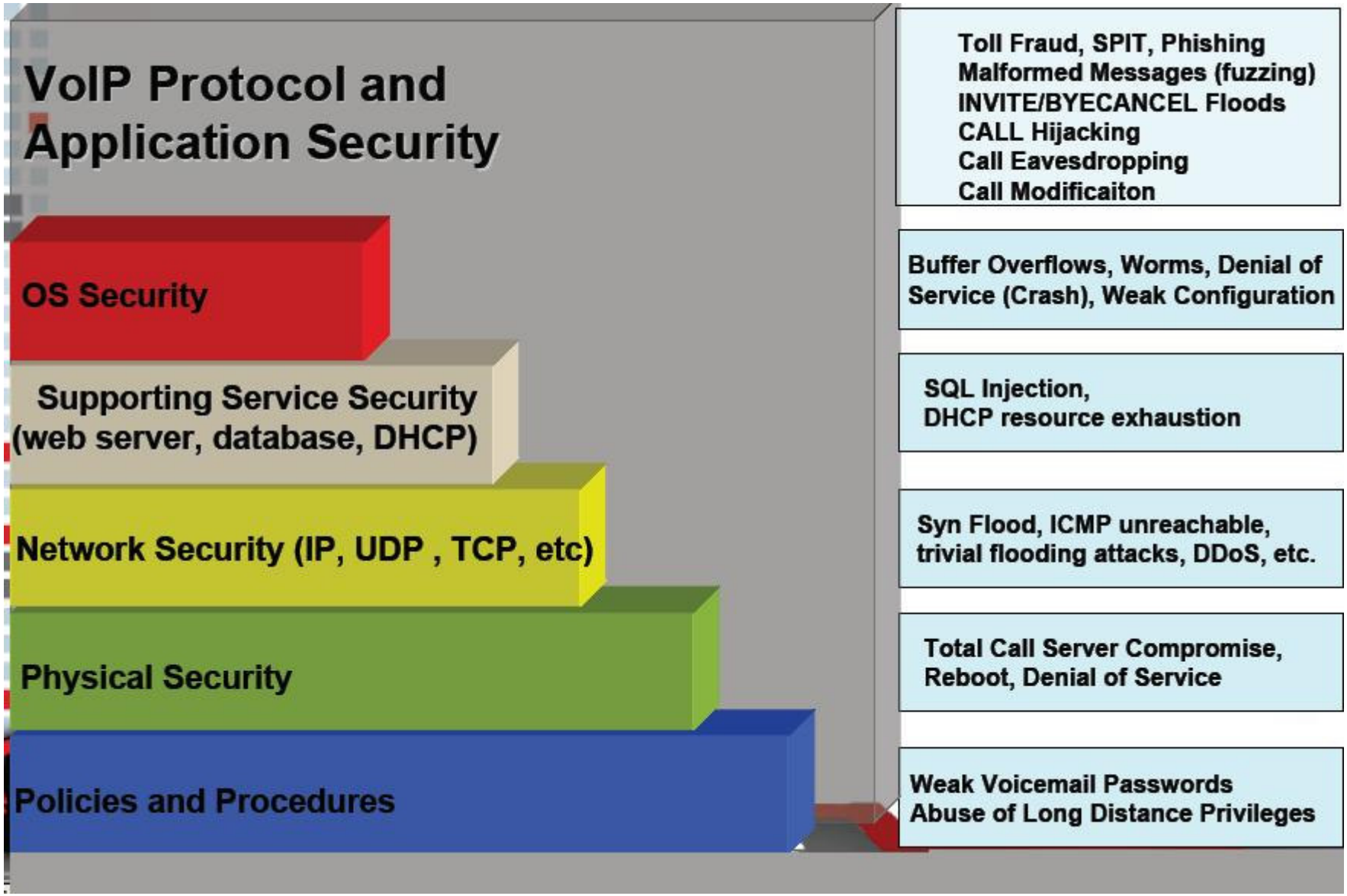
The birth of VoIPhreaking
“I’m not dead yet… only feeling better…”

CRAP Omer!!! Packet voice can save you some bucks, more then you can earn through your life and it is secure as well.

May be I am against evolution or a fundamentalist catholic who still thinks that earth is flat.

Ohhhhhh reallllllllllllllllllly !!!!!!

TAKE THAT CRUNCHIES!!!


VoIP Protocol and Application Security
OS Security
Supporting Service Security (web server, database, DHCP)
Network Security (IP, UDP , TCP, etc)
Physical Security
Policies and Procedures
Toll Fraud, SPIT, Phishing
Malformed Messages (fuzzing)
INVITE/BYECANCEL Floods
CALL Hijacking
Call Eavesdropping
Call Modificaiton
Buffer Overflows, Worms, Denial of Service (Crash), Weak Configuration
SQL Injection,
DHCP resource exhaustion
Syn Flood, ICMP unreachable, trivial flooding attacks, DDoS, etc.
Total Call Server Compromise, Reboot, Denial of Service
Weak Voicemail Passwords
Abuse of Long Distance Privileges

VoIPhreaking techniques

- Media attacks
  - Eavesdropping
  - Injection
- Signaling attacks
  - Hijacking
  - Rerouting
  - Dr. DoS
- PSTN attacks
  - MG intrusion

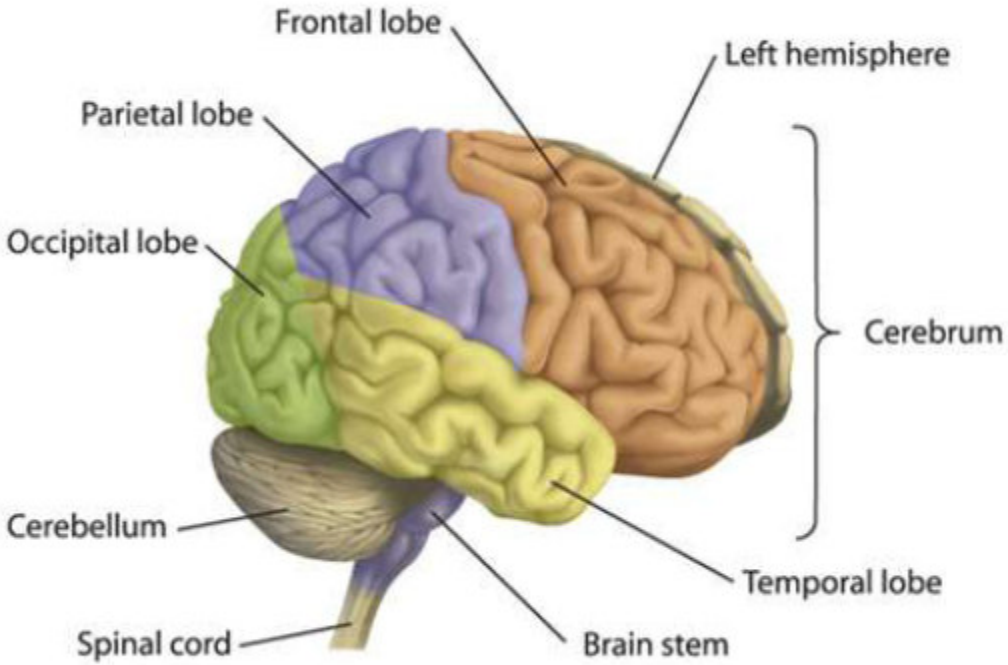
TOOLS

Remember: a fool with a tool….

…….is still a fool ☺

Introducing the only tool in the world that really works effectively today……

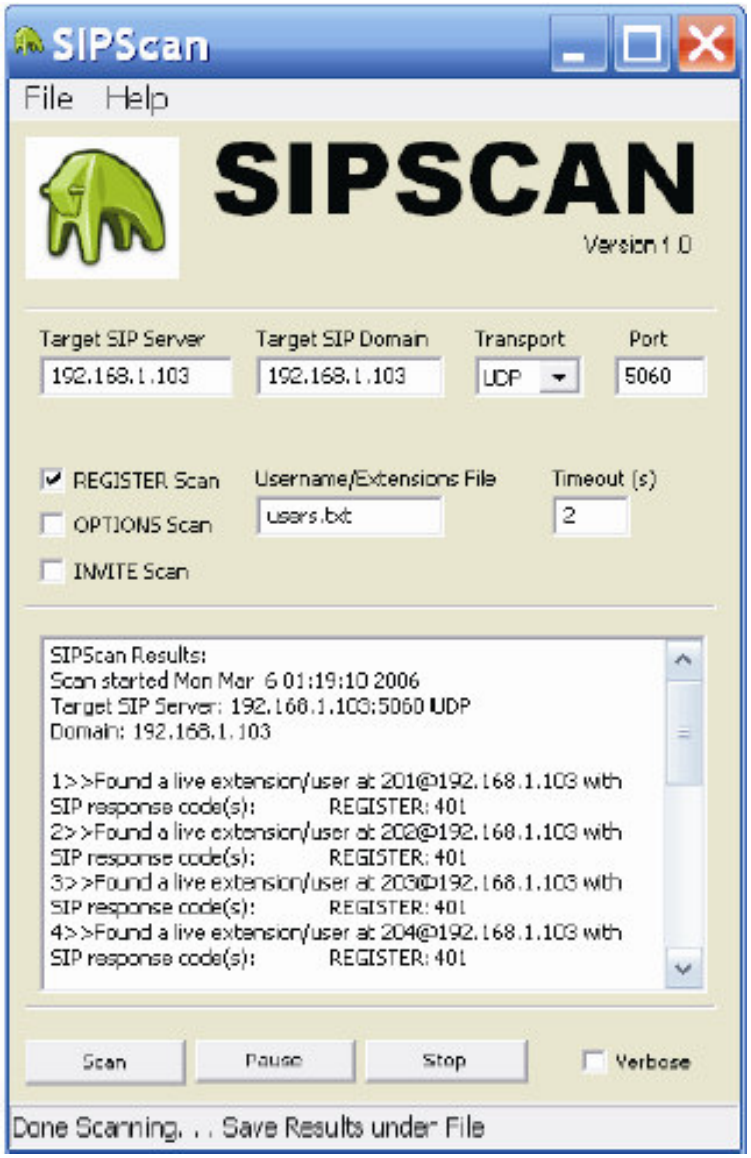
CocoNUT or WallNUT or whatEVER…



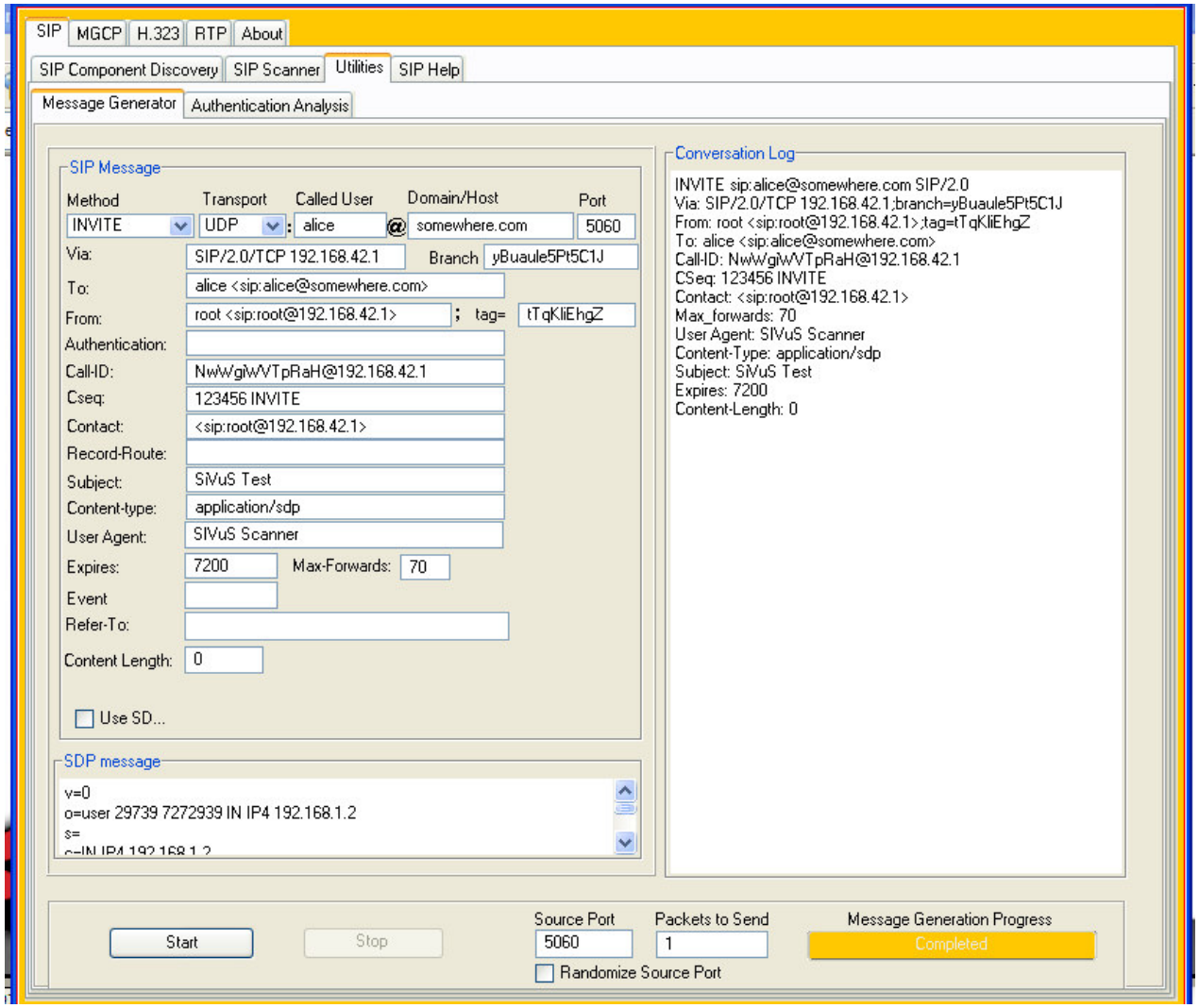
Tools (Cont'd)

- Hail to "Man In The Mirror" (oh sorry Middle)
  - Arpspoof (dsniff suite), ettercap, Cain, Hunt
- Sniff…..Sniff (RTP stream)
  - Wireshark (formerly known as ethereal), Tethereal, TCPDump, or build one of your own
  - RTP analyzer >> Follow Stream >> Decode & Publish
  - …and a successful eavesdropping attack
- VoIPong
  - Another RTP stream builder goodie
- RTP injection
  - Add noise

SIPScan


SIPScan
File Help
SIPSCAN
Version 1.0
Target SIP Server
192.168.1.103
Target SIP Domain
192.168.1.103
Transport
UDP
Port
5060
REGISTER Scan
OPTIONS Scan
INVITE Scan
Username/Extensions File
users.txt
Timeout (s)
2
SIPScan Results:
Scan started Mon Mar 6 01:19:10 2006
Target SIP Server: 192.168.1.103:5060 UDP
Domain: 192.168.1.103
1>>Found a live extension/user at 201@192.168.1.103 with
SIP response code(s): REGISTER: 401
2>>Found a live extension/user at 202@192.168.1.103 with
SIP response code(s): REGISTER: 401
3>>Found a live extension/user at 203@192.168.1.103 with
SIP response code(s): REGISTER: 401
4>>Found a live extension/user at 204@192.168.1.103 with
SIP response code(s): REGISTER: 401
Scan
Pause
Stop
Verbose
Done Scanning. . . Save Results under File

Dr. Dos (SiVus)
INVITE flood



Social Threats

- SPIT
- VoIPhishing

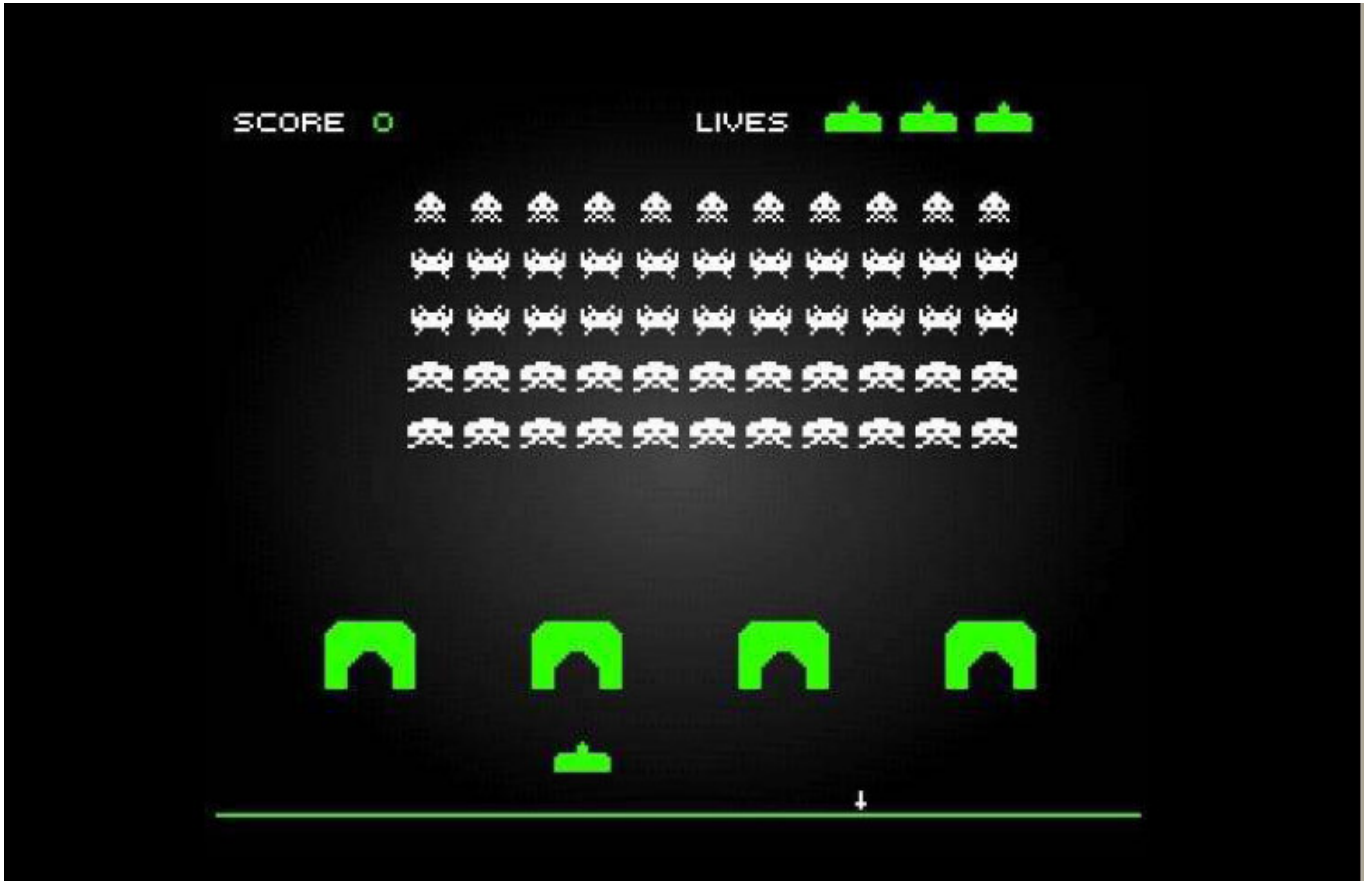
SPIT

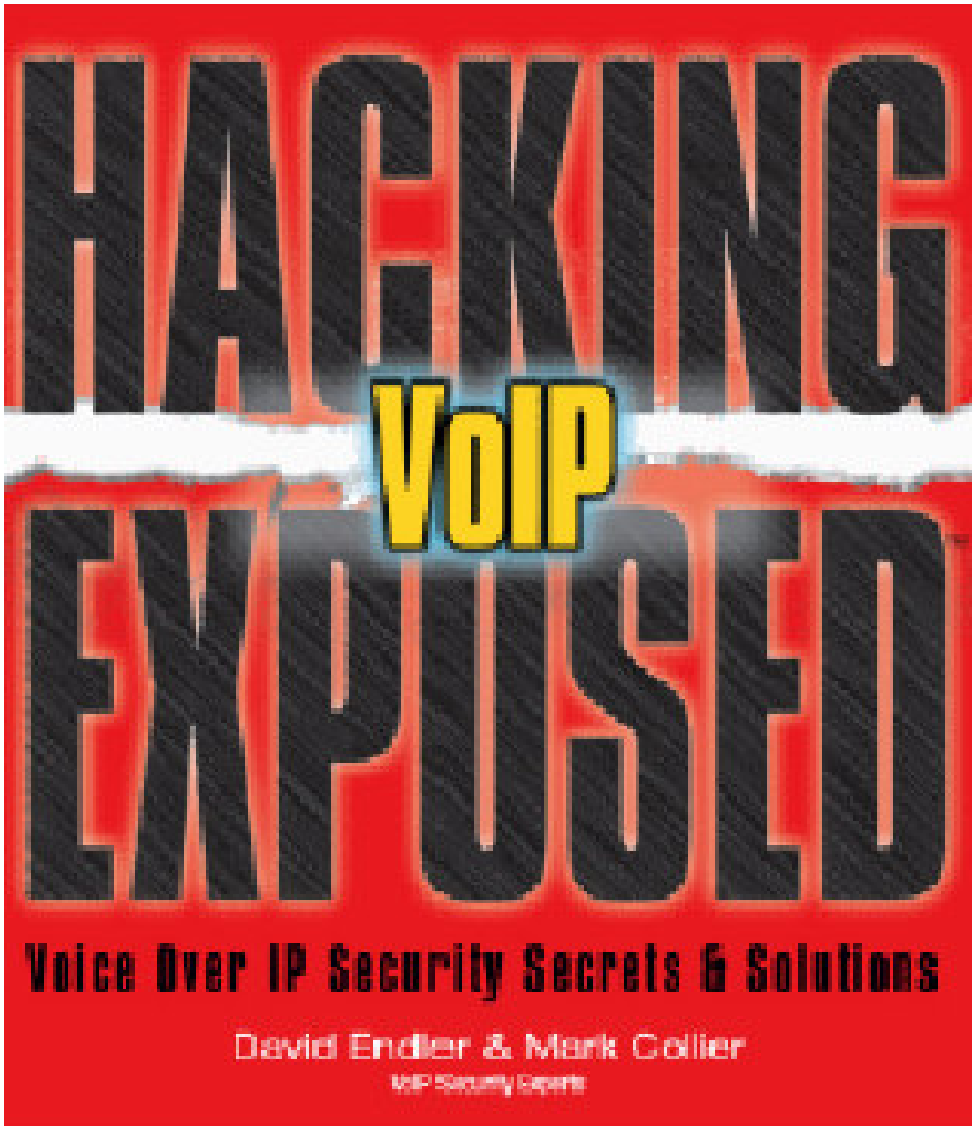

VIAGRA
3 pills - 100mg
$85
ORDER
DROWNING IN DEBT?
WE CAN HELP...
GARANTIE
SPANISH FLY

SPIT

- How easily your voice mail boxes can be spammed with unwanted advertisements..
- Asterisk (http://www.asterisk.org) turns out to be a fairly useful tool for performing SPIT. .
- Popularity Dialer (http://www.popularitydialer.com) is an example of what Asterisk can be modifedto do
- Can be used to send phone calls with prerecorded conversation in the future

Question and Answers??




HACKING
VoIP
EXPOSED
Voice Over IP Security Secrets & Solutions
David Endler & Mark Collier

Thank you

Catch me at:
venommy@gmail.com