Redpill Linpro

Free and Open Source Software in relation to Asterisk*

Lars Strand

lars.strand@redpill-linpro.com
Ibidium's Asterisk course
Oslo, NR, 8.-11. September 2009

Redpill Linpro

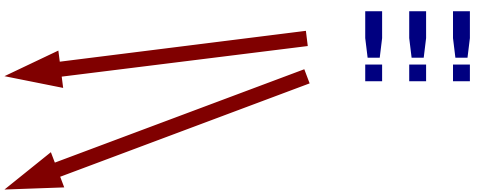
What is this?

- What is free software?
- What is the difference between «free software» and «open source»?
- What is the GPL license? Are there others..?
- What are open standards?
- How is VoIP related to open standards and free/open source software?
- Why do I need to know about this?
- What is a Linux distribution?
- How does Asterisk fit into all this?

Redpill Linpro

Key concept: Source code!

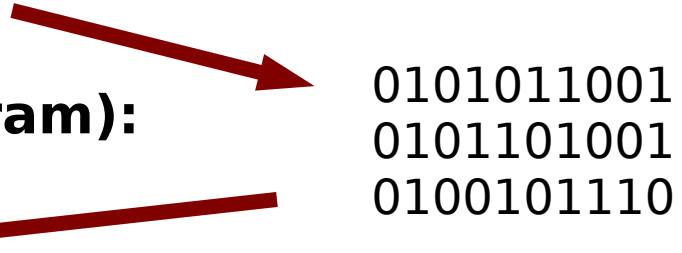
1. Source code:




```
#include <stdio.h>

int main() {

printf("Hello world!\n");

return 0;

}
```

2. Must be compiled:

```
gcc -s hello.c -o hello
```



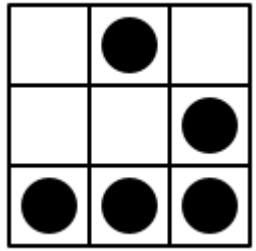
3. Then executed (ordinary program):

```
./hello

Hello world!
```

Redpill Linpro

Brief history

- **Free software is not new** Have roots all the way back to first computing (1960s). Academics sharing thoughts, ideas, papers and source code.
- **Sharing and openness was essential**
- **They called themselves «hackers».** Richard Stallman (RMS) was part of this «community».
- **This tradition was threatened by software companies**
  - Hackers had to sign NDAs preventing them to share
  - “The story of a printer”
- **This culminated in...**



Redpill Linpro

Free Software Foundation (FSF)

- Founded by RMS in 1984
- Had one main project: A free UNIX!
- Project that would do that: GNU
  - GNU's Not Unix (GNU)
- Protected by a license called: GPL
  - GNU General Public License
- Active today: http://www.fsf.org

Redpill Linpro

GPL Free Software

Free as in Freedom

Gnu General Public license

- GPL is a software license
- Goal: To ensure freedom!
- Used to ensure the four freedoms:

1) The freedom to run the program, for any purpose (freedom 0).
2) The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.
3) The freedom to redistribute copies so you can help your neighbor (freedom 2).
4) The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.

Redpill Linpro

"***In simplest terms, the GPL locks software programs into a form of communal ownership.***"

--- «Free as in Freedom»

Redpill Linpro

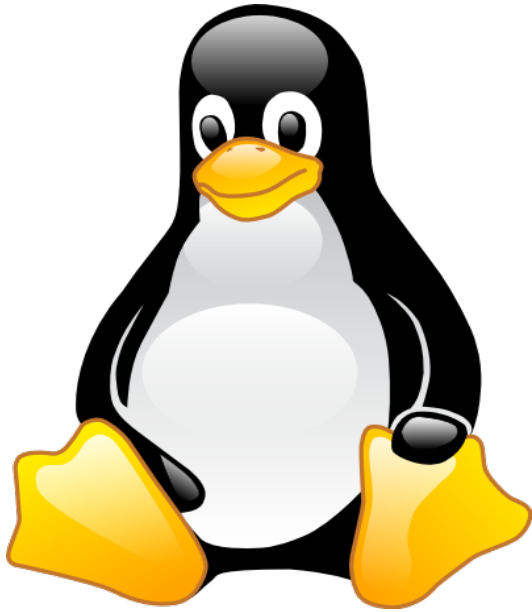
GNU's Not Unix (GNU)

- Why: No free Unix
- Write our own Unix.
- Implemented all tools
  - Compiler (gcc)
  - Debugger (gdb)
  - Editor (Emacs)
  - ...
- Mostly complete in the early 90s, but missing a (functional) kernel
  - TRIX – Mach – HURD

Redpill Linpro

GNU and Linux

- GNU project was almost complete
  - All necessary tools created
- Linus Torvalds, a student, created (with help from others) a kernel – called it Linux (early 90s)
- GNU software + the Linux kernel = GNU/Linux
- Today we use “Linux”, but it refers to both GNU and Linux.
- The Linux kernel is licensed under GPLv2



Redpill Linpro

Linux distributions

debian

redhat

- A Linux distributions usually consist of:
  - GNU tools, Linux kernel, other programs/tools
- These are packed and “branded” distributions specific
  - Some distribution specific tools to administer
  - Small differences in how to manage
  - But it is (more or less) the same source code!
- Many distributions exists
  - RedHat, Ubuntu, Debian, SuSe, ...

Redpill Linpro

Open Source vs. Free Software

- Linux “took off” in the late 90s
- Problem: People had problems with “FREE software”
  - Does that mean no cost? (No it does not)
- “Open Source” was launched as an alternative jargon, including Open Source Initiative (OSI)
- Disagreement:
  - FSF – “it is imperative that we ensure our FREEdom!”
  - OSI – “we're pragmatists. We need it to work and play along business.”
- Also called..
  - Free *Libre* Open Source Software (FLOSS)
  - Free Open Source Software (FOSS)
  - Open Source Software (OSS)

Redpill Linpro

Open Source lisences

- OSI have a set of criterias that must be fulfilled before you can call it an open source license
  - Not so strict as FSF
  - Can be approved by OSI
- Other licenses
  - BSD
  - MIT
  - Apache
  - .....
- For more info:
  - http://en.wikipedia.org/wiki/Open_source_license
  - http://en.wikipedia.org/wiki/List_of_FSF_approved_software_licences

Redpill Linpro

FLOSS today

- Major companies behind developers/products
  - Kernel developers
  - Dual-license
- Gartner:
  - *“Open source impossible to avoid”*
  - *“80% of commercial apps to use open source by 2012”*
  - *“Open Source will quietly take over”*

Redpill Linpro

Asterisk – dual licensed

- Several companies have dual a license
  - MySQL, Trolltech, Asterisk
- How does it work?
  - One open source license (f.ex. GPL)
  - One proprietary license (costs money)
- Requirement: The company must have ownership of all the code
- The company (product) can reap the benefits of a open source community and circumvent the open source license requirements (if the customer buys a licence)

Redpill Linpro

Open standards

- Another important concept is open standards
- Not a clear-cut definition, but good enough
- Crucial for Open Source to have open standards
- Internet is built on open standards (RFC from IETF)
- What about VoIP?
  - SIP and RTP are open standards
  - .. but first..

Redpill Linpro

VoIP

- Voice over IP (VoIP) protocols and technology is a merge of telecom and data communication
- What is VoIP?
  - Broad definition: Sending and receiving media (voice/video) over IP
- Why VoIP?
  - Added functionality and flexibility – which may be hard to provide over PSTN
  - Reduced cost – uses Internet as carrier
  - Less administration – no separate telephone and data network
- Industry have high focus on VoIP today
- But, VoIP is known to be insecure
  - Inherits problems from traditional IP networks
  - Multiple attack on SIP based VoIP exists

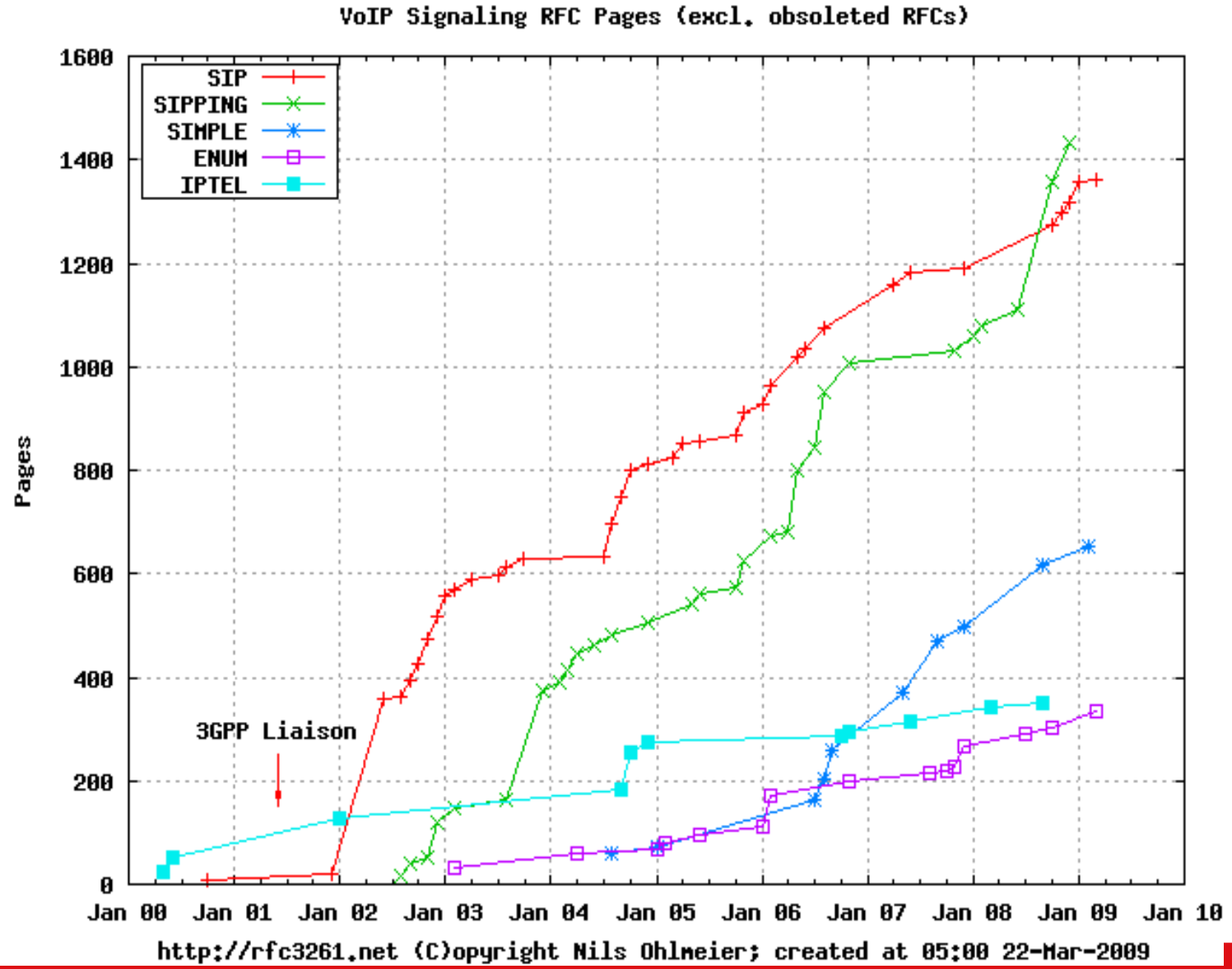
Redpill Linpro

SIP

- Session Initiation Protocol (SIP) is the *de facto* standard signaling protocol for VoIP
  - Application layer (TCP, UDP, SCTP)
  - Setting up, modifying and tearing down multimedia sessions
  - Not media transfer (voice/video)
  - Establishing and negotiating the *context* of a call
- RTP transfer the actual multimedia
- SIP specified in RFC 3261 published by IETF 2002
  - First iteration in 1999 (RFC2543) – ten years old
  - Additional functionality specified in over 120 different RFCs(!)
  - Even more pending drafts...
  - Known to be complex and sometimes vague – difficult for software engineers to implement
  - Interoperability conference - “SIPit”

SIP specification

– huge, complex and sometimes vague



Redpill Linpro

Excerpts from an email posted on IEFT RAI mailing list:

I'm finally getting into SIP. I've got Speakeasy VoIP service, two sipphone accounts, a Cisco 7960 and a copy of x-ten on my Mac.

And I still can't make it work. Voice flows in one direction only. I'm not even behind a NAT or firewall -- both machines have global addresses, with no port translations or firewalls.

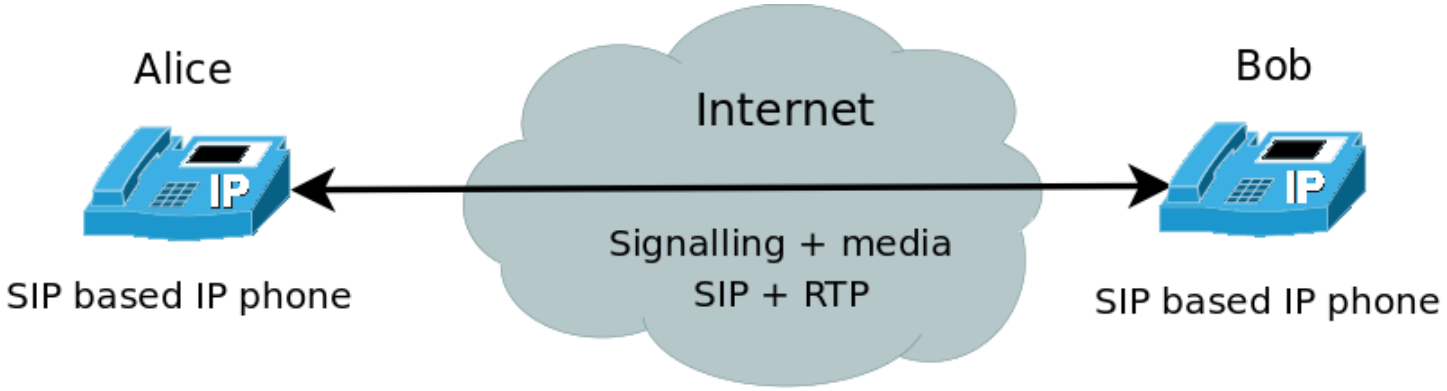
*I've been working with Internet protocols for over 20 years. I've implemented and contributed to them. And if *I* can't figure out how to make this stuff work, how is the average grandmother expected to do so?* ***SIP is unbelievably complex, with extraordinarily confusing terms.***

There must be half a dozen different "names" -- Display Name, User Name, Authorization User Name, etc -- and a dozen "proxies". Even the word "domain" is overloaded a half dozen different ways. This is ridiculous!

Sorry. I just had to get this off my chest. Regards,

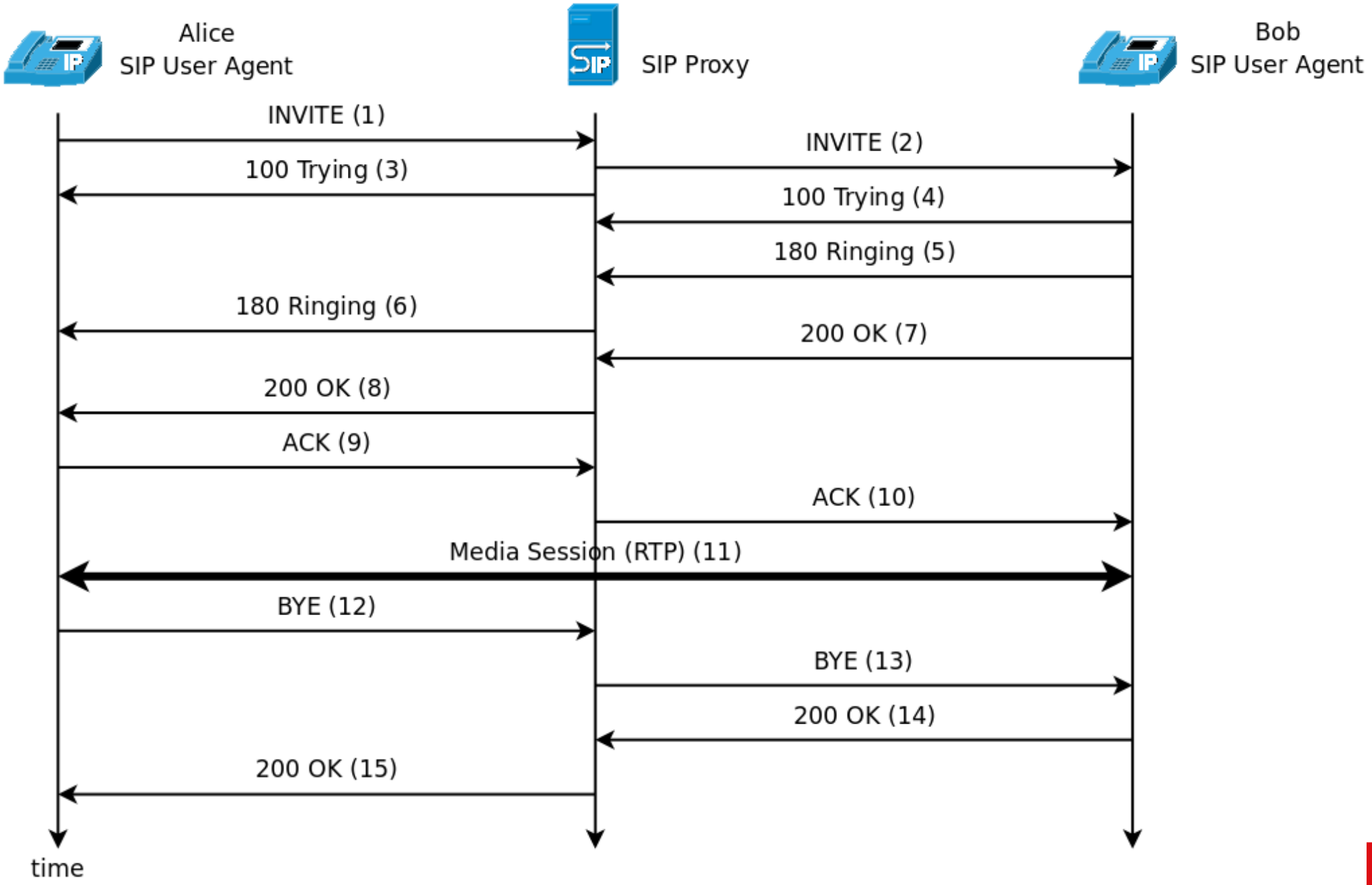
Reference: http://www.ietf.org/mail-archive/web/rai/current/msg00082.html

SIP example
- Direct call UA to UA



- Caller must know callee's IP or hostname
- No need for intermediate SIP hosts
- **Problems:**
  - Traversing firewalls
  - Seldom know IP/hostname of user
  - Mobility – change IP/hostname

SIP example proxied call



SIP message syntax - INVITE

Start line (method)

```
INVITE sip:bob@NR SIP/2.0
```

Message headers

```
Via: SIP/2.0/UDP 156.116.8.106:5060;rport;branch=z9hG4b
From: Alice <sip:alice@NR>;tag=2093912507
To: <sip:bob@NR>
Contact: <sip:alice@156.116.8.106:5060>
Call-ID: 361D2F83-14D0-ABC6-0844-57A23F90C67E@156.116.8
CSeq: 41961 INVITE
Max-Forwards: 70
Content-Type: application/sdp
User-Agent: X-Lite release 1105d
Content-Length: 312
```

Message body (SDP content)

```
v=0
o=alice 2060633878 2060633920 IN IP4 156.116.8.106
s=SIP call
c=IN IP4 156.116.8.106
t=0 0
m=audio 8000 RTP/AVP 0 8 3 98 97 101
.............
```

Redpill Linpro

VoIP threat taxonomy*

- Social threats
  - Balancing security and privacy. Unsolicited calls, intrusion of users privacy, fraud, identity theft and misrepresentation of identity or content
- Eavesdropping
  - A method by which an attacker is able to monitor the entire signaling and/or data stream
- Interception and modification
  - A method by which an attacker is able to see the entire signaling and/or data stream, and can also modify the traffic
- Service abuse
  - A large category of improper use including fraud, improper bypass, billing fraud, bypassing authentication, call conference abuse, ...
- Interruption of service
  - Can be classified into general and VoIP specific Denial of Service (DoS), physical intrusion, resource exhaustion, loss of external power, performance latency.

*) *"VoIP Security and Privacy Threat Taxonomy"*, VOIPSA (2005) http://www.voipsa.org/

Redpill Linpro

"*It's appalling how much worse VoIP is compared to the PSTN. If these problems aren't fixed, VoIP is going nowhere.*"

--- Philip Zimmerman on VoIP security in

“SIP Security”, Sisalem et. al. (2009)

With VoIP, Old Attacks Find New Targets

April 16, 2009
By David Needle
Submit Feedback »
More by Author »

IT professionals can add VoIP to the growing list of security threats they need to monitor. Security firm WatchGuard Technologies detailed seven leading threats to Voice over IP services in a release this week. While they aren't all new, they stand to become higher profile as the bad guys seek to exploit VoIP's increased popularity.

"Some of these are tested and true blue data hacks that have been around for a while, and now there's a lucrative new field for hackers and criminals to go after on the VoIP side," WatchGuard spokesman Chris McKie told *InternetNews.com*. "The bad guys are going to go where the money is."

WatchGuard says recent reports predict as much as 75 percent of corporate phone lines will be using VoIP in the next two years. By the end of this year, the total number of VoIP subscribers worldwide (residential and commercial) is expected to reach nearly 100 million.

Heading WatchGuard's list are Denial of Service (DoS) attacks, similar to those made to data networks. VoIP DoS attacks leverage the same tactic of running multiple packet streams, such as call requests and registrations, to the point where VoIP services fail.

These types of attack often target SIP (Session Initiation Protocol) extensions, according to WatchGuard, that ultimately exhaust VoIP server resources, which cause busy signals or disconnects.

Post a comment
Email Article
Print Article
Share Articles

Another is Spam over Internet Telephony (SPIT). Like unwanted e-mail, SPIT can be generated in a similar way with botnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, clog voicemail boxes and inhibit user productivity.

Security Strategy

Hackers to attack VoIP in two years

Video and all, Nortel says...

Tags: hackers, voip, nortel

By Dan Ilett

Published: 19 October 2005 13:25 BST

Show related articles

Hackers will attack voice over IP (VoIP) telephone conversations with spam and malicious code within two years, equipment manufacturer Nortel has claimed.

Companies using VoIP and other multimedia services, such as videoconferencing, should plan to defend against unsolicited adverts appearing mid-conversation, the company said.

SECURITY dark READING
Protect The Business Enable Access

WHITE PAPER: Modern Day Malware
Learn the methods criminals use to Install malware, and ways to stop them
Download Now

ATTACKS / BREACHES | VULNERABILITIES | APPLICATION
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTI

E-mail this page | Print this page | BOOKMARK

Experts: VOIP Attacks Are Tough to Stop

A recent VOIP hack is serving as a catalyst for VOIP security efforts, experts say

Jul 10, 2006 | 04:00 AM

By Mark Sullivan
DarkReading

Security experts say a high-profile VOIP hack is setting operators into action to protect against future problems. (See Two Charged in VOIP Hacking Scandal.)

Early last month federal authorities arrested Edwin Pena and Robert Moore for allegedly participating in a scheme that exploited the network weaknesses of several VOIP providers.

The feds accused the duo of secretly routing calls through legitimate VOIP networks, forcing those companies to foot the bill for the extra traffic they were carrying. On the flipside, Pena allegedly collected some $1 million in connection fees from other phone companies that he sold minutes to. (See VOIP Hacker Blues.)

Companies familiar with the Pena/Moore debacle worry that others will try, using relatively unsophisticated means, to exploit or take down their networks.

BusinessEdge security expert Yaron Raps says the Pena/Moore attack resulted in two large Tier 1 telcos calling on his company to do full security audits of their VOIP networks. Raps is the former head of technology and engineering at deltathree Inc. (Nasdaq: DDDC).

SANS why SANS? pick a course why certify? register now
The most trusted source for computer security training, certific
training certification resources vendor portal storm center college

SECURITY

VoIP hackers run up $120,000 phone bill

By Staff writers
Jan 22, 2009 1:37 PM
Tags: voip | hacker | perth | small | business | exploit | pbx

Hackers have breached the VoIP PBX telephone system of a 'small Perth business' and made over 11,000 international calls in 46 hours, resulting in a bill in excess of $120,000, according to WA Police.

Detectives from the West Australian Police Technology Crime Investigations unit said the business was only alerted to the security breach 'when they received an invoice from their service provider'.

The unit detectives called sophisticated compromises of VoIP systems an 'emerging trend' and warned businesses 'to utilise security software' to help protect their systems.

"Business operators should invest in appropriate security software to protect their communication systems," said Detective Sergeant Jamie McDonald.

Spam, DoS Headed VoIP's Way

Spam over Internet Telephony (SPIT) and DoS attacks could make IP telephony as vulnerable as e-mail.

August 23, 2004
By Susan Kuchinskas: *More stories by this author.*

Internet telephony, or Voice over IP (define), is picking up steam, as telcos get wise to the benefits of turning speech into packets to be delivered via the Internet. But some experts say that security efforts are lagging.

Denial of Service (DoS) attacks against VoIP networks are a real possibility, according to Frost & Sullivan analyst Jon Arnold -- and there's even a distant risk of spam over Internet telephony, or SPIT.

"The proliferation of Voice over IP is so small right now, it's not the kind of magnet for attacks that e-mail is," Arnold said.

SANS Top-20 2007 Security Risks (2007 Annual Update)

For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If y
Summary pointing out newsworthy highlights of the SANS 2007 Top Internet Se

...erabilities in:

...erabilities in:

...Services

...ers

Security Policy and
H1. Excessive User Rights a
H2. Phishing/Spear Phishing
H3. Unencrypted Laptops a

Application Abuse:
A1. Instant Messaging
A2. Peer-to-Peer Programs

Network Devices:
N1. VoIP Servers and Phones

Zero Day Attacks:
Z1. Zero Day Attacks

VoIP toll fraud attack racks up a £57K bill in two days

A recent report from the Australian press relates the story of a ... where hackers made 11,000 calls via the company's VoIP runn... AU$ 120,000 (£57,000) . This figure ranks this incident am... expensive of documented toll-fraud attacks.

Do events like this throw the viability of this technology into do... wakeup call that is needed to force a more serious view of VoIP s...

To misuse a VoIP system in this way an attacker needs to be ... things; to connect to the targeted system and then to make calls.

The first step is easy, there are a number of legitimate reason... system should allow external connections, for example provid... corporate phone services for home workers or roaming users.

October 11, 2004

Kill Voice Spam Before It Grows

Spammers have come close to ruining e-mail--and threaten to do the same to Internet telephony. The time to stop them is now.

By Eric Hellweg

Share » | Favorite | Print | E-mail

Its not uncommon to arrive at work in the morning, fire up your e-mail program and find your inbox littered with spam. Weve become accustomed to the ritual of deleting these pitches. But what if you arrived at work and your voicemail announced that you had 40 new messages--and that 35 of them were unsolicited commercial calls? Listening to and deleting these messages would be more time-consuming than trashing your junk e-mail.