

VoIP – some threats, security attacks and security mechanisms

Lars Strand

RiskNet – Open Workshop

Oslo, 24. June 2009

"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.

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

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.

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.

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 Kuchinskias: [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.

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



A recent report from the Australian press [relates](#) the story of a Perth business where hackers made 11,000 calls via the company's VoIP system in two days for AU\$ 120,000 (£57,000) . This figure ranks this incident among the most expensive of documented toll-fraud attacks.

Do events like this throw the viability of this technology into doubt and make a wakeup call that is needed to force a more serious view of VoIP security?

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

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

ATTACKS / BREACHES	VULNERABILITIES	APPLICATION
SECURITY MANAGEMENT	STORAGE SECURITY	ENCRYPT

[E-mail this page](#) | [Print this page](#) | [BOOKMARK](#) [Facebook](#) [Twitter](#) [LinkedIn](#)

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).

[Post a comment](#)

[Email Article](#)

[Print Article](#)

[Share Articles »](#)

SANS why SANS? pick a course why certify? register now

The most trusted source for computer security training, certification

training certification resources vendor portal storm center college

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

For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If you want a summary pointing out newsworthy highlights of the SANS 2007 Top Internet Security Risks, click here.

- Vulnerabilities in:**
- H1. Excessive User Rights and Privileges
 - H2. Phishing/Spear Phishing
 - H3. Unencrypted Laptops and Mobile Devices
- 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?

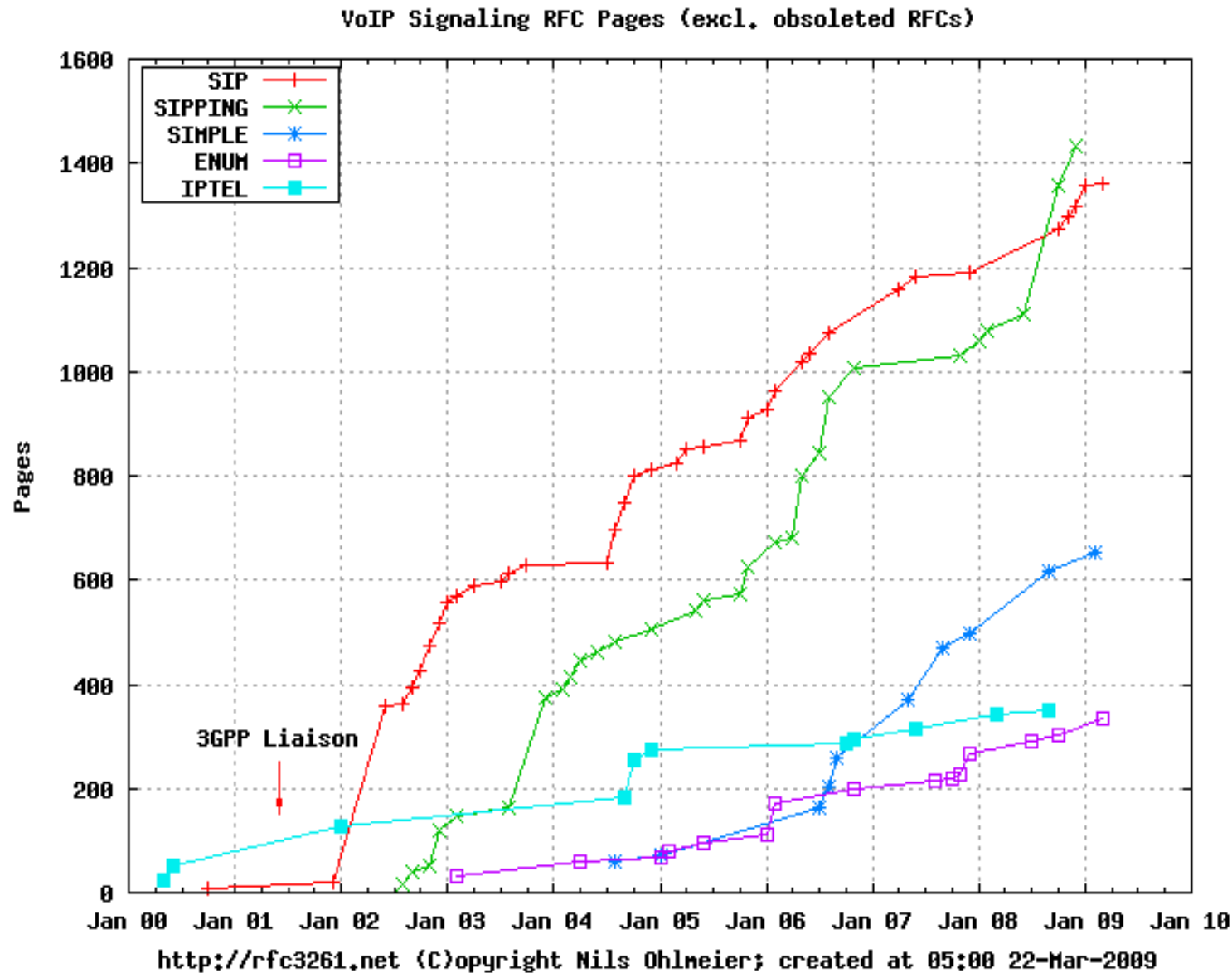
- Voice over IP (VoIP) protocols and technology is a merge of telecom and data communication
- **What is VoIP?**
 - Broad definition: Sending and receiving media (voice/video) over IP
- **Why VoIP?**
 - Added functionality and flexibility – which may be hard to provide over PSTN
 - Reduced cost – uses 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

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



Excerpts from an email posted on IETF 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.

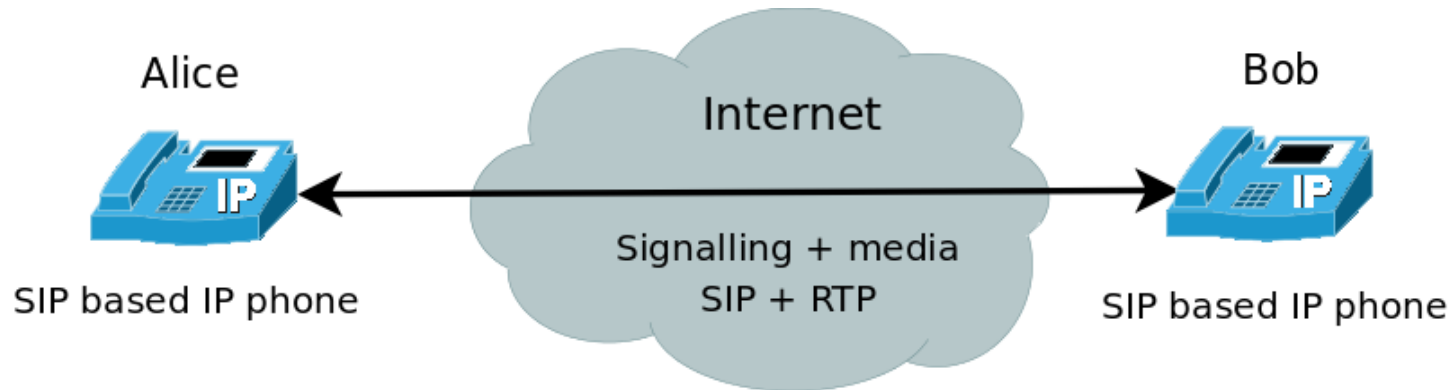
*I've been working with Internet protocols for **over 20 years**. I've implemented and contributed to them. And if **I** can't figure out how to make this stuff work, how is the average grandmother expected to do so? **SIP is unbelievably complex, with extraordinarily confusing terms**. There must be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

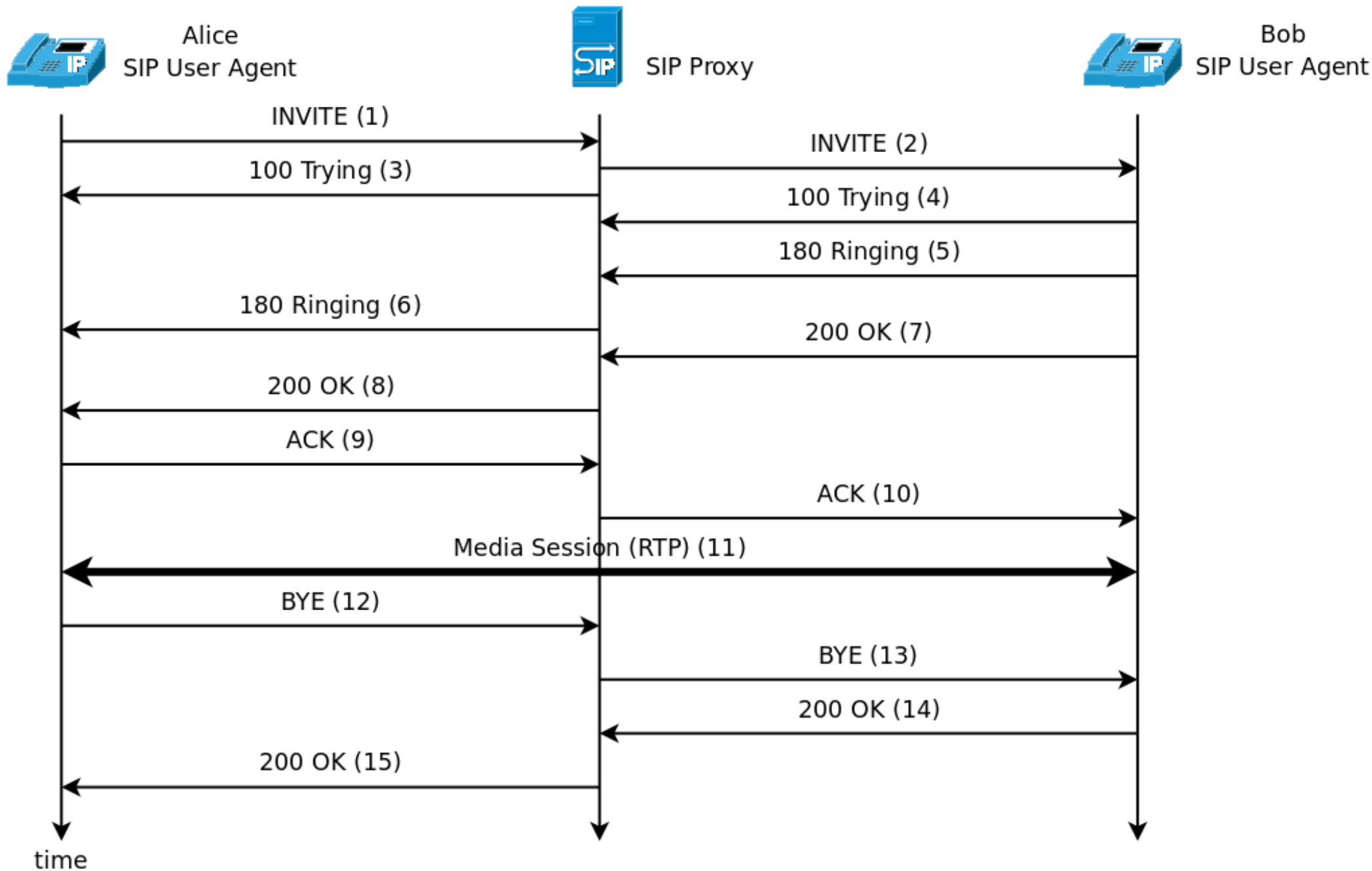
SIP example

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=z9hG4bL  
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)**

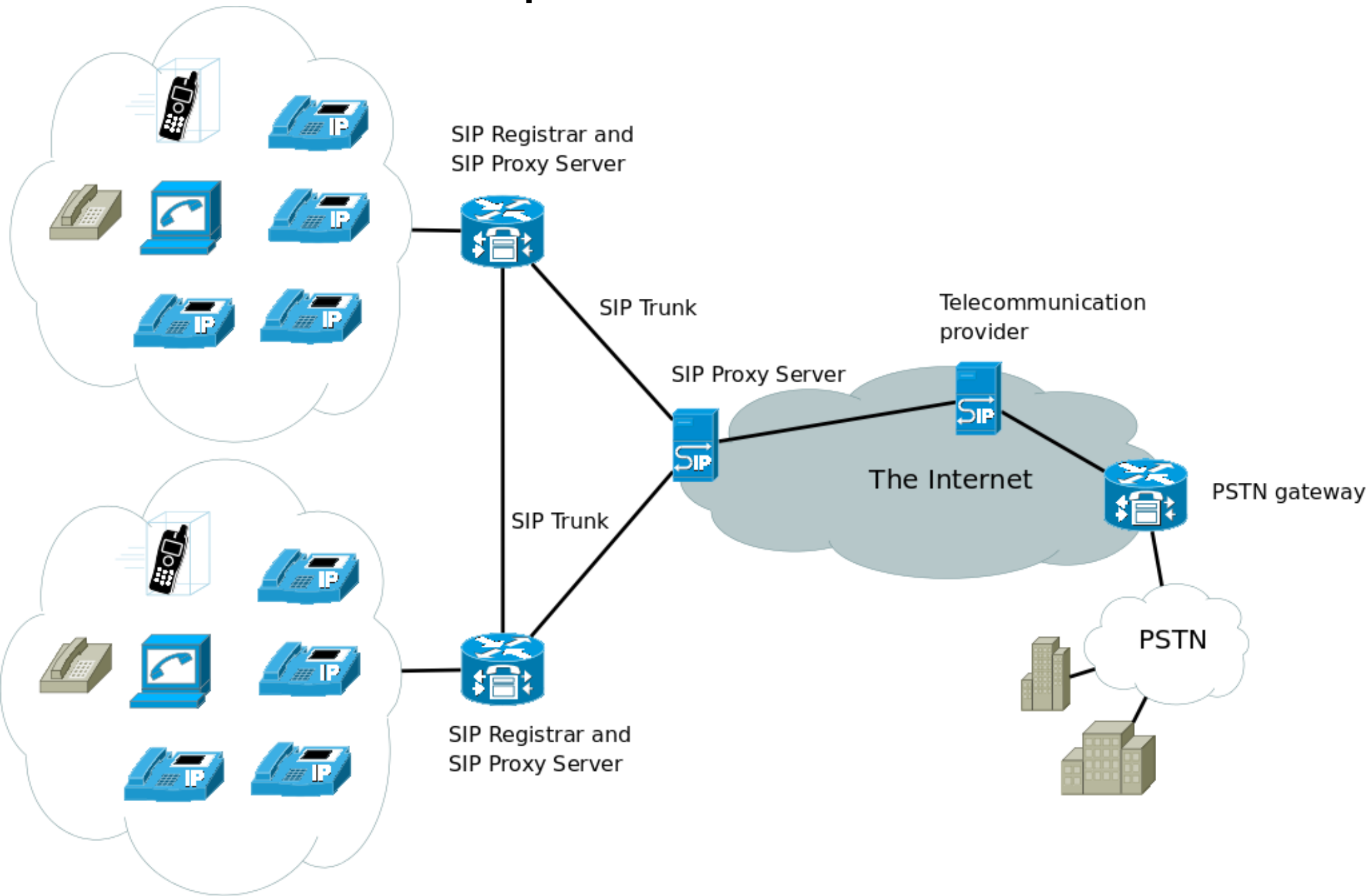
```
v=0  
o=alice 2060633878 2060633920 IN IP4 156.116.8.106  
s=SIP call  
c=IN IP4 156.116.8.106  
t=0 0  
m=audio 8000 RTP/AVP 0 8 3 98 97 101  
.....
```

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/>

Example VoIP scenario



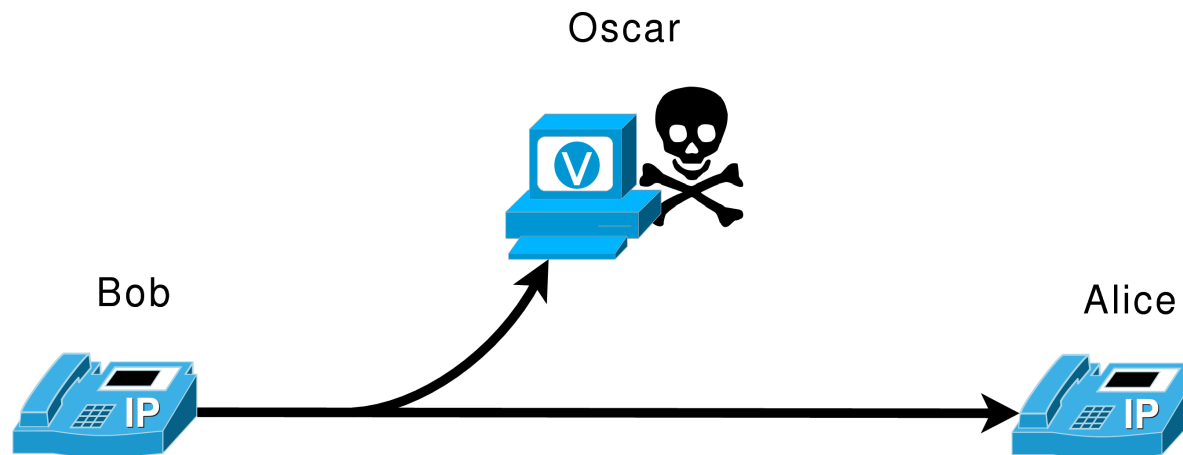
Social threats

- Eavesdropping the environment
 - (Mis)Configure phone to accept SIP header “Alert-Info: Ring Answer”
 - Example: Asterisk and Polycom SoundPoint IP550:
 - `exten => XXXXXXXX,n,SIPAddHeader(Alert-Info: Ring Answer)`
 - `exten => XXXXXXXX,n,Dial(SIP/XXXXXXXX,1)`
 - **The phone silently answer the incoming call. Audio from the environment is transmitted to the caller.**



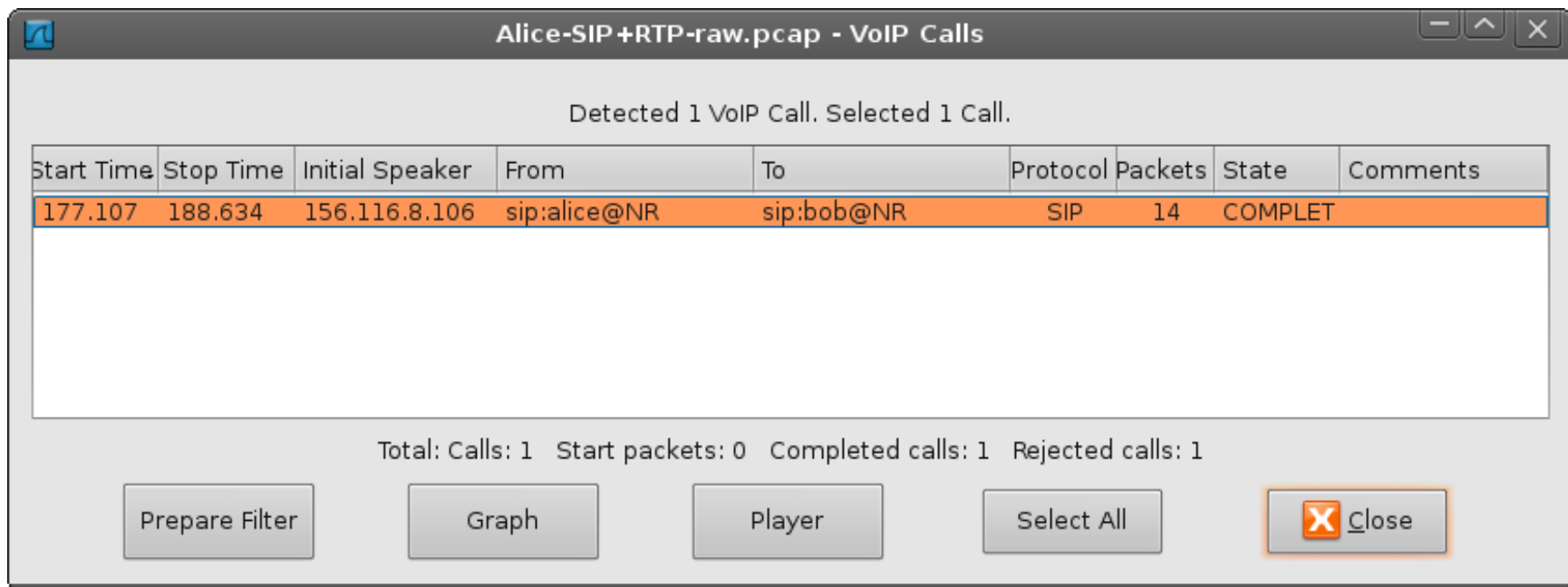
Eavesdropping

- Traffic capture (release of message contents)
 - i.e. wiretapping/record the call
- Call pattern tracking (traffic analysis)
 - i.e. “I know a call took place”



Eavesdropping - tools

- Any tool that can sniff (and analyze) network traffic
 - tcpdump, wireshark, ...
- Problem: Must control one intermediate host/network link.



Detected 1 VoIP Call. Selected 1 Call.

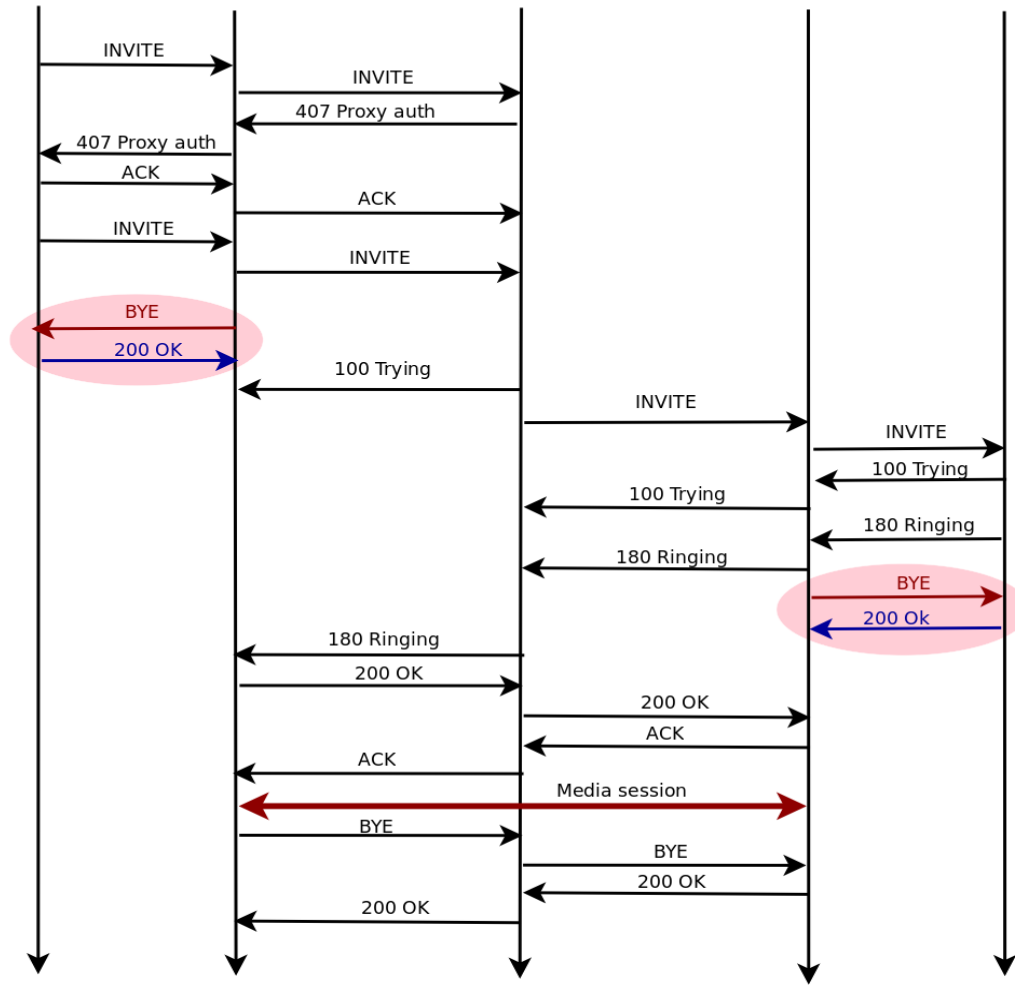
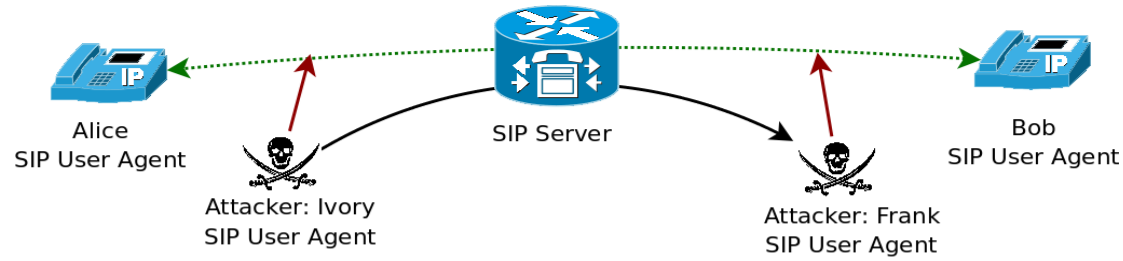
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
177.107	188.634	156.116.8.106	sip:alice@NR	sip:bob@NR	SIP	14	COMPLET	

Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 1

Buttons: Prepare Filter, Graph, Player, Select All, Close

Interception and modification

- Call hijacking - Take over a SIP INVITE session:



Interception and modification - tools

- SiVuS – SIP generator (and more)

The screenshot shows the SiVuS application interface. The window title is "SiVuS - The VoIP Vulnerability Scanner v1.10". The interface has a yellow header with tabs for "SIP", "MGCP", "H.323", "RTP", and "About". Below the header are sub-tabs for "SIP Component Discovery", "SIP Scanner", "Utilities", and "SIP Help". The main area is divided into two panes: "Message Generator" and "Authentication Analysis".

The "Message Generator" pane contains a form for creating SIP messages. The form has the following fields:

Method	Transport	Called User	Domain/Host	Port
INVITE	UDP	alice	euxcs1.nr.no	5060

Other fields in the form include:

- Via: SIP/2.0/UDP 156.116.20.50 Branch eI6Vb5No2CnQnu
- To: Alice <sip:alice@NR >
- From: Bob <sip:bob@NR >; ta... qDTevEISPx
- Authentication:
- Call-ID: VvrbgxhoerL@192.168.20.50
- Cseq: 123456 INVITE
- Contact: <sip:bob@192.168.20.50:5060 >
- Record-Route:
- Subject: SiVuS Test
- Content-type: application/sdp
- User Agent: SiVuS Scanner
- Expires: 7200 Max-Forwards: 70
- Event:
- Refer-To:
- Content Leng... 0

There is a checkbox labeled "Use SDP?" which is checked.

The "Conversation Log" pane is empty.

Service abuse

- Registration attack
 - Weak/no password
 - Example: Company X used the last three digits in the phone number as password
 - SIP REGISTER with digest authentication example
- Misconfiguration
 - Services not used
 - Web-GUI – default password

*“Moore said what made the hacking job so easy was that 70% of all the companies he scanned were insecure, and 45% to 50% of VoIP providers were insecure. **The biggest insecurity? Default passwords.**”*

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

DoS attack is

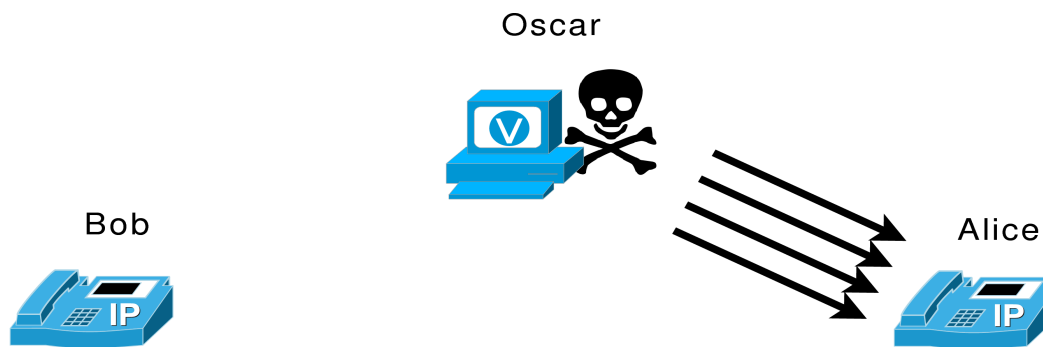
HARD!

Why: KISS

(and brutally effective)

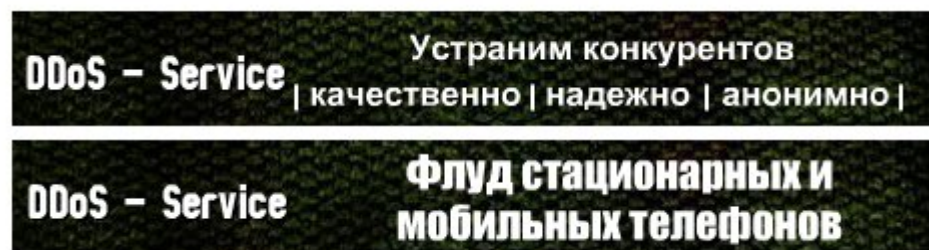
Interruption of Service (aka. DoS attack)

- VoIP DoS attack
 - Flooding with SIP INVITE or REGISTER
 - SIP messages are (often) not authenticated
 - Most hard-phones have limited hardware
 - Results: Crash, halt or degrade performance of device
- “Normal” DoS attack
 - Below application layer in the network stack – UDP/TCP or just IP/ICMP
 - An Distributed DoS (DDoS) with spoofed sender IP effective and hard to protect against



DDoS for sale

Russian ad for launching DDoS VoIP attack against an competitor:



The ad scrolls through several messages, including

- "Will eliminate competition: high-quality, reliable, anonymous."
- "Flooding of stationary and mobile phones."
- "Pleasant prices: 24-hours start at \$80. Regular clients receive significant discounts."
- "Complete paralysis of your competitor/foe."

Flooding of victims phones can be devastating

- SPIT can also turn out to be a major problem

Reference: <http://isc.sans.org/diary.html?storyid=5380>

RiskNet Workshop



Part 2:

Security mechanisms

Secure communication

To secure the communication between two parties:

1) Mutual authentication

2) Key exchange

- enables the participant to obtain a shared secret

3) Symmetric cryptographic algorithms

- enables the communication to be integrity protected and confidential

Secure SIP

- Basically: SIP + TLS = SIPS
- The same security mechanism as https
- Solves a lot of security threats and provides
 - integrity protection
 - confidentiality (encryption)
 - stronger authentication (certificates)
- Problem: Intermediate SIP proxies need to read/edit SIP headers.
- Solution: TLS only provide single hop of confidentiality and authentication (between SIP proxies)
- If a proxy don't support SIPS, it must decline the request.
 - What if one proxy cheats?

Media security: SRTP

- Basically: RTP + TLS = SRTP
- Again: The same security mechanism as https
- Solves a lot of security threats and provides
 - integrity protection
 - confidentiality (encryption)
 - stronger authentication (certificates)

Why so hard?

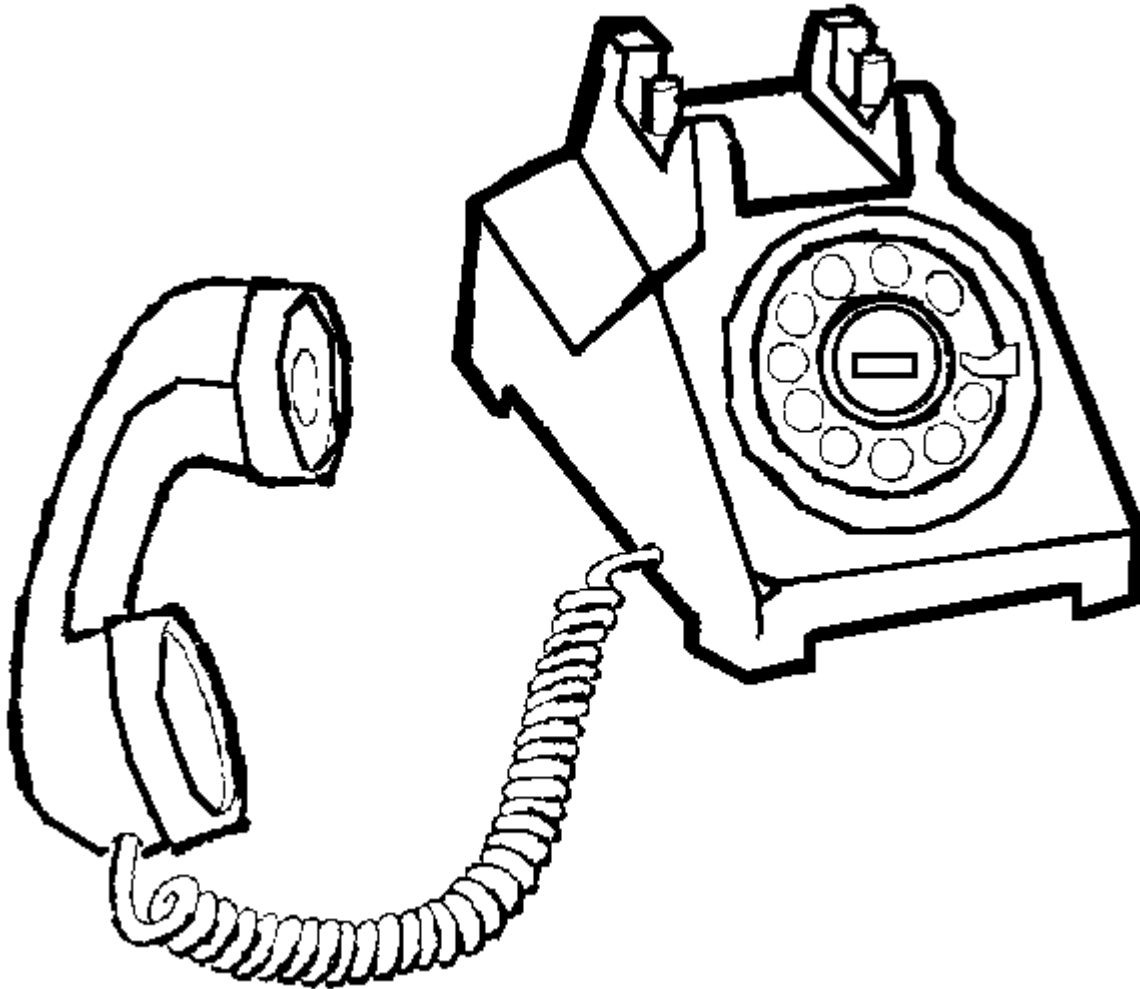
- Cryptography provides reasonable solutions to all known security problems
- Why then is security an issue at all?
- Security mechanisms are deployed partially or not at all
- VoIP uses multiple components in an already complex architecture



Highly relevant issue: Monitoring

- What do you use to monitor your infrastructure?
- Do you know what is going on?
 - How much CPU load?
 - Network utilization?
 - Number of SIP calls at *this* moment?
- **Do you know or do *think* you know?**
- What tools do you use?
 - Munin?
 - Nagios?
 - MRTG?

Thank you



Project homepage: <http://eux2010sec.nr.no>

RiskNet Workshop

