Improving SIP authentication

Lars Strand
Wolfgang Leister

Stockholm, 3. Dec 2010

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

"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.

Post a comment
Email Article
Print Article
Share Articles

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 darkREADING
Protect The Business · Enable Access

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).

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.

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.

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

nerabilities in:

nerabilities in:

Services

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

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 t 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 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.

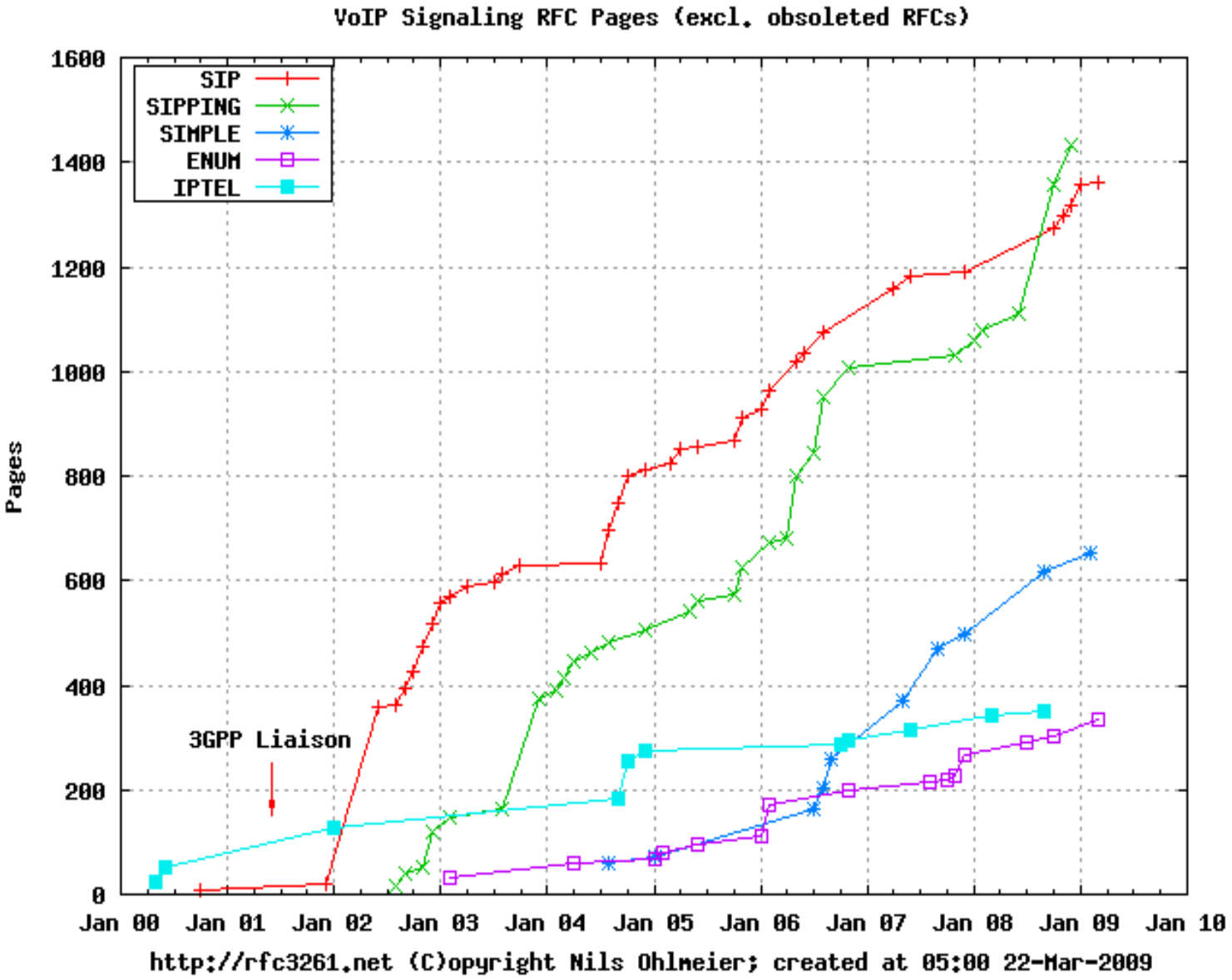
VoIP?

- 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 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.

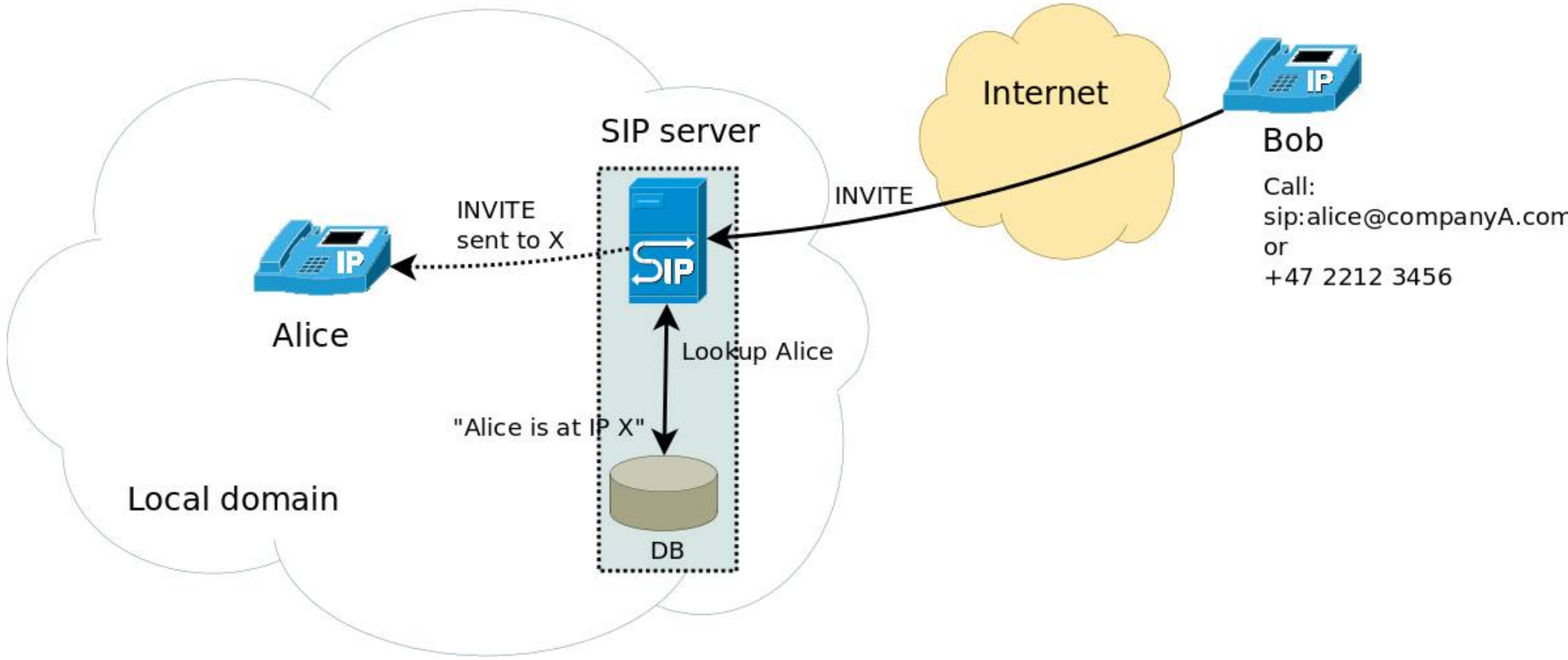
And I still can't make it work. Voice flows in one direction only. I'm not even behind a NAT or firewall -- both machines have global addresses, with no port translations or firewalls.

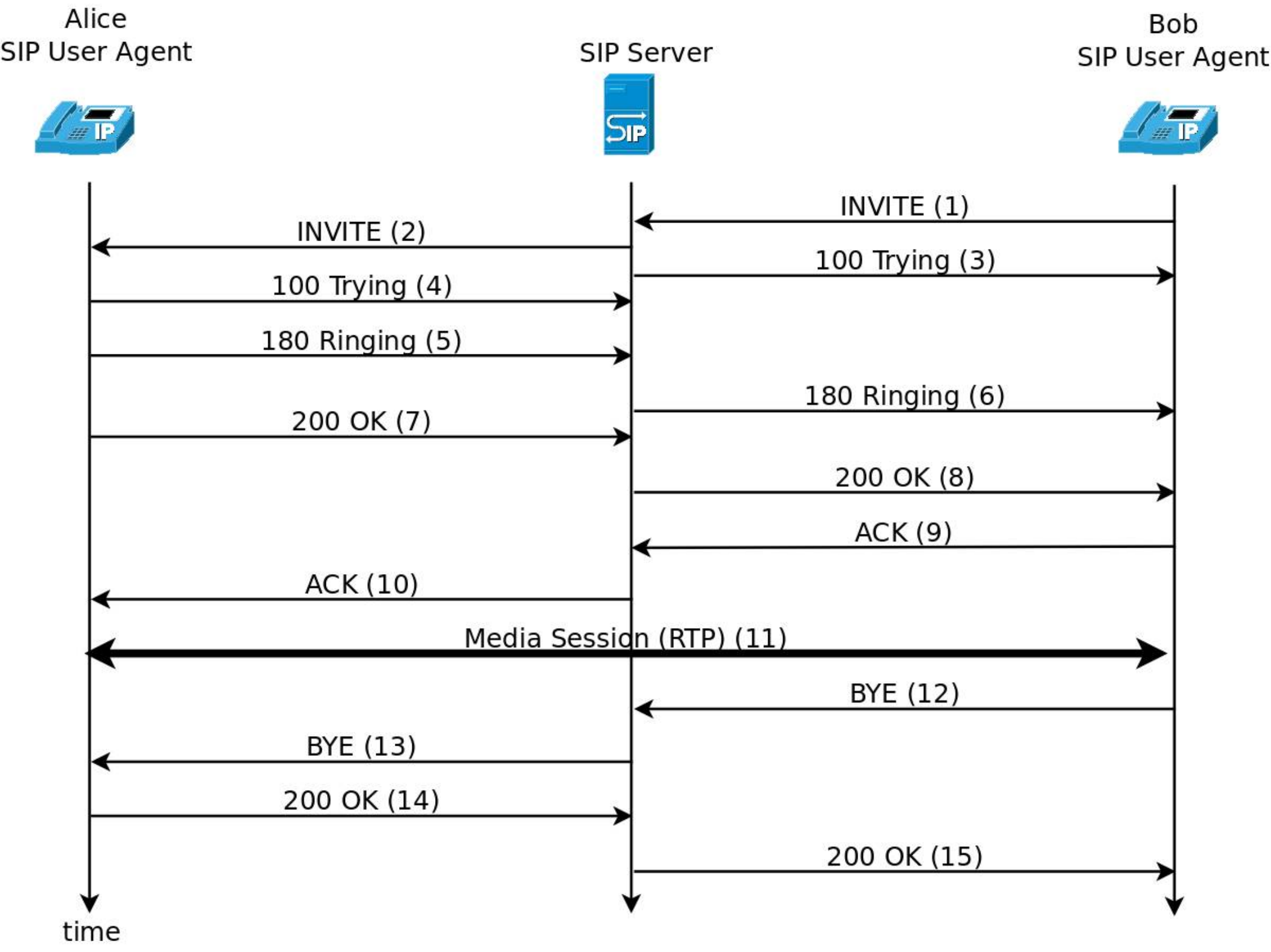
*I've been working with Internet protocols for over 20 years. I've implemented and contributed to them. And if *I* can't figure out how to make this stuff work, how is the average grandmother expected to do so?* ***SIP is unbelievably complex, with extraordinarily confusing terms.*** *There must be half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

VoIP call flow




Alice
SIP User Agent
SIP Server
Bob
SIP User Agent
INVITE (1)
INVITE (2)
100 Trying (3)
100 Trying (4)
180 Ringing (5)
180 Ringing (6)
200 OK (7)
200 OK (8)
ACK (9)
ACK (10)
Media Session (RTP) (11)
BYE (12)
BYE (13)
200 OK (14)
200 OK (15)
time

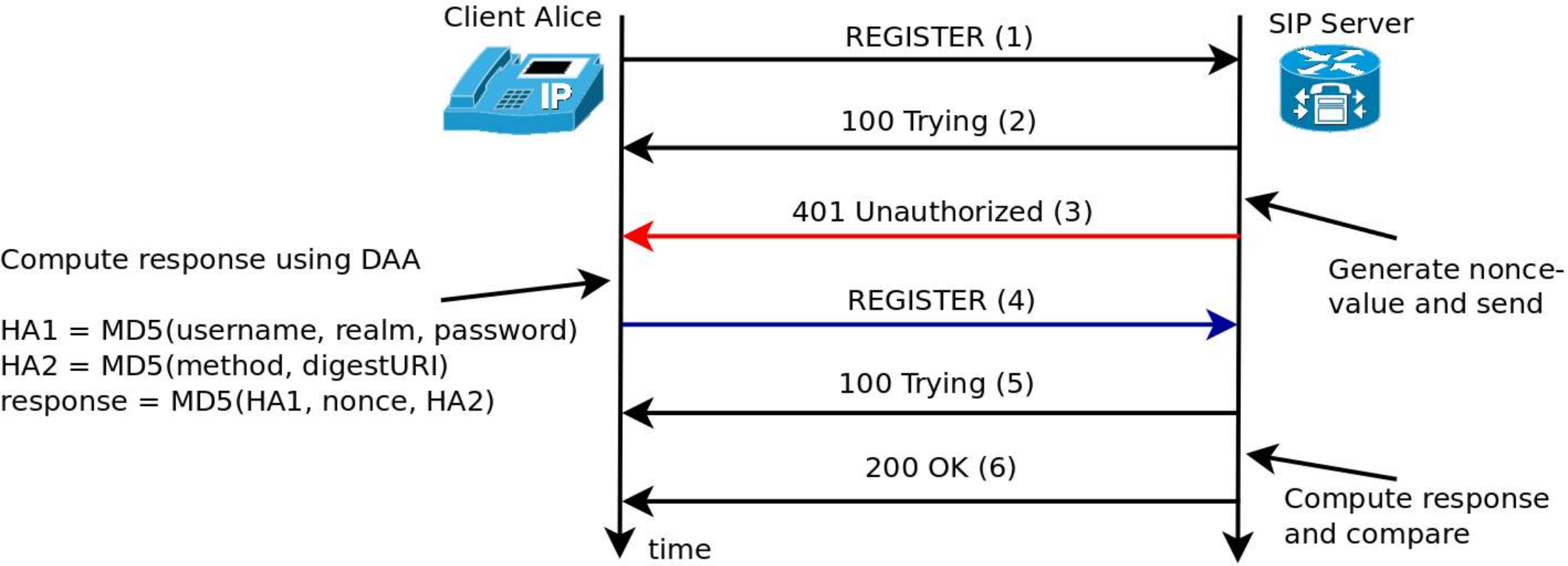
Alice must REGISTER her IP/hostname
to the local SIP Server

Problem:

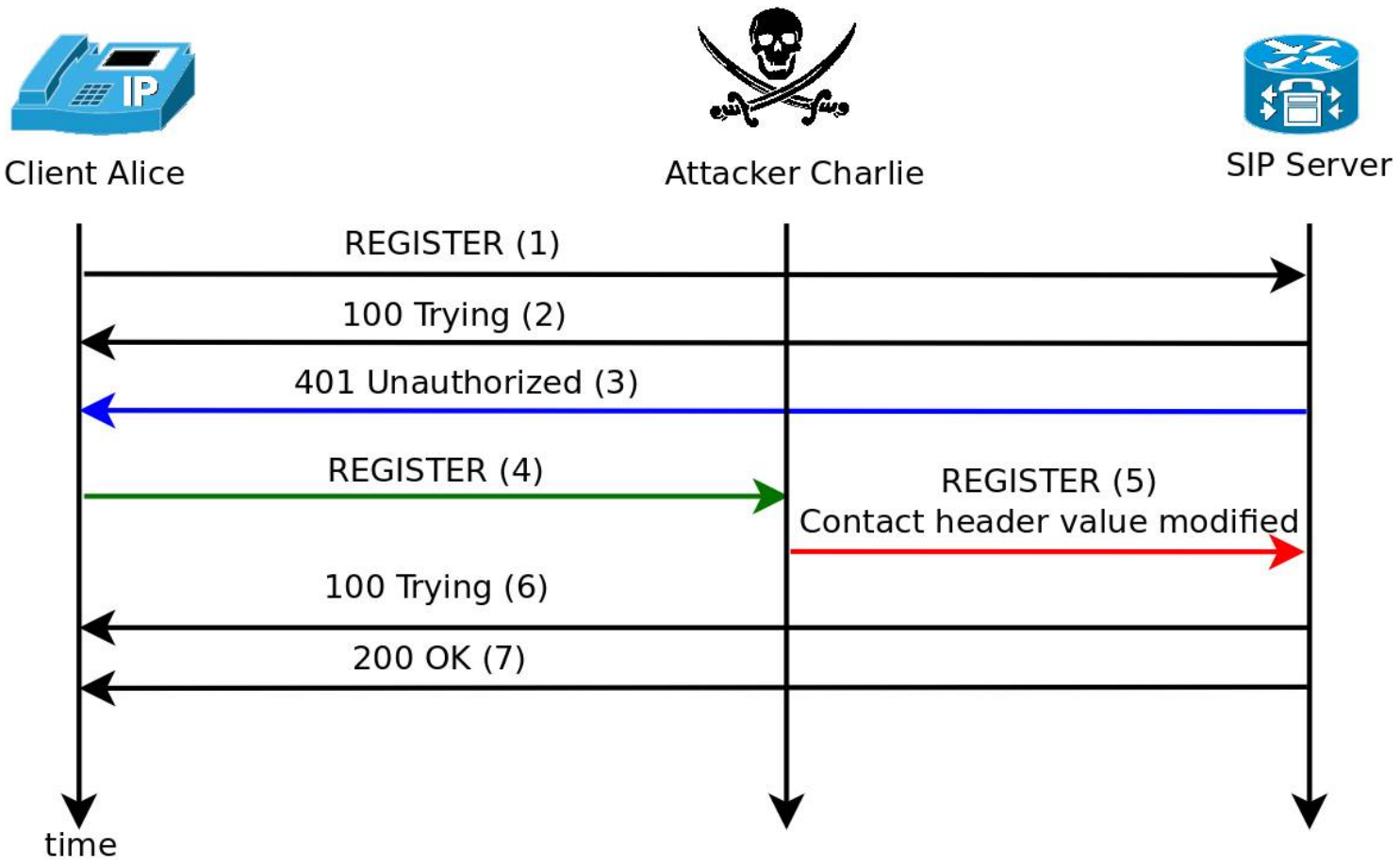
The authentication method in SIP is weak

(Uses the Digest Access Authentication)

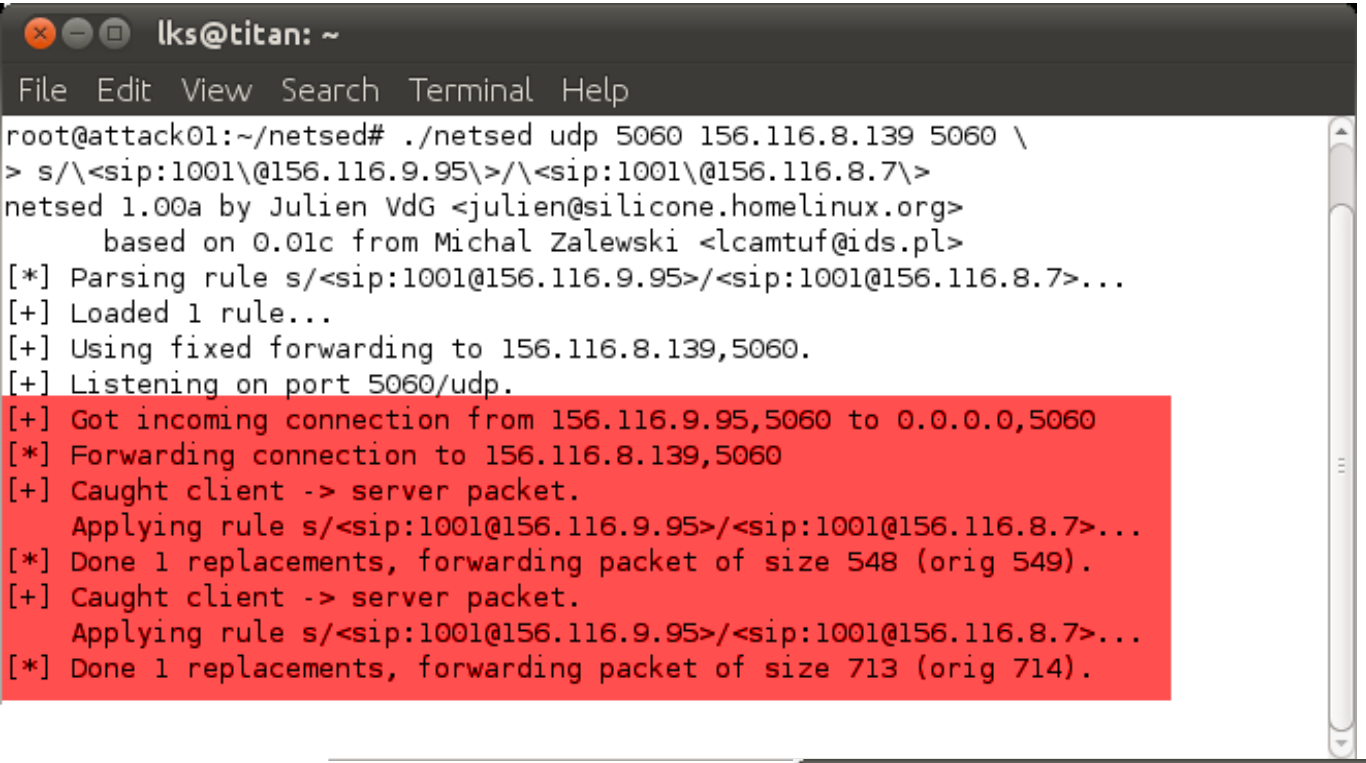
SIP REGISTER using DAA



MitM attack – modify Contact



Execution of the attack



Attack:

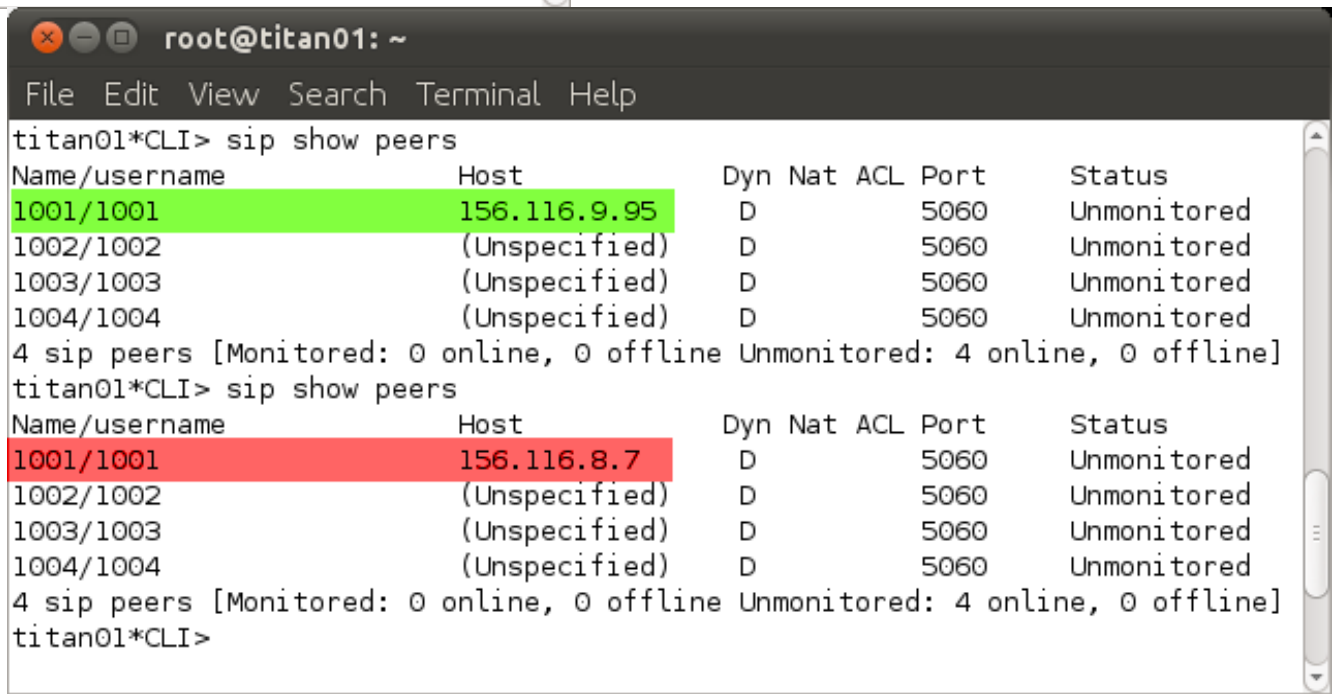
We use NetSED to modify the network stream live.

Can use search and replace based on regexp

SIP server (Asterisk):

The location of Alice is registered with the attackers IP/hostname *WITHOUT the server/client knowledge*

Result: All calls are forwarded to the attacker



To counter the attack: Modify DAA

To fix the vulnerability and counter the attack, add the Contact value as part of the digest hash:

```
HA0 = MD5(A0) = MD5(ContactURIs)
HA1 = MD5(A1) =
MD5(username:realm:password)
HA2 = MD5(method:digestURI)
response = MD5(HA0:HA1:nonce:HA2)
```

SIP message syntax - REGISTER

```
1.  REGISTER sip:CompanyA SIP/2.0
2.  Via: SIP/2.0/UDP
    156.116.9.95;branch=z9hG4bK32F3EC44EB23347BFB0D488459C69E4E
3.  From: Alice <sip:alice@CompanyA>;tag=1234648905
4.  To: Alice <sip:alice@CompanyA>
5.  Contact: "Alice" <sip:alice@156.116.9.95:5060>
6.  Call-ID: 2B6449C74C10D4F95006A6C034E79E8E@CompanyA
7.  CSeq: 19481 REGISTER
8.  User-Agent: PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392
9.  Authorization: Digest
    username="alice",realm="asterisk",nonce="3b7a1395",response="
    ccbde1c3c129b3dcaa14a4d5e35519d7",uri="sip:CompanyA",algorith
    m=MD5
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0
```

Conclusion

- DAA is weak
- Easily exploitable in a real-world attack
- Attack works surprisinlgy well
- The result is nasty
- Requirement: Attacker must be MitM
- Future work:
  - NAT?
  - Improve DAA for other SIP methods? Like INVITE?
  - Replace DAA with another authentication method?