

Migration towards a more secure authentication in the Session Initiation Protocol

Lars Strand
Wolfgang Leister
Alan Duric

*The Fifth International Conference on Emerging Security Information, Systems and
Technologies (SECURWARE 2011)
21-27 August 2011
Nice, France*

"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
SECURITY MANAGEMENT	STORAGE SECURITY	ENCRYPTED COMMUNICATIONS

[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, 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 noteworthy highlights of the SANS 2007 Top Internet Security Risks, click here.

Vulnerabilities in:

Vulnerabilities in:

Services

re

ers

e

Security Policy and

- H1. Excessive User Rights at
- 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?

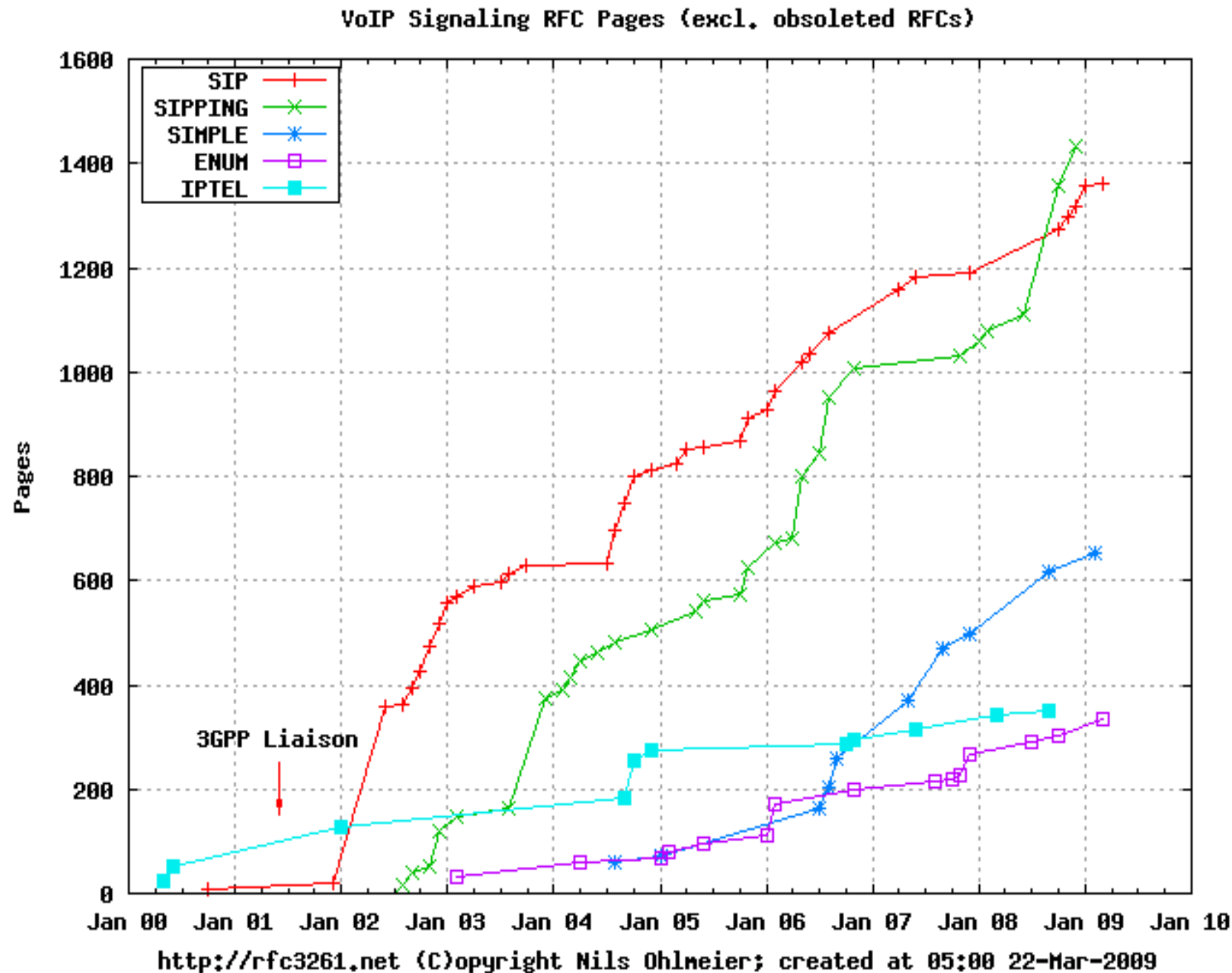
- Voice over IP (VoIP) protocols and technology is a merge of telecom and data communication
- **What is VoIP?**
 - Broad definition: Sending and receiving media (voice/video) over IP
- **Why VoIP?**
 - Added functionality and flexibility – which may be hard to provide over PSTN
 - Reduced cost – uses 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
 - Establishing and negotiating the *context* of a call
 - No media transfer (voice/video)
- RTP transfer the actual multimedia
- SIP specified in RFC 3261 published by IETF 2002
 - First iteration in 1999 (RFC2543)
 - 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.

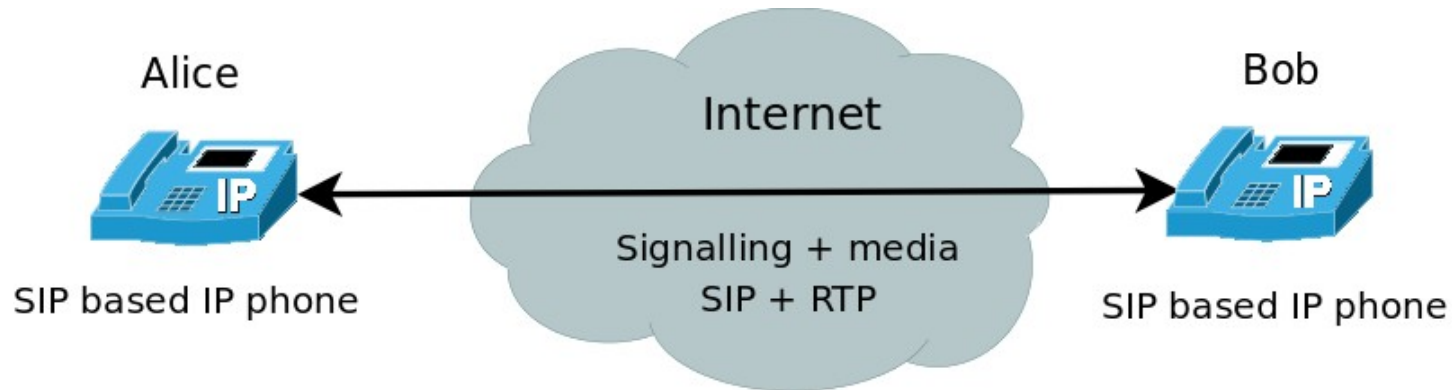
*I've been working with Internet protocols for **over 20 years**. I've implemented and contributed to them. And if **I** can't figure out how to make this stuff work, how is the average grandmother expected to do so? **SIP is unbelievably complex, with extraordinarily confusing terms**. There must be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

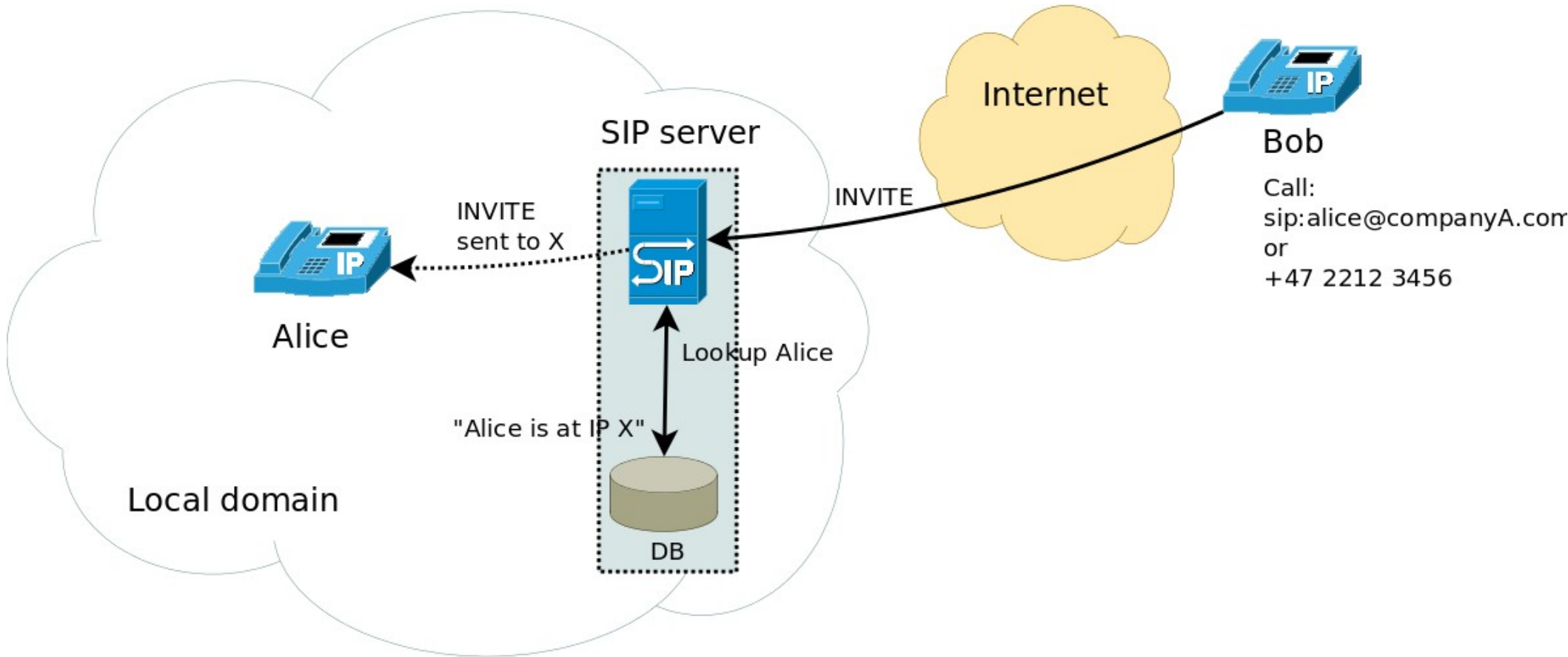
SIP example

Direct call UA to UA

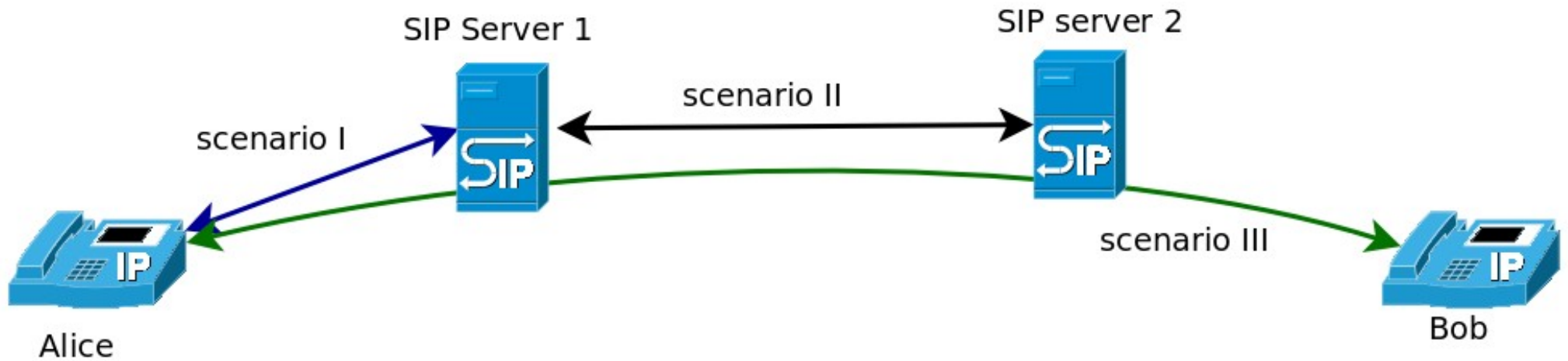


- Caller must know callee's IP or hostname
- No need for intermediate SIP hosts
- **Problems:**
 - Traversing firewalls
 - Seldom know IP/hostname of user
 - Mobility – change IP/hostname

SIP call flow



Three SIP authentication scenarios



SIP authentication - today

1) Digest Access Authentication (DAA) (RFC3261)

- Mandatory but weak
- widespread adoption - “everyone” use this
- used to authenticate locally within a domain/realm (during REGISTER or INVITE)

2) S/MIME (RFC3261)

- Goal: Security service end to end
- Uses certificates, needs PKI = “complex and expensive”
- Not supported, not used.

3) Transport Layer Security (TLS)

- 1) Well-known and widely adopted technology (HTTPS)
- 2) SIPs have industrial momentum
- 3) TLS only provide hop-by-hop security, and rely on PKI.

4) Other user identity handling methods

- P-Asserted identity (RFC3325) – in a trusted environment
- Strong Identity (RFC4474) – using authentication service
- Other academic approaches.

WANTED:

**Strong and flexible authentication
method in SIP!**

We propose a two-step migration:

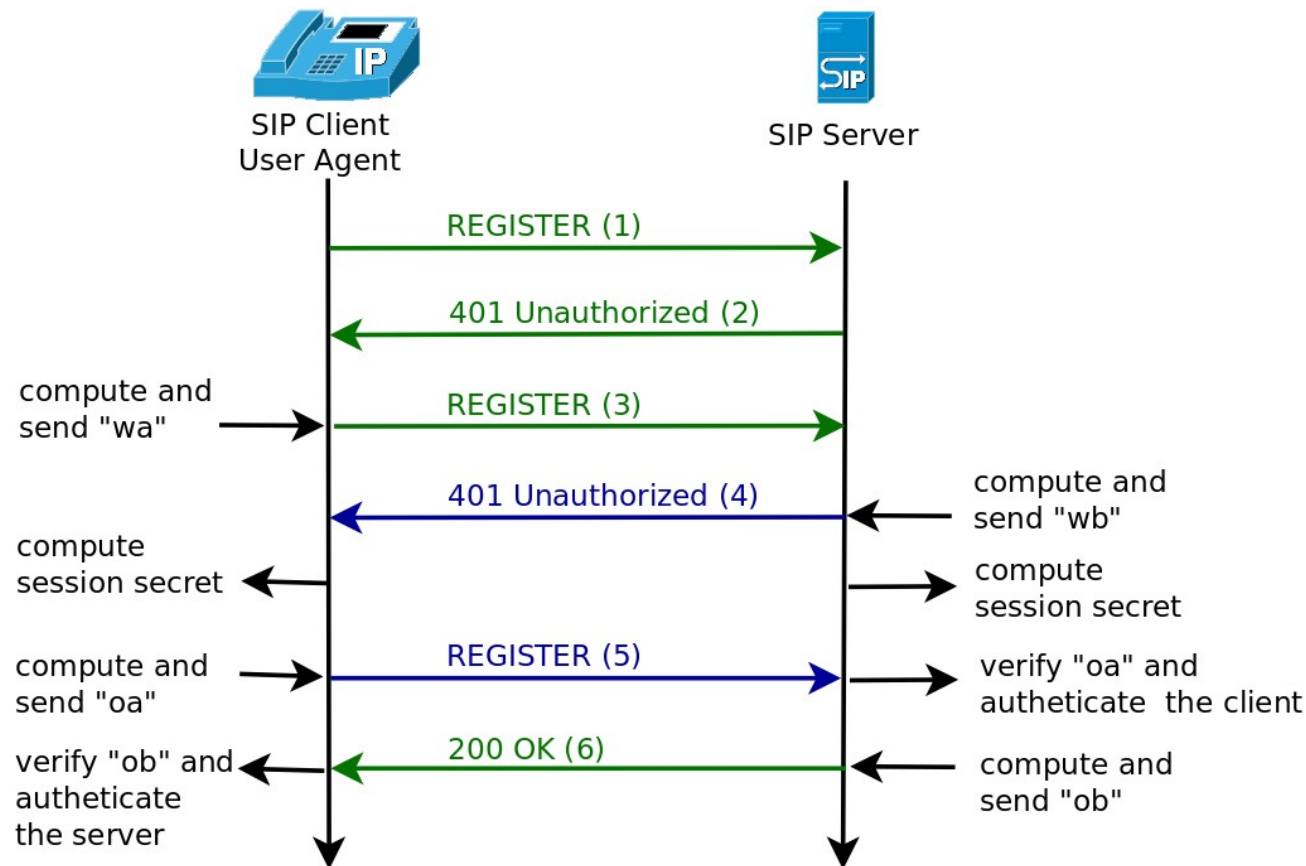
- 1. PAKE**
- 2. SASL**

Problem and goal

- SIP is flexible
- Problem: Different usage scenarios have different security requirements
 - Handheld devices vs. high-end SIP servers
- Goal: Modification to the SIP standard should be minimum
- Goal 2: A strong and flexible authentication methods wanted
- Solution: Add support for PAKE and SASL

1. PAKE

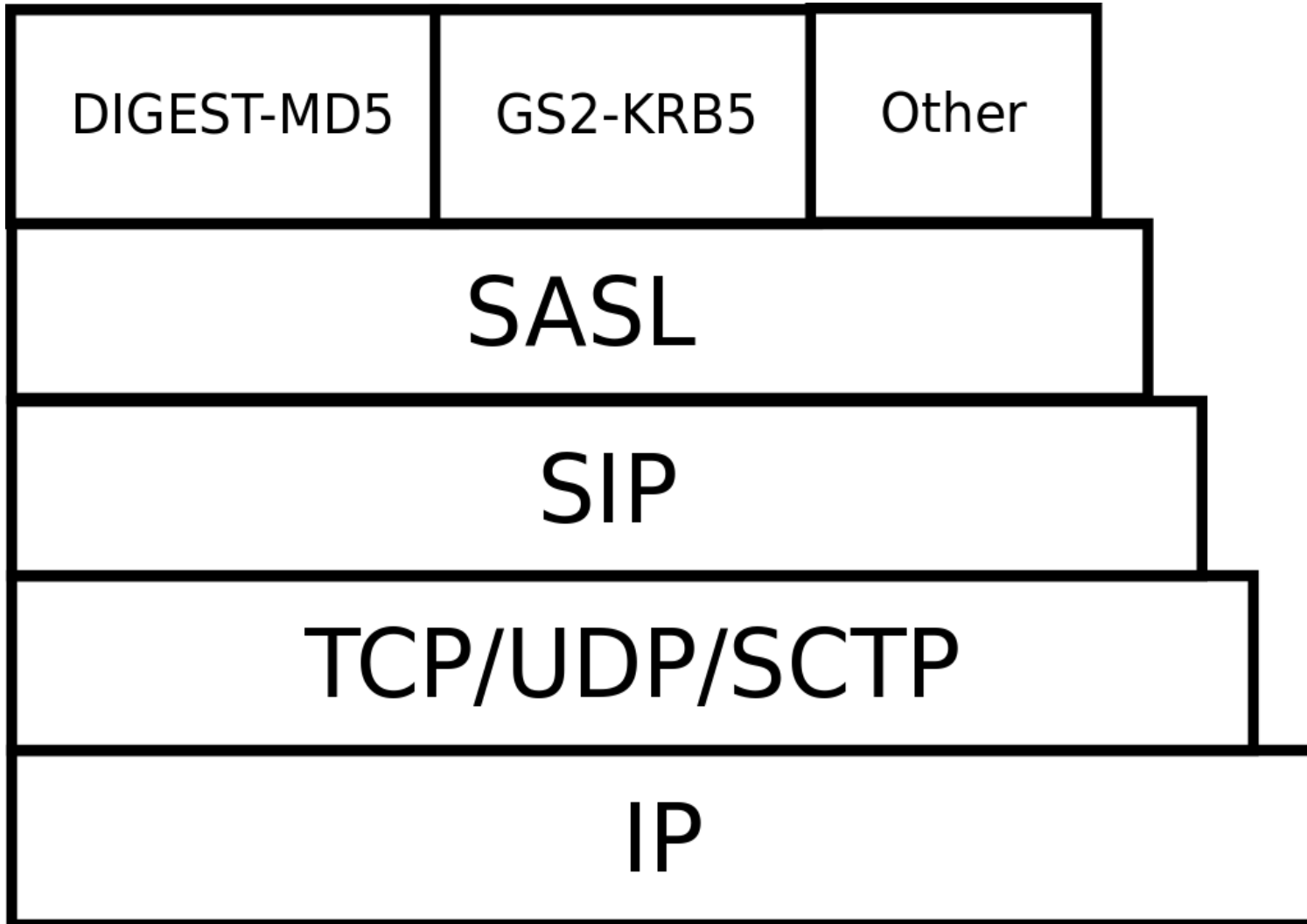
- “Password Authenticated Key Exchange” (PAKE)
 - Provides mutual authentication of client and server
 - Reuse the shared secret used by the DAA
 - Stronger than DAA
- PAKE + HTTP currently worked on in the IETF

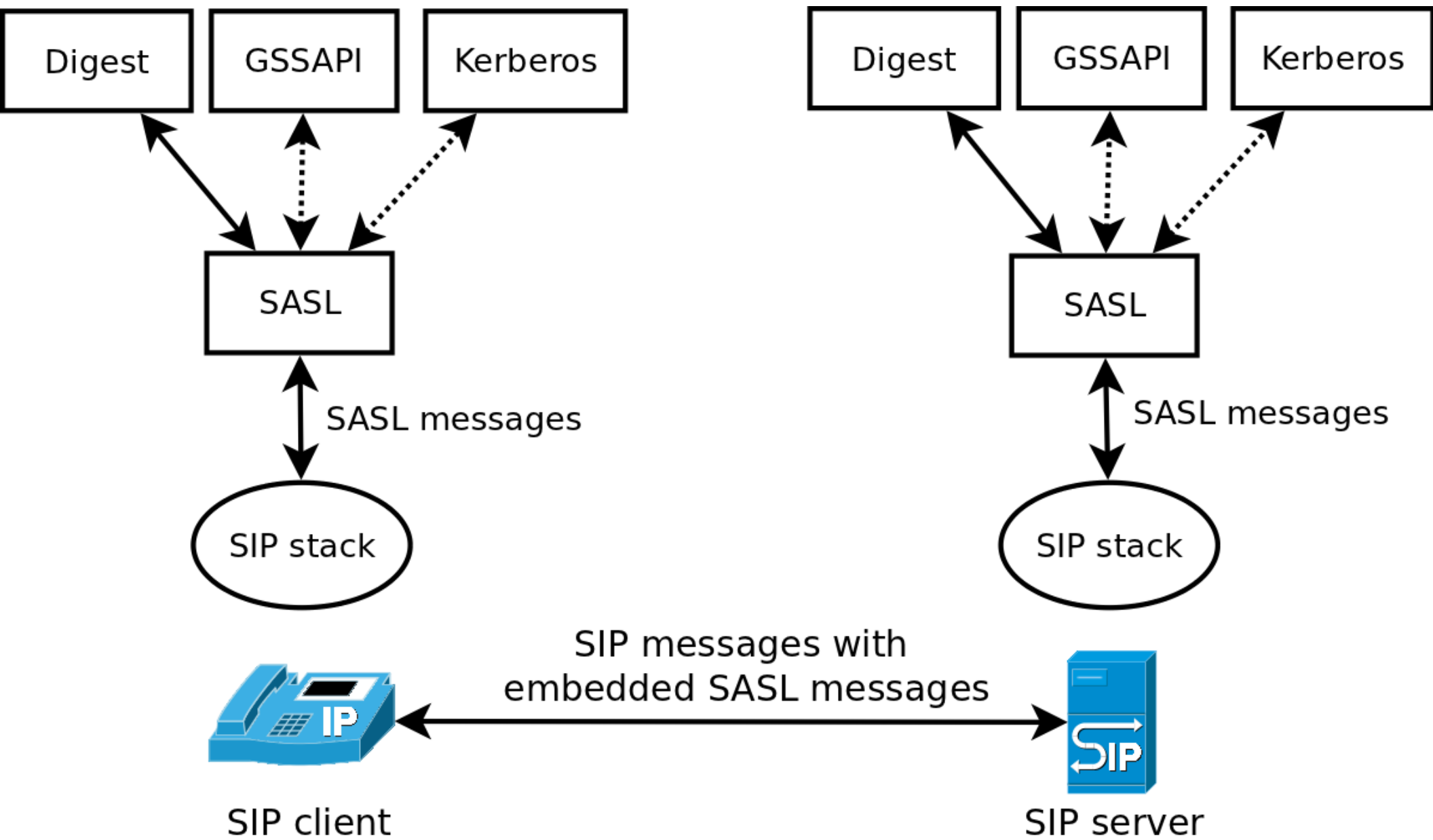


2. SASL

- Simple Authentication and Security Layer = Interface for an application to access security services
- Mature and well-proven standard (RFC4422)
- NOT a communication protocol
 - Relies on the application (SIP) to pass *SASL messages* between client and server
- Does NOT provide any security in itself
 - Relies on underlying security mechanisms
- SASL implementations (may) support different authentication methods
 - Digest-MD5
 - Kerberos
 - GSSAPI
 - ...
- All methods are *transparent* to the application

SASL stack (with SIP)



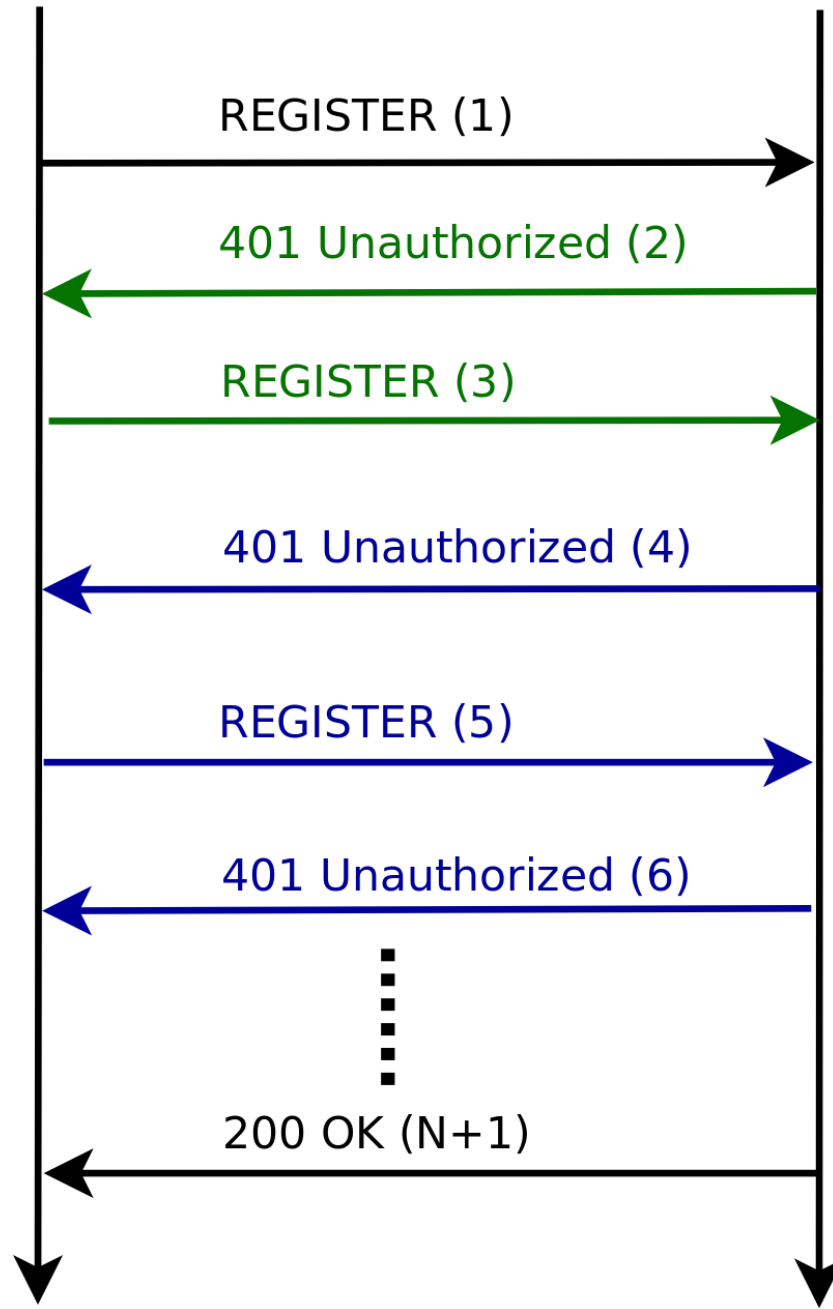




SIP Client



SIP Server



SIP REGISTER message

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP
192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFB0D488459C69E4E
3. From: Alice <sip:alice@CompanyA>;tag=1234648905
4. To: Alice <sip:alice@CompanyA>
5. Contact: "Alice" <sip:alice@192.168.1.102:5060>
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",
algorithm=MD5
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0

DAA →

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP
192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFB0D488459C69E4E
3. From: Alice <sip:alice@CompanyA>;tag=1234648905
4. To: Alice <sip:alice@CompanyA>
5. Contact: "Alice" <sip:alice@192.168.1.102:5060>
6. Call-ID: 2B6449C74C10D4F95006A6C034E79E8E@CompanyA
7. CSeq: 19481 REGISTER
8. User-Agent: PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392
9. Authorization: SASL mechanism="DIGEST-MD5"
data="YAzgusSGGeRFGw9nfUvOAxcedzZCBmKY1H2ElnegaccBcx3DUSkGNW
Y4qfiSwcXwjLtoqW0eBNog7ixHN"
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0

SASL →

Conclusion

- We propose a two-step migration towards a more secure authentication
 1. PAKE replace the weak DAA
 2. SASL in the long term
- Our solution require minimal changes to the SIP protocol standard
- With SASL
 - Add support to a range of different authentication methods
 - Flexible – different implementations can support different authentication methods
 - New authentication methods can be added later WITHOUT change to the SIP standard
- Future work
 - Benchmark testing
 - IETF draft
 - Add an SIP extension to maintain backwards compatibility?
 - SASL: Require some authentication methods to be supported as standard? Which?
 - Vulnerable to a REGISTRATION attack?
 - Compare and look into different SASL auth methods

Thank you!

