Sikkerhet i IP-telefoni – en introduksjon

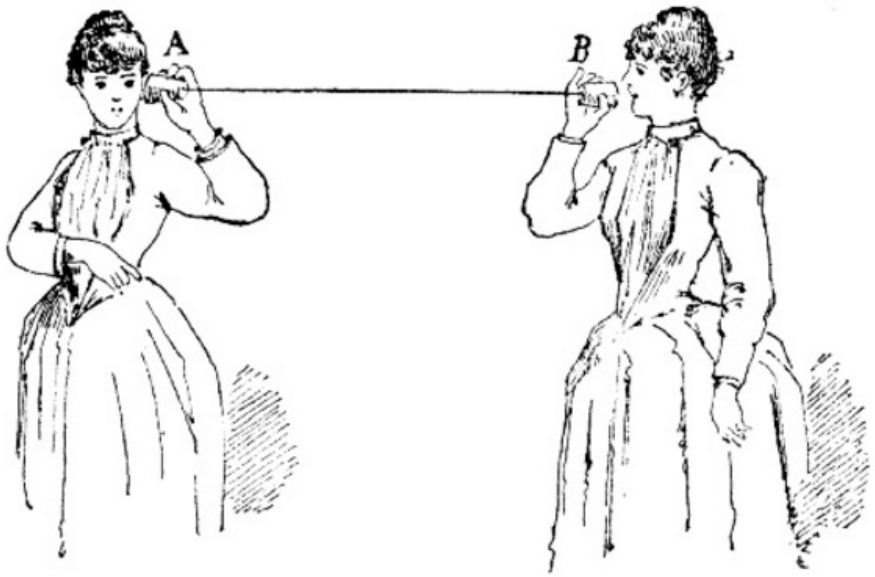


Fig. 76. Trådtelefon.

ITF20205 – Datakommunikasjon, HIØ
2017.09.25, Halden
Lars Strand

Lars Strand?

M.Sc. (2004)
PhD (2011)

Forsvarets forskningsinstitutt

UNIK UNIVERSITETSSENTERET PÅ KJELLER

NR Norsk Regnesentral NORWEGIAN COMPUTING CENTER

Redpill Linpro

2004 - 2011

NOFAS Financing · Research · Strategy

2012 - 2015

NSM

2015 – d.d.

http://www.linkedin.com/in/larsstrand

Dagens tema

A. Kort introduksjon om IKT-sikkerhet
B. Hva er VoIP (IPTelefoni)?
C. Hva er SIP? Hvordan virker det?
D. Hva er RTP? (og SDP)?
E. SIP og sikkerhet (autentisering)
F. SIP i dag (SIP Peering) vs. opprinnelig tenkt benyttet (“email model”)

A. IKT-sikkerhet

Engelsk		**Norsk**
Security	→	**Sikkerhet**
Safety	→	Trygghet
Certainty	→	Visshet

Security
Safety
Certainty
} → Sikkerhet

Hva er sikkerhet?

Definisjon 1: Sikkerhet i sin alminnelighet defineres som fravær av uønskede hendelser, frykt eller fare.

Definisjon 2: Beskyttelse av verdier mot tilsiktede uønskede handlinger og tilfeldige (utilsiktede) hendelser.

- Tilsiktede uønskede handlinger: Data-angrep («sikkerhetsangrep»)
- Utilsiktede hendelser: Brann, strømbrudd, bugs («uhell»)

Verdi: Alle type aktiva («assets»)

- Eiendeler, virksomhets-prosesser, data / informasjon, lokaler, ...
- “Alt du eier og har”

Sikkerhet – for hva?

1. Datamaskinsikkerhet
   - Betegner sikkerhet i alle systemer som benyttes på én datamaskin
   - Engelsk: Host security
2. Nettverkssikkerhet
   - Brukes ofte til å betegne sikkerheten som har med transmisjon av data mellom maskiner og alle mekanismer som må brukes for å få dette til.
   - Engelsk: Network security
3. Applikasjonsikkerhet / produktsikkerhet (ofte upresist kalt systemsikkerhet)
   - IKT-teknisk sikkerhet ved applikasjon(er) som implementeres i et system
   - Engelsk: Application security

$\Rightarrow$ IKT-sikkerhet / datasikkerhet / cybersikkerhet

- Brukes ofte til å betegne sikkerhet i alle IKT-systemer som benyttes – både datamaskinsikkerhet, nettverkssikkerhet og applikasjonsikkerhet.
- Engelsk: Computer security, security in computing, ICT security

Behov for sikkerhetsrammeverk

- *«Kan vi ikke bare løse alle sikkerhetsutfordringer en gang for alle?»*
- **100 % sikkerhet en umulighet:**
  - Kontinuerlig teknologiske nyvinninger som introduserer nye sårbarheter
  - Økende digitalisering («alt og alle på nett»)
  - Banditter følger pengene («bare en ny angrepsvektor»)
  - Sikkerhet er ikke en integrert del av utviklingen av IKT-systemer (styringssystem for sikkerhet mangler)
  - Stadig skiftende trussellandskap
  - Stadig nye (og ofte sofistikerte) angrepsverktøy («våpenkappløp») - APT

- **Konklusjon: Vi blir aldri ferdig med sikkerhetsarbeidet. Det er en kontinuerlig prosess.**

Vi trenger informasjonssikkerhet!
(Hvor begynner jeg?)

- Identifiser: Hvilke verdier har vi? Hva er det vi har som..
  - ..er interessant for en trusselaktør?
  - ..er viktig for oss og vår virksomhet?
- Som regel en kombinasjon av:
  - Maskinvare (klienter, servere, skrivere, ..)
  - Software (OS, app, ..)
  - **Data/informasjon (kildekode, dokumenter, databaser, ..)**
  - Personer (ansatte, konsulenter, ..)
  - Forretningsprosesser, internprosesser, ..
  - Lokaler
  - ...

Informasjonstilstand

- Informasjon/data eksisterer i en av tre mulige tilstander:
  1) Lagret (i ro)
  2) Transport (i transit)
  3) Prosess (i bruk)

- Sikringstiltak for alle tilstandene er påkrevd!

Eks: Dokument Lagret i Google Docs

1. Lagret: Hos Google

3. Prosess: På din datamaskin

Trussel, sårbarhet og angrep

- Trussel: En *mulig* tilsiktet (villet) uønsket handling, oftest ondsinnet.
  - Muliggjøres gjennom sårbarheter
- Sårbarhet: En svakhet i et system som en trusselaktør *kan* utnytte og forårsake skade.
  - Muliggjør at trusselaktører lykkes
  - Eks: Bug, feilkonfigurasjon, mangelfull grunnsikring, ..
- Angrep: En tilsiktet uønsket handling, oftest ondsinnet, muliggjort gjennom sårbarhet(er).
  - Eks: Sending av e-post med malware.

Eksempler

- **Eksempel 1: Din sykkel (verdi)**
  - Trussel: Sykkel blir stjålet
  - Trusselaktør: En tyv
  - Sårbarhet: Mangler sykkellås
  - Angrep: Tyven stjeler sykkelen fra sykkelparkeringen
- **Eksempel 2: Dine dokumenter (verdi)**
  - Trussel: Løsepengevirus / “ransomware” eks: WannaCry
  - Trusselaktør: En hacker (vinningskriminell)
  - Sårbarhet: Mangelfull antivirus/mangelfull opplæring (åpne ondsinnet vedlegg i e-post) + sårbarhet i windows (mangelfull patching).
  - Angrep: En hacker sender e-post med malware som krypterer alle dine dokumenter.

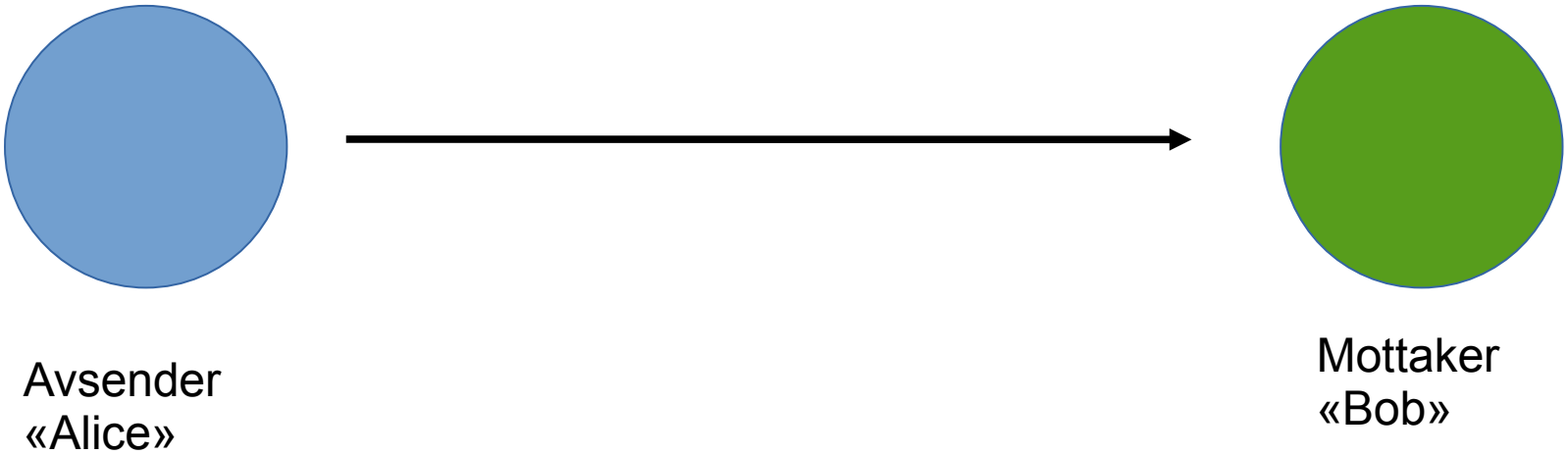
Sikkerhetstjenester

Tre grunnleggende:

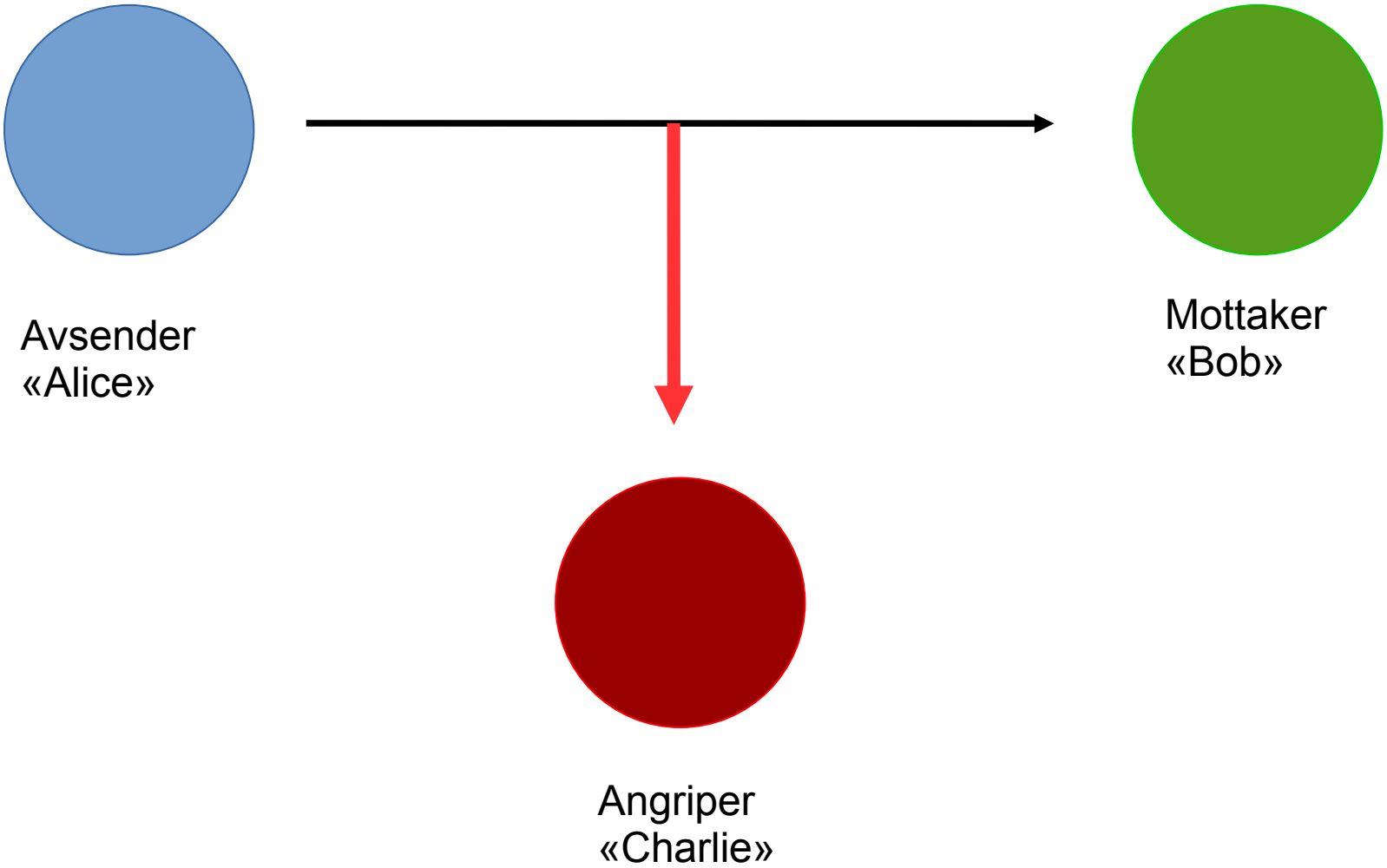
1. **Konfidensialitet:** Hindre uautorisert *lesning* av informasjon
2. **Integritet:** Hindre uautorisert *modifikasjon* av informasjon
3. **Tilgjengelighet:** Hindre uautorisert *blokkering* av informasjon

- ..men også sporing, autentisering, aksesskontroll, ikke-fornektelse.

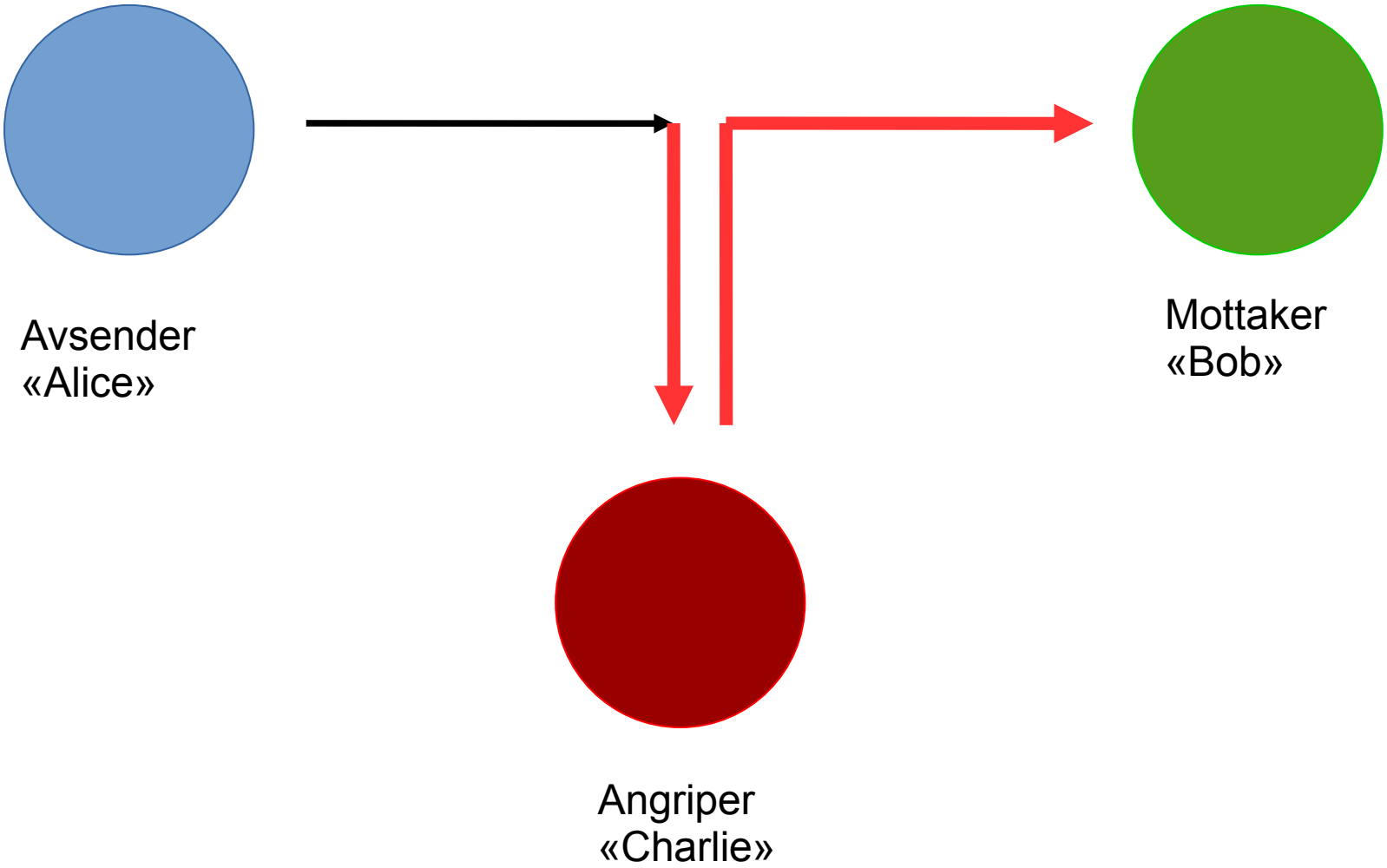
Normal informasjonsflyt



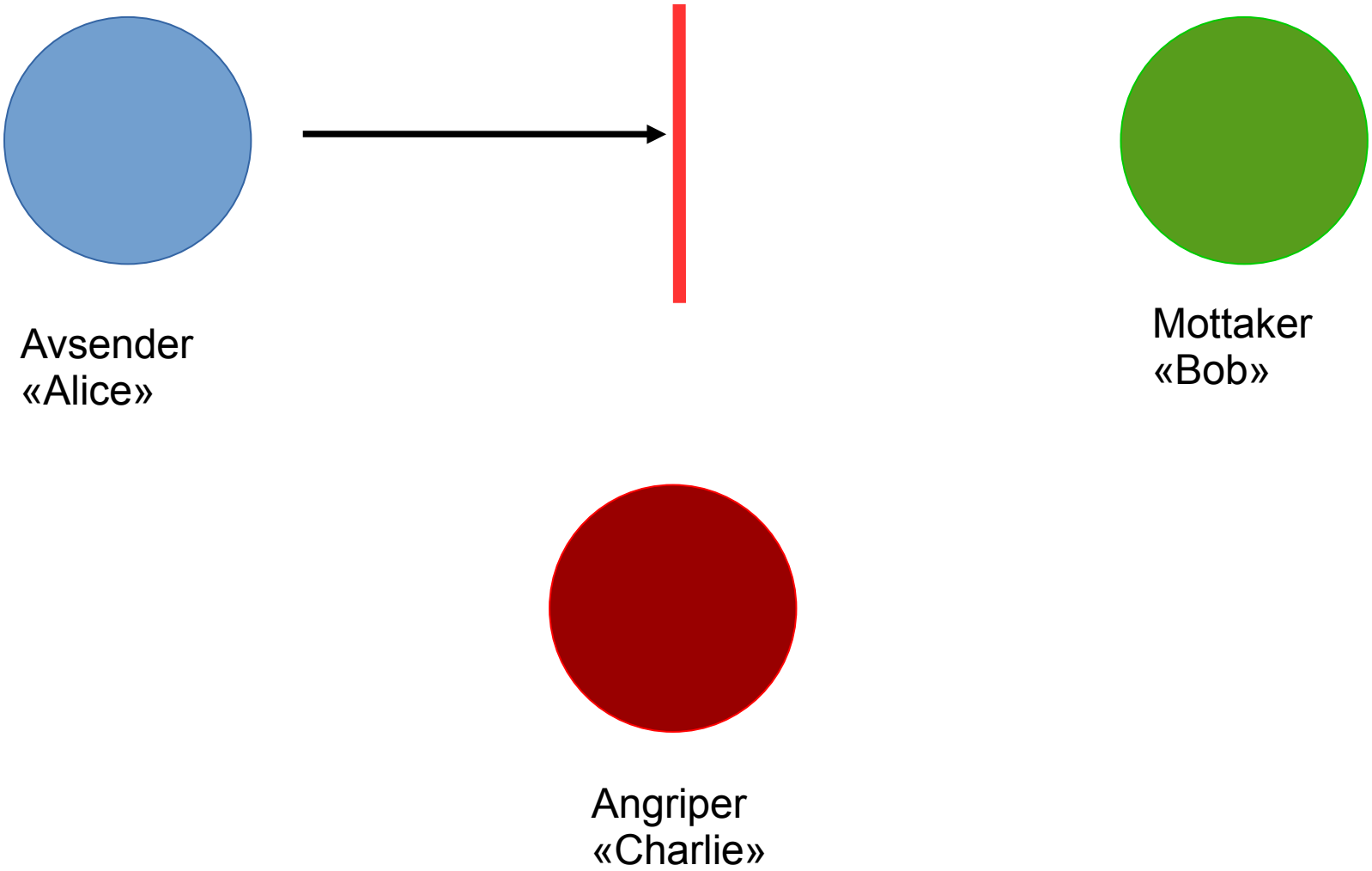
Angrep på konfidensialitet



Angrep på integritet



Angrep på tilgjengelighet

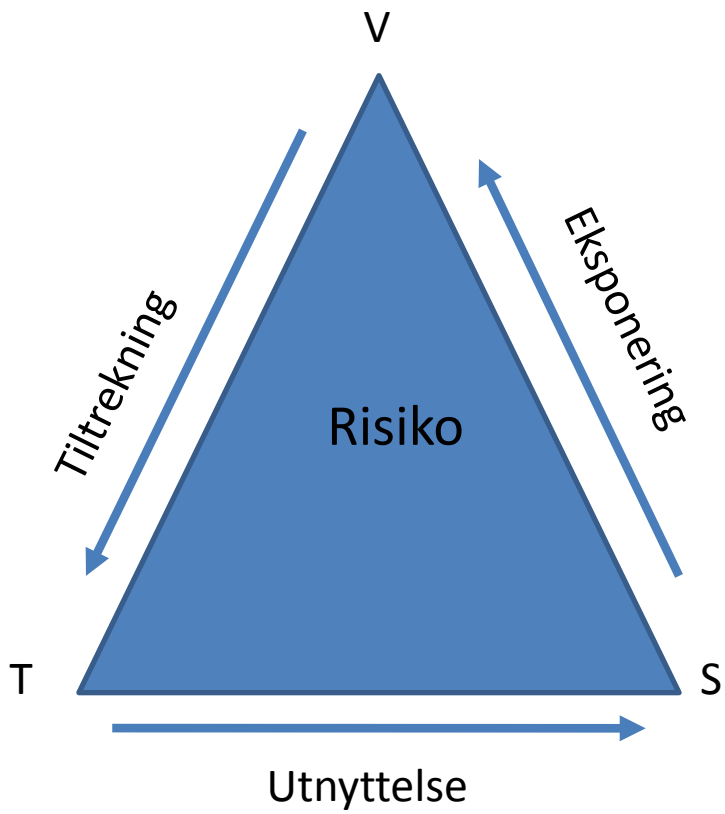


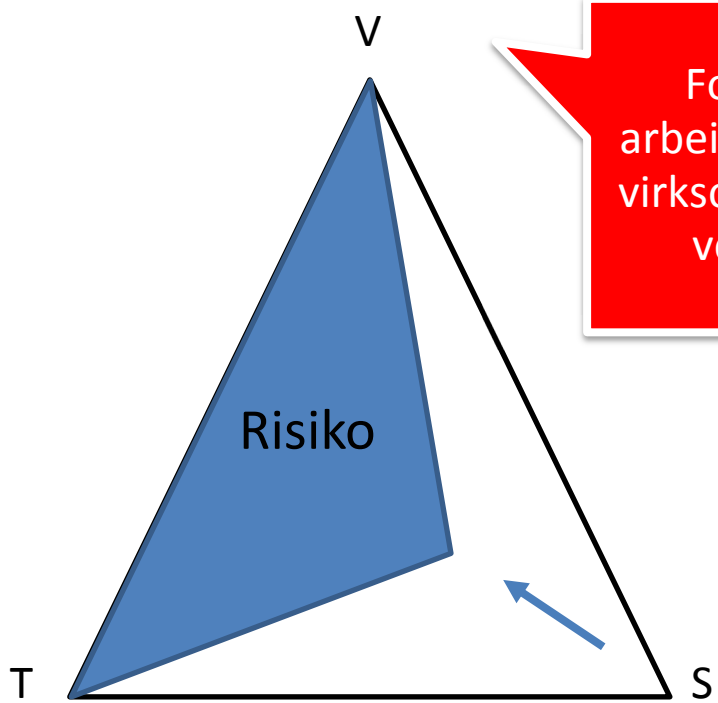
Sikringstiltak er mer enn de teknologiske alene

Tiltakskategorier				
	Barriere	Deteksjon	Verifikasjon	Reaksjon
Personell-sikkerhet				
Fysisk sikkerhet				
IKT-sikkerhet	Brannvegg	IDS	Logganalyse	Re-tanking

Risikotrekanten

Din risiko = forhold mellom verdi, trusler og sårbarheter





Fokuser arbeidet rundt virksomhetens verdier

Det er dette virksomhetene Kan gjøre noe med selv

Alle virksomheter må leve med en viss risiko, men det er avgjørende at virksomhetene vet hva de må beskytte og på hvilken måte dette bør gjøres.

NSMs veileder i sikkerhetsstyring

Nivå av sikkerhet

1. **Statssikkerhet** – ivareta statens eksistens og suverenitet, suverene rettigheter og integritet.
   - ✓ Sikkerhetsloven (sektorovergripende)

2. **Samfunnssikkerhet** – ivareta befolkningens liv, helse og trygghet, og sikre sentrale samfunnsfunksjoner og viktig infrastruktur
   - ✓ Sektorspesifikke regler, lover og føringer

3. **Virksomhetssikkerhet** – sikre sin drift og sine interesser
   - ✓ ISO27000-serien, NSMs grunnprinsipper for IKT-sikkerhet

4. **Individets sikkerhet**
   - ✓ Opplæring, årvåkenhet, NorSIS

- Gjensidig avhengighet mellom nivåene!
- I hvor stor grad skal myndighetene engasjere seg i sikkerhetsarbeidet i samfunnet? Hvor inngripende rolle?

Oppsummert – del A

- Verdivurdering – du må vite hvilke verdier du har!
- Risikobasert tilnærming viktig for sikkerhetsarbeidet:
  - Risikovurdering
  - Risikodempende tiltak
  - Risikoaksept
- Sikkerhet er mer enn…
  - Bare teknologiske sikringstiltak
  - Noe du gjør èn gang («fire and forget»)
  - Bare noe «sikkerhetsfolka» jobber med
- Implementer og ta i bruk et ***styringssystem for sikkerhet***

Del B: Hva er VoIP?

Public Switched Telephony Network (PSTN)

- Standardization body:
  - International Telecommunication Union Standardization (ITU-T) can be traced back to 1865

- Historically:
  - Big operators (only one for smaller countries)
  - Peering agreement between them
  - E.164 addresses (telephone numbers)

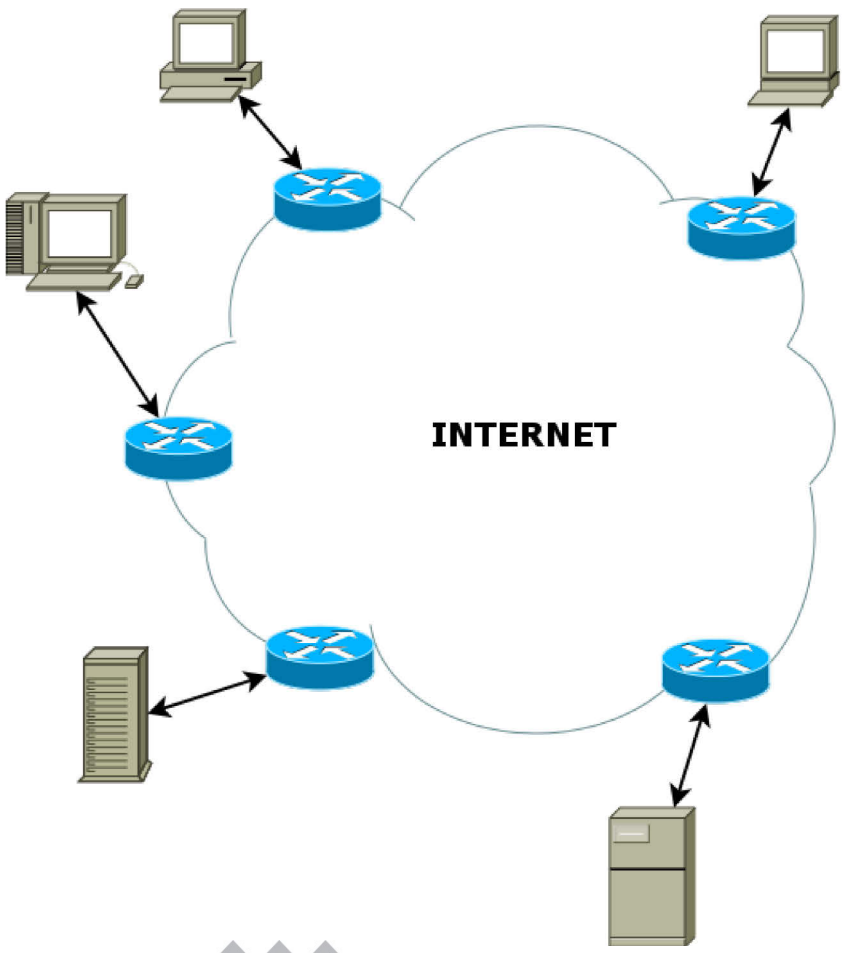
Plain Old Telephony Service (POTS)

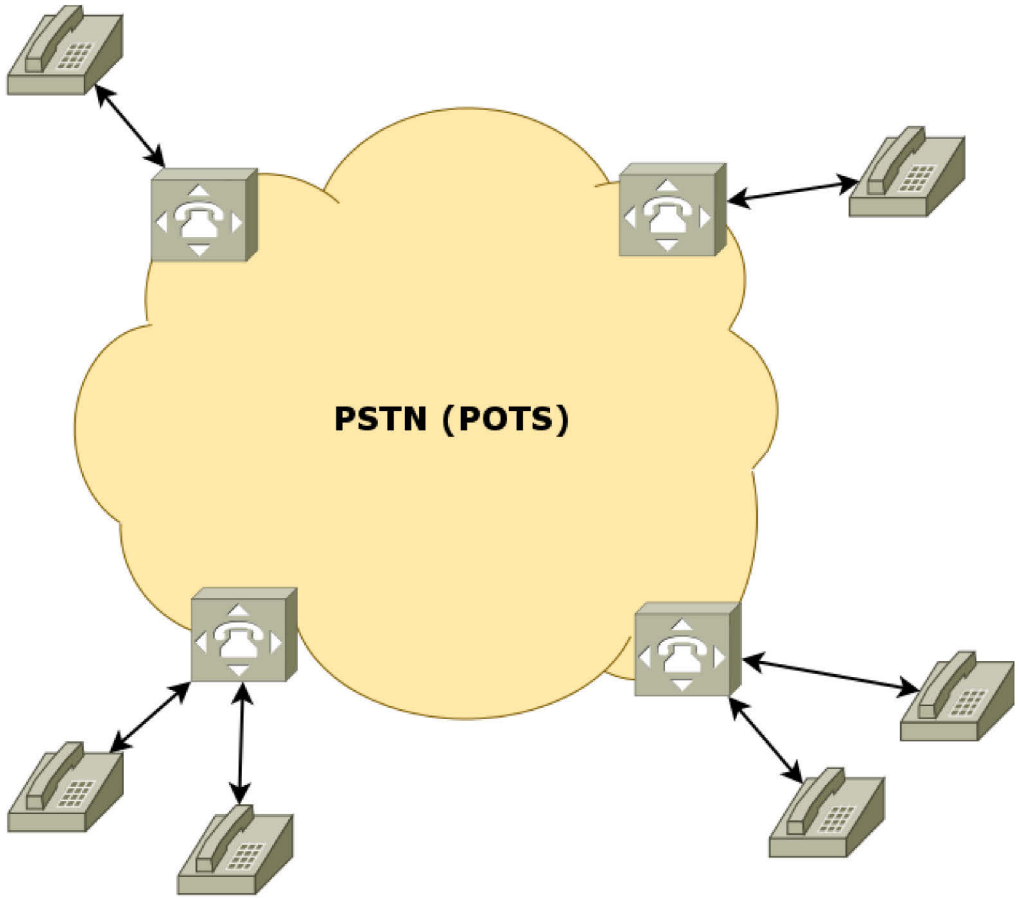
- “Just works”
- 100+ year old technology
- PSTN: 99.999% uptime, “the five nines” = 5.26 min/year (D.R. Kuhn, 1997)

“Can call anyone, anytime, anywhere with a good-quality telephonic conversation”

“This is an elusive, currently-unachievable goal for the VoIP-industry” (Minoli, 2006)

Voice over IP (VoIP) protocols and technology is a merge of data communication and telecom





IETF®

VoIP?

- What is VoIP?
  - Broad definition: Sending and receiving media (voice/video) over IP
- Why VoIP?
  1) Added functionality and flexibility – which may be hard to provide over PSTN
  2) Reduced cost – uses Internet as carrier
  3) Less administration – no separate telephone and data network
  4) (Open standards, no vendor-lock-in)

VoIP!

- Industry have had high focus on VoIP for years (and still have)
  - All major network players onboard: Cisco, Juniper, Huawei, ZTE, ++

- VoIP is here to stay
  - Replacing PSTN at a rapid rate
  - Integrated into a lots of different services (Skype/Lync)
  - Buzzword (the last 5-10-15+ years): Unified Communication (UC): Instant messaging, presence, “HD voice”, mobility, web & video conference, desktop/file sharing

- BUT! VoIP loaded with security issues
  - Inherit (traditional) packet switched network security issues and introduces new ones (because of new technology).
  - Multiple attacks on SIP based VoIP exists

VoIP – how does it work?

- “The signaling battle” in the mid 1990s
  - H.323 developed by ITU-T gained some industry adoption but “lost”.
  - H.323 too complex
  - SIP developed by IETF gained more momentum
  - (“Battle: The telco-world vs. the hackers”)
- Session Initiation Protocol (SIP) is the *de facto* standard signaling protocol for VoIP
  - Application layer (TCP, UDP, SCTP)
  - Purpose: Negotiate, establish, change and tear-down the context of a multimedia flow
  - No media transfer (voice/video)
- Real-time Transport Protocol (RTP) transfer the actual multimedia

"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

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

Show related articles

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.

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

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

SHA

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 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

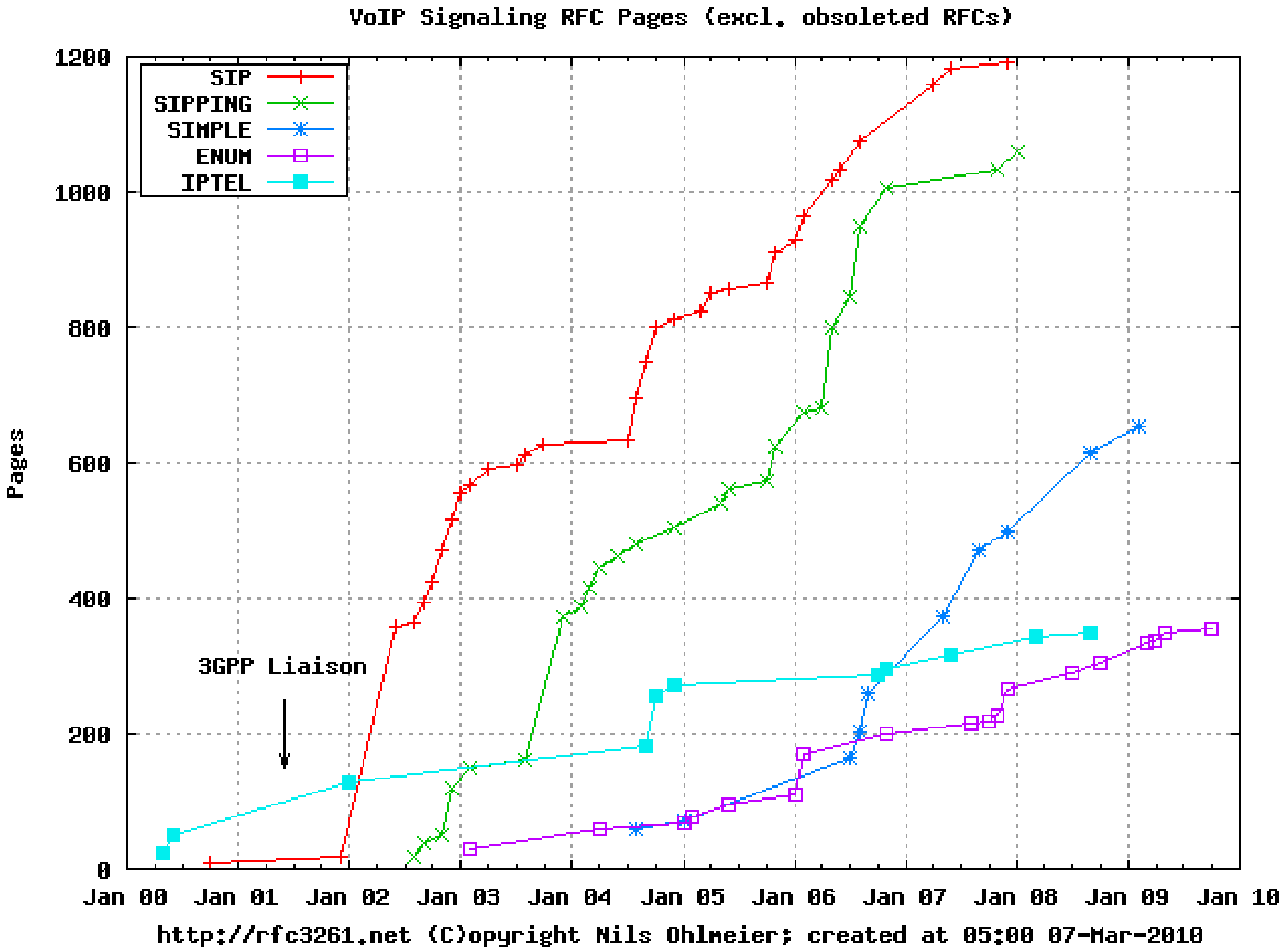
To misuse a VoIP system in this way an attacker needs to be things; to connect to the targeted system and then to make calls.

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.

SIP

Specified in RFC 3261 published by IETF 2002

- First iteration in 1999 (RFC 2543), draft iterations years before that
- One of the largest (in terms of page numbers) ever defined by IETF
- Additional functionality specified in over 120 different RFCs(!)
- Even more pending drafts...
- One RFC that list relevant specifications under the “SIP umbrella”..
- Known to be complex and sometimes vague – difficult for software engineers to implement
- Interoperability conference - “SIPit”
  - www.sipit.net


VoIP Signaling RFC Pages (excl. obsoleted RFCs)
SIP
SIPPING
SIMPLE
ENUM
IPTEL
3GPP Liaison
Pages
0
200
400
600
800
1000
1200
Jan 00
Jan 01
Jan 02
Jan 03
Jan 04
Jan 05
Jan 06
Jan 07
Jan 08
Jan 09
Jan 10
http://rfc3261.net (C)opyright Nils Ohlmeier; created at 05:00 07-Mar-2010

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!*

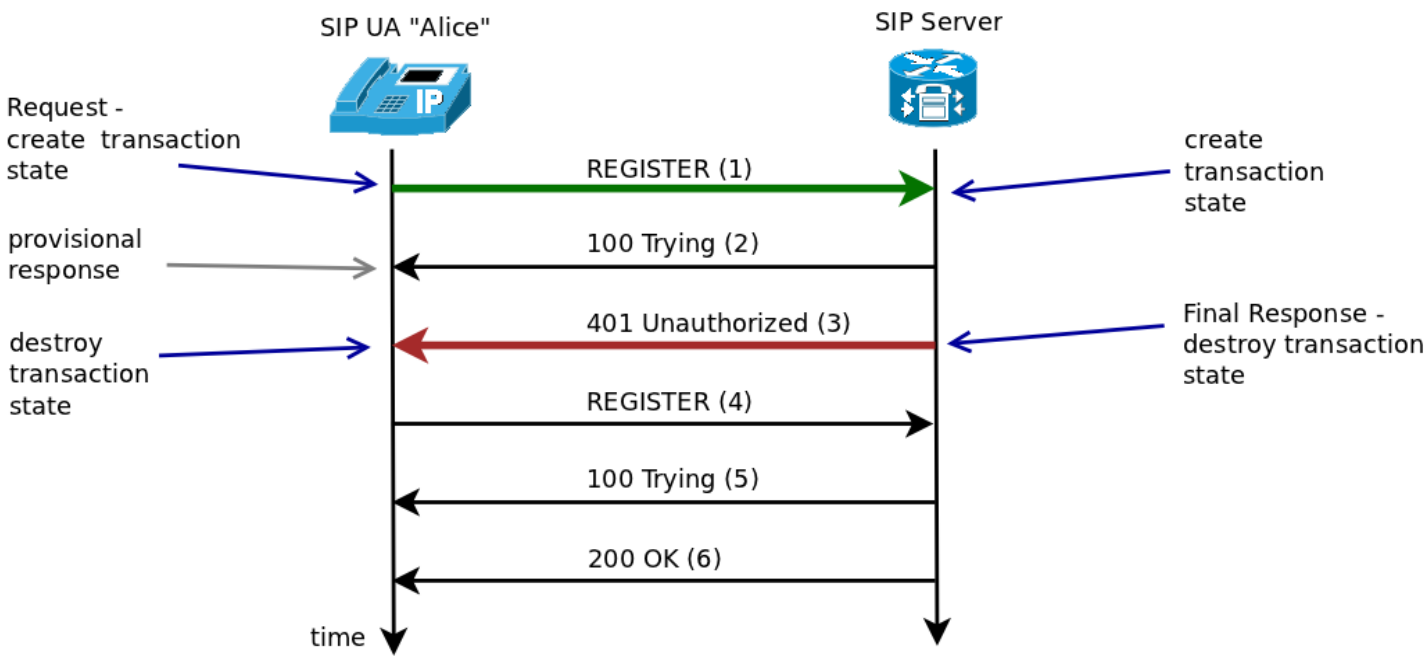
Sorry. I just had to get this off my chest. Regards,

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

SIP (2)

Modeled after HTTP (and SMTP):

- Text-based (easy to debug!)
- Response codes similar to/borrowed from HTTP
- Based on a request/response transaction model (HTTP)
- Each transaction consist of a request that invokes a particular method on the server and at least one response.
- Related transactions are called a “SIP dialog” (1-6):



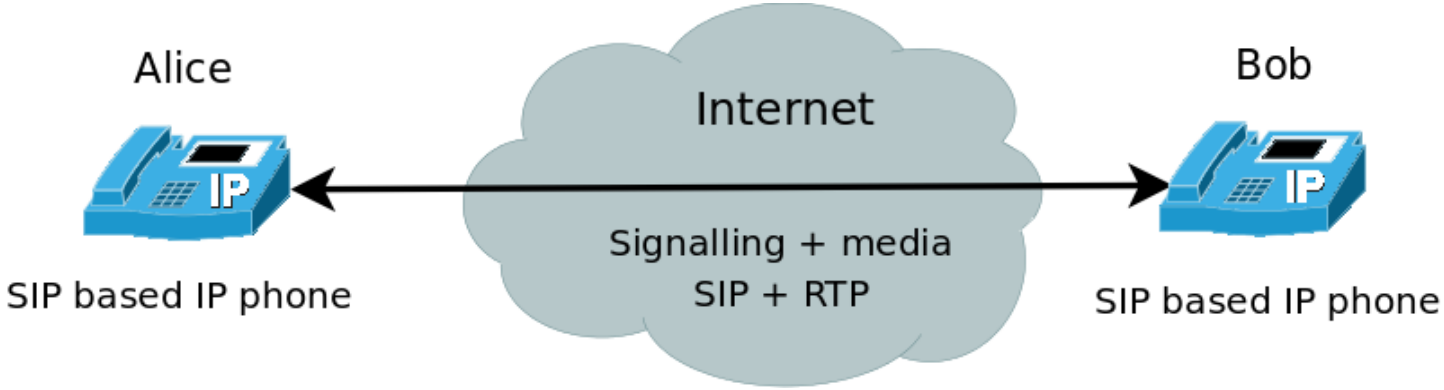
SIP request methods (RFC3261)

SIP method:	Description:
ACK	Acknowledge a request/session
BYE	Terminate a sesion (call)
CANCEL	Cancel any pending requests
INVITE	Initiate a session (call)
OPTIONS	Query servers about their capabilities
REGISTER	Register contact information for a UA to a location service.

Additional SIP request methods have been defined later. For a starting point:

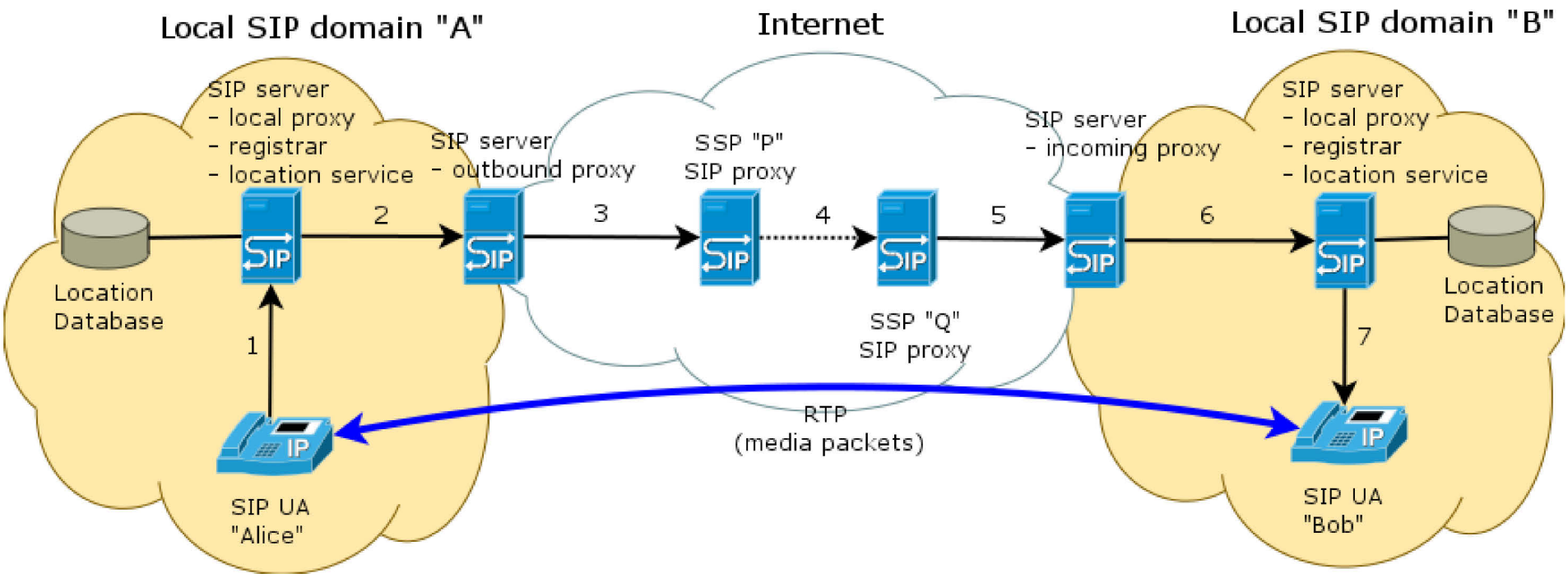
http://datatracker.ietf.org/wg/sip/documents/
http://en.wikipedia.org/wiki/List_of_SIP_request_methods

SIP example
Direct call UA to UA

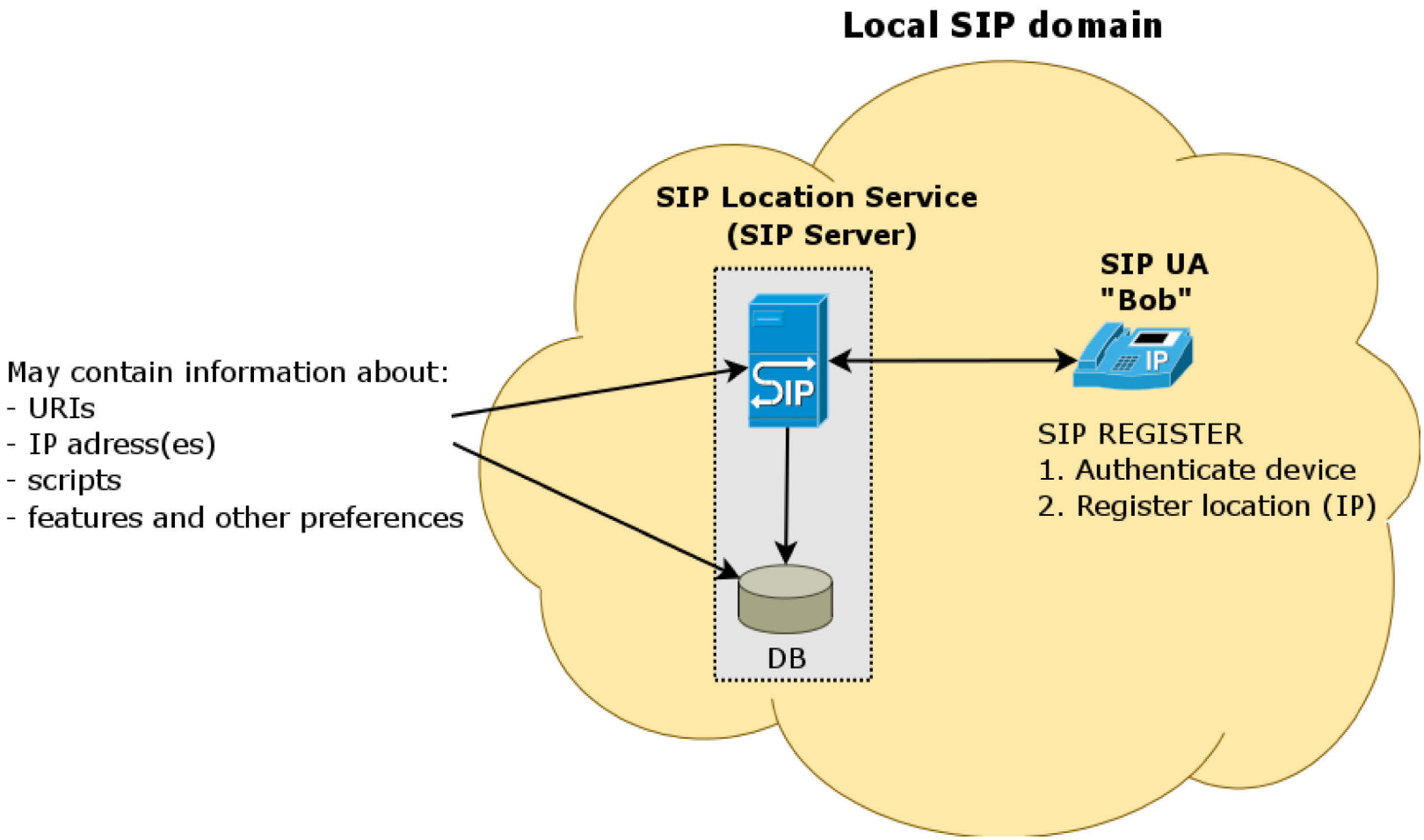


- Caller must know callee's IP or hostname
- No need for intermediate SIP nodes
- **Problems:**
    - Traversing firewalls / NAT
    - Must know IP/hostname of user
    - Mobility – change IP/hostname

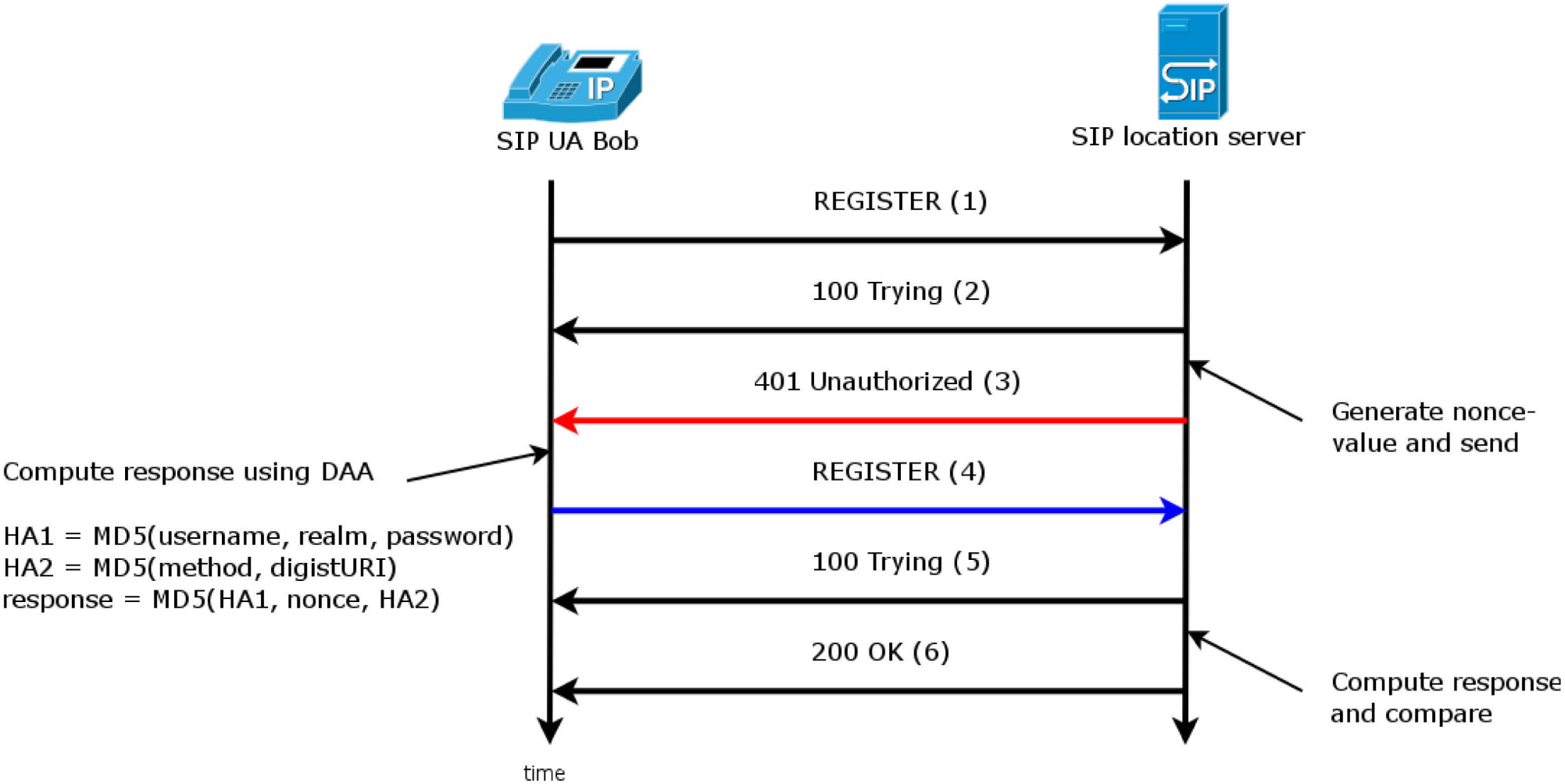
SIP communication network (session/call setup)



SIP REGISTER
(registration and authentication)



SIP REGISTER message flow (using Digest Access Authentication)



SIP message structure - REGISTER

Start line (method)

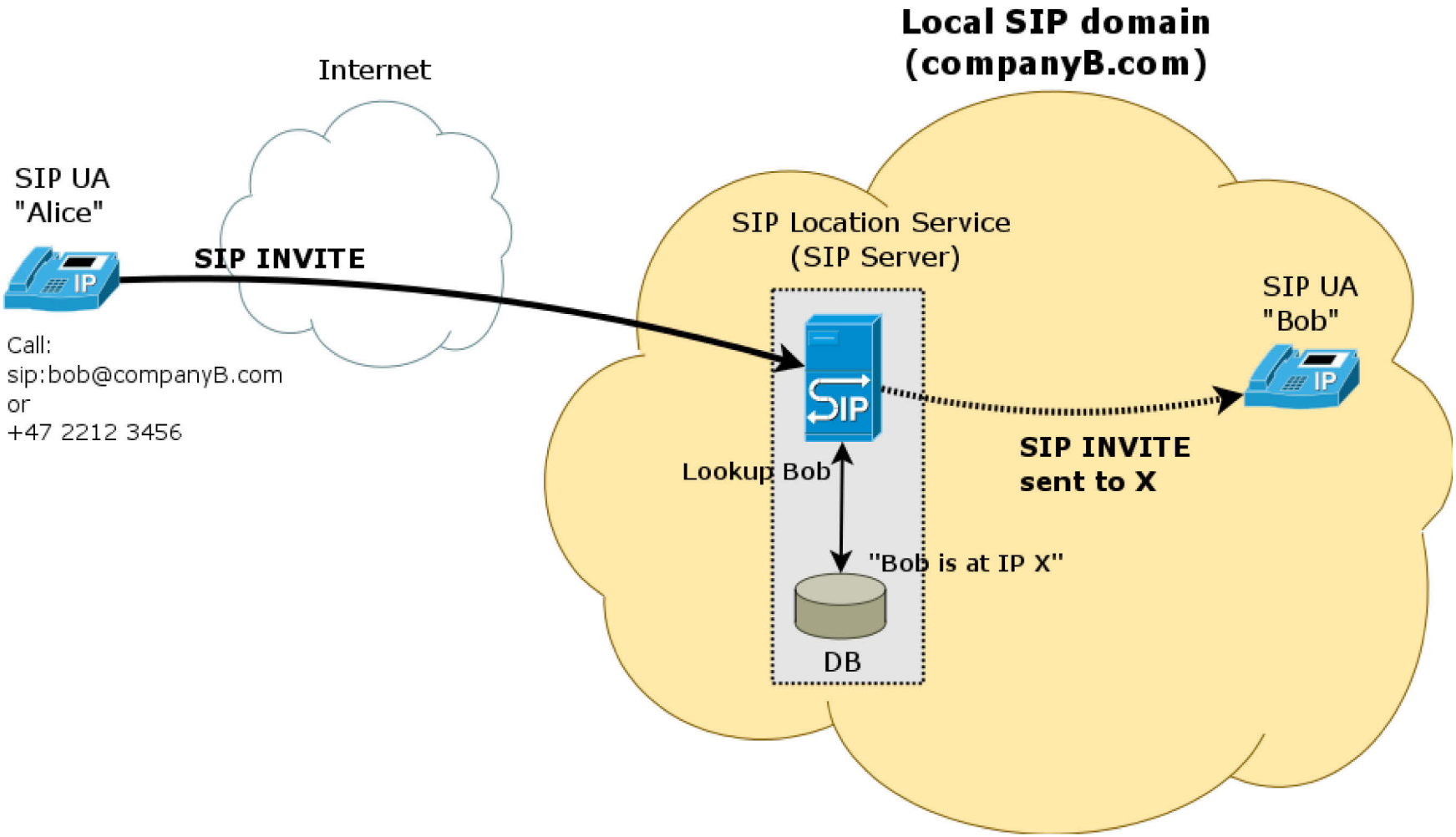
```
REGISTER sip:156.116.8.139:5060 SIP/2.0
```

Message header

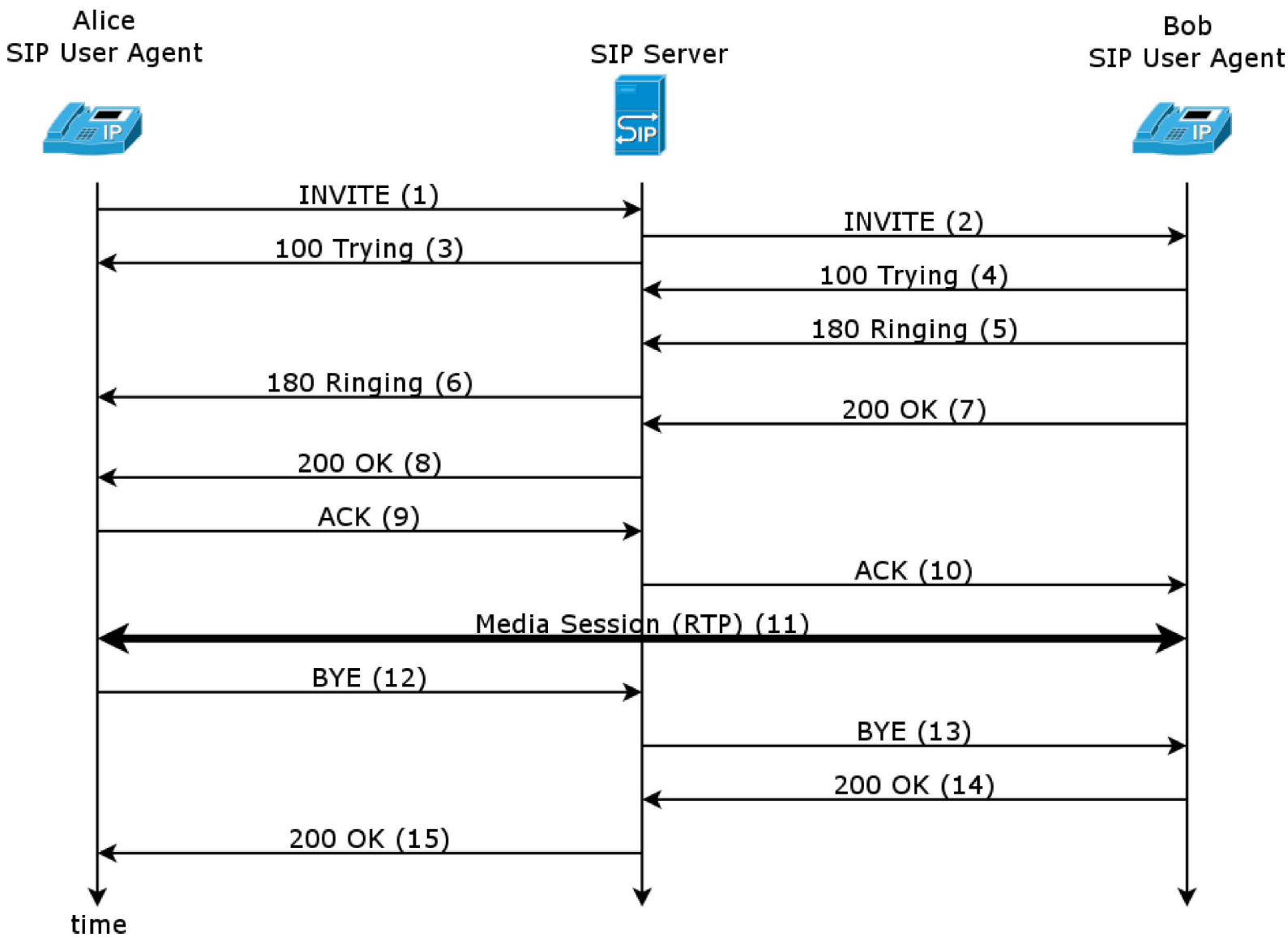
```
Via: SIP/2.0/UDP 156.116.9.67;branch=z9hG4bKd9828eb03D78A219
From: Bob <sip:bob@156.116.8.139>;tag=2A69C69E-E6A7587
To: Bob <sip:bob@156.116.8.139>
CSeq: 2 REGISTER
Call-ID: f7ce9763-f9c8678c-7f5df1f5@156.116.9.67
Contact: <sip:bob@156.116.8.139>;methods="INVITE, ACK, BYE, CANCEL, OPTIONS,
         INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER"
User-Agent: PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392
Authorization: Digest username="bob", realm="NRtestlab", nonce="39d307ea",
         uri="sip:156.116.8.139:5060", response="e47f2b8946a6b0312c0b99160e8849f4",
         algorithm=MD5
Max-Forwards: 70
Expires: 3600
Content-Length: 0
```

Message body

SIP INVITE
(session setup)



SIP INVITE message flow



SIP message structure - INVITE

Start line (method)

```
INVITE sip:bob@companyB.com SIP/2.0
```

Message headers

```
Via: SIP/2.0/UDP sip.companyA.com:5060;rport;branch=z9hG4bK2EA
From: Alice <sip:alice@companyA.com>;tag=2093912507
To: Bob <sip:bob@companyB.com>
Contact: <sip:alice@phone1.companyA.com:5060>
Call-ID: 361D2F83-14D0-ABC6-0844-57A23F90C67E@156.116.8.106
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
.............
```

Session Description Protocol (SDP)

- Developed by IETF, first RFC 1998
- Goal: Describe the context and content of multimedia session
- Does NOT deliver media but is used for negotiation of parameters
- Session description:

  `<character>=<value>`

- SDP content is transported using SIP INVITE message (payload)

Real-time Transport Protocol (RTP)

- **Transport voice over packet networks**
  - Not new: First RFC on the subject from 1977 (NVP)
  - RTP developed 1992-1996
  - Originally developed for multicast, but proven popular for unicast
  - Used by applications that are more sensitive to latency than to packet loss (for instance speech / video) – used over UDP
  - A RTP session is usually initiated using SIP (or H.323)
- **RTP carries the media stream**
  - “Container protocol” for multimedia streams
  - Identifies the content (multimedia) type
  - End-to-end (phone to phone), real-time, timing recovery, loss detection, media synchronization
  - One stream for video and voice (different ports)
  - SIP negotiate the context of RTP using SDP
  - Does not support congestion control, but when used in together with RTCP (RTP Control Protocol) the application can get enough information to adjust flow parameters.

NAT

- SIP designers: “IPv6 right around the corner” (mid 1990s)
  - NAT would not be an issue…
  - IETF have guidelines for protocol designs
    - One major recommendation is that application layer protocol SHOULD NOT transport IP addresses and port numbers
    - SIP violates this

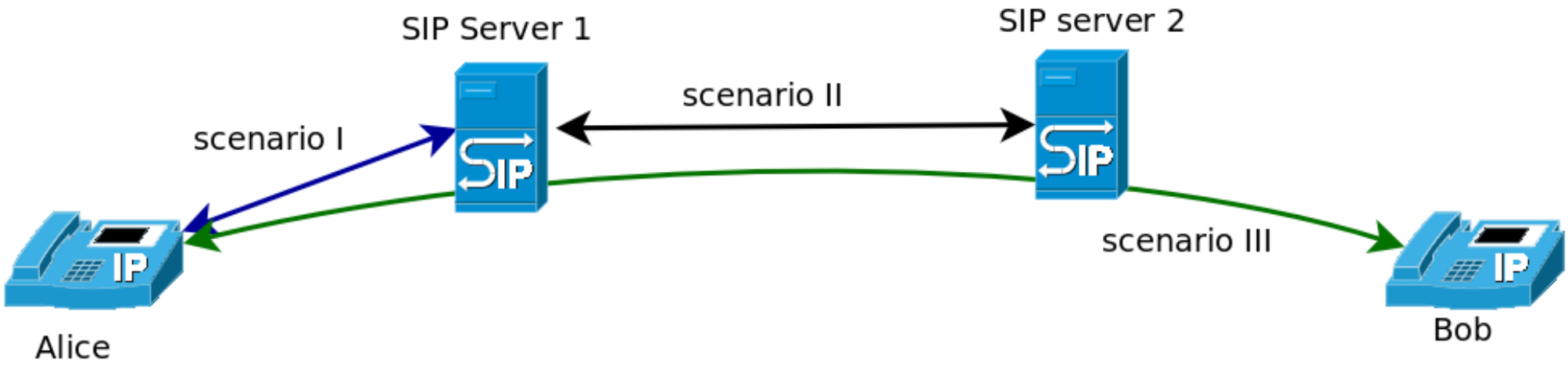
- **Problem:**
  - NAT operates transparently of application layer
  - Different types of NAT mechanisms (port translation, IP, ++)
  - SIP INVITE may contain internal local IP-addresses in:
    - Header: Via
    - Header: Contact
    - SDP (for RTP)

- Solutions: Use additional extensions (protocols) or specialized gateways that handles SIP/RTP:
  - IETF standardized three protocols to assist in NAT traversal: STUN, TURN and ICE

  OR use a
  - Application Layer Gateway (ALG), also called Session Border Gateways

SIP Security

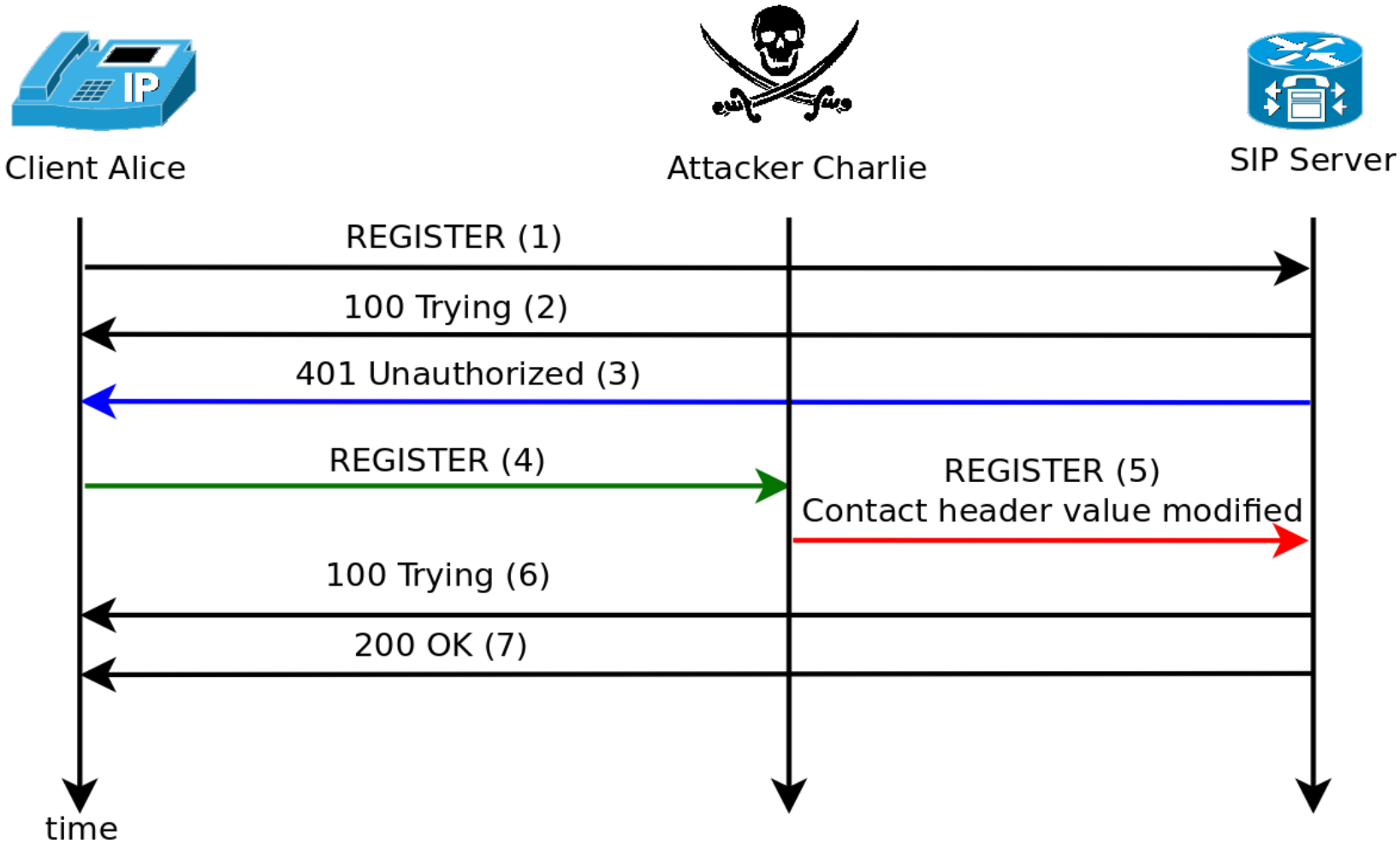
Three SIP authentication scenarios



SIP authentication

1) **Digest Access Authentication (DAA) (RFC 3261) – scenario I**
   - Mandatory but weak
   - Widespread adoption - “everyone” uses this
   - Used to authenticate locally within a domain/realm (during REGISTER or INVITE)
2) **S/MIME (RFC 3261) – scenario III**
   - Goal: Security service end to end
   - Uses certificates, needs PKI = “complex and expensive”
   - Not supported, not used.
3) **Other user identity handling methods – scenario II++**
   - Secure SIP (SIPS): SIP + TLS (but must be terminated for each hop! Uses TCP)
   - P-Asserted Identity (RFC 3325) – in a trusted environment
   - Strong Identity (RFC 4474) – using a “authentication service”
   - Other academic approaches.

SIP DAA authentication
MitM attack



Execution of the attack

```
lks@titan: ~
File  Edit  View  Search  Terminal  Help
root@attack01:~/netsed# ./netsed udp 5060 156.116.8.139 5060 \
> s/\<sip:1001\@156.116.9.95\>/\<sip:1001\@156.116.8.7\>
netsed 1.00a by Julien VdG <julien@silicone.homelinux.org>
      based on 0.01c from Michal Zalewski <lcamtuf@ids.pl>
[*] Parsing rule s/<sip:1001@156.116.9.95>/<sip:1001@156.116.8.7>...
[+] Loaded 1 rule...
[+] Using fixed forwarding to 156.116.8.139,5060.
[+] Listening on port 5060/udp.
[+] Got incoming connection from 156.116.9.95,5060 to 0.0.0.0,5060
[*] Forwarding connection to 156.116.8.139,5060
[+] Caught client -> server packet.
    Applying rule s/<sip:1001@156.116.9.95>/<sip:1001@156.116.8.7>...
[*] Done 1 replacements, forwarding packet of size 548 (orig 549).
[+] Caught client -> server packet.
    Applying rule s/<sip:1001@156.116.9.95>/<sip:1001@156.116.8.7>...
[*] Done 1 replacements, forwarding packet of size 713 (orig 714).
```

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

```
root@titan01: ~
File  Edit  View  Search  Terminal  Help
titan01*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
1001/1001                  156.116.9.95     D          5060     Unmonitored
1002/1002                  (Unspecified)    D          5060     Unmonitored
1003/1003                  (Unspecified)    D          5060     Unmonitored
1004/1004                  (Unspecified)    D          5060     Unmonitored
4 sip peers [Monitored: 0 online, 0 offline Unmonitored: 4 online, 0 offline]
titan01*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
1001/1001                  156.116.8.7      D          5060     Unmonitored
1002/1002                  (Unspecified)    D          5060     Unmonitored
1003/1003                  (Unspecified)    D          5060     Unmonitored
1004/1004                  (Unspecified)    D          5060     Unmonitored
4 sip peers [Monitored: 0 online, 0 offline Unmonitored: 4 online, 0 offline]
titan01*CLI>
```

To counter the attack: Modify DAA

To fix the vulnerability and counter the attack, add the Contact header 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)
```

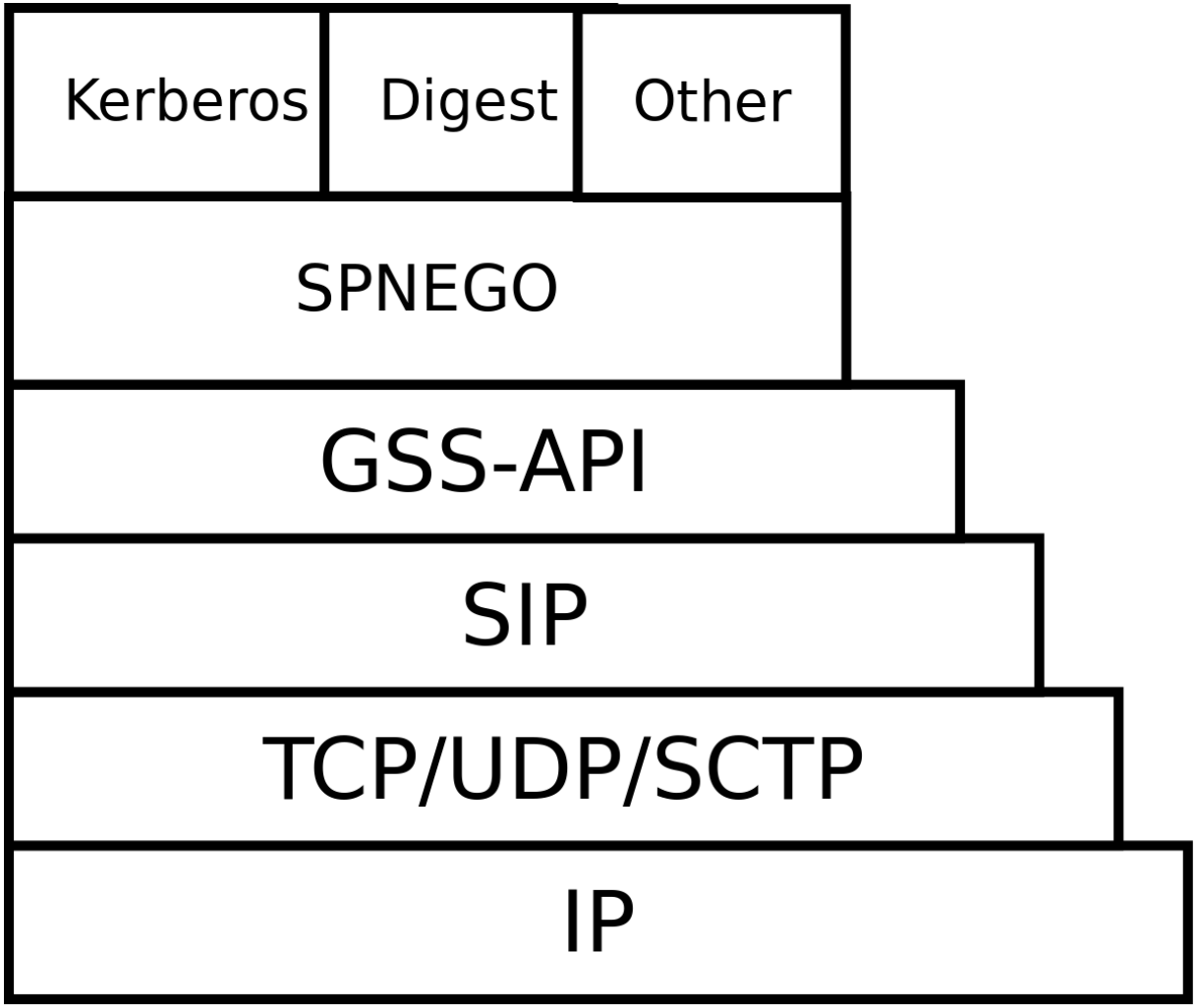
SIP Authentication: Can it be fixed?

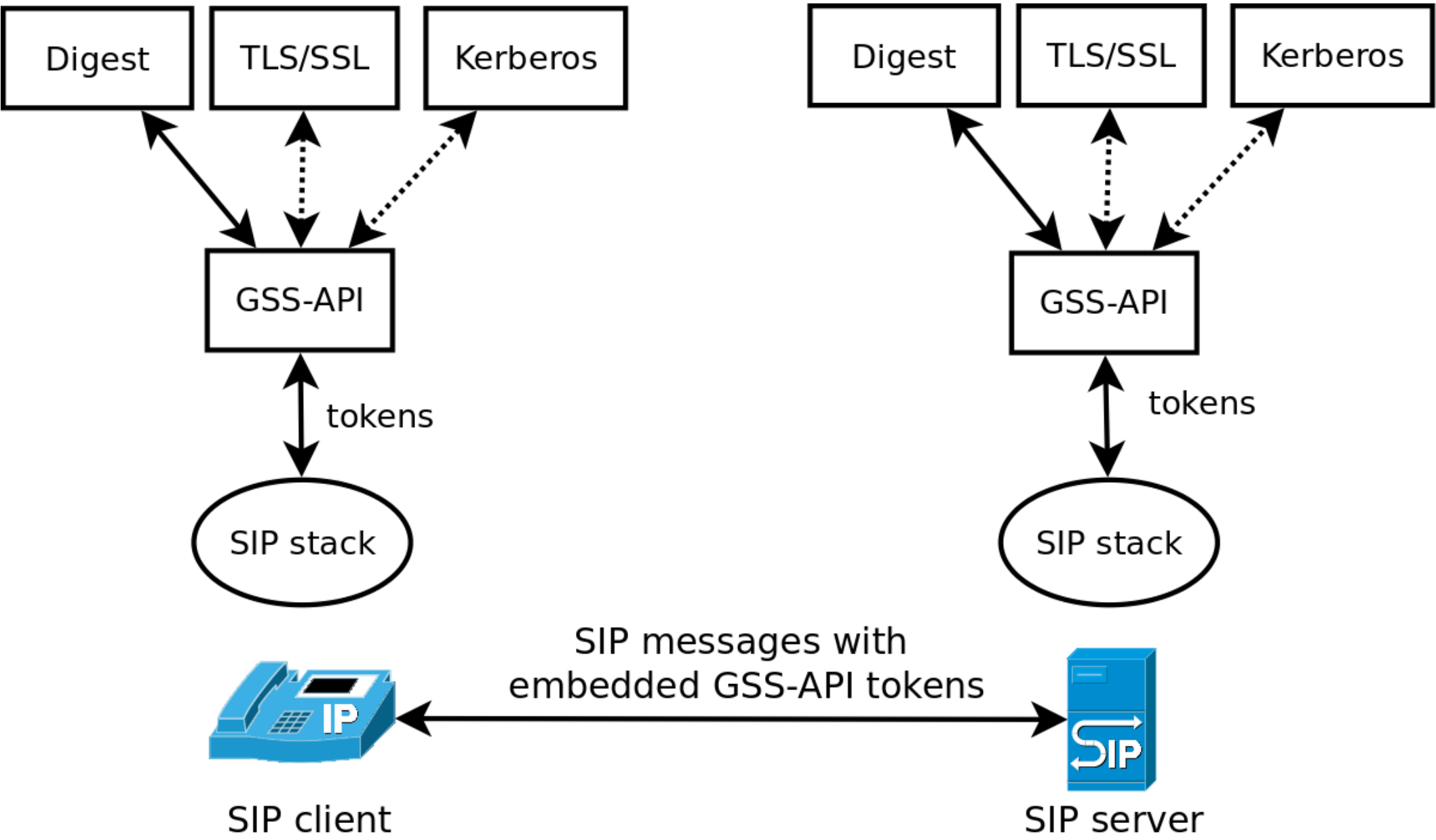
- SIP is flexible
- Problem: Different usage scenarios have different security requirements
  - Handheld devices vs. high-end SIP servers
- Goal: Modification to the SIP standard should be minimum
- Goal 2: A strong and flexible authentication methods wanted
- Solution: Add support for GSS-API

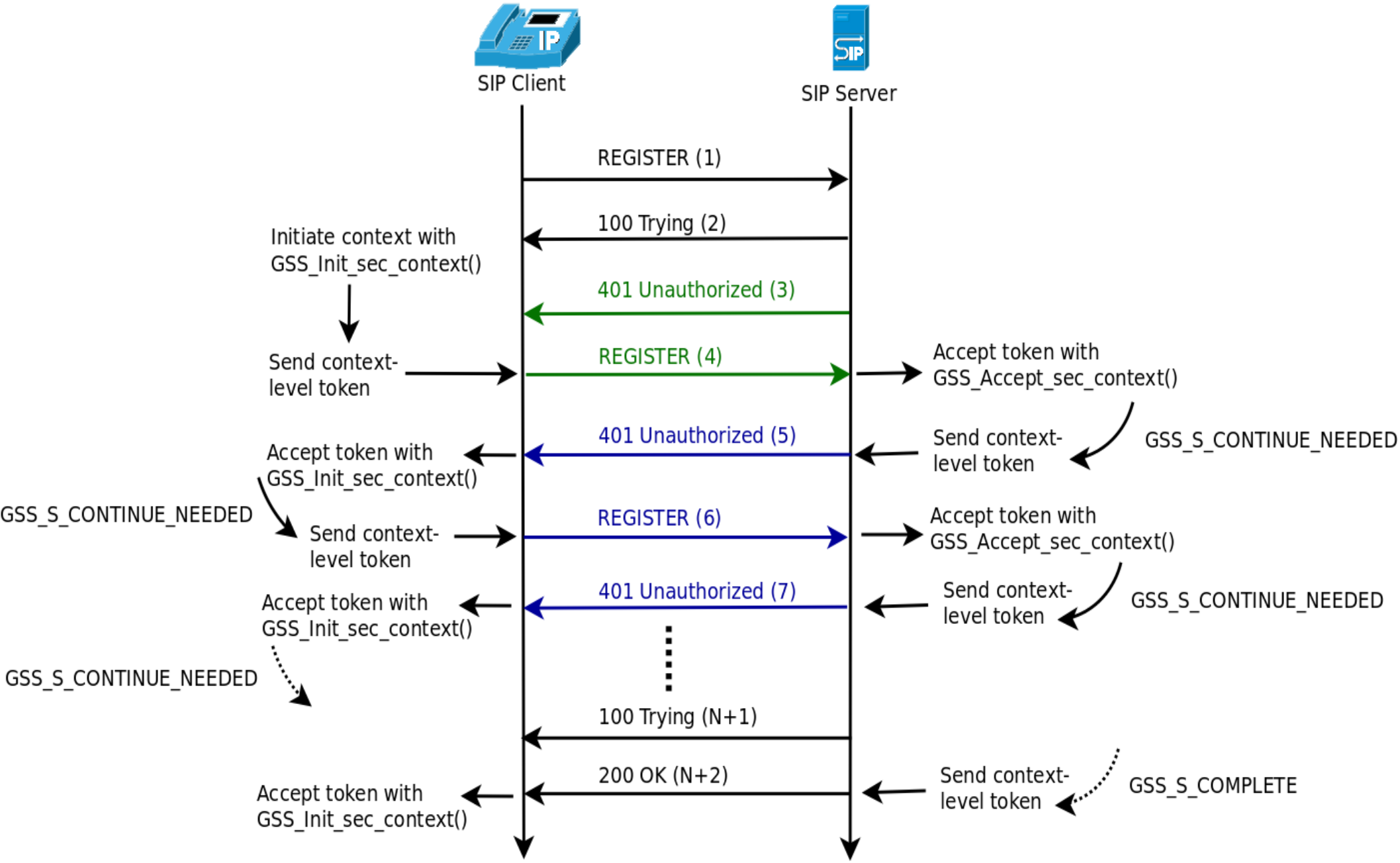
GSS-API

- Generic Security Services Application Program Interface = Interface for an application to access security services
- Mature and well-proven standard (RFC2743)
- NOT a communication protocol
  - Relies on the application (SIP) to pass data *tokens* between client and server
- Does NOT provide any security in itself
  - Relies on underlying security mechanisms
- GSS-API implementations (may) support different authentication methods
  - Digest
  - Kerberos
  - TLS
  - …
- All methods are *transparent* to the application

GSS-API stack (with SIP)




Digest
TLS/SSL
Kerberos
GSS-API
tokens
SIP stack
Digest
TLS/SSL
Kerberos
GSS-API
tokens
SIP stack
SIP messages with
embedded GSS-API tokens
IP
SIP
SIP client
SIP server


SIP Client
SIP Server
REGISTER (1)
100 Trying (2)
Initiate context with
GSS_Init_sec_context()
401 Unauthorized (3)
Send context-
level token
REGISTER (4)
Accept token with
GSS_Accept_sec_context()
401 Unauthorized (5)
Send context-
level token
GSS_S_CONTINUE_NEEDED
Accept token with
GSS_Init_sec_context()
GSS_S_CONTINUE_NEEDED
Send context-
level token
REGISTER (6)
Accept token with
GSS_Accept_sec_context()
401 Unauthorized (7)
Send context-
level token
GSS_S_CONTINUE_NEEDED
Accept token with
GSS_Init_sec_context()
GSS_S_CONTINUE_NEEDED
100 Trying (N+1)
200 OK (N+2)
Send context-
level token
GSS_S_COMPLETE
Accept token with
GSS_Init_sec_context()

SIP REGISTER message

DAA

```
1.   REGISTER sip:CompanyA SIP/2.0
2.   Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFB0D488
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="ccbde1c
     519d7",uri="sip:CompanyA",algorithm=MD5
10.  Max-Forwards: 70
11.  Expires: 3600
12.  Content-Length: 0
```

GSS-API token

```
1.   REGISTER sip:CompanyA SIP/2.0
2.   Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFB0D488
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: GSSAPI ttype="context"
     token="0401000B06092A864886F712010202DACD139402AAF44350CDE32"
10.  Max-Forwards: 70
11.  Expires: 3600
12.  Content-Length: 0
```

SIP today
Peering vs. the “email model”

Global reachability?

- SIP has won the “signaling battle” (over H.323)
  - (like SMTP won over X.400)
  - SIP incorporates many elements from HTTP and SMTP
- **Design goal: Global reachability like SMTP**
  - We call this the “email model”
- SIP has reached deployment worldwide
  - VoIP has reached high penetration both in companies and for ISP customers
  - But very few *open* SIP servers – like originally planned
  - **Why?**

SIP follows an “email alike model”

1) Email and SIP addresses are structured alike
   - username@domain
   - address-of-record (AoR): **`sip:alice@example.com`**
2) Both SIP and email rely on DNS
   - Map domain name to a set of ingress points that handle the particular connection
3) The ingress points need to accept incoming request from the Internet
4) No distinction between end-users and providers
   - Any end-user can do a DNS lookup and contact the SIP server directly
5) No need for a business relationship between providers
   - Since anyone can connect
6) Clients (usually) do not talk directly to each other – often one or more intermediate SIP/SMTP nodes

(Read more: RFC 3261 and RFC 3263)

Why has the email model failed?

1) **Business** – “sender keeps all” → breaks tradition
   - The traditional economic model is based on termination fee (PSTN)
   - Since anybody can connect to anybody, no business relationship is needed
   - No (economical) incentives for providers to deploy open SIP servers
2) **Legal requirements** → written for PSTN
   - Operators must comply to a wide range of regulatory requirements
   - Example: Wiretapping, caller-id, hidden number, emergency calls, etc
3) **Security considerations**
   A) Unwanted calls (SPam over Internet Telephony - SPIT)
   B) Identity
   C) Attack on availability (DoS)

A) Unwanted calls (SPIT)

- **Hard** – unknown attack vector
  - When there are enough open SIP servers, attackers will start to exploit them
  - Low amount of SPIT today (because few open SIP servers)
- **Worse than SPAM**
  - Content only available *after* the user picks up the phone = harder to filter and detect than email
  - Users tend to pick up the phone when it rings = disruptive (users can choose when to check their email)
- A number of SPIT mitigation strategies have been proposed (active research)

"We're afraid of SPIT, so we don't have open SIP Servers"

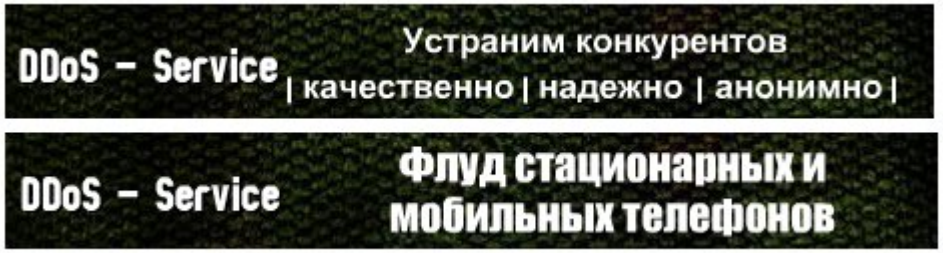
B) Identity

- PSTN
  - Provide (reasonable) good caller-id
  - Providers trust each others signaling
- SIP's email model breaks this
  - Anyone can send
  - SIP (INVITE) easily spoofed
- **The SIP authentication is terrible**
  - Modeled (copied) after HTTP Digest authentication
  - SIP also support TLS (and certificate authentication) but very limited deployment
- “SIP Identity” tries to fix this (RFC4474)
  - Computes a hash over selected INVITE headers and then signed
  - Rely on certificates
  - Not based on transitive trust between providers (signed part can be removed without implications)
  - But, no one uses this..

“Since SIP has so poor identity handling, we don't want to expose our SIP servers to the Internet”

C) Attack on availability (DoS)

- **Denial of Service (DoS) attacks are HARD!**
  - Simple and effective: Send more bogus traffic than the recipient can handle
  - No simple solution to prevent DoS



- Example: DDoS for sale - 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."

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

“We're terrified to become a victim of a DDoS attack”

So, what is the result?

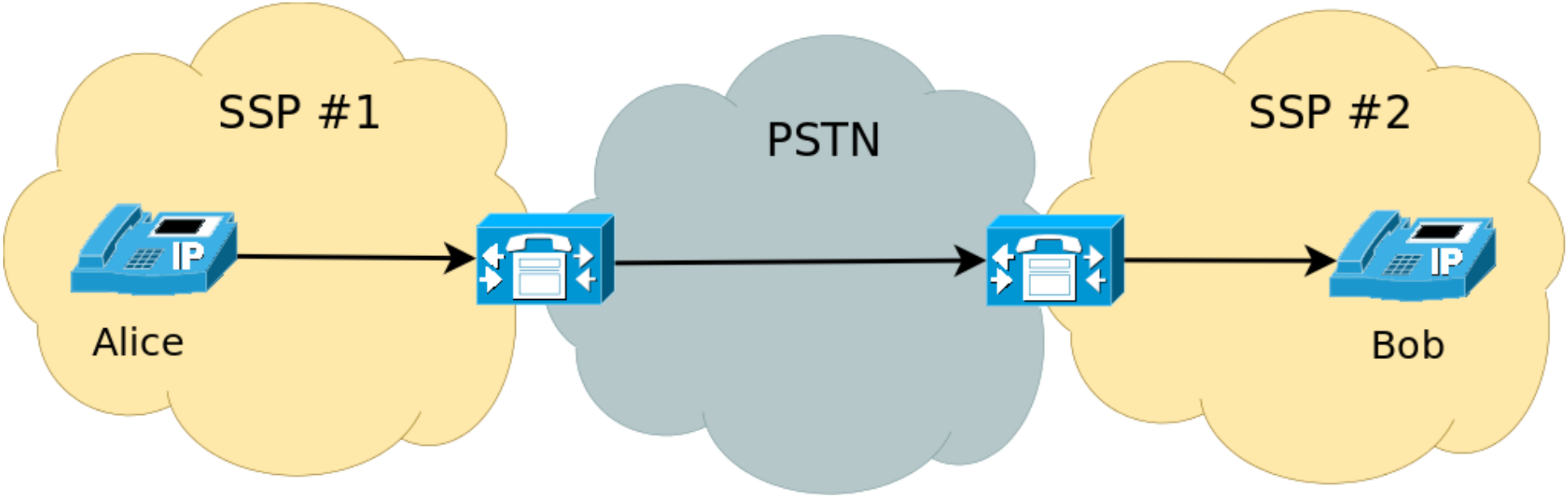
Providers do NOT have open SIP servers

All non-local calls are sent to the PSTN

Why is that a bad thing?

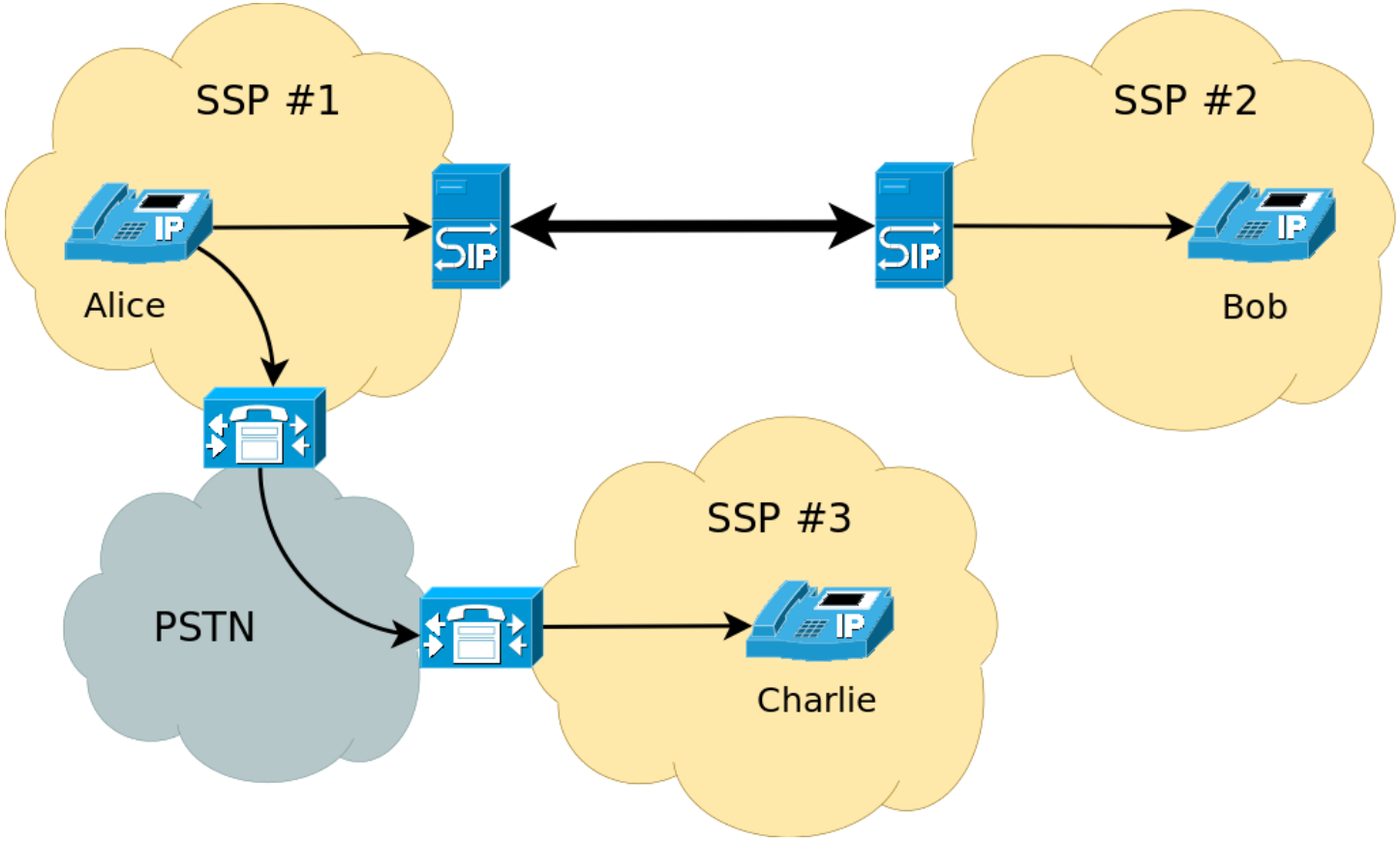
Disadvantages

1) Administrative overhead – more systems to keep track of
   - IP-to-PSTN gateway
2) More expensive than “SIP only”
   - Must pay a termination fee to the PSTN provider
   - Must maintain the IP-to-PSTN gateway
3) Poor(er) voice quality
   - Voice must be transcoded from G.711 to the PSTN (and back again)
   - Can not use wide-band codecs, like G.722 that provides superior sound quality (“HD sound”)
4) Only applies to voice – miss out other functionality that SIP supports
   - IM, presence, mobility, etc.



SIP Peering

- Peering overcome these disadvantages
- Do not need an open SIP server on the Internet
- Industry started to do this ad-hoc
  - Was not standardized in any way
  - IETF SPEERMINT WG



Closing remarks

- VoIP = SIP + RTP
- SIP is flexible and easily extended
- SIP have wide industry adoption
- SIP does not play well with NAT
- SIP have security flaws
- SIP peering used extensively today
- SIP is pretty hard to implement in a native web browser environment
  - “The future is web”
  - WebRTC:
    - API defined by W3C
    - Protocol specification by IETF
      - IETF WG rtcweb: “Real-Time Communication in WEB-browsers”
      - Get involved yourself: https://tools.ietf.org/wg/rtcweb/

Ex: https://appear.in/ and others

Try for yourself!

- SIP Server: Install Asterisk on Linux

  ..or download AsteriskNOW (Linux distro)
- SIP Client: X-Lite, Bria (iOS, Android)

Spørsmål?