Voice over IP (VoIP) using the Session Initiation Protocol (SIP)

INF5050 - “Protokoller og ruting i Internett”
2016.04.08, UiO
Lars Strand
Lars Strand?

PhD (2011)

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

1. What is VoIP?
2. What is SIP? How does it work?
3. What is RTP (and SDP)?
4. SIP and security (authentication)
5. SIP today (SIP Peering) vs. originally intended (“email model”)
Switchboard operators
Problem: Scalability

the New York Telephone Exchange 1888

Salt Lake City, over 50 women, ca 1914

70 foot poles were part of the scenery in the early days. (Photo courtesy of Pennsylvania Bell.)
Automatic telephone exchange
(Private Branch Exchange - PBX)
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.
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, 2001
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 not 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 McNeish 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 (SIP). Like unwanted e-mail, SPIT can be generated in a similar way with bitnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, clog e-mail boxes and inhibit user productivity.

Security Strategy

Hackers to attack VoIP in two years

Video and all, Nate LLP says...

Tags: adware, spy, virus
By Dan Hirt
Published: 19 October 2005 10:25 BST

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

Companies using VoIP and other multimedia services, such as videotelephony, 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 Helvie

A recent report from the Australian press relates the story of a local where hackers sent 11,000 calls via the company’s VoIP system to a US company, each costing $3.00. This figure is a perfect example of how easily hackers can use VoIP to their advantage.

The first step is easy, there are a number of legitimate reasons why to use VoIP. For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If you have news worthy highlights of the SANS 2007 Top Internet Security Risks, please let us know.

Security Policy and audit:
1. Excessive User Rights
2. Unpatched Systems
3. Encrypted Network Links

Application Abuse:
1. Instant Messaging
2. Peer-to-Peer Programs

Voice Services:
1. VoIP Servers and Phones
2. Zero Day Attacks
3. A9. Peers-to-Peer Programs
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
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,

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):

![Diagram of SIP transaction flow](image)
# SIP request methods (RFC3261)

<table>
<thead>
<tr>
<th>SIP method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>Acknowledge a request/session</td>
</tr>
<tr>
<td>BYE</td>
<td>Terminate a session (call)</td>
</tr>
<tr>
<td>CANCEL</td>
<td>Cancel any pending requests</td>
</tr>
<tr>
<td>INVITE</td>
<td>Initiate a session (call)</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Query servers about their capabilities</td>
</tr>
<tr>
<td>REGISTER</td>
<td>Register contact information for a UA to a location service.</td>
</tr>
</tbody>
</table>

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

http://datatracker.ietf.org/wg/sip/documents/
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
(call setup)
SIP REGISTER
(registration and authentication)

Local SIP domain

SIP Location Service
(SIP Server)

May contain information about:
- URIs
- IP address(es)
- scripts
- features and other preferences

DB

SIP UA
"Bob"

SIP REGISTER
1. Authenticate device
2. Register location (IP)
SIP REGISTER message flow (using Digest Access Authentication)

SIP UA Bob

SIP location server

REGISTER (1)

100 Trying (2)

401 Unauthorized (3)

REGISTER (4)

100 Trying (5)

200 OK (6)

Compute response using DAA

HA1 = MD5(username, realm, password)

HA2 = MD5(method, digestURI)

response = MD5(HA1, nonce, HA2)

Generate nonce-value and send

Compute response and compare

time
**SIP message structure - REGISTER**

<table>
<thead>
<tr>
<th>Start line (method)</th>
<th>REGISTER sip:156.116.8.139:5060 SIP/2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Via:</td>
<td>SIP/2.0/UDP 156.116.9.67;branch=z9hG4bKd9828eb03D78A219</td>
</tr>
<tr>
<td>From:</td>
<td>Bob <a href="">sip:bob@156.116.8.139</a>;tag=2A69C69E-E6A7587</td>
</tr>
<tr>
<td>To:</td>
<td>Bob <a href="">sip:bob@156.116.8.139</a></td>
</tr>
<tr>
<td>CSeq:</td>
<td>2 REGISTER</td>
</tr>
<tr>
<td>Call-ID:</td>
<td>f7ce9763-f9c8678c-7f5df1f5@156.116.9.67</td>
</tr>
<tr>
<td>Contact:</td>
<td><a href="">sip:bob@156.116.8.139</a>;methods=&quot;INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER&quot;</td>
</tr>
<tr>
<td>User-Agent:</td>
<td>PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392</td>
</tr>
<tr>
<td>Max-Forwards:</td>
<td>70</td>
</tr>
<tr>
<td>Expires:</td>
<td>3600</td>
</tr>
<tr>
<td>Content-Length:</td>
<td>0</td>
</tr>
</tbody>
</table>
SIP INVITE
(session setup)

Call:
sip:bob@companyB.com
or
+47 2212 3456
SIP INVITE message flow
# SIP message structure - INVITE

<table>
<thead>
<tr>
<th>Start line (method)</th>
<th>INVITE sip:<a href="mailto:bob@companyB.com">bob@companyB.com</a> SIP/2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Via: SIP/2.0/UDP sip.companyA.com:5060;rport;branch=z9hG4bK2EACE3AF14BF466648A37D2E1B587744</td>
</tr>
<tr>
<td></td>
<td>From: Alice <a href="">sip:alice@companyA.com</a>;tag=2093912507</td>
</tr>
<tr>
<td></td>
<td>To: Bob <a href="">sip:bob@companyB.com</a></td>
</tr>
<tr>
<td></td>
<td>Contact: <a href="">sip:alice@phone1.companyA.com:5060</a></td>
</tr>
<tr>
<td></td>
<td>Call-ID: 361D2F83-14D0-ABC6-0844-57A23F90C67E@156.116.8.106</td>
</tr>
<tr>
<td></td>
<td>CSeq: 41961 INVITE</td>
</tr>
<tr>
<td></td>
<td>Max-Forwards: 70</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/sdp</td>
</tr>
<tr>
<td></td>
<td>User-Agent: X-Lite release 1105d</td>
</tr>
<tr>
<td></td>
<td>Content-Length: 312</td>
</tr>
</tbody>
</table>

| 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:
  \[ <\text{character}> = <\text{value}> \]
- 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)**
   - 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)**
   - Goal: Security service end to end
   - Uses certificates, needs PKI = “complex and expensive”
   - Not supported, not used.

3) **Other user identity handling methods**
   - 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

Client Alice
Attacker Charlie
SIP Server

REGISTER (1)
100 Trying (2)
401 Unauthorized (3)
REGISTER (4)
REGISTER (5)
Contact header value modified
100 Trying (6)
200 OK (7)

time
Execution of the attack

**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

**Attack:**

We use NetSED to modify the network stream live.

Can use search and replace based on regexp

```bash
@attack01:~$ .netsed udp 5060 156.116.8.139 5060
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).
```
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:

\[
\begin{align*}
HA0 &= \text{MD5}(A0) = \text{MD5}(\text{ContactURIs}) \\
HA1 &= \text{MD5}(A1) = \\
&\text{MD5}(\text{username:realm:password}) \\
HA2 &= \text{MD5}(\text{method:digestURI}) \\
\text{response} &= \text{MD5}(HA0:HA1:nonce:HA2)
\end{align*}
\]
SIP Authentication: 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 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)

- Kerberos
- Digest
- Other
- SPNEGO
- GSS-API
- SIP
- TCP/UDP/SCTP
- IP
SIP REGISTER message

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFBO7D88
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
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BFBO7D88
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="0401000B06092A864886F712010202DACD139402A4F44350CDE32"
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)
- The research project “SPIDER” looked at SPIT
  - Good informative deliverables
  - Project finished

“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)
  - 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

![DDoS - Service](image)

• 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."


“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)
Thank you