VoIP: SIP

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti, Reiti di telecomunicazioni C, a.a. 2009/2010

http://www.tlc.unipr.it/veltri

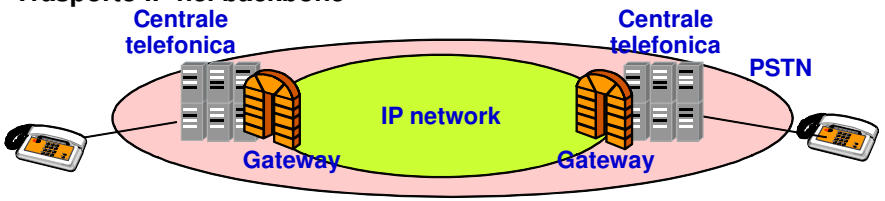
Indice

Voice over IP (VoIP)

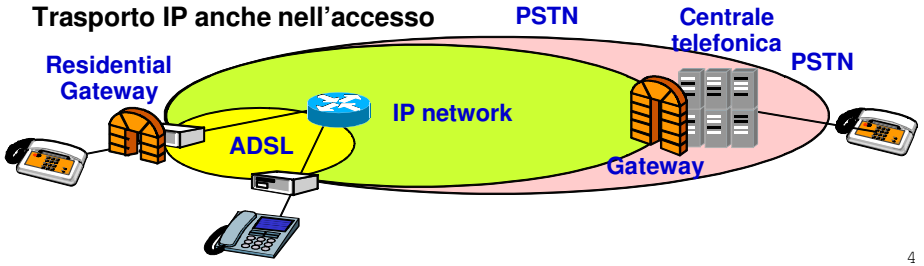
- Trasporto del segnale vocale convertito in forma digitale su una rete IP
  - **Il trasporto su IP può avvenire a partire dai terminali di utente o essere utilizzato in un tratto interno alla rete**
- Nel caso in cui la piattaforma di rete è incentrata su IP , è possibile aggiungere al tradizionale servizio voce punto-punto altri servizi multimediali quali ad esempio:
  - **chiamata auidio/video**
  - **conference**
  - **IM**
  - **presence**
- In tal caso si parla più genericamente di IP Telephony
  - **se la rete IP coincide con la rete Internet (pubblica) allora si usa anche il termine di**
    - Internet Telephony

Scenari VoIP: Operatore pubblico, accesso residenziale

Trasporto IP nel backbone

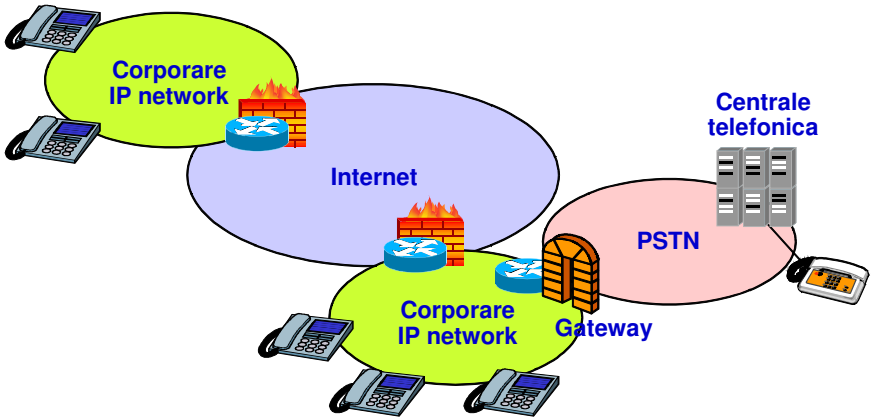


Trasporto IP anche nell'accesso



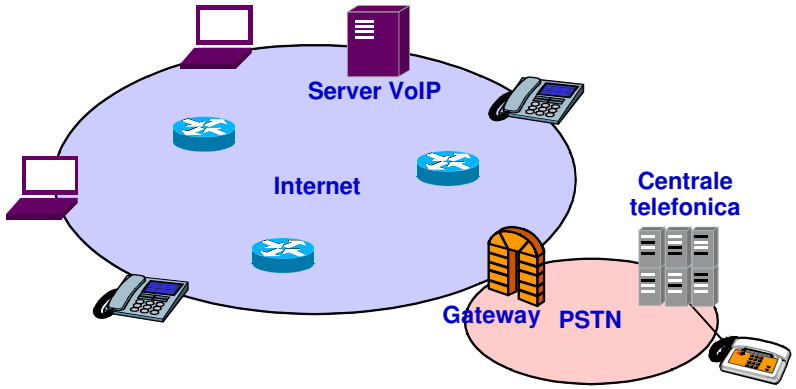
Scenari VoIP: Rete VoIP aziendale

Trasporto IP nell'accesso e come VPN

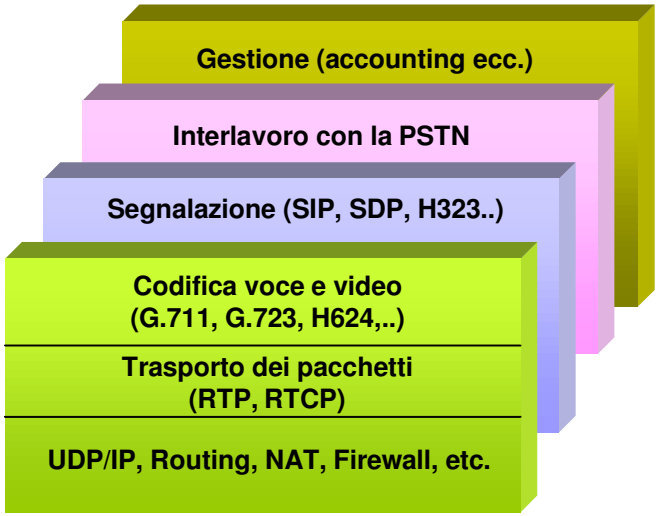


Scenari VoIP: Internet telephony

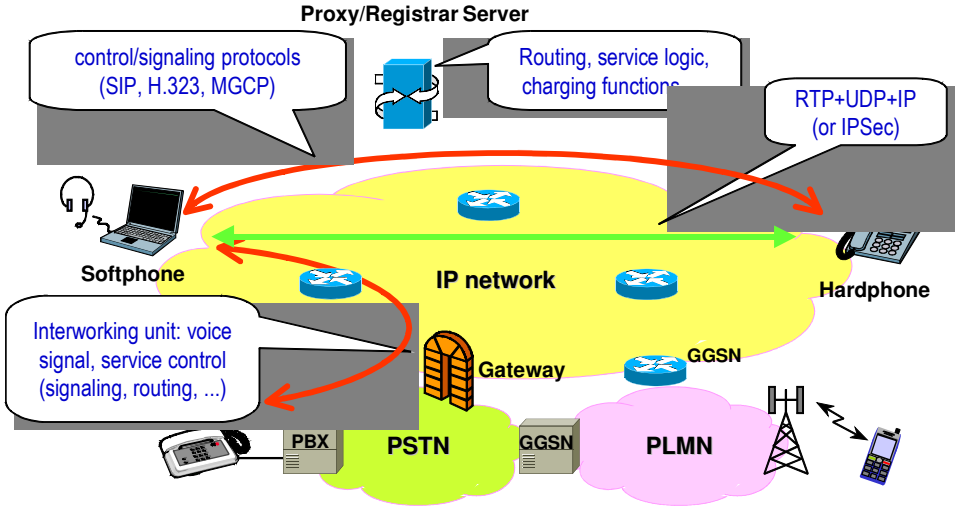
Trasporto IP end-to-end tramite rete Internet



Architettura generale e componenti dei sistemi VoIP



Componenti base dei sistemi VoIP



Componenti base dei sistemi VoIP (cont.)

- Data plane
  - **Codec/decodec (audio, video)**
  - **RTP/RTCP**
  - **IP Multicast**
  - **IPv6**
  - **Security protocols (TLS,DTLS,SRTP,IPSec)**
  - **QoS enforcement**
  - **Firewall, NAT**
- Control plane
  - **Signaling protocols (SIP, SDP, H323, MGC, others)**
  - **Media Server Control (RTSP)**
    - VCR like controls
      - Fast-forward, play, rewind, pause, record
  - **Session Announcement (SAP)**
    - announcement protocol for multimedia sessions
      - uses IP multicast to a well-known address/port

Componenti base dei sistemi VoIP (cont.)

- Control plane (cont.)
  - **AAA (Authentication, Authorization, Accounting)**
    - RADIUS
    - Diameter
  - **QoS**
    - Integrated Services Resource Reservation (RSVP)
    - Differentiated Services
  - **Firewall and NAT traversal**
    - STUN, TURN, ICE

Vulnerabilità del VoIP

VoIP Security

- VoIP services are provided via IP-based systems and supporting servers, often running on non-secure operating systems
  - **e.g. IP PBXs, supporting servers, media gateways, switches, routers, firewalls, cabling, and IP phones/softphones**
- Securing a VoIP network is much more complex and arduous than securing a traditional circuit-switched voice network
  - **VoIP is vulnerable to traditional IP attacks**
    - same attacks that knock out other types of servers
  - **VoIP is as secure as the weakest link on the network**

VoIP Security (cont.)

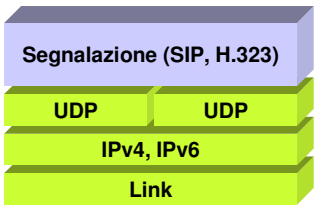
- There are several characteristics and requirements unique to VoIP that make providing security much more difficult
  - **VoIP has unique real-time and reliability requirements that make it highly susceptible to DoS attacks**
    - for example, any delay of the media by as much as 500ms makes a conversation unusable
- VoIP standards are complex, and many implementations have flaws
  - **standards are very young**

More..

- Traditional data security devices are not designed to adequately address the real-time requirements of voice communications
  - **Most firewalls slow data transfer, impeding the flow of traffic and adding an unacceptable latency to RTP packets**
  - **VoIP requires up to six additional ports to be opened for the duration of each call**
  - **Conventional firewalls were not designed to handle this type of complex traffic**

Vulnerabilità ereditate dai protocolli sottostanti

- Vulnerabilità ereditate da:
  - **sistema DNS**
  - **TCP/UDP**
  - **IP**
  - **Ethernet e altri collegamenti**



Man in the middle

Arp poisoning, DNS Spoofing, DNS Poisoning, DHCP Spoofing, ICMP Redirection

Denial of Service

DDoS, ICMP Smurfing, SYN Flood, Virus

Information Theft

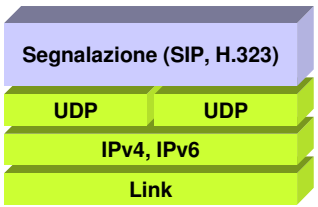
Sniffing, Buffer Overflow, Password Cracking, Social Engineering, Malware

Hijacking

TCP Hijacking

Vulnerabilità della segnalazione

- Vulnerabilità introdotte da:
  - **SIP**
  - **H.323**
  - **altri**



Hijacking

Registration Hijacking, 3XX Responce Code Messages

Man in the middle

Impersonating a Proxy Server, 3xx Responce Code Messages, Impersonating a Registrar Server

Denial of Service

Tearing down a session, Modifing a session, Cancelling a session, SIP DoS Attack, Distributed Denial of Service, Responce code messages

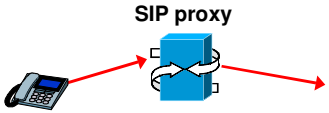
SIP

Session Initiation Protocol (SIP)

- Protocollo di segnalazione a livello applicativo per instaurare, mantenere e abbattere sessioni multimediali tra due o più partecipanti
  - **le sessioni includono chiamate audio/video via rete IP, conferenze, messagistica**
  - **SIP permette di negoziare il tipo di sessione e scambiare informazioni legate ai media**
  - **SIP non si occupa direttamente dello scambio dei dati multimediali ne di riservare eventuali risorse per i corrispondenti flussi dati**
- SIP è definito dallo standard ETF RFC 3261 (June 2002) e successivi
- SIP è stato scelto e utilizzato dal 3GPP come protocollo di segnalazione per la parte multimediale delle reti di terza generazione (UMTS)

Caratteristiche

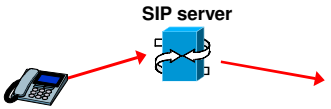
- Protocollo applicativo client-server, sopra UDP (default), ma può appoggiarsi anche su TCP, TLS or SCTP
- Protocollo text-based (simile a HTTP)
- SIP utilizza indirizzi (SIP URI) simili a quelli di posta elettronica
  - **example:** `<sip:alice@wondelrand.net>`
- I messaggi SIP di segnalazione possono essere scambiati direttamente tra i terminali (SIP User Aagent), o tramite noi intermedi chiamati SIP proxy

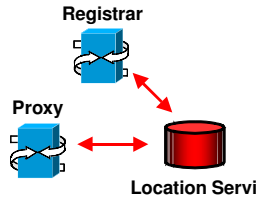


- Un terminale (SIP UA) può segnalare la sua presenza in rete tramite registrazione su appositi server chiamati SIP registrar

SIP architectural elements

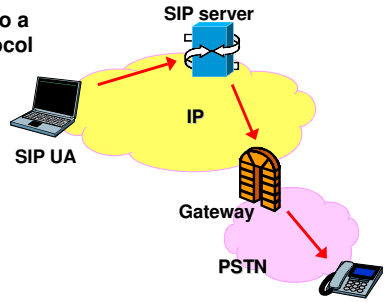
- User Agent (UA)
  - **end system (terminal)**
  - **can initiates calls, acting as caller**
  - **User Agent Client (UAC)**
  - **can respond, redirect and refuse entering calls, acting as callee**
  - **User Agent Server (UAS)**
- SIP Server
  - **system that may proxy or redirect SIP messages**
  - **may keep information on user location**
    - Location Service
  - **can be:**
    - Proxy
    - Redirect
    - Registrar



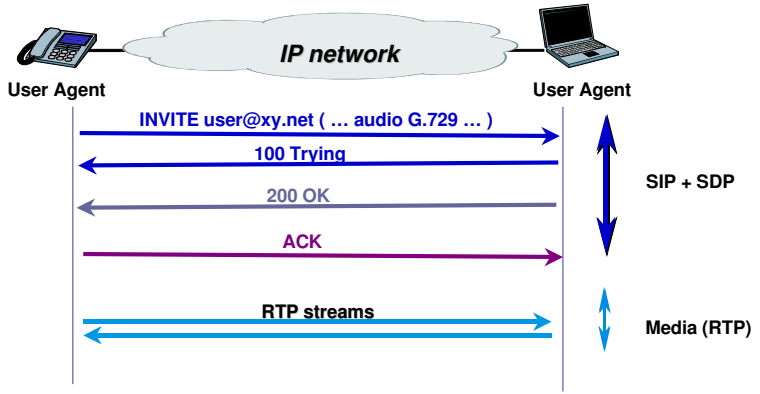


SIP architectural elements (cont.)

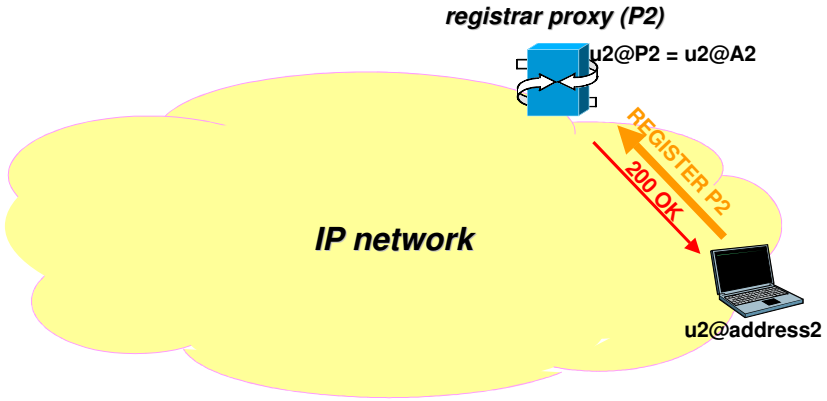
- SIP Gateway
  - **system that interfaces a SIP network to a network using another signaling protocol**
    - e.g. SIP/PSTN GW
  - **it may act as:**
    - signaling GW (SGW)
    - media GW (MGW)
  - **on both side it acts like a terminal**
    - eventually supporting lots of users



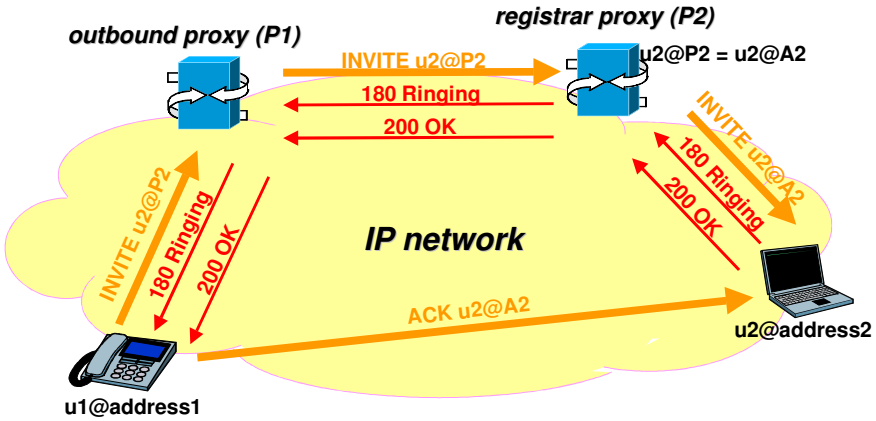
SIP call setup



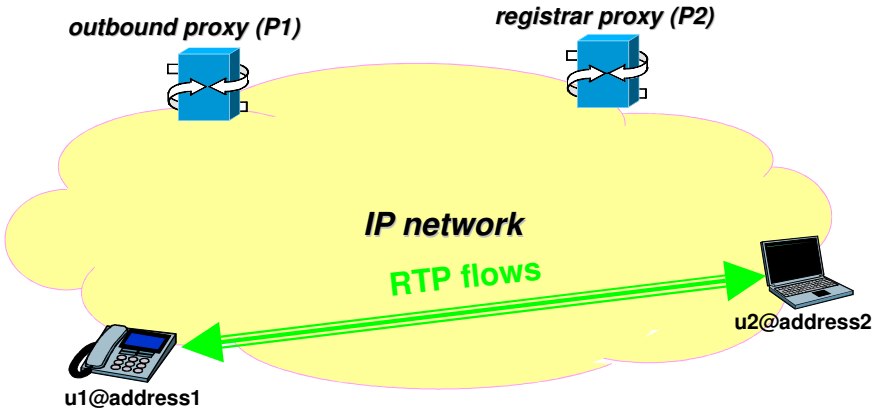
SIP Registration



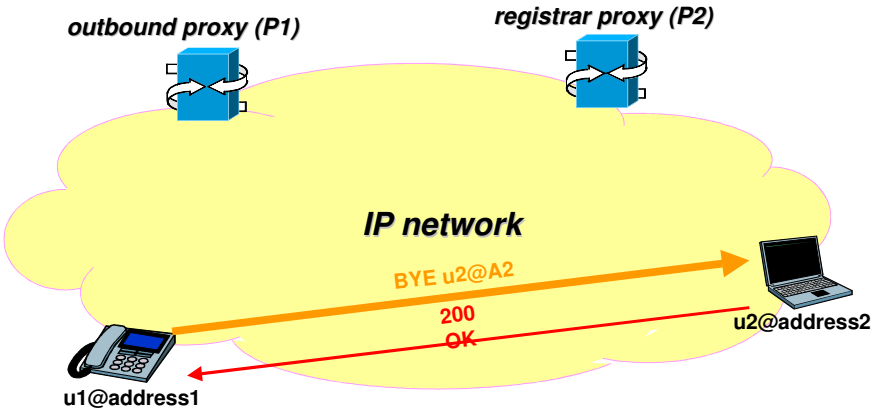
SIP Call: Instsurazione chiamata (Setup)



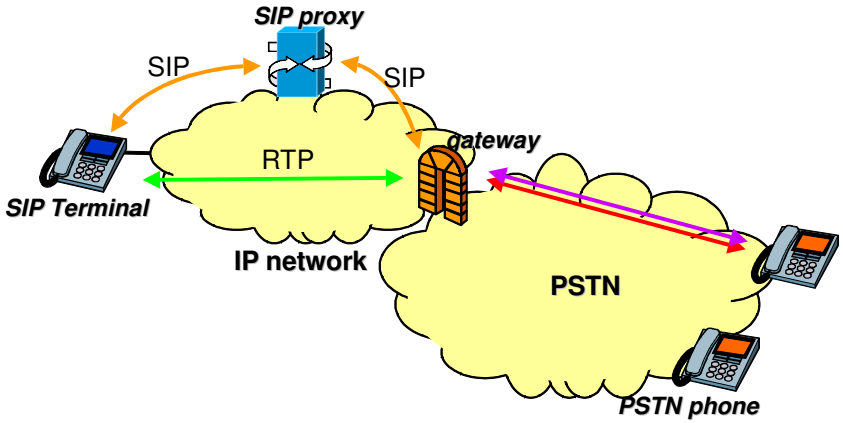
SIP Call: In chiamata (On call)



SIP Call: Abbattimento (Tear down)



SIP Call: PSTN Gateway



Messaggi SIP

- Richieste
  - **INVITE, ACK, CANCEL, BYE, SUBSCRIBE, NOTIFY, MESSAGE, etc.**
  - **alcuni esmpi:**
    - INVITE: utilizzato per iniziare una sessione, può includere descrizione del media tramite SDP
    - ACK: conferma la ricezione di una risposta definitiva ad una precedente richiesta di INVITE
    - BYE: abbatte una connnessione
    - REGISTER: serve per registrare la corrispondenza tra un indirizzo pubblico SIP (con cui si identifica un utente) e un contatto del UA (indirizzo dove può essere raggiunto l'utente)
- Risposte (provvisorie o finali)
  - 1xx (provvisorie)
  - 2xx successo (finale)
  - 3xx ridirezione (finale)
  - 4xx errore/fallimento del UA (finale)
  - 5xx errore/fallimento del server (finale)
  - 6xx errore/fallimento generale (finale)

Messaggi SIP (cont.)

- Una richiesta SIP è formata da
  - **una request line**
  - **dei campi di intestazione (header field)**
  - **un payload (message body) opaco per SIP**
    - può contenere la descrizione delle sessioni che si volgiono instaurare
    - tale descrizione è riportata in accordo al protocollo SDP (Session Description Protocol)
- Una risposta SIP è formata da
  - **una response line (con un codice di risposta)**
  - **dei campi di intestazione (header field)**
  - **un payload (message body) opaco per SIP**

Esempio di messaggio INVITE

```
INVITE sip:alice@wonderland.net SIP/2.0
Via: SIP/2.0/UDP phone32.wonderland.net
CSeq: 5452 INVITE
To: <sip:alice@ wonderland.net>
From: <sip:peter@neverland.net>
Content-Type: application/sdp
Call-ID: 1804289383@phone32.neverland.net
Subject: New Call
Content-Length: 182
Contact: <sip:peter@phone32.neverland.net >

v=0
o=username 0 0 IN IP4 192.168.200.2
c=IN IP4 192.168.200.2
t=0 0
m=audio 33422 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=ptime:20
m=video 22000 RTP/AVP 31
```


Esempi di codici di risposta di errore

4xx client error

400 bad request
401 unauthorized
403 forbidden
404 not found
407 proxy authentication required
408 request timeout
420 bad extension
480 temporarily unavailable
481 call leg doesn't exist
482 loop detected
483 too many hops
484 address incomplete
485 ambiguous
486 busy here
487 request cancelled

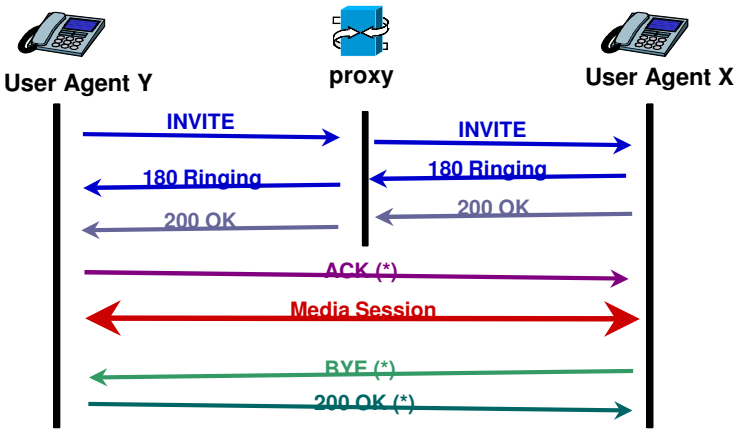
5xx server error

500 server internal error
501 not implemented
502 bad gateway
503 service unavailable
504 gateway timeout
505 version not supported

6xx global failure

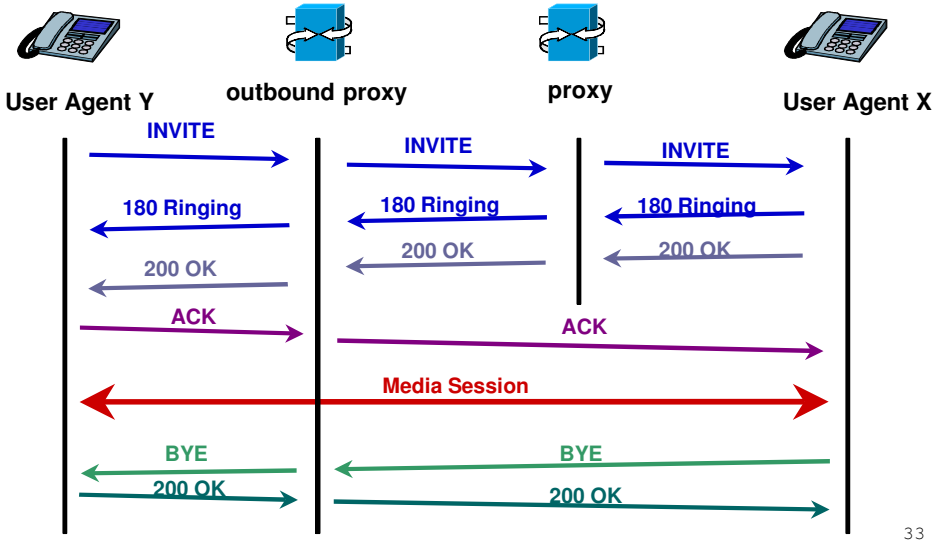
600 busy
601 decline
602 does not exist
606 not acceptable

Esempio di call setup tramite destination proxy



(*) può essere diretto o rilanciato dal proxy

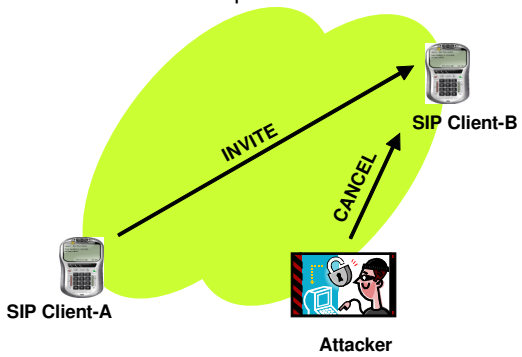
Esempio di call setup tramite outbound e destination proxy



Basic SIP attacks

Attacks: DoS

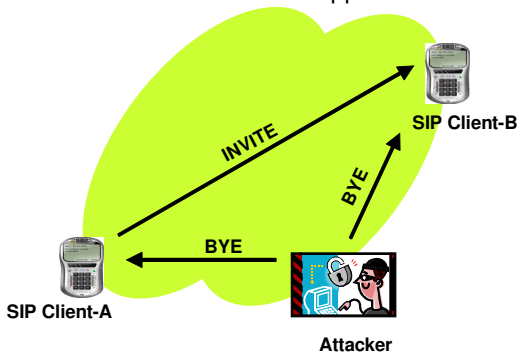
- Impedire al SIP Client-A di portare a termine una chiamata



- L'attaccante cancella una richiesta pendente (INVITE)
  - **deve conoscere i campi esatti da inserire nel messaggio (Call-ID, TO, From, e Cseq identificano univocamente una chiamata)**

Attacks: DoS

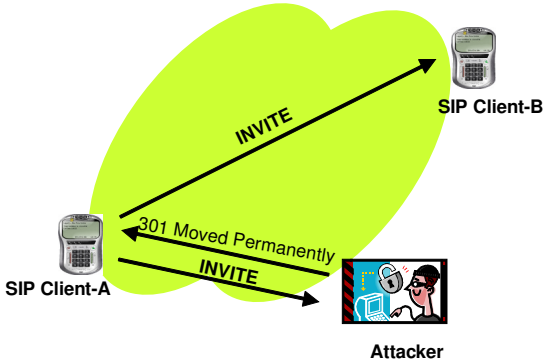
- Il SIP Client-A rilascia la chiamata appena iniziata



- L'attaccante chiude una chiamata appena instaurata
  - **deve conoscere i campi esatti da inserire nel messaggio (Call-ID, TO, From, e Cseq identificano univocamente una chiamata)**

Attacks: Call Hijacking

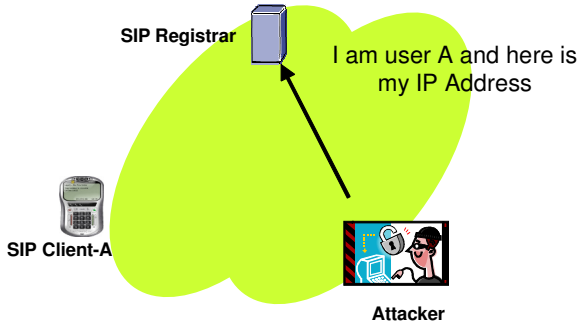
- Dirottamento di chiamata
  - **Dopo che il SIP Client-A ha inviato l'INVITE, l'attaccante manda un messaggio 301 "Moved Permanently" per dirottare la chiamata verso dove vuole lui (nell'esempio lui stesso)**



- Deve conoscere i campi esatti da inserire nel messaggio (Call-ID, TO, From, e Cseq identificano univocamente una chiamata)

Attacks: Identity Theft

- Furto di identità
  - **l'attaccante si registra al posto di un altro utente (sorpassando i meccanismi di autenticazione)**
    - per poter usare la sua identita'
    - per poter usar ei sui diritti
    - per impedirgli di riceve chiamate



SIP Security

Securing SIP

- SIP defines several mechanisms for user authentication, message authentication, and message confidentiality
- Some mechanisms are
  - **HTTP digest authentication (UAS and Proxy)**
    - with extensions, such as AKA (3GPP)
  - **use of Transport Layer Security (TLS)**
  - **use of IPSec**
  - **S/MIME encapsulation**
- Other Security-related SIP extensions
  - **Privacy Mechanism for SIP (RFC 3323)**
  - **Security Mechanism Agreement for the SIP (RFC 3329)**
  - **SIP Authenticated Identity Body (AIB) (RFC 3893)**
  - **Enhancements for Authenticated Identity Management in the SIP (RFC 4474)**
  - **etc.**

Securing SIP Hop-by-hop or End-to-end

- Hop-by-hop authentication, integrity or confidentiality
  - **HTTP Proxy authentication**
  - **TLS**
  - **IPSec**
- End-to-end authentication, integrity or confidentiality
  - **HTTP Server authentication**
  - **S/MIME encapsulation**

SIP over IPSec

- Two popular alternatives for providing security at the transport and network layer are, respectively, TLS and IPSec
- IPSec is most commonly used in architectures in which a set of hosts or administrative domains have an existing trust relationship with one another
  - **usually implemented at the operating system level in a host, or on a security gateway**
  - **provides confidentiality and integrity for all traffic it receives from a particular interface (as in a VPN architecture)**
- IPSec can also be used on a hop-by-hop basis
  - **however, sometimes is arduous to add IPSec to SIP UAs**

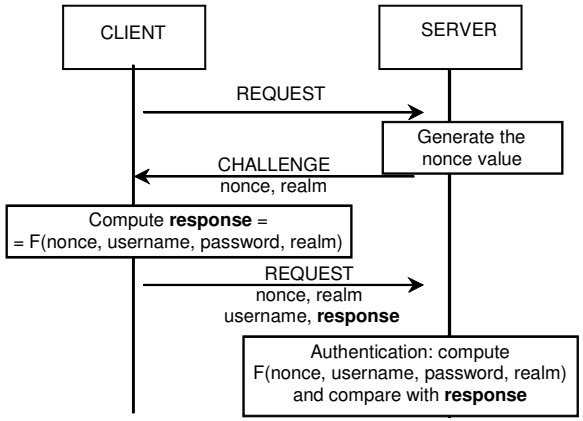
SIP over TLS

- SIP runs on top of several different transport protocols
  - **UDP (default), TCP, TLS, DTLS, SCTP, etc.**
  - **however only UDP and TCP are mandatory**
- TLS can provide transport-layer security to SIP
  - **hop-by-hop security**
- SIP defines also a SIPS URI scheme
  - **SIPS allows resources to specify that they should be reached securely**
  - **request messages sent to the resource identified by a SIPS URI are required to be sent over each SIP hop over TLS**
- It also possible "best-effort TLS"
  - **TLS transport without SIPS URIs**

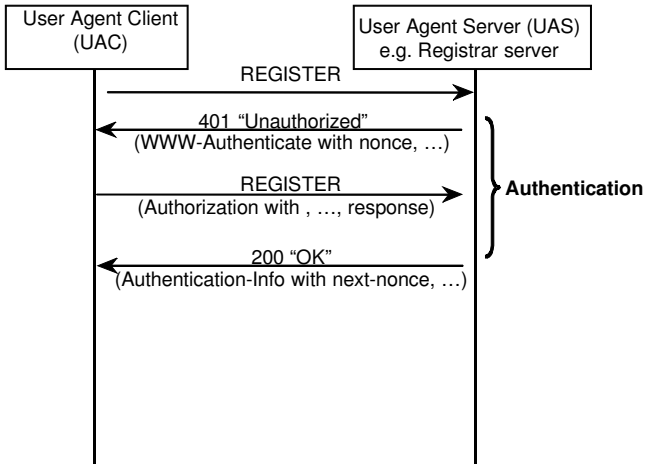
SIP/HTTP Digest authentication

- SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP
- Any time that a proxy server or UA receives a request, it MAY challenge the initiator of the request to provide assurance of its identity
- The "Digest" authentication mechanism provides
  - **message authentication and replay protection only**
  - **without message integrity or confidentiality**
- Note that due to its weak security, the usage of "Basic" authentication (RFC2543) has been deprecated
  - **servers MUST NOT accept credentials using the "Basic" authorization scheme, and servers also MUST NOT challenge with "Basic"**

Digest authentication: Challenge/response



UAC-to-UAS Authentication



UAC-to-UAS Authentication

- Header di una response 401Unauthorized:

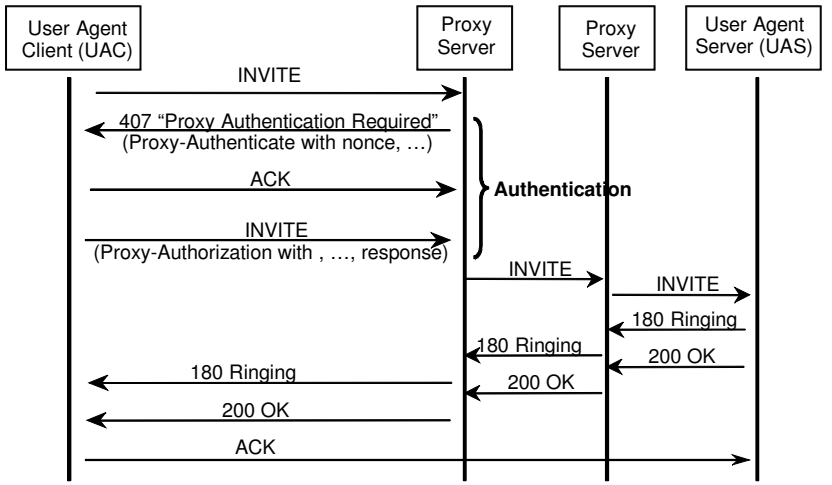
WWW-Authenticate: Digest, realm="biloxi.com", qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
algorithm=MD5

- Header della request contenente la risposta alla sfida:

Authorization: Digest username="bob", realm="biloxi.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="sip:bob@biloxi.com, qop=auth,
response="6629fae49393a05397450978507c4ef1"

- response = F(nonce, username, passwd, realm, metodo, sip uri)

(UAC-to-)Proxy Authentication



S/MIME encoded body

- I messaggi SIP possono trasportare un body codificato in MIME
- lo standard MIME prevede dei meccanismi per proteggere messaggi MIME
  - **Secure MIME (S/MIME)**
  - **permette di garantire sia controllo di integrità/autenticità che confidenzioalità**
    - 'multipart/signed'
    - 'application/pkcs7-mime'
- S/MIME può fornire quindi un metodo per inviare e ricevere messaggi SIP proteggendo il body (e.g. la negoziazione dei media)
  - **S/MIME encoded SDP body**
- There may be network intermediaries that rely on viewing or modifying the bodies of SIP messages (e.g. SDP)
  - **S/MIME may prevent these sorts of intermediaries from functioning**

Example of S/MIME encoded body

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
   handling=required

**********************************************************
* Content-Type: application/sdp                          *
*                                                        *
* v=0                                                    *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com    *
* s=-                                                    *
* t=0 0                                                  *
* c=IN IP4 pc33.atlanta.com                              *
* m=audio 3456 RTP/AVP 0 1 3 99                          *
* a=rtpmap:0 PCMU/8000                                   *
**********************************************************
```


S/MIME encapsulation: Tunneling SIP

- SIP can encapsulate entire SIP messages (or a message fragment) within MIME bodies of type "message/sip" and then apply MIME security (S/MIME)
  - **use encryption to protect and hide the body and/or some specific header fields**
  - **integrity and/or confidentiality**
  - **some header fields must always have a plaintext version since they are required for routing SIP messages**
  - **there may be discrepancies between the values in the "inner" message and values in the "outer" message**

S/MIME encapsulation: Tunneling SIP (cont.)

- Confidentiality
  - **message is encrypted and encapsulated**
  - **header fields may be included in the encrypted body that are not present in the "outer" message**
  - **some header fields must always have a plaintext version because they are required header fields in requests and responses**
    - e.g. To, From, Call-ID, CSeq, Contact
- Integrity
  - **for SIP header fields if the header fields to be secured are replicated in a "message/sip" signed MIME body**

Example of encrypted and signed message

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Anonymous <sip:anonymous@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:pc33.atlanta.com>
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568

--boundary42
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
   handling=required
Content-Length: 231

**********************************************************
* Content-Type: message/sip                              *
*                                                        *
* INVITE sip:bob@biloxi.com SIP/2.0                      *
* Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8 *
* To: Bob <bob@biloxi.com>                               *
* From: Alice <alice@atlanta.com>;tag=1928301774         *
```



```
* Call-ID: a84b4c76e66710                                *
* CSeq: 314159 INVITE                                    *
* Max-Forwards: 70                                       *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                    *
* Contact: <sip:alice@pc33.atlanta.com>                  *
*                                                        *
* Content-Type: application/sdp                          *
*                                                        *
* v=0                                                    *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com    *
* s=Session SDP                                          *
* t=0 0                                                  *
* c=IN IP4 pc33.atlanta.com                              *
* m=audio 3456 RTP/AVP 0 1 3 99                          *
* a=rtpmap:0 PCMU/8000                                   *
**********************************************************

  --boundary42
  Content-Type: application/pkcs7-signature; name=smime.p7s
  Content-Transfer-Encoding: base64
  Content-Disposition: attachment; filename=smime.p7s;
     handling=required

  ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
  4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
  n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
  7GhIGfHfYT64VQbnj756

  --boundary42-
```