VoIP Security Threat Analysis

Saverio Niccolini, Jürgen Quittek, Marcus Brunner, Martin Stiemerling

(NEC, Network Laboratories, Heidelberg)

Introduction

- Security attacks taxonomy
  - "Denial of Service (DoS)" attacks
  - "Abuse of service" attacks
  - "Interception and modification" attacks

- Threats
  - confidentiality: it refers to the fact that the information is accessible only to those authorized to have access
  - integrity: it refers to the validity of data
  - availability: it refers to the expectation of availability and quality of resources

"Denial of Service (DoS)" attacks

- SIP-specific

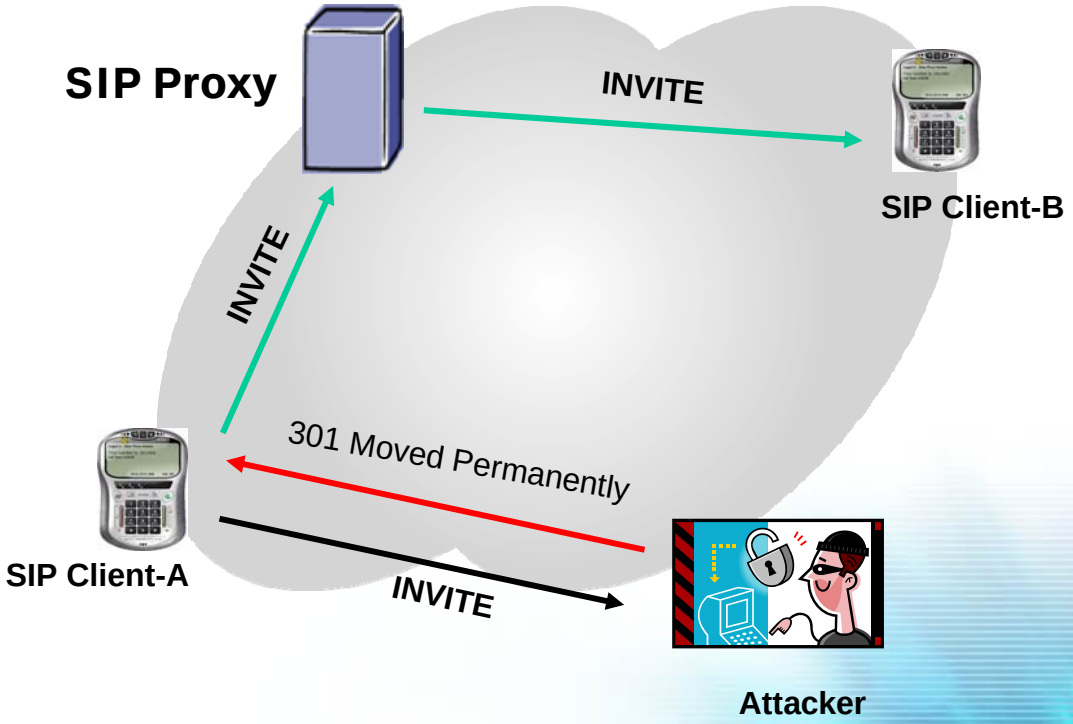
Attack name	Type of threat		
	Confidentiality	Integrity	Availability
SIP malformed methods			X
SDP malformed bodies			X
SIP messages causing buffer overflow			X
SIP methods flooding (to default SIP ports or to other ports)			X
Session tear down (using SIP CANCEL/BYE methods or Temporary Unavailable response)		X	X
Session hijacking (using SIP methods)	X	X	X
Session hijacking (using SDP body)	X	X	X

"Denial of Service (DoS)" attacks

- SIP-specific
  - SIP malformed methods / buffer overflow
    - one single message can stop the server/client from working properly
      - poor implementations (lot of them unfortunately…)
  - SIP methods flooding
    - will keep the SIP server busy / make it crashing
      - not responding to registration updates
        - » clients not able to place calls
        - » preventing mobility
  - SIP random messages
      - can keep busy/crash SIP server depending on FSM implementation (already at low rates) because of high number of checks

"Denial of Service (DoS)" attacks

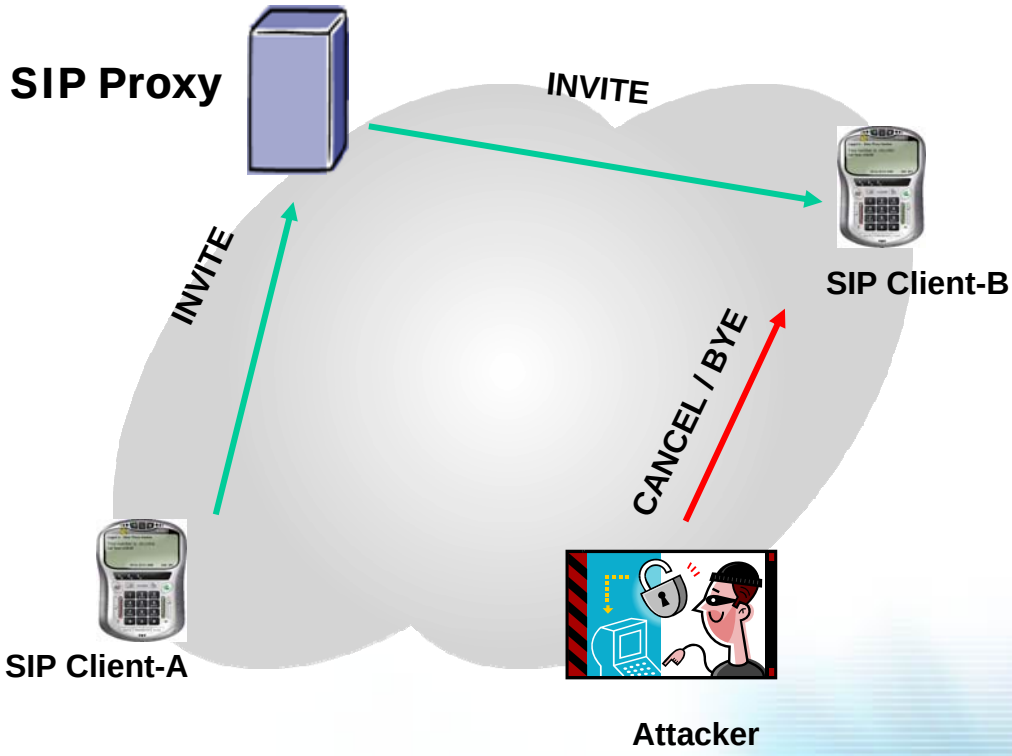
- Session Hijacking (using SIP methods)
  - After INVITE message, a 301 "Moved Permanently" message would hijack the call towards whoever the attacker decides (himself of another client)



- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

Internet Telephony Security: DoS attacks

- Session Tear down (not limited to SIP clients, but also to SIP servers)



- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

"Denial of Service (DoS)" attacks

- RTP/RTCP-specific DoS attacks

Attack name	Type of threat		
	Confidentiality	Integrity	Availability
RTP/RTCP malformed messages			X
RTP/RTCP messages causing buffer overflow			X
RTP/RTCP message flooding (to open and closed ports)			X
RTP/RTCP session tear down (using RTCP bye)		X	X
RTP SSRC collision		X	X
RTCP forged reception report		X	X

"Denial of Service (DoS)" attacks

- RTP/RTCP-specific DoS attacks
  - RTCP "BYE", not in sync with the Signaling protocol
    - Result: The Signaling protocol is not aware that there is no exchange of voice samples any more
  - Forging Reception Reports
    - Reporting more Packet Loss
      - Result: usage of a poor quality codec with an adaptive system
    - Report more Jitter
      - Result: usage of a poor quality codec with an adaptive system

"Denial of Service (DoS)" attacks

- General DoS attacks

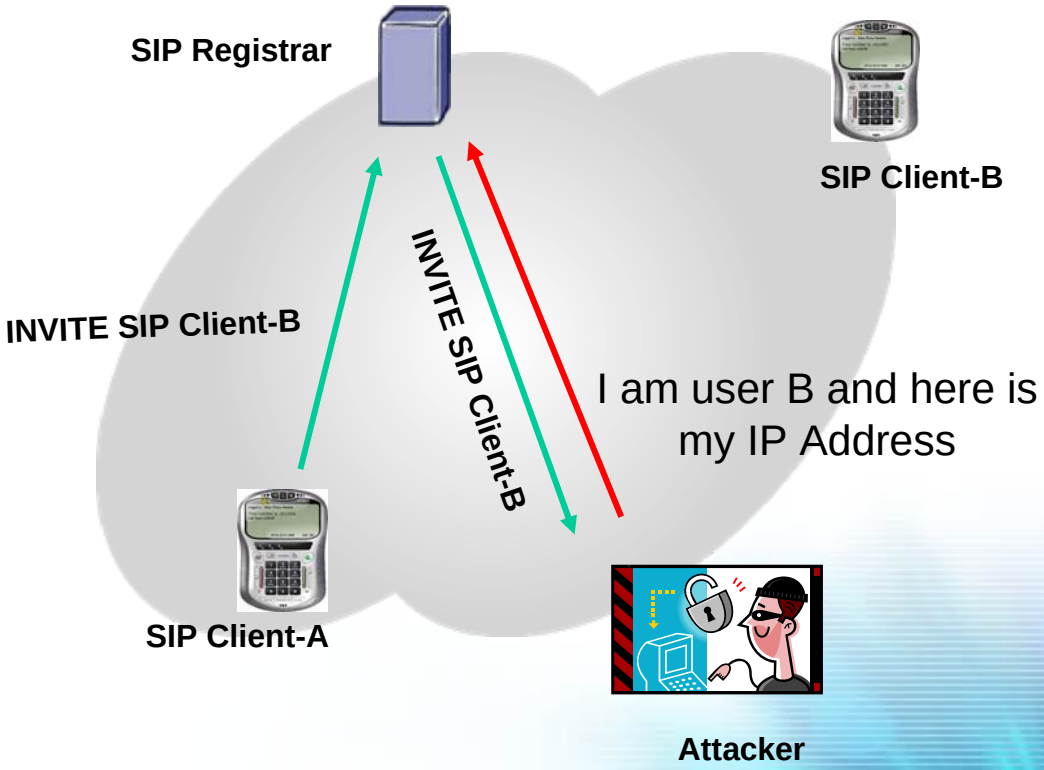
Attack name	Type of threat		
	Confidentiality	Integrity	Availability
Malformed packets			X
Packets causing buffer overflow			X
Packet flooding			X
Call tear down using ICMP error message		X	X
DHCP server impersonation	X	X	X
TFTP server impersonation	X	X	X

"Abuse of service" attacks

Attack name	Type of threat		
	Confidentiality	Integrity	Availability
Identity theft (registration hijacking)	X	X	X
Replay attack		X	X
Proxy impersonation	X	X	X
Bypassing refused consent		X	X
False caller ID		X	X
False capabilities to fool billing		X	X
Improper access to services		X	X
SPIT (SPam over Internet Telephony)		X	X

"Abuse of service" attacks

- Identity Theft
  - Registering address instead of other (if requires authentication might use another type of attack)



SPAM over Internet Telephony (SPIT)

- Same thread as with email (hundreds of calls just with publicity messages, the phone is ringing all day, etc.)
- SIP allows field forging (like with email)
- Problem increase with respect to traditional telephony
  - Cheaper call rates than traditional telephony
  - Flexibility of receiving calls from anywhere from anybody in the world
- Consequences are worse than with email
  - SIP voice call interrupts user immediately
  - And SIP is not voice only, but applies to Instant Messaging, and Presence too
  - Mailboxes become full over night
    - less means to distinguish “spam” and “ham”
- NEC Network Laboratories: Patent on SPIT avoidance submitted on June 2005

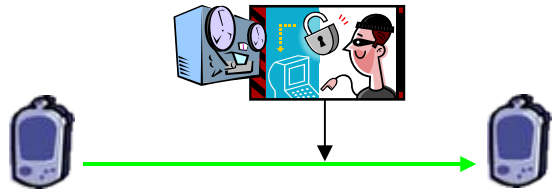
"Interception and modification" attacks

Attack name	Type of threat		
	Confidentiality	Integrity	Availability
Signaling spying	X		
Call content eavesdropping	X		
RTP play-out	X	X	X
Filtering	X	X	X
Key manipulation	X	X	X

"Denial of Service (DoS)" attacks

- RTP play-out

  - Same SSRC, higher sequence number, higher timestamp
    - Result: The fake content will be played before the real one
      - This means that from now on we will be able to play what ever we wish to this side of the conversation since all the next transmissions of the other side will look "old" to the receiving party



- Call Eavesdropping
  - Capturing RTP flows
    - Since RTP identifies the codec being used (statically) or either using a "dynamic" identified codec it is easy to reconstruct the voice sampling (even in real time)
    - Result: listen/record conversations
    - Result: listen DTMF tones to steal passwords and PINs

Need to be in the middle?

- It is not very difficult to get in the middle, and WLAN technology simplifies you the job
  - DNS (modify entries to point all traffic to a hacker's machine)
  - DHCP (make all traffic go to hackers machine as default gateway, or change DNS entry to point at hacker's machine so all names resolve to hacker's IP address)
  - ARP (reply with hacker's MAC address, gratuitous ARPs or regular ARP replies)
  - Flood tables in switches to destroy existing MAC addr/port associations so all traffic is broadcast out every port, and then use ARP attacks
  - Routing protocols (change routing such that traffic physically passes through a router/machine controlled by hacker)
  - Spanning tree attacks to change layer 2 forwarding topology
  - Physical insertion (e.g. PC with dual NIC cards, be it Ethernet-based or WLAN-based)

Existing security features within SIP Protocol

- Encryption
  - it can prevent a malicious user to read the SIP signaling (or part of it)
  - SIP signaling information can be used to launch an attack
  - the encryption itself can not do anything against dictionary attacks guessing the fields
- Encryption is useful for attacks like
  - Session tear-down (SIP-specific DoS attack)
  - Session hijacking (SIP-specific DoS attack)
  - Identity theft (Abuse of service attack)
  - Replay attack (Abuse of service attack)
  - Signaling spying (Interception and modification attack)
- Available solutions
  - hop-by-hop encryption
    - IPSec (protocol suite)
    - SIPS (SIP using Transport Layer Security, TLS, RFC 2246 currently being update at v1.1)
  - end-to-end encryption
    - S/MIME (Secure/Multipurpose Internet Mail Extensions), RFC 2633
- Cons
  - consumes time, introduces another delay
  - can introduce additional problems in NAT/FW traversal if no special means are adopted

Existing security features within SIP Protocol

- Authentication (mostly used only with REGISTER and INVITE, if you are lucky)
  - SIP signaling should be authenticated to deny access to not-authorized users
- Can help to prevent the following set of attacks:
  - Session tear-down (SIP-specific DoS attack)
  - Session hijacking (SIP-specific DoS attack)
  - SIP/SDP malformed methods (SIP-specific DoS attack)
  - SIP messages causing buffer overflow (SIP-specific DoS attack)
  - SIP methods flooding (SIP-specific DoS attack)
  - Identity theft (Abuse of service attack)
  - Replay attack (Abuse of service attack)
  - Proxy impersonation (Abuse of service attack)
  - Bypassing refused consent (Abuse of service attack)
  - Improper access to services (Abuse of service attack)
- Available solutions
  - Client to Server
    - Digest authentication, RFC 2617
    - S/MIME
  - Server to Server
    - IPSec
    - SIPS (works only in the "trapezoid" scheme)
- Cons
  - require trust relationship like a shared secret
  - there is no dynamic key exchange protocol established solution

Existing security features within SIP Protocol

- Identity framework in SIP
  - draft-ietf-sip-identity-05
    - each domain authenticate its own users
      - HTTP digest authentication
      - each client maintains a persistent TLS connection to the server (the client verifies the server identity using TLS) and make a digest exchange over TLS
    - the domain itself can assert the identity of the sender with a signature when relying the message from that user to another domain

Existing security features within RTP/RTCP Protocol

- Encryption and authentication
  - Secure Real Time Protocol (SRTP), RFC 3711 (not widely adopted yet)
    - Provides a framework for encryption and message authentication of RTP and RTCP streams
    - Default cryptographic transforms and possible additions
    - Has no pre-defined key management scheme
    - It is compatible with MIKEY (Multimedia Internet KEYing), RFC 3830,
      - does not need modifications when used with MIKEY
    - Can help to prevent the following set of attacks:
      - RTP/RTCP session tear down (RTP/RTCP-specific DoS attack)
      - RTP SSRC collision (RTP/RTCP-specific DoS attack)
      - RTCP forged reception report (RTP/RTCP-specific DoS attack)
      - Call content eavesdropping (Interception and modification attacks)
      - RTP play-out (Interception and modification attacks)
  - IPSec

- Cons
  - consumes time, introduces another delay
  - can introduce additional problems with Lawful Interception (LI) if no special means are adopted

Additional security features

- Pattern detection/prevention systems
  - the signatures or rules can be
    - deterministic models
    - statistical models
    - a combination of both
- Anomaly detection/prevention systems
  - auto-learning intelligence
- Better parsing
  - of SIP signaling
  - of RTP/RTCP messages

Considerations on VoIP management

- VoIP management is still in its infancy
  - Henning Schulzrinne, Columbia University, USA:
    - traditional management tools are of only limited help in this environment
  - which direction to take?
- What about of VoIP Security management?
  - maybe it is not yet born…
  - needs different solutions from the VoIP management?
  - if yes, which? which direction to take?

NEC Network Laboratories directions

- On-going works
  - VoIP Security applied to Session Border Controllers (SBCs)
    - Intrusion Detection/Prevention System
    - SPAM prevention
    - Lawful Interception
- Future directions (starting in 2nd Half of '05)
  - VoIP Security IPS (not limited to SBCs)
  - VoIP management
    - client/server configuration is complex
      - are MIBs enough?
        - » what is possible here?
    - can P2P help?
      - maybe more on the client side than on the server side
  - VoIP Security Management (servers need to be configured and queried from a security point of view)

Thank you!

Questions?