Junior Consulting

CONSEL

# Sicurezza dei servizi Voice over IP con SIP e RTP


**Program Manager:**
Francesco Limone
f.limone@elis.org

**Project Manager:**
Emilio Tonelli

**Team Members CONSEL:**
Sebastiano Di Gregorio
Matteo Mogno
Alessandro Tatti

TELECOM ITALIA
INFORMATION TECHNOLOGY

CONSEL
CONSORZIO ELIS
per la Formazione Professionale Superiore
Roma - Via S. Sandri, 45 - Tel. 06 4356041


Junior Consulting

CONSEL

## Contents



CONSEL

# Concept

**To:**

***Realizzazione di uno studio strategico sulla sicurezza del VoIP***

**In a way that:**

***Studio del VoIP***
***Realizzazione di un'architettura VoIP***
***Identificazione di attacchi in VoIP***
***Sperimentazione degli attacchi***

**So that:**

***Identificazione di un'architettura di riferimento per l'erogazione in sicurezza dei servizi multimediali basati su VoIP***



Junior Consulting

CONSEL

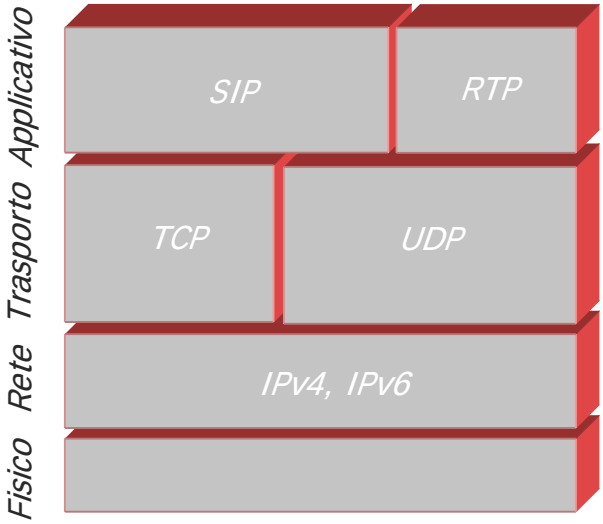
# Stadi del progetto

| Studio | | Analisi | Sviluppo | |
|---|---|---|---|---|
| 1.1 Voice over IP | 1.2 Aspetti di sicurezza | 2.1 Attacchi con SIP e RTP | 3.1 Sperimentazione | 3.2 Progettazione ALG |
| 29 Mar 04 | 19 Apr 04 | 6 Giu 04 | 4 Lug 04 | 27 Set 04 |

**Deliverables**

- *Technical Reports*
- *Diagrammi SDL dell'Application Level Gateway*

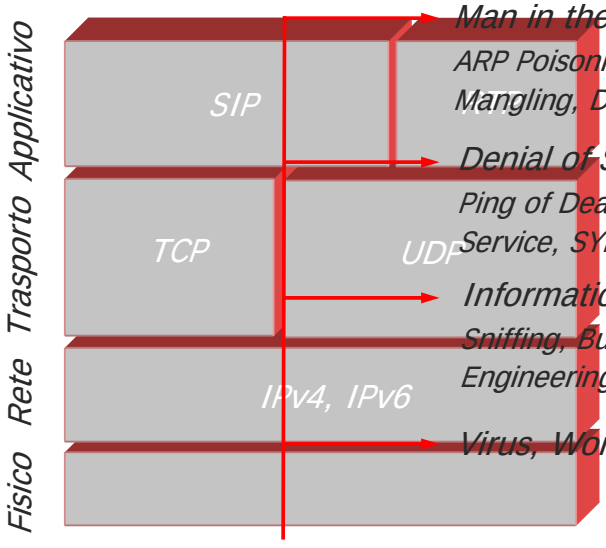
# Aspetti di sicurezza






Junior Consulting
1.1 Voice over IP | 1.2 Aspetti di sicurezza | 2.1 Attacchi con SIP e RTP | 3.1 Sperimentazione | 3.2 Progettazione ALG
CONSEL

# Aspetti di sicurezza




*Man in the Middle*

*ARP Poisoning, DNS Spoofing, DNS Poisoning, STP Mangling, DHCP Spoofing, ICMP Redirection*

*Denial of Service*

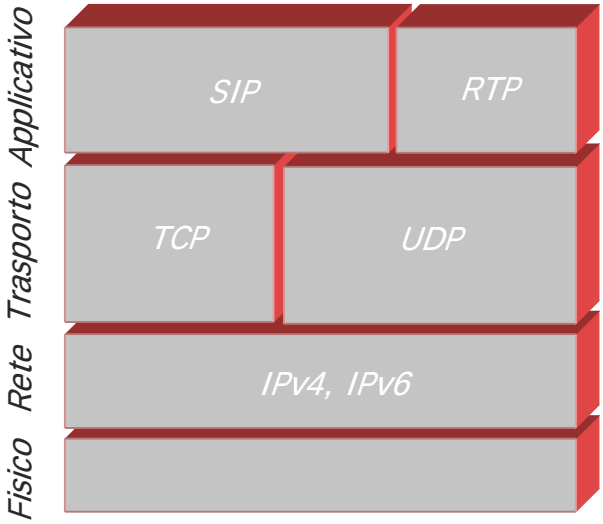
*Ping of Death, ICMP Smurfing, Distribuited Denial of Service, SYN Flood*

*Information Theft*

*Sniffing, Buffer Overflow, Password Cracking, Social Engineering, Code Injection*

*Virus, Worm, Trojan e Rootkit*

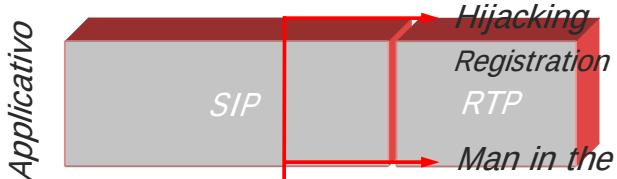
# Aspetti di sicurezza








# Attacchi SIP




*Hijacking*

*Registration Hijacking, 3XX Response Code Messages*

*Man in the Middle*

*Impersonating a Proxy Server, 302 and 305 Response Code Messages, Impersonating a Registrar Server*

*Denial of Service*

*Tearing down a session, Modifying a session, Cancelling a session, SIP DoS Attack and Amplification, Response Code Messages*

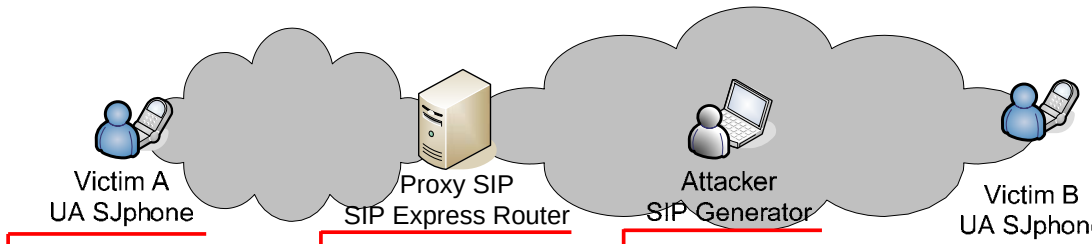
# Attacchi RTP

- *Man in the Middle*
  *Modifying IP address*
- *Denial of Service*
  *Malicious payload format, RTCP Timing Rules Incorrectly, Change Synchronization Source Field, BYE Attack, Sequence Number and Timestamp higher, Injecting Malicious Reception Reports*






# Sperimentazione




- *UA opensource di SJ Labs*
- *Proxy SIP di Iptel.org*
- *Sviluppo, attraverso il linguaggio C, di un generatore di messaggi SIP*

# Sicurezza in VoIP

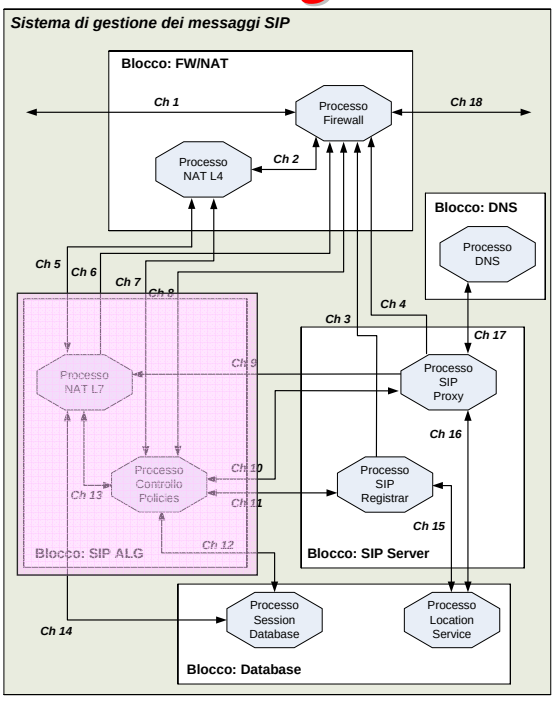
*Esigenze*

- *Risolvere il "problema Firewall"*
- *Risolvere il "problema NAT"*
- *Impedire gli attacchi con SIP*





# Progettazione del SIP ALG




*Processi del blocco SIP ALG:*

- Processo Controllo Policies
- Processo NAT L7



# Contents

- **Introduzione al progetto**
  - Concept
  - Scenario del progetto
  - Stadi del progetto
- Technology
- Conclusioni

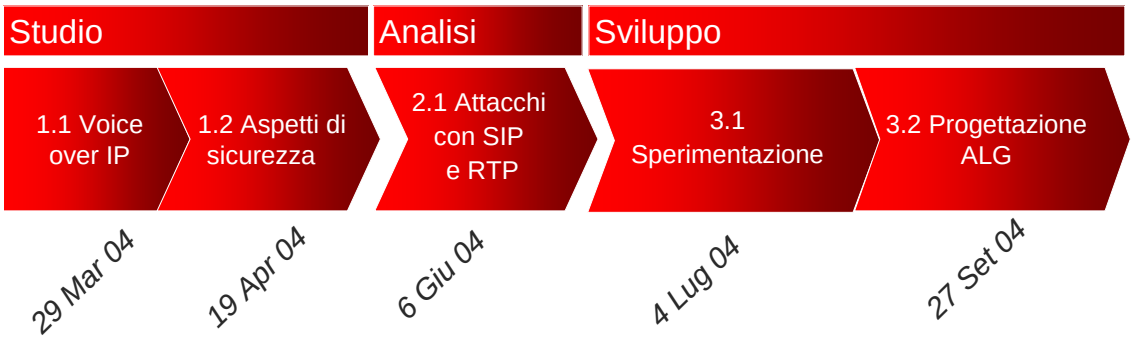




# Concept

| | |
|---|---|
| To: | ***Realizzazione di uno studio strategico sulla sicurezza del VoIP*** |
| In a way that: | ***Studio del VoIP***<br>***Realizzazione di un'architettura VoIP***<br>***Identificazione di attacchi in VoIP***<br>***Sperimentazione degli attacchi*** |
| So that: | ***Identificazione di un'architettura di riferimento per l'erogazione in sicurezza dei servizi multimediali basati su VoIP*** |

# Stadi del progetto




**Deliverables**

- *Technical Reports*
- *Diagrammi SDL dell'ALG*



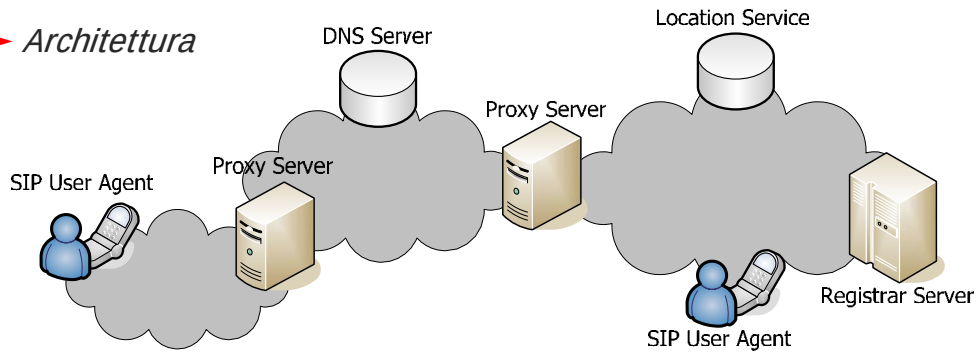


# Contents

# SIP

*Protocollo di segnalazione di tipo client-server di livello applicativo che permette di creare, modificare e terminare sessioni multimediali con uno o più partecipanti*

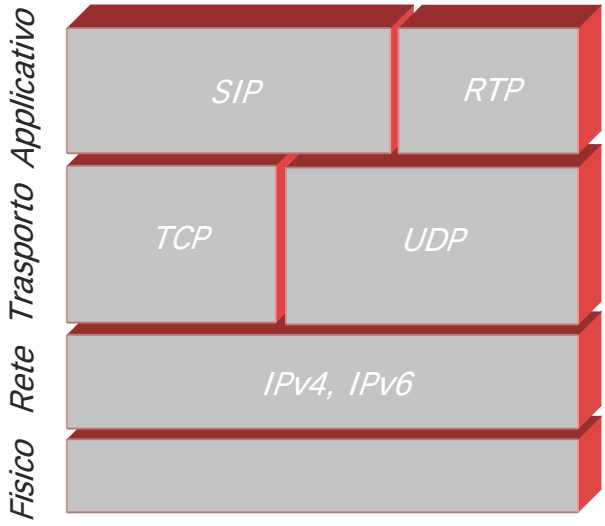
*Architettura*



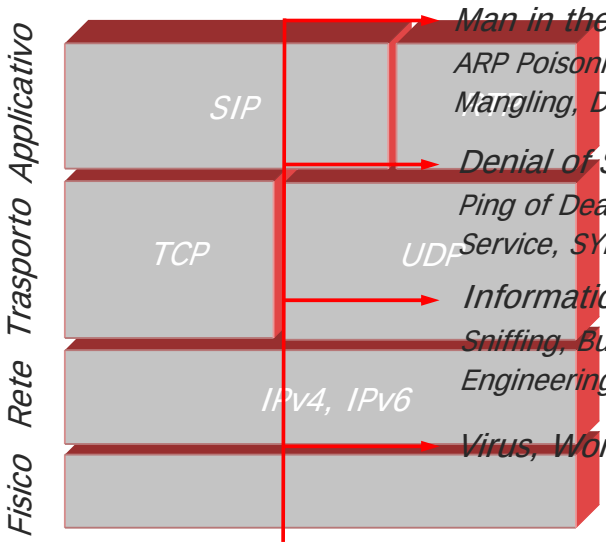





# Aspetti di sicurezza



# Aspetti di sicurezza




*Man in the Middle*

*ARP Poisoning, DNS Spoofing, DNS Poisoning, STP Mangling, DHCP Spoofing, ICMP Redirection*

*Denial of Service*

*Ping of Death, ICMP Smurfing, Distribuited Denial of Service, SYN Flood*

*Information Theft*

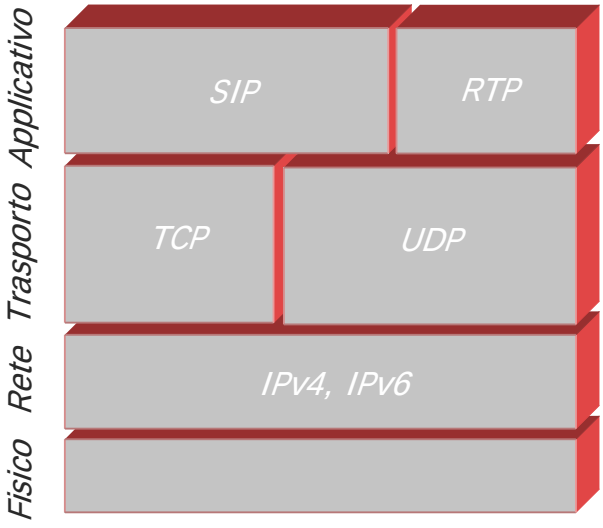
*Sniffing, Buffer Overflow, Password Cracking, Social Engineering, Code Injection*

*Virus, Worm, Trojan e Rootkit*

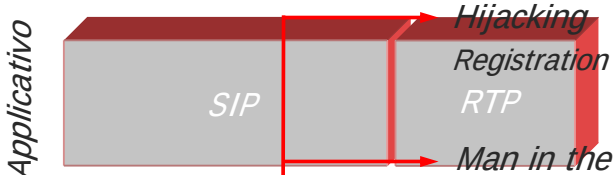


Junior Consulting
1.1 Voice over IP | 1.2 Aspetti di sicurezza | 2.1 Attacchi con SIP e RTP | 3.1 Sperimentazione | 3.2 Progettazione ALG

# Aspetti di sicurezza



# Attacchi SIP




*Hijacking*

*Registration Hijacking, 3XX Response Code Messages*

*Man in the Middle*

*Impersonating a Proxy Server, 302 and 305 Response Code Messages, Impersonating a Registrar Server*

*Denial of Service*

*Tearing down a session, Modifying a session, Cancelling a session, SIP DoS Attack and Amplification, Response Code Messages*





# Attacchi RTP

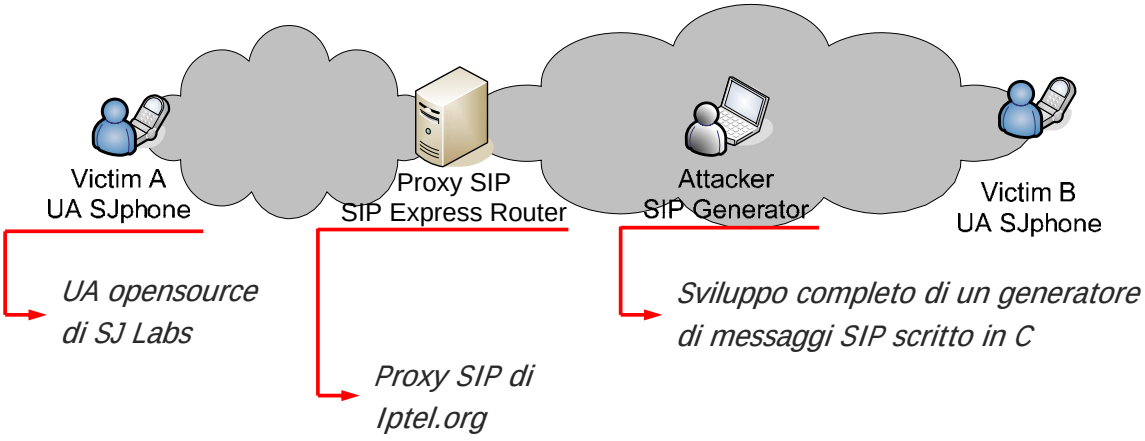
*Man in the Middle*

*Modifying IP address*

*Denial of Service*

*Malicious payload format, RTCP Timing Rules Incorrectly, Change Synchronization Source Field, BYE Attack, Sequence Number and Timestamp higher, Injecting Malicious Reception Reports*

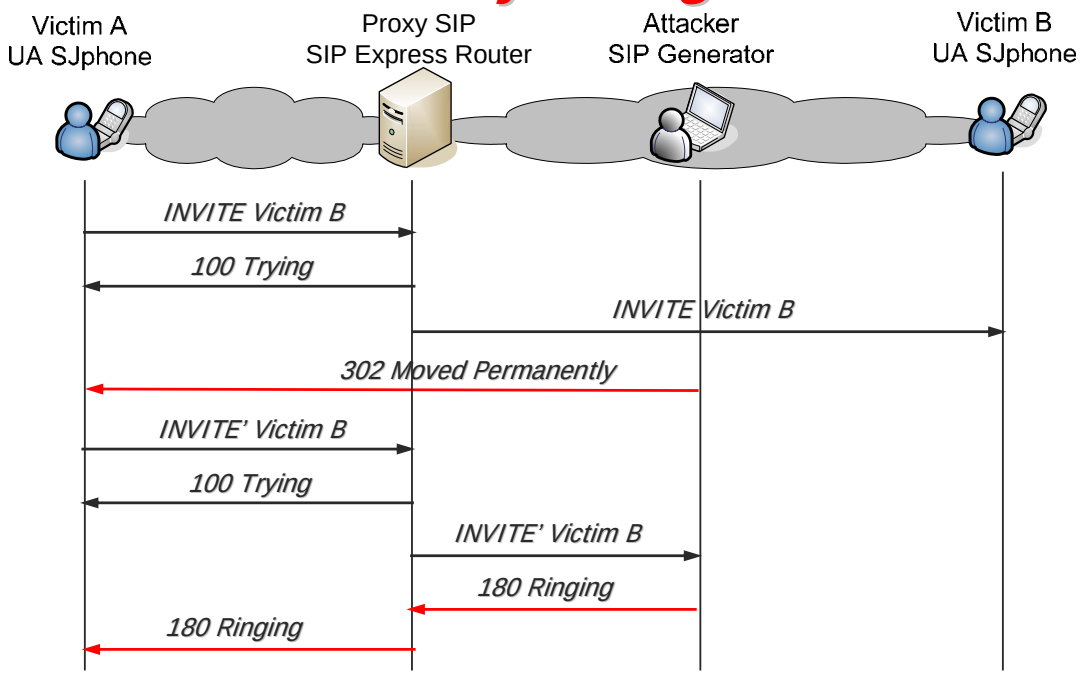
# Sperimentazione



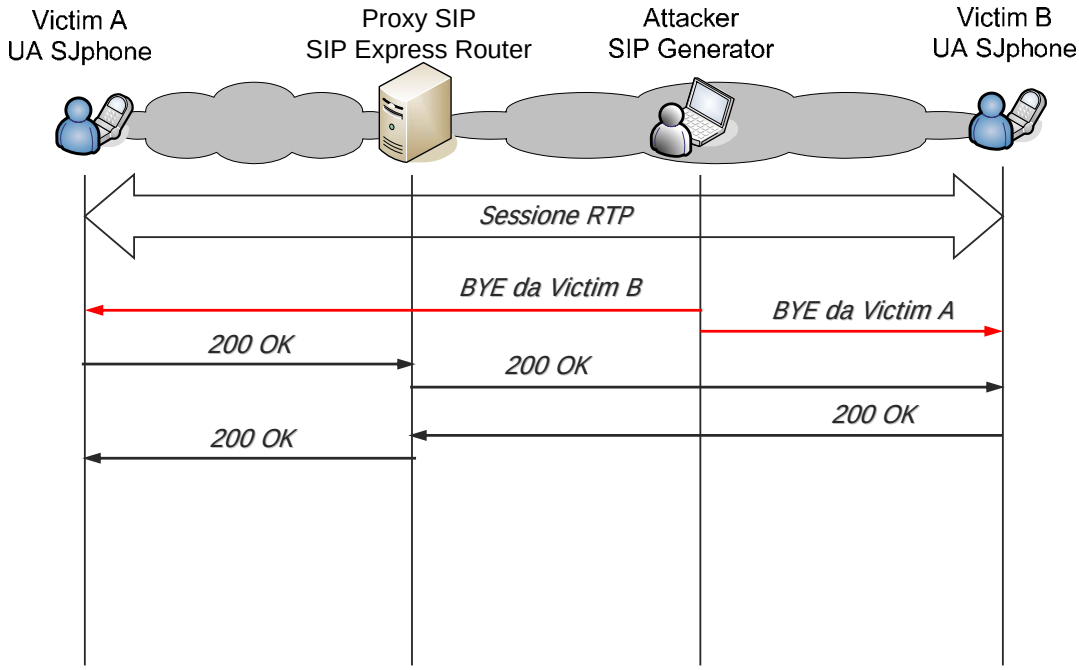





# Hijacking



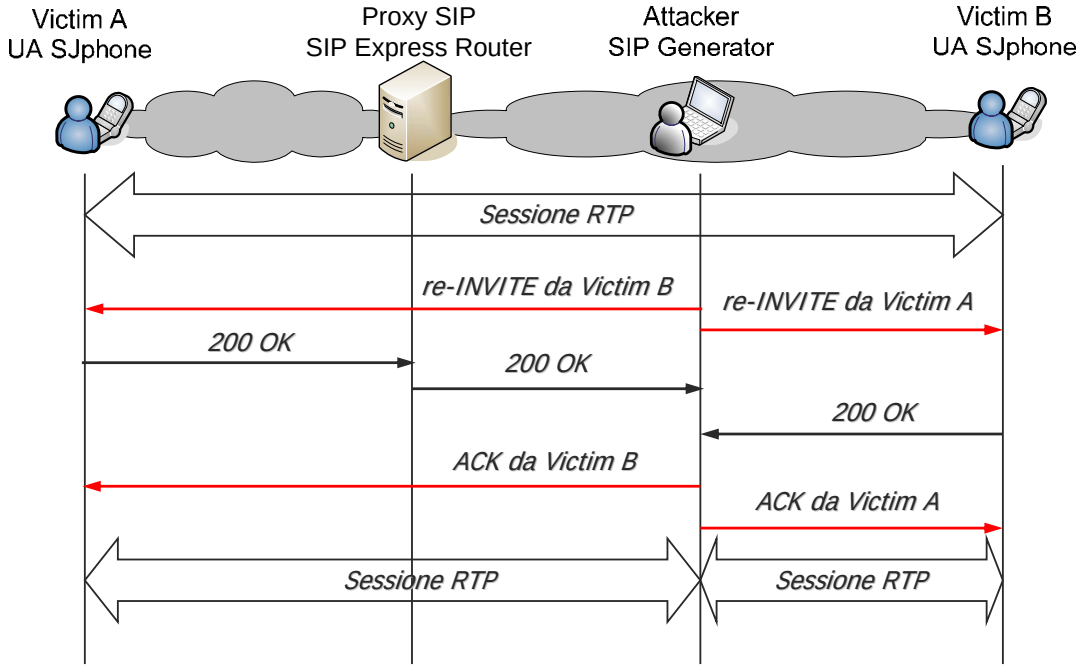
# DoS


Victim A
UA SJphone
Proxy SIP
SIP Express Router
Attacker
SIP Generator
Victim B
UA SJphone
Sessione RTP
BYE da Victim B
BYE da Victim A
200 OK
200 OK
200 OK
200 OK





# MitM RTP


Victim A
UA SJphone
Proxy SIP
SIP Express Router
Attacker
SIP Generator
Victim B
UA SJphone
Sessione RTP
re-INVITE da Victim B
re-INVITE da Victim A
200 OK
200 OK
200 OK
ACK da Victim B
ACK da Victim A
Sessione RTP
Sessione RTP

# Sicurezza in VoIP

*Esigenze*

- *Risolvere il "problema Firewall"*
- *Risolvere il "problema NAT"*
- *Impedire gli attacchi con SIP*

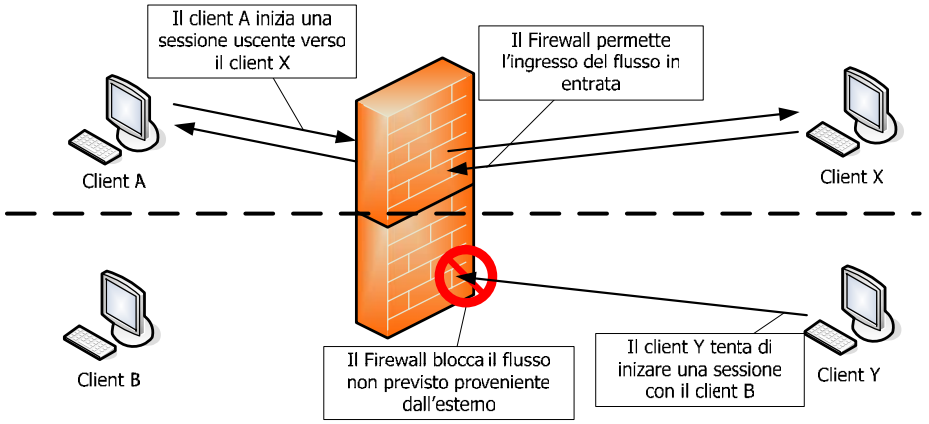


Junior Consulting
1.1 Voice over IP | 1.2 Aspetti di sicurezza | 2.1 Attacchi con SIP e RTP | 3.1 Sperimentazione | 3.2 Progettazione ALG
CONSEL

# Sicurezza in VoIP

*Esigenze*

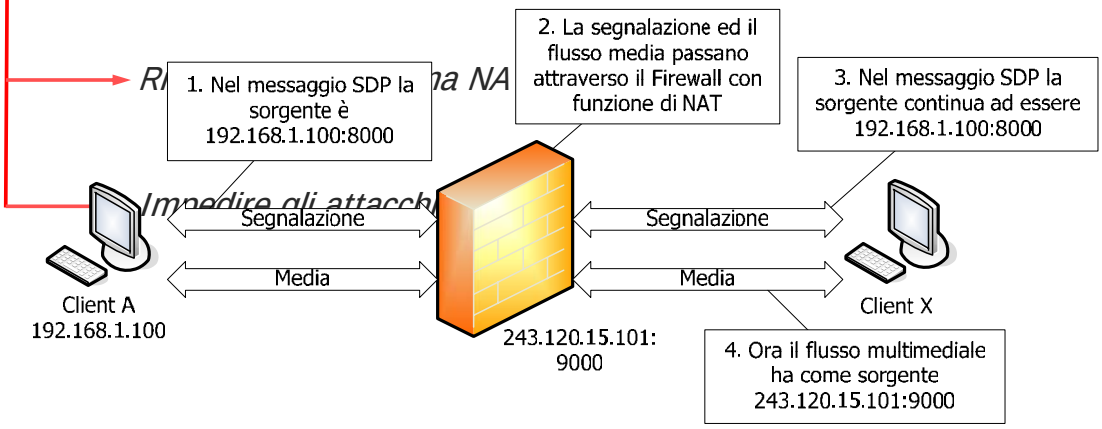
- *Risolvere il "problema Firewall"*



# Sicurezza in VoIP

*Esigenze*

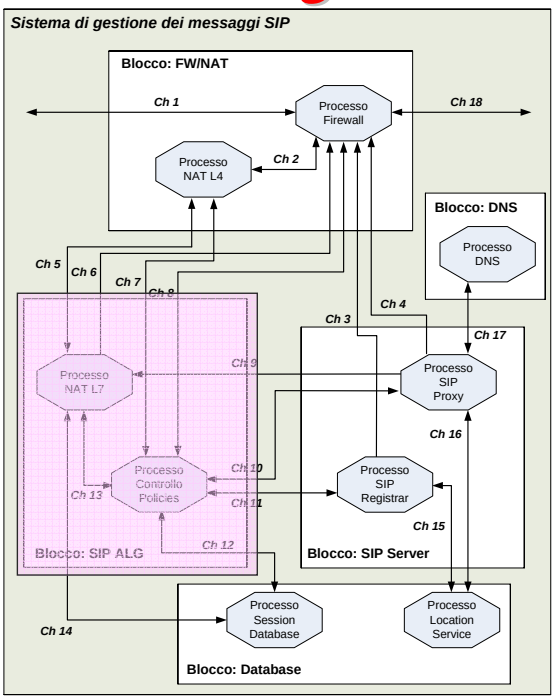
- *Risolvere il "problema Firewall"*
- *Ri… NA*
- *Impedire gli attacch…*



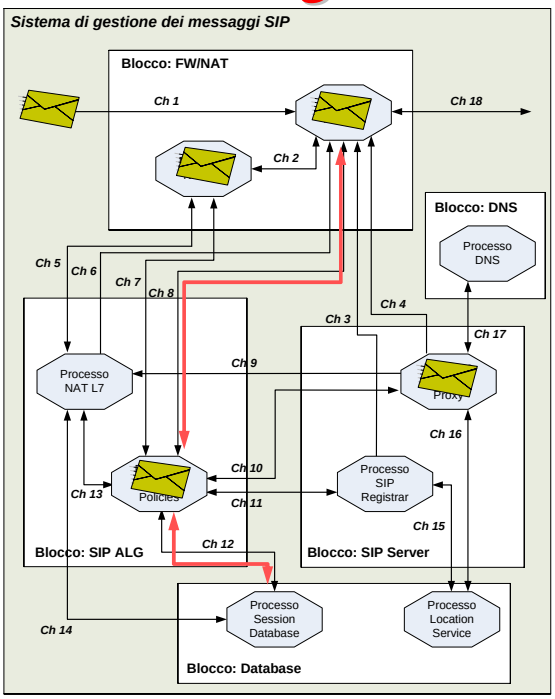





# Progettazione del SIP ALG



# Progettazione del SIP ALG




*Processi del blocco SIP ALG:*

Processo Controllo Policies

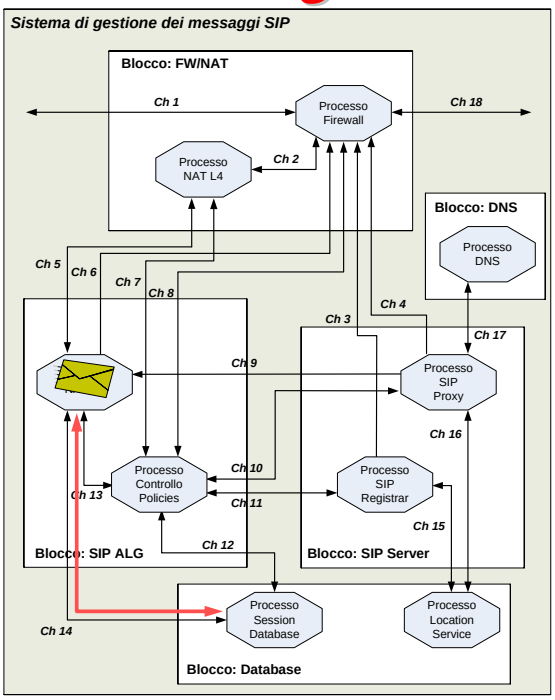
*Macchina a stati finiti estesa (EFSM):*

- *Gestire ogni messaggio SIP entrante o uscente dal dominio*
- *Verificare la corretta sequenzialità del messaggio all'interno del dialogo SIP*
- *Rilevare un eventuale tentativo di attacco*
- *Gestire l'apertura e la chiusura delle porte sull'interfaccia esterna del Firewall*
- *Aggiornare il processo Session DB*



Junior Consulting
1.1 Voice over IP | 1.2 Aspetti di sicurezza | 2.1 Attacchi con SIP e RTP | 3.1 Sperimentazione | 3.2 Progettazione ALG

# Progettazione del SIP ALG




*Processi del blocco SIP ALG:*

Processo NAT L7

*Macchina a stati finiti estesa (EFSM):*

- *Interrogare il processo Session DB*
- *Sostituire ogni occorrenza di indirizzi privati all'interno dei messaggi SIP e SDP con l'indirizzo pubblico dell'interfaccia esterna del firewall*
- *Sostituire ogni occorrenza della porta dello UA all'interno dei messaggi SIP e SDP con la porta assegnata dal NAT L4 sull'interfaccia esterna del firewall*



# Contents

- Introduzione al progetto
- Technology
- **Conclusioni**





# Conclusioni

- *Identificate le vulnerabilità e le minacce a cui sono esposte le soluzioni VoIP realizzate con SIP e RTP*
- *Identificati i "Problema Firewall" e "Problema NAT"*
- *Progettazione di una soluzione (SIP ALG) che risolve i problemi precedentemente esposti*

# Sviluppi Futuri

- *Valutazione delle prestazioni e controllo della QoS*
- *Sviluppo della compatibilità con servizi di Instant Messaging*
- *Sviluppo di un protocollo standard per l'interazione tra processi SIP e processi Firewall*