

# Attacks in SIP

Manos Antonakakis, [manos@cc.gatech.edu](mailto:manos@cc.gatech.edu)

## ***“Survey of Security Vulnerabilities In SIP”***

*D. Geneiatakis, G. Kabourakis, C. Lambrinoudakis and S. Gritzalis,  
University of the Aegean*

*S. Ehlert and D. Sisalem, Fraunhofer Fokus Institute*

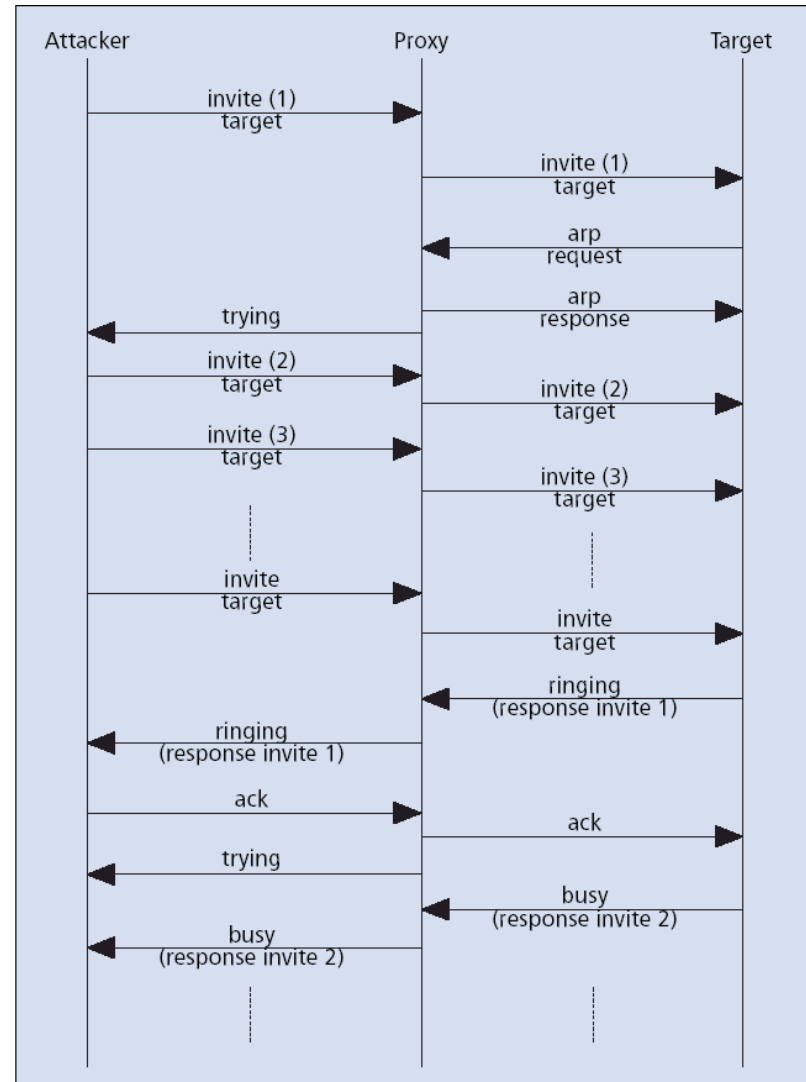
# Available Security Mechanisms

- SIP Authentication
  - HTTP Digest authentication (RFC 2617)
- IPsec and SIP
  - IP is vulnerable to spoofing, session hijacking, eavesdropping
  - IPsec, ESP – AH: Confidentiality, integrity, anti-replay, data oriented authentication and protection against eavesdropping
- Authentication, authorization, Accounting Services in SIP
  - Authentication during handshaking and IPsec security
- S/MIME and SIP
  - PKI for MIME messages
    - Ensures C.I.A
    - Requires a global PKI infrastructure



# DoS Attacks in SIP II

- Flooding the Proxy Server and End-User
  - INVITE msg: One of the most utilized in SIP
  - Until the connection is complete the SIP proxy must keep the connection state for 3 min (RFC 3261)
  - How: The attacker will try to DoS the proxy and/or target with different INVITE scenarios



# SIP Parser Attacks

- Parser attacks
  - SIP as a text based protocol provides highly degree of freedom
  - Long messages (by adding additional headers)
  - Poor implementation – No 413 message capability
  - Parser Servers should check:
    - Message soundness and proper size
    - Reject long messages – 413 message
    - Disable TCP connections – this will prevent TCP Dos type of attacks

```
From: ...
To: ...
Contact: <sip:user1@sip.org>
Contact: <sip:user2@sip.org>
Contact: <sip:user3@sip.org>
Contact: <sip:user4@sip.org>
Call-ID: ...
CSeq: ...

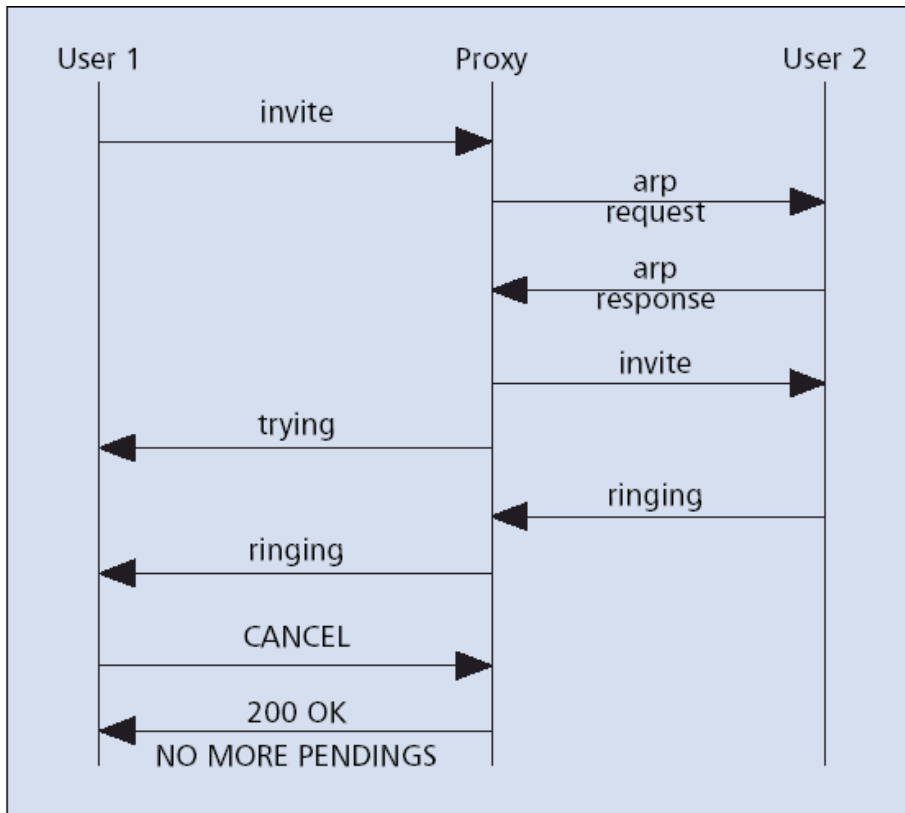
From: ...
To: ...
Contact: <sip:user1@sip.org>
Contact: <sip:user2@sip.org>
Contact: <sip:user3@sip.org>
Contact: <sip:user4@sip.org>
Call-ID: ...
CSeq: ...

Contact: <sip:user1@sip.org>
From: ...
Contact: <sip:user2@sip.org>
To: ...
Contact: <sip:user3@sip.org>
Call-ID: ...
CSeq: ...
Contact: <sip:user4@sip.org>
```

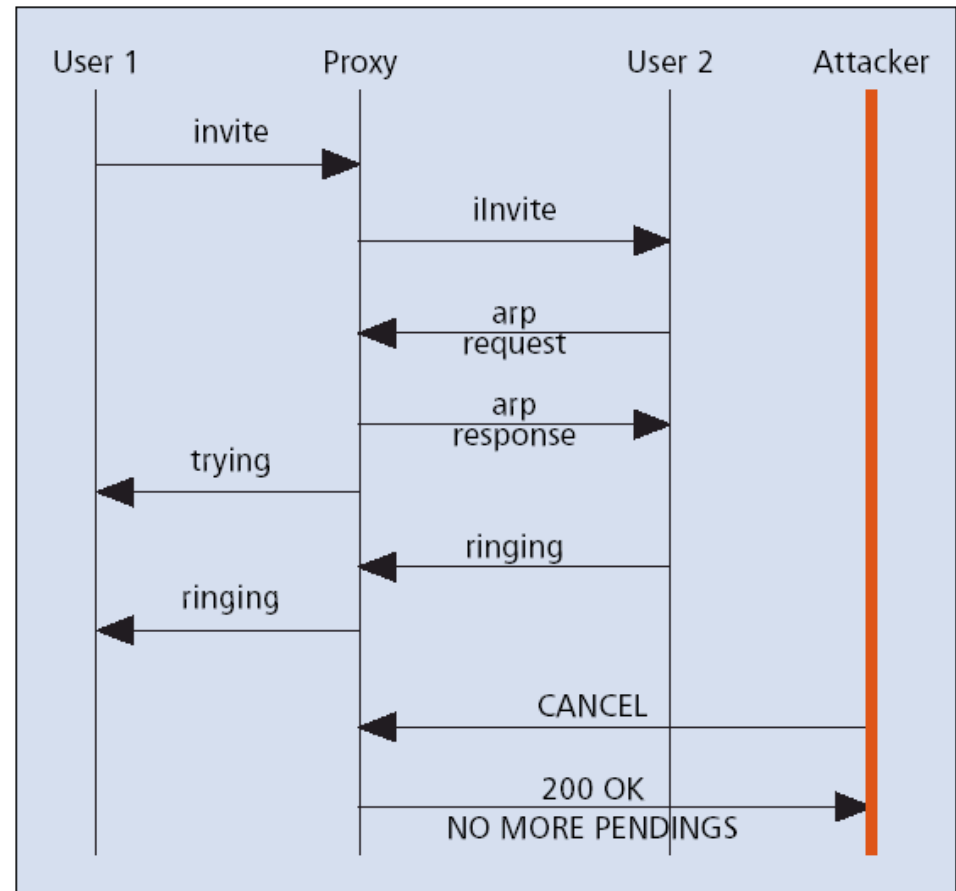
# SIP Application Level Attacks I

- Attacks based on SIP signaling
  - ❑ The “BYE” attack
  - ❑ The “CANCEL” attack
  - ❑ The “REFER” attack
  - ❑ The “Re-INVITE” attack
  - ❑ The “UPDATE” attack
  - ❑ The “INFO” attack

# The “CANCEL” attack in detail



Normal “CANCEL” request



Attack on “CANCEL” request

# SIP Application Level Attacks II

- SQL Injection attack in SIP
  - ❑ SIP relies on DBs in order to store user credentials
  - ❑ Important for authentication process
    - subscriber table
    - location table
  - ❑ SQL injection in SIP similar to WWW injection
  - ❑ This attack take place usually during user authentication

*At the SIP Proxy during the UA credential verification*

```
SELECT password FROM subscriber WHERE user-  
name='gkar' AND realm='195.251.164.23'
```

*Insert malicious code in the AH*

```
Authorization:Digest username="gkar";  
Update subscriber set first_name='malicious'  
where username='gkar'--",  
realm="195.251.164.23", algorithm="md5",  
uri="sip:195.251.164.23",  
nonce="41352a56632c7b3d382b5f98b9fa03b",  
response="a6466dce70e7b098d127880584cd57"
```

*The select will fail but not the update*

```
SELECT password FROM subscriber WHERE user-  
name= 'gkar';
```

```
UPDATE subscribe SET first_name='malicius'  
WHERE username='gkar'—
```

# Attacks in SIP - Summary

Threat/attack	(A)ctive/ (P)assive	(I)nternal/ (E)xternal	(S)ingle/ (M)ulti	(D)irect / (I)ndirect	Vulnerability	Affected Security Issue	Possible consequences
Registrar flooding	A	I-E	S-M	D-I		Av-R	DoS
Proxy flooding	A	I-E	S-M	D-I		Av-R	DoS
End user flooding	A	I-E	S-M	D-I	Lack of authentication	Av-R	DoS
Route/record route attack	A	I	M	I	Lack of (1) authentication, (2) integrity checking	I-Av-R	DoS
SIP parser attack	A	I-E	S	D	Implementation errors	Av-R	DoS, UnA
BYE attack	A	I-E	S	D	Lack of authentication	Av	DoS
Cancel attack	A	I-E	S	D	Lack of authentication	Av	DoS
Refer attack	A	I-E	S	D	Lack of authentication	C-I-Av	UnA
Re-invite attack	A	I-E	S	D	Lack of authentication	Av-C-R	UnA, DoS
Update attack	A	I-E	S	D	Lack of authentication	Av-R	DoS
Info attack	A-P	I-E	S	D	Lack of (1) authentication, (2) integrity checking (3) Confidentiality	Av-R-C-I	DoS, UnA
SQL injection attack	A	I-E	S	D	Lack of integrity checking	I-Au-Av	UnA, DoS

---

## Open research questions – Possible projects ideas

- Covert channels detection in VoIP – First we have to create one!
  - Security schema for improving the Mutual Authentication of the end client and the SIP Server.
  - VoIP security over wireless networks
-