SURVEY OF SECURITY VULNERABILITIES IN SESSION INITIATION PROTOCOL

洪胤勛

Outline

- VoIP security issue

- SIP security

- Media security

- Solution

VoIP security issue

- PSTN rely on closed network

- VoIP is based on an open environment

- VoIP inherit vulnerabilities from underlying transport protocols

  - IP, UDP, TCP

VoIP security issue

- Some security mechanisms have been proposed for SIP-based infrastructures, but vulnerabilities still exist
- Exhaust available resources
- Discover vulnerabilities in the applications

SIP security (DoS)

- Denial of Service (DoS), interruption/destruction of service provisioning
- Distributed Denial of Service (DDoS), use multiple computers to paralyze the target system
  - flood target's bandwidth
  - consume target's resources

SIP security (DDoS)

- Flooding Registrar Server
- Attacker launches an attack against a REGISTRAR by employing lots of **registration requests**
  - Guess legitimate users' passwords
 - Cause a DoS in the SIP registrar

SIP security (DDoS)

- Flooding Proxy Server and End-User Terminal
- Attacker launches several **SIP INVITE**
  - SIP proxy must keep the connection state until redirect transaction has been replied
  - Parazyle proxy server & end user
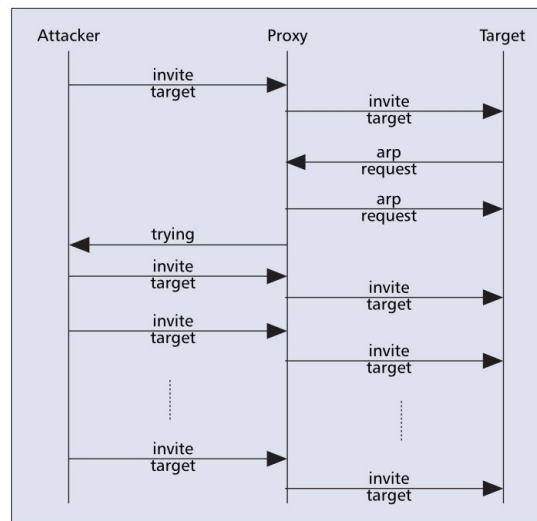
**Figure 6.** *Flood with INVITE messages.*

SIP security (Parser Attack)

- SIP is a text-based protocol, so an efficient parser is important
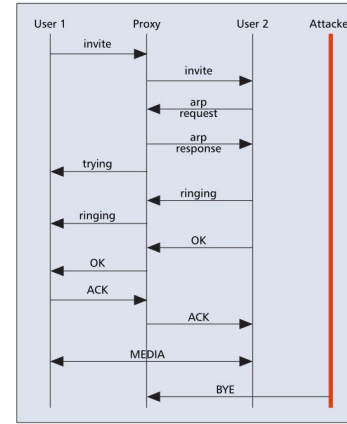- Some message headers are vital for processing (e.g. To, Via, etc.)
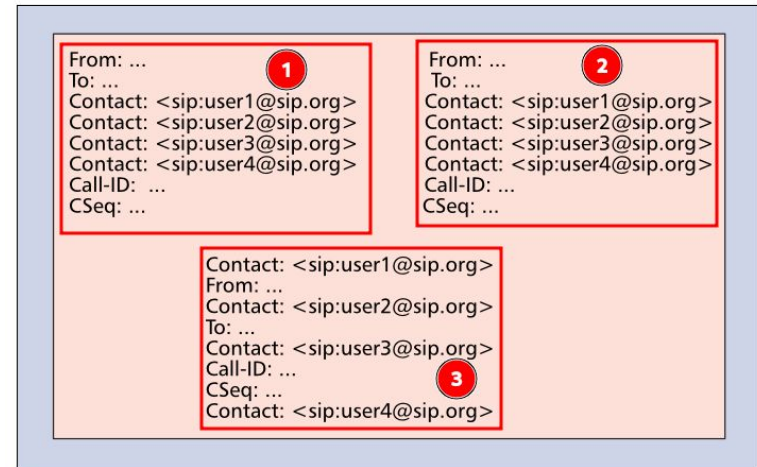
Figure 8. *Multiple header possibilities.*
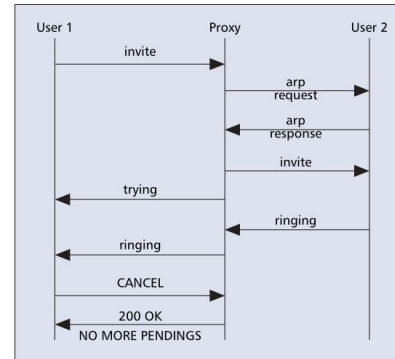
8

SIP security (Application Attack)

- BYE/CANCEL Attack
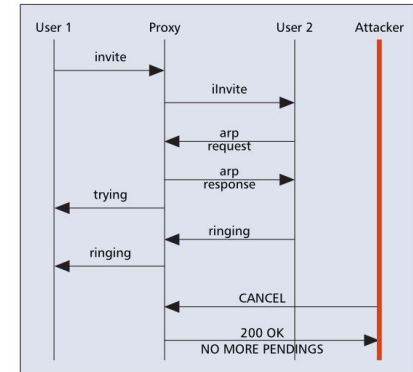- Attacker needs to learn all necessary session parameters Session-ID, RTP Port, etc.
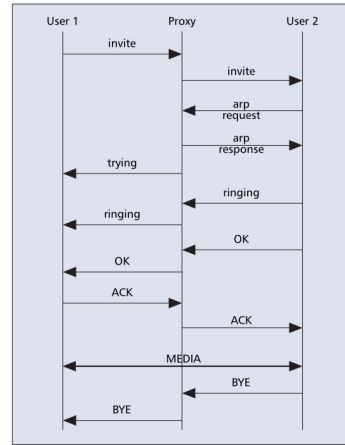
Figure 9. *Normal session termination.*
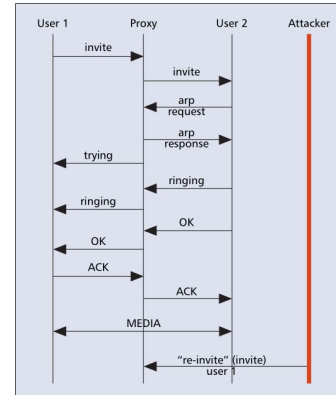

Figure 10. *BYE attack.*

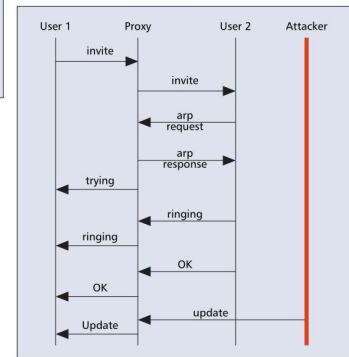**Figure 11.** *CANCEL request.*

Figure 12. *CANCEL attack.*

9

SIP security (Application Attack)

- Re-INVITE/UPDATE Attack
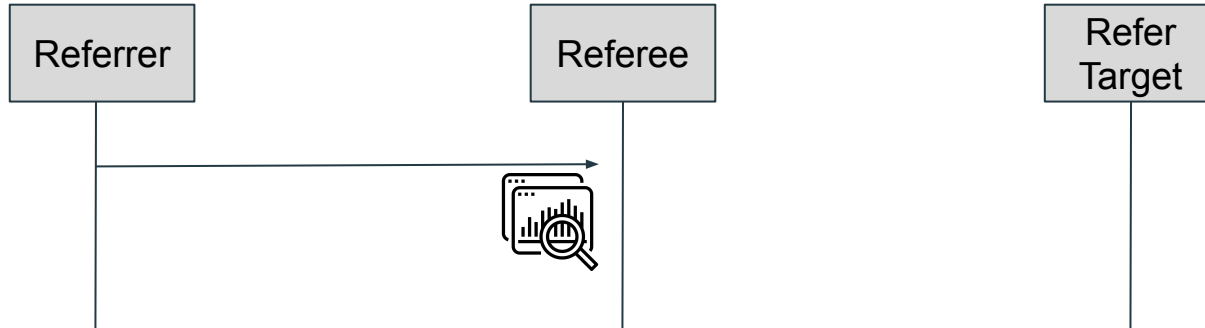- Modify the parameters of the dialog-session

Figure 13. *"Re-INVITE" attack.*

Figure 14. *UPDATE attack.*

10

SIP security (Application Attack)

- REFER Attack
- MITM(Man In The Middle) attacks

SIP security (Application Attack)

- SQL Injection Attack
- SIP relies on databases such as MySQL, Postgress, etc. to store administer user credentials and appropriate data (e.g. user name, password)
- The utilization of WEB interfaces for the provision of SIP services makes this attack more attractive

SQL injection example

- User need input username and password

- ```
  SELECT password FROM subscriber WHERE username=?;
  ```

- bob; UPDATE subscriber SET password=abc WHERE username=bob

```
SELECT password FROM subscriber WHERE username=bob;
UPDATE subscriber SET password=abc WHERE username=bob;
```

Media security

- RTP doesn't provide any mechanisms for eavesdropping(竊聽) or other attacks. (Not encrypted)

Solution (Enctryption)

- Prevent eavesdropping
- IPsec (Internet Protocol Security)
- TLS (Transport Layer Secure)
- S/MIME (Secure Multipurpose Internet Mail Extensions)
- SRTP (Secure RTP)
  - SRTP encrypts only payload of a voice packet without adding additional encryption headers

Solution (AAA)

- Authentication
  - Identifying a user
- Authorization
  - Determining user privilege
- Accounting
  - Monitors/Control the resources a user consumes

Solution (SIP Parser, SQL)

- Server Application Side
  - Check if the input is malicious
- Database API
  - Only one SQL statement can be executed during one system call
- Database Side
  - Restrict user permissions

Solution (Flooding)

- None of the underlying security mechanisms to prevent SIP flooding
- Ban malicious users

Conclusion

- Easy
  - Eavesdropping, Forge(偽造)
- Medium
  - Parser, SQL Attack
- Hard
  - Flooding Attack

Thank you for your listening!