Mitigating SIP security threats with OpenSIPS

- workshop -

Liviu Chircu

OpenSIPS Developer

OpenSIPS Solutions

Mitigating SIP security threats with OpenSIPS

- workshop -

Outline

- unregister attack
- replay attack
- plaintext attack
- brute force attack
- SIP scanners
- malicious message fields
- social engineering
- fraud patterns

Mitigating SIP security threats with OpenSIPS

- workshop -

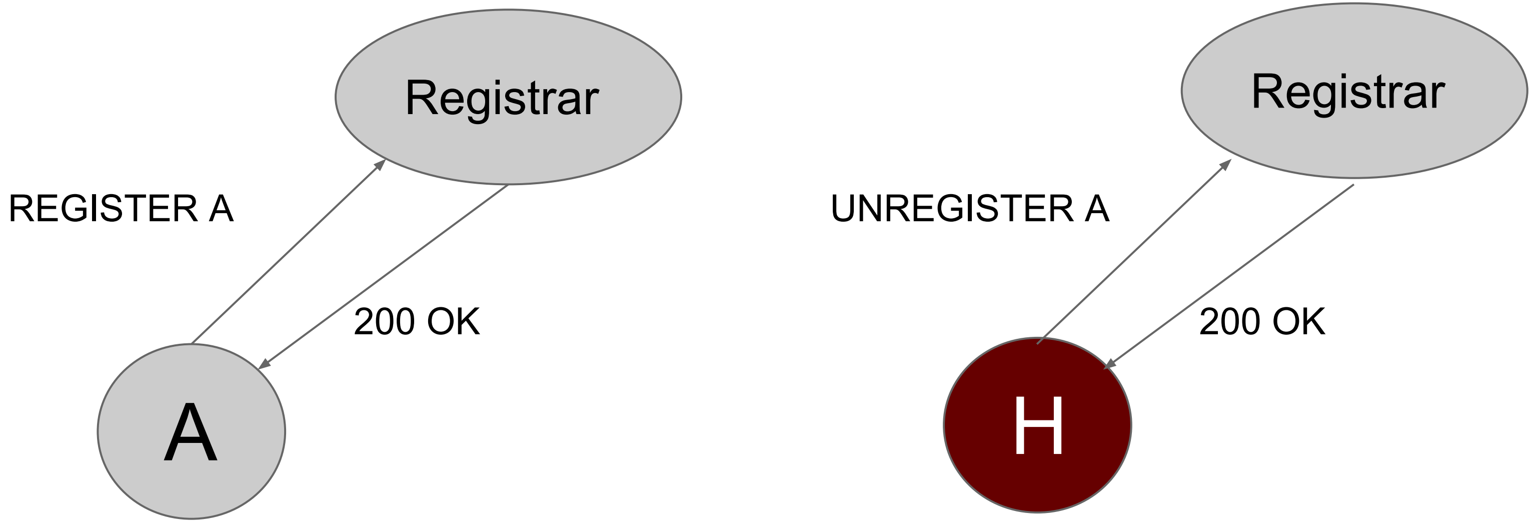
Unregister attack

- SIP security 101
- assumes a free-for-all type of platform

Mitigating SIP security threats with OpenSIPS

- workshop -

Unregister attack



Mitigating SIP security threats with OpenSIPS

- workshop -

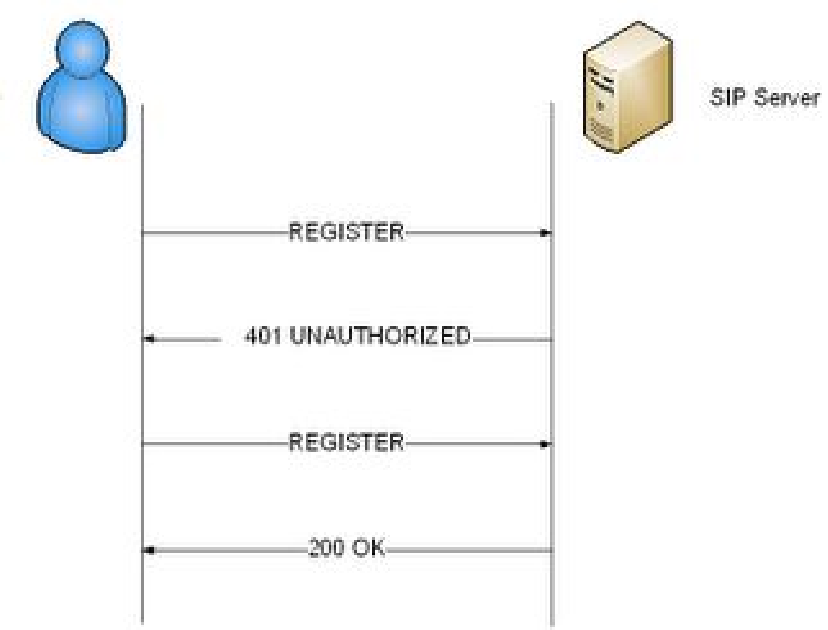
Digest authentication

- RFC 2617, written a century ago (1999), obsoleted by 7616 (sep 2015)
- allows clients to share a **password** with servers
- used by SIP and HTTP

Mitigating SIP security threats with OpenSIPS

- workshop -

Digest authentication



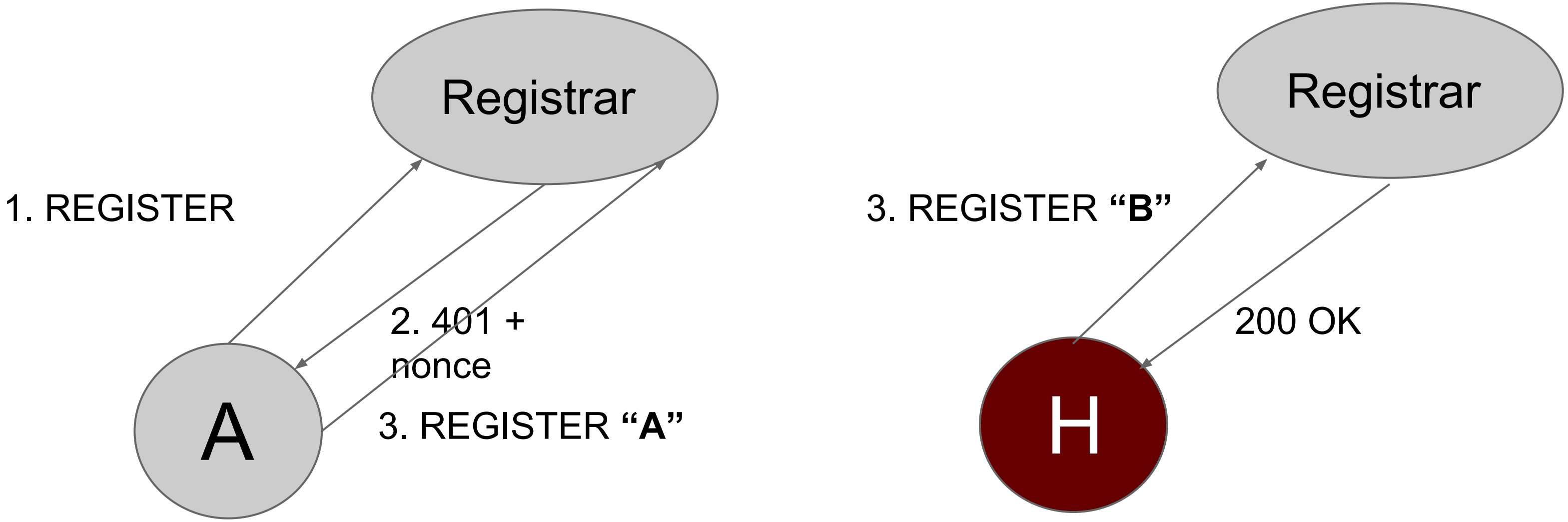
Replay attack

- attacker sniffs authenticated request (e.g. REGISTER)
- while server challenge is valid, he sends similar request (“replays it”)

Mitigating SIP security threats with OpenSIPS

- workshop -

Replay attack



Mitigating SIP security threats with OpenSIPS

- workshop -

Replay attacks and OpenSIPS

- nonce re-usage disabled by default

Plaintext attacks

- attacker intercepts traffic
- builds a “nonce: response” table for a given user
- eventually, he will be able to match any input nonce

Plaintext attacks: mitigation

- RFC 2617 includes Quality of Protection (“qop=” header param.)
- forces client to generate and use a nonce as well (“cnonce=”)
- attacker now has to populate N lookup tables: *unfeasible*!

Mitigating SIP security threats with OpenSIPS

- workshop -

Plaintext attacks and OpenSIPS

- *www_challenge(realm, **qop**)*
- *proxy_challenge(realm, **qop**)*
- tradeoff between compatibility and security

“**real life**” (*SIP security definition*):

when RFC 2617 cannot help you anymore!

Mitigating SIP security threats with OpenSIPS

- workshop -

Brute force attacks

- relentless attempts at guessing a subscriber's password
- should not be ignored - people tend to use bad passwords
- can be seen as DoS attempts

Mitigating SIP security threats with OpenSIPS

- workshop -

Brute force attacks and OpenSIPS

- expiring cache entry per subscriber
- limits amount of retries within the given interval

- scripting demo -

SIP scanners

- (distributed) software which scans for SIP port 5060
- traffic should be blacklisted / absorbed (should not reply)

SIP scanners and OpenSIPS

- validate the *“User-Agent”* header field
- *dialplan* module (regex matching, update w/o restarting proxy)

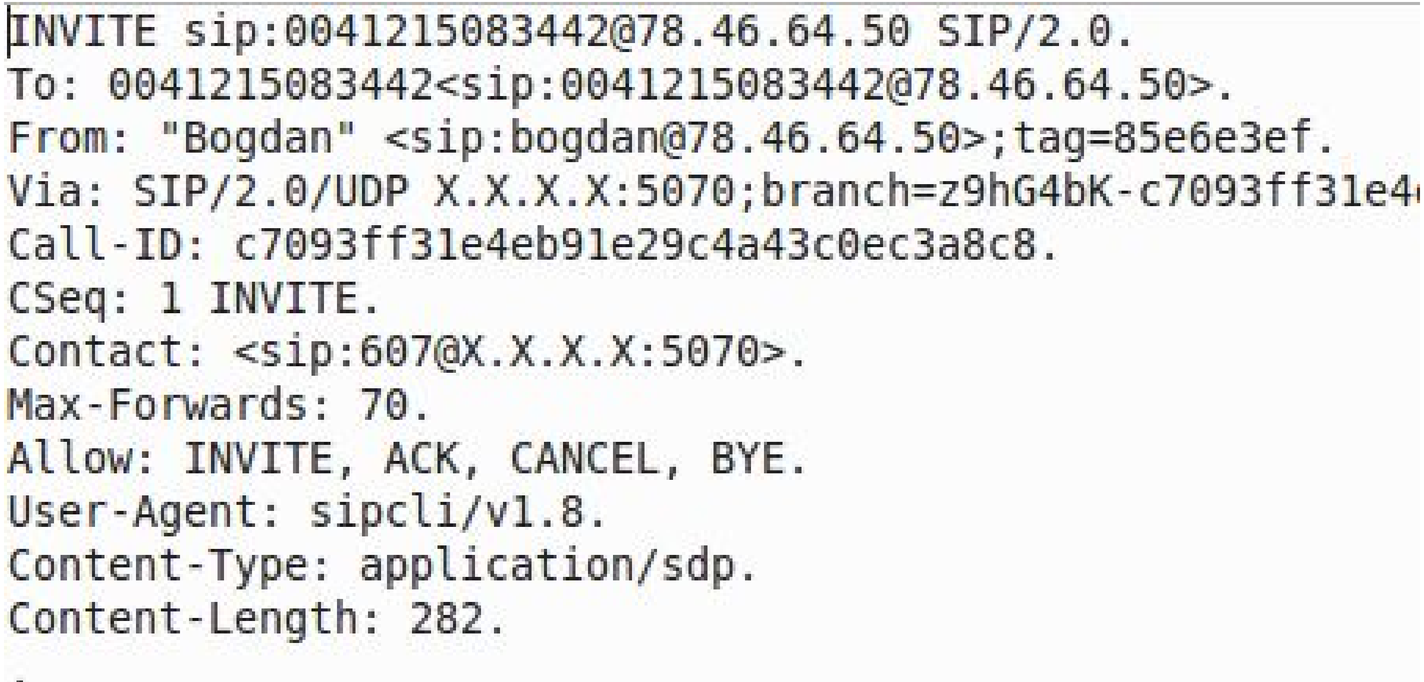
- scripting demo -

Mitigating SIP security threats with OpenSIPS

- workshop -

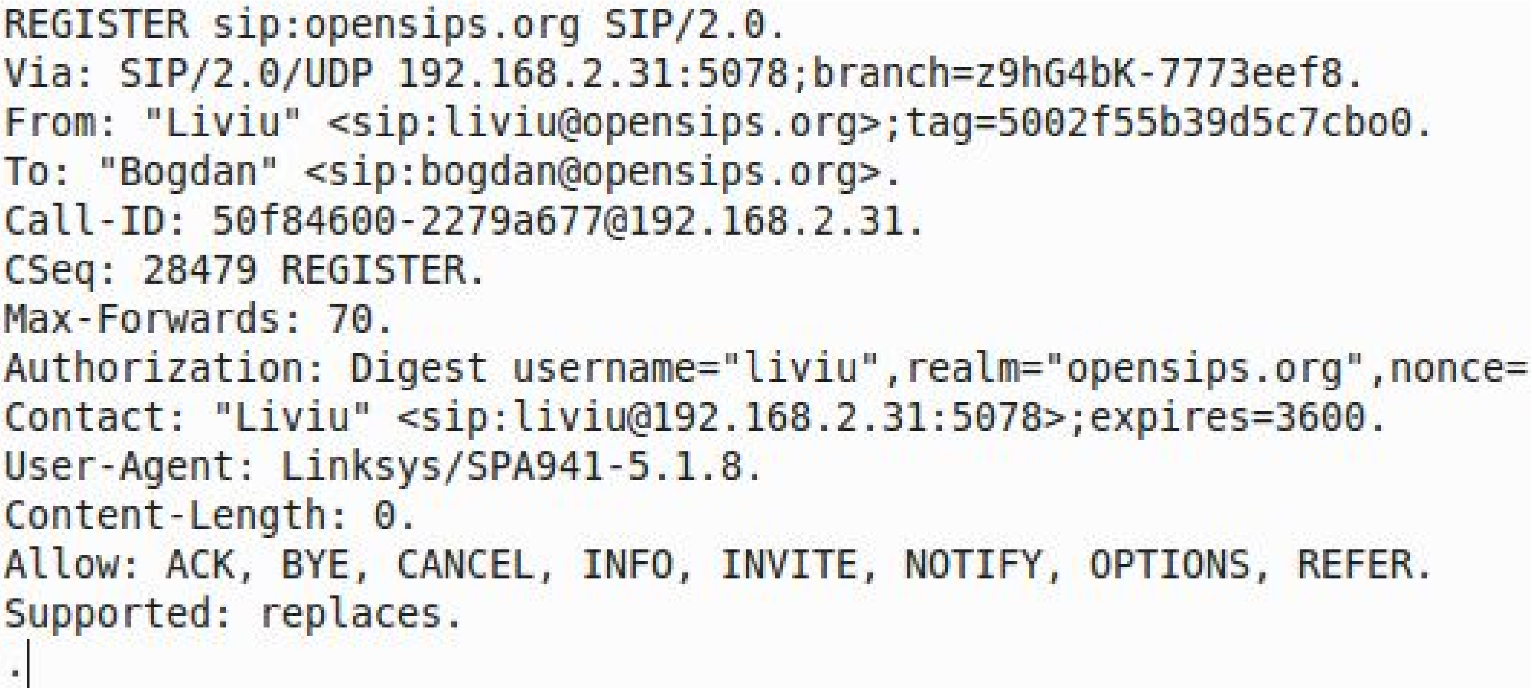
Up next...

Malicious messages - fake SIP usernames (From header)



```
INVITE sip:0041215083442@78.46.64.50 SIP/2.0.
To: 0041215083442<sip:0041215083442@78.46.64.50>.
From: "Bogdan" <sip:bogdan@78.46.64.50>;tag=85e6e3ef.
Via: SIP/2.0/UDP X.X.X.X:5070;branch=z9hG4bK-c7093ff31e4
Call-ID: c7093ff31e4eb91e29c4a43c0ec3a8c8.
CSeq: 1 INVITE.
Contact: <sip:607@X.X.X.X:5070>.
Max-Forwards: 70.
Allow: INVITE, ACK, CANCEL, BYE.
User-Agent: sipcli/v1.8.
Content-Type: application/sdp.
Content-Length: 282.
```

Malicious messages - fake SIP usernames (To header)



```
REGISTER sip:opensips.org SIP/2.0.
Via: SIP/2.0/UDP 192.168.2.31:5078;branch=z9hG4bK-7773eef8.
From: "Liviu" <sip:liviu@opensips.org>;tag=5002f55b39d5c7cbo0.
To: "Bogdan" <sip:bogdan@opensips.org>.
Call-ID: 50f84600-2279a677@192.168.2.31.
CSeq: 28479 REGISTER.
Max-Forwards: 70.
Authorization: Digest username="liviu",realm="opensips.org",nonce=
Contact: "Liviu" <sip:liviu@192.168.2.31:5078>;expires=3600.
User-Agent: Linksys/SPA941-5.1.8.
Content-Length: 0.
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER.
Supported: replaces.
.
```

Malicious messages - fake SIP usernames and OpenSIPS

- db_check_from()
- db_check_to()
- included by default in “Residential” configuration script

Mitigating SIP security threats with OpenSIPS

- workshop -

Malicious messages - FQDNs in “Contact” header URI

- attacker may insert a domain pointing to internal GWs / other registrars
- regex matching

- scripting demo -

Mitigating SIP security threats with OpenSIPS

- workshop -

Malicious messages - FQDNs in Request-URI

- attacker may insert a R-URI domain pointing to internal GWs / other registrars
- blacklists

- scripting demo -

Mitigating SIP security threats with OpenSIPS

- workshop -

Social engineering

- stolen passwords
- easy passwords (e.g. “1234”)
- handing over passwords to untrusted sources

Mitigating SIP security threats with OpenSIPS

- workshop -

Social engineering: match INVITE src IP with REGISTER src IP

- reduces losses caused by stolen passwords
- OpenSIPS 2.2+: is_ip_registered(), *registrar* module
- others: use local cache and store “contact_domain_port: srcIP” mappings

Mitigating SIP security threats with OpenSIPS

- workshop -

Social engineering: employ fraudulent pattern detection

- reduces losses caused by stolen passwords
- *fraud_detection* module
  - warning/logging system
  - monitor *cpm, totalc, cdur, cc, seqc*
  - provision various thresholds for ^ into DB (can be grouped too!)
- detailed tutorial available on opensips.org/Documentation/Tutorials

Mitigating SIP security threats with OpenSIPS

- workshop -

Conclusions

- SIP, as any other VoIP protocol, is a lot more insecure due to the open nature of IP networks, as opposed to PSTN
- every new SIP extension always always introduces new security holes that a knowledgeable attacker may exploit
- for each possible security threat, there is always at least one solution!

  (to be demonstrated…)

Asynchronous operations with OpenSIPS 2.1

- workshop -

Resources

- latest OpenSIPS manual
  - opensips.org/Documentation/Manual-2-2

- RFC 2617
  - ietf.org/rfc/rfc2617.txt

Asynchronous operations with OpenSIPS 2.1

- workshop -

?