The #1 Issue on VoIP, Fraud!

How to identify, prevent and reduce damages caused by fraud

Flavio E. Goncalves
About me

• Author of the book “Building Telephony Systems with OpenSIPS”

• CEO of sippulse.com a turnkey OpenSIPS solution for Telcos and Hosted PBX.

• Member of the OpenSIPS foundation.
Agenda

1. How big is the problem?
3. Types of attacks
4. Mitigation techniques
5. How to reduce damage if all previous measures failed

Warning: This presentation is about VoIP fraud, there are many security issues, such as DOS and Eavesdropping not covered here!
How big is the problem?

• June, 2009 – announced it had broken up a $55 million toll fraud ring that was operating internationally and targeting enterprise PBXs
  Source: Network World

• December, 2010 – 11 million Euros on VoIP Fraud, calling to premium numbers in Somalia, Sierra Leone....
  Source: SipVicious Blog
Anatomy of a simple attack.

Step 1 – Buy a Premium Rate Number

Step 2 – Find a vulnerable VoIP device
And call the premium rate number

Step 3 – Cash-out in the premium number
<table>
<thead>
<tr>
<th>ID</th>
<th>Country</th>
<th>Range</th>
<th>Payout</th>
<th>Currency</th>
<th>Paymentterms</th>
<th>Testnumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000252</td>
<td>ALBANIA</td>
<td>355</td>
<td>0,09</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>355 511 810 62</td>
</tr>
<tr>
<td>5000246</td>
<td>ANTARCTICA</td>
<td>88234</td>
<td>0,2</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>88.234.607.76</td>
</tr>
<tr>
<td>5000333</td>
<td>AUSTRIA</td>
<td>43810959</td>
<td>0,03</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>43.810.959200</td>
</tr>
<tr>
<td>5000153</td>
<td>AUSTRIA</td>
<td>438208931</td>
<td>0,1</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>43.820.893100</td>
</tr>
<tr>
<td>5000331</td>
<td>AUSTRIA</td>
<td>4382094</td>
<td>0,1</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>43.820.893000</td>
</tr>
<tr>
<td>5000156</td>
<td>AUSTRIA</td>
<td>438208930</td>
<td>0,09</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>43.820.893000</td>
</tr>
<tr>
<td>5000199</td>
<td>AUSTRIA</td>
<td>438101043</td>
<td>0,07</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>43.810.104300</td>
</tr>
<tr>
<td>5000364</td>
<td>BELARUS</td>
<td>37560</td>
<td>0,07</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>375.602.605279</td>
</tr>
<tr>
<td>5000414</td>
<td>BULGARIA</td>
<td>3599997</td>
<td>0,08</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>359.999.753.498</td>
</tr>
<tr>
<td>5000354</td>
<td>BULGARIA</td>
<td>3599997</td>
<td>0,13</td>
<td>USD</td>
<td>7 / 1 days</td>
<td>359.999.726499</td>
</tr>
<tr>
<td>5000253</td>
<td>BURKINA FASO</td>
<td>226</td>
<td>0,11</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>226 507 700 12</td>
</tr>
<tr>
<td>5000339</td>
<td>BURUNDI</td>
<td>2577485</td>
<td>0,09</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>257.748.55000</td>
</tr>
<tr>
<td>5000272</td>
<td>CENTRAL AFRICAN REPUBLIC 2</td>
<td>236</td>
<td>0,13</td>
<td>EUR</td>
<td>7 / 1 days</td>
<td>236.217.50010</td>
</tr>
<tr>
<td>5000074</td>
<td>CHAD</td>
<td>309500</td>
<td>0,06</td>
<td>USD</td>
<td>7 / 1 days</td>
<td>309.500.000000</td>
</tr>
</tbody>
</table>
Common ways to get a password

1. SIP Scan and Brute force
2. TFTP attacks
3. Phone vulnerabilities
4. Signaling Attacks
5. PBX web interface vulnerabilities
Under Heavy Attack!

- **Basic Scan** – sipvicious, friendly-scanner
- **Distributed SCAM by W32.Sality virus** (discovered by Symantec/2010)

Thousands of Corporate PBXs

Source: Symantec

http://www.symantec.com/connect/blogs/distributed-cracker-voip
SIP Scan Mitigation

• Mandatory strong passwords
  – 8 digits minimum, special chars...

• Detect multiple authentication failures
  – Block IP with Fail2Ban
  – Block IP with Event Interface (OpenSIPS 1.7)

• Early detection and discard
  – Detect specific signatures and patterns
Signaling Attacks

• Malformed BYEs.

- Malformed BYEs:
  - SIP Proxy: Bye with wrong Cseq/Routing Set
  - Radius Server: Generate incorrect duration on CDR
  - SIP: Bye with wrong Cseq
  - Radius Server: Generate incorrect duration on CDR

• Example:
  - By IP phone
  - SIP Proxy: Bye with wrong Cseq/Routing Set
  - SIP: Bye with wrong Cseq
  - Radius Server: Generate incorrect duration on CDR
  - Radius Server: Generate incorrect duration on CDR

- Result:
  - BYE DETECTED
  - STOP BILLING!!
  - WRONG CSEQ
  - DISCARD!!
Mitigation for Signaling Attacks

• Dialog Aware Proxy

```c
if (has_totag()) /*sequential requests*/
if (!validate_dialog())
    fix_route_dialog();
```
TFTP Attack

• Trivial Attack against VoIP Infrastructure
  – 1\textsuperscript{st} Option bruteforce tftp server
  – 2\textsuperscript{nd} Option sniff tftp files using MitM techniques

Get file 0001234A5B6C.cfg
Get file 0001234A5B6D.cfg

Plaintext Configuration File
With credentials in plain text
XML or not

Solution

– Use HTTPS or Encrypted config files
Attacks on SIP Phones

• How many of you change the default password for IP phones?
• How many of you update the IP Phone’s firmware regularly?
More sophisticated attacks

- SIP Digest Leak

1. INVITE in Mute
2. 200OK, User Answered
3. BYE, No Audio?
4. 401, WWW-Authenticate?
5. BYE, With Phone Credentials

Current estimated time needed to break all 8 chars length passwords

1. [a-zA-Z0-9]{1,8} ... 497 days
2. [a-z0-9]{1,8} ...... 6 days

Credits to Sandro Gaudio: blog.sipvicious.org
Mitigation for phone attacks

- Don’t allow http/ssh access to the phones
- Disable the web interface when possible.
- Prefer secure automatic provisioning
- Standardize phones, update regularly.
- For SIP Digest Leak, drop 401 or 407 originated by subscribers.
Malformed Packets

• Attack
  – Malformed packets can be used to exploit buffer overflows on phones.
    • Tools: Protos TEST suite

• Mitigation
  – Detect malformed packets using OpenSIPS
    • Use Error_route to generate alerts
    • Handle exceptions
  – Use the event interface or fail2ban to ban the offenders

failregex= Auth Error for .* from <HOST> cause -[0-9] Malformed SIP request from user .* from <HOST>
TLS and SRTP

- Not very effective against fraud
- TLS is not used for authentication in most cases
- TLS can help to avoid MitM attacks
- SRTP and ZRTP protect you against eavesdropping, but do not prevent a fraudulent call to a premium rate number
What OpenSIPS can offer to help you?

- Subscribers
- Security and Admission Box
  - Event and Alerting System
  - Firewall Layer
- VoIP Infrastructure
What OpenSIPS can offer?

- TLS and protocol translation
- Nonce re-usage prevention
- PIKE to detect spikes in req/s
- Rate-Limit to throttle SIP traffic
- Access any SIP header for sanity checks
  - Signature detection
- Use the new event interface
  - Predefined events E_PIKE_BLOCKED
  - raise_event(event_name[, attrs] [, vals])
- Connect the event interface to a firewall and/or alerting system
- Global Blacklists for premium rate numbers
Tips to prevent attacks

1. Use strong passwords
2. Detect and drop specific signatures
3. Ban IPs with authentication or malformed failures
4. Drop 401 and 407 from subscribers
5. Validate sequential requests, mainly BYEs
6. Use secure provisioning for phones
7. Do not allow unsecure external access to your system
8. Update phones regularly
9. Use TLS when possible to avoid MitM attacks
10. Use a secure network
   1. ARP Inspection
   2. Secure voice VLAN
Damage Control

• Face a simple fact, sooner or later, a system open to the Internet will be compromised.

• The hacker’s advantage
  – Administrators have to defend against all attacks, while one vulnerability is enough for the attacker!
  – The administrator is one, attackers are many!
Tips to reduce possible damages?

1. Do not allow all routes to all users.
2. Block premium-rate numbers (1-900)
3. Do not route numbers without a defined rate
4. Limit the number of simultaneous calls
5. Drop calls after a certain period of time.
6. Prefer prepaid, for postpaid use quotas
7. Consider geo-ip restrictions for customers
8. Build an alert system for unusual patterns
9. Use two-way authentication for high-risk routes
Thank You!

Next OpenSIPS eBootcamp September 19th
Learn OpenSIPS!

Visit www.sippulse.com, a turnkey solution based on OpenSIPS

Questions and contact, please send an email to flavio@sippulse.com or flavio@opensips.org