“Know your enemy”
Sun Tzu's The Art of War

The #1 Issue on VoIP, Fraud!

How to identify, prevent and reduce damages caused by fraud

Flavio E. Goncalves

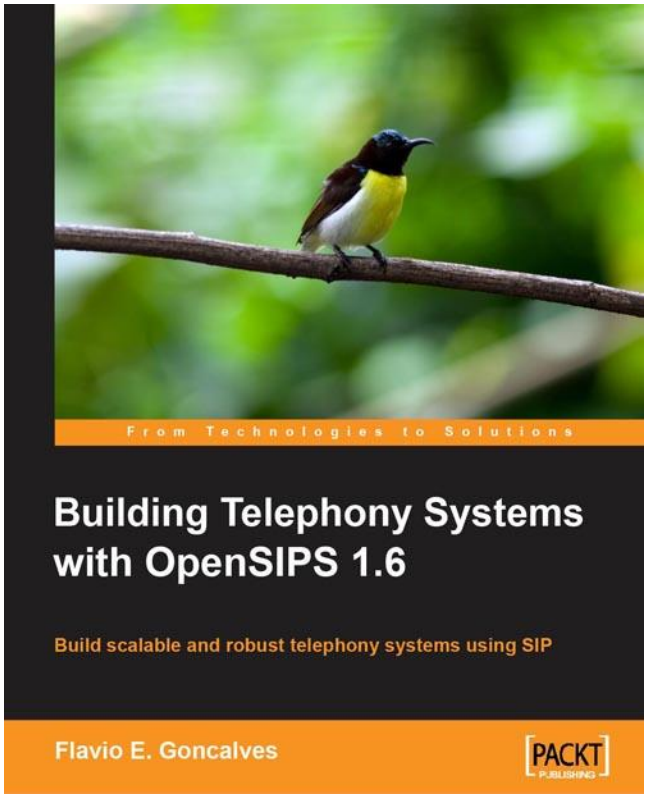
SIP Platform

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?
2. Anatomy of an attack.
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?

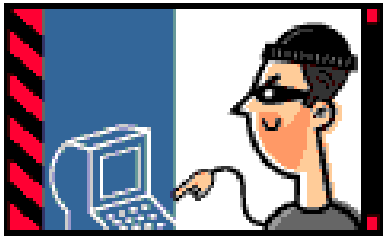
- *June, 2009 – announced it had broken up a $55 million toll fraud ring that was operating internationally and targeting enterprise PBXs*

  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

How do I get started?

DOWNLOAD CONTRACT

Fill in contract and return via email

DOWNLOAD

ORDER NUMBER

Number will work within 1 hour

ORDER

START EARNING MONEY NOW!

CONTACT US

Great solution - Try it | New Country | Payout increased | Payout decreased | additional info available

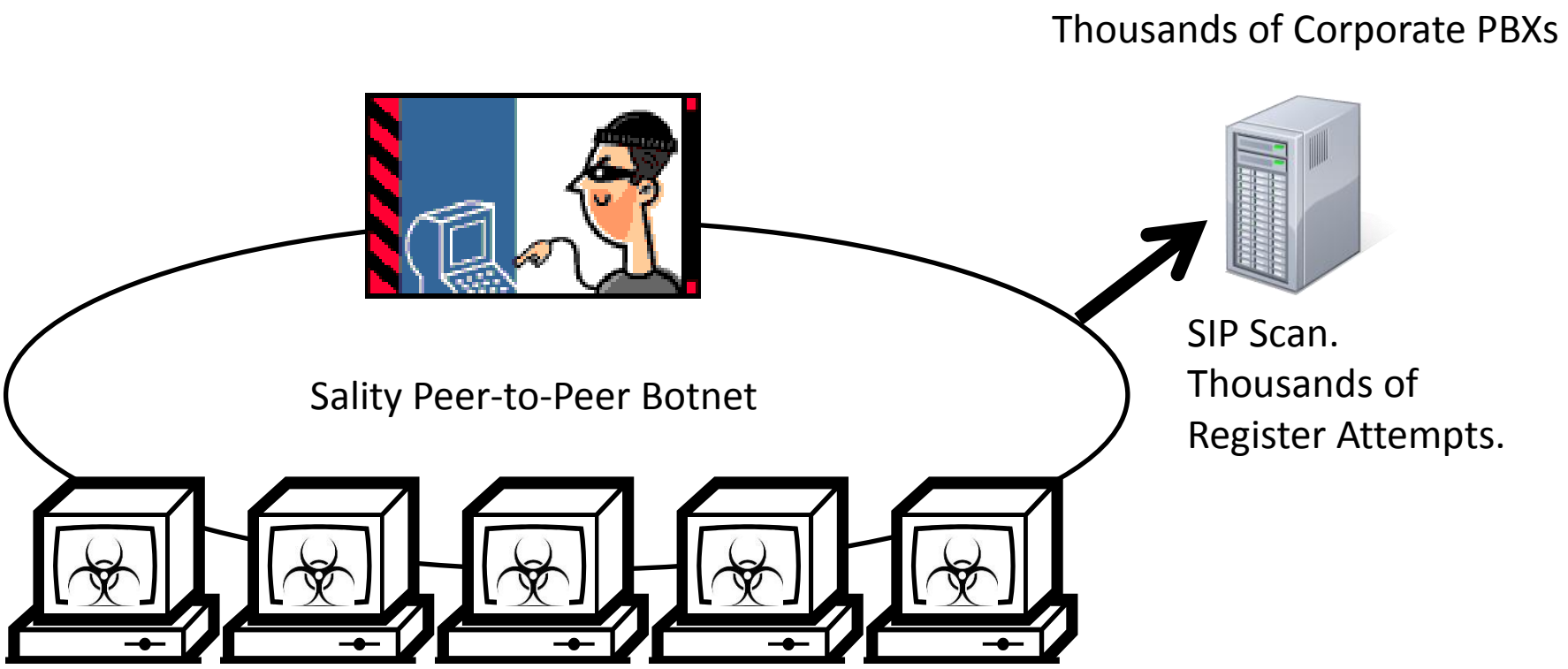
	ID	Country	Range	Payout	Currency	Paymentterms	Testnumber
	5000252	ALBANIA	355	0,09	EUR	7 / 1 days	355 511 810 62
	5000246	ANTARCTICA	88234	0,2	EUR	7 / 1 days	88.234.607.76
	5000333	AUSTRIA	43810959	0,03	EUR	7 / 1 days	43.810.959200
	5000153	AUSTRIA	438208931	0,1	EUR	7 / 1 days	43.820.893100
	5000331	AUSTRIA	4382094	0,1	EUR	7 / 1 days	43.820.946000 43.820.891249 43.820.894149 43.820.896149
	5000156	AUSTRIA	438208930	0,09	EUR	7 / 1 days	43.820.893000
	5000199	AUSTRIA	438101043	0,07	EUR	7 / 1 days	43.810.104300
	5000364	BELARUS	37560	0,07	EUR	7 / 1 days	375.602.605279 375.602.606899
	5000414	BULGARIA	359999	0,08	EUR	7 / 1 days	359.999.753.498
	5000354	BULGARIA	3599997	0,13	USD	7 / 1 days	359.999.726499 359.999.727199
	5000253	BURKINA FASO	226	0,11	EUR	7 / 1 days	226 507 700 12
	5000339	BURUNDI	2577485	0,09	EUR	7 / 1 days	257.748.55000
	5000272	CENTRAL AFRICAN REPUBLIC 2	236	0,13	EUR	7 / 1 days	236.217.50010 236.227.40110 236.216.1450

Common ways to get a password

1. SIP Scan and Bruteforce
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)*



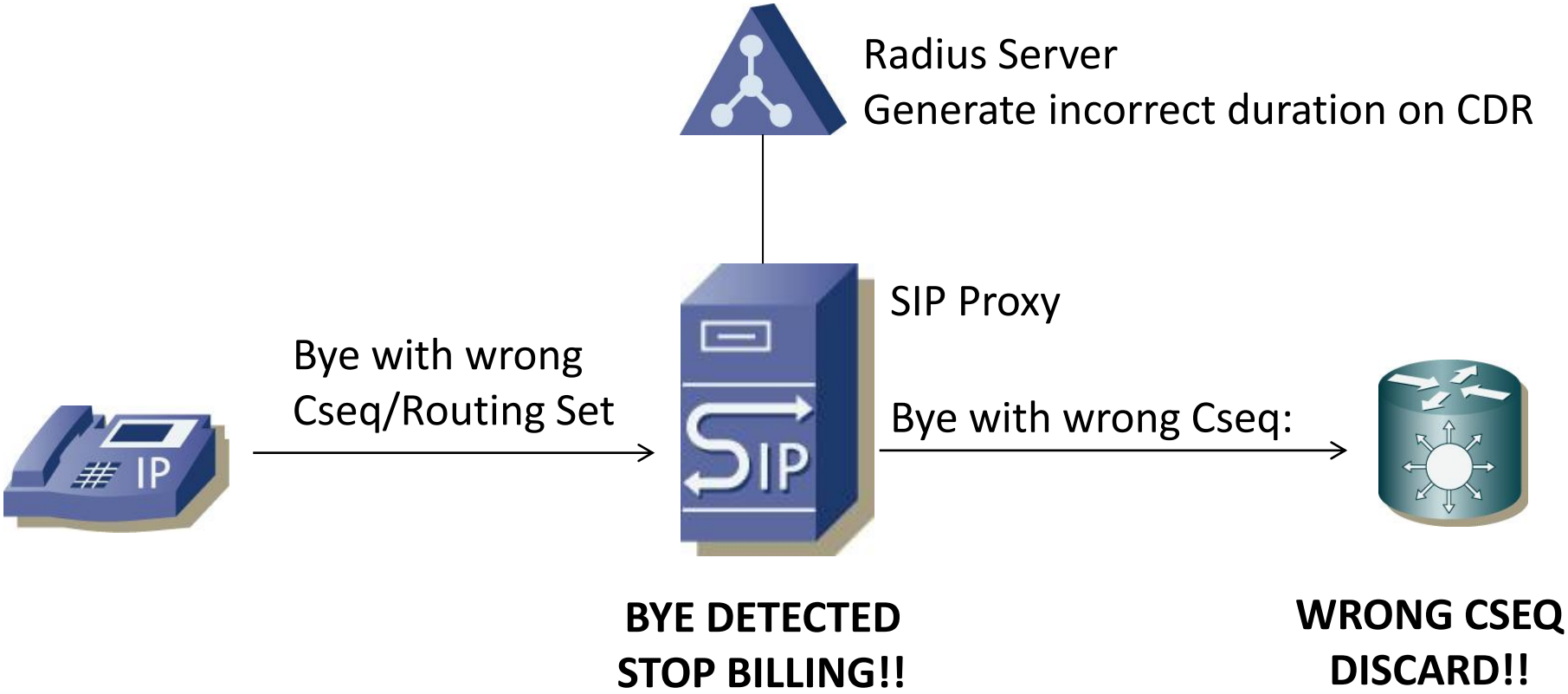
Source: Symantec
http://www.symantec.com/connect/blogs/distributed-cracker-voip

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.



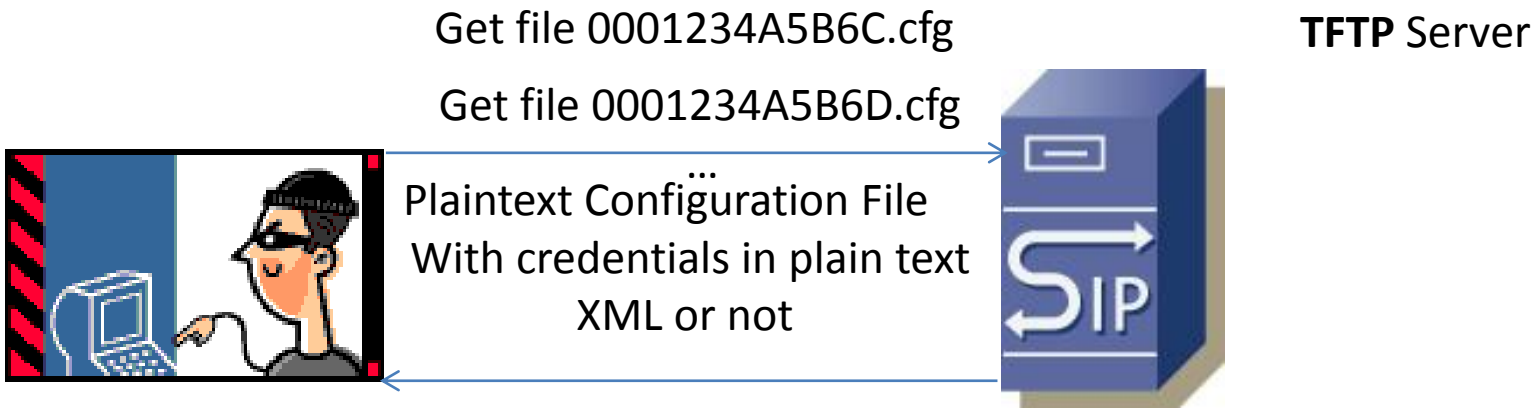
Mitigation for Signaling Attacks

- Dialog Aware Proxy

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

TFTP Attack

- Trivial Attack against VoIP Infrastructure
  - 1st Option bruteforce tftp server
  - 2nd Option sniff tftp files using MitM techniques



- Solution
  - Use HTTPS or Encrypted config files

Attacks on SIP Phones

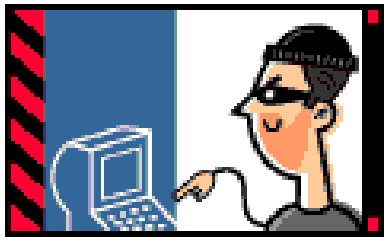
- How many of you change the default password for IP phones?
- How many of you update the IP Phone's firmware regularly?

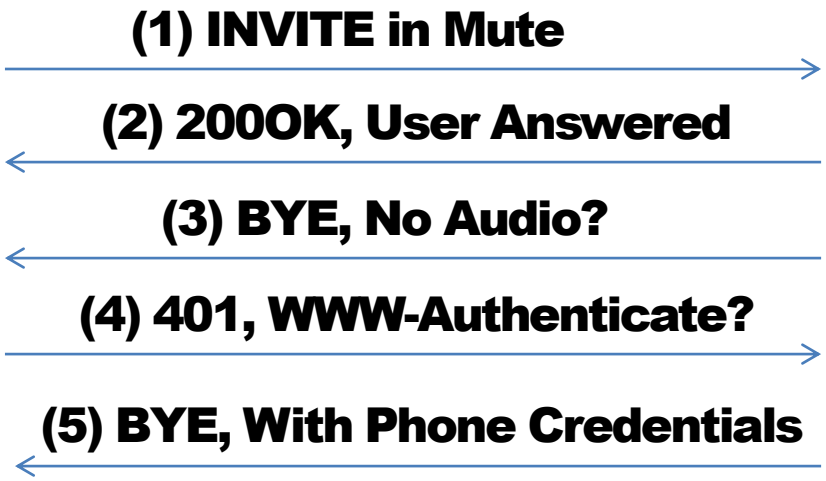
Video #2

Video #1

More sophisticated attacks

- SIP Digest Leak





Current estimated time needed to break all 8 chars length passwords
[a-zA-Z0-9]{1,8} ... 497 days
[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 ofenders

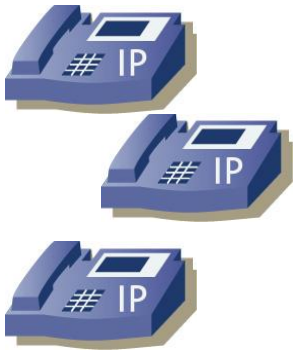
```
failregex=  Auth Error for .* from <HOST> cause -[0-9]
            Malformed SIP request from user .* from <HOST>
```

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



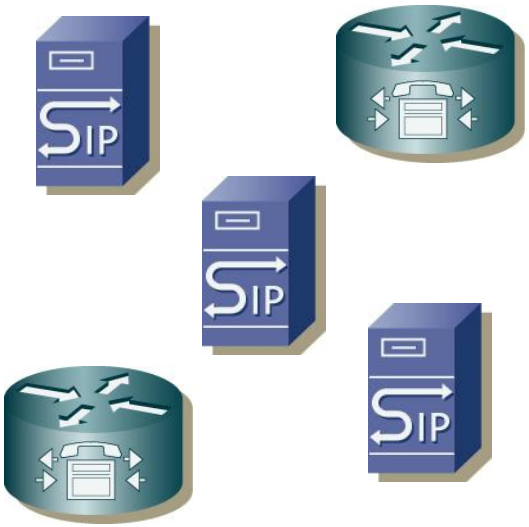
Security and Admission Box

opensips

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