Seguridad en Asterisk: Un Acercamiento Detallado

Moises Silva
Gerente de Ingeniería de Software
Sangoma Technologies

ELASTIX WORLD 2015

SANGOMA

No puedes considerar el problema de defensa sin primero entender el problema del ataque

Doug Tygar

Agenda

- **Importancia de la Seguridad Informática**
- **Entendiendo los Ataques a VoIP**
- **Vulnerabilidades en Asterisk**
- **Medidas de seguridad para proteger Asterisk**

Importancia de la Seguridad

- **Pérdidas económicas directas (e.g La cuenta del mes)**
- **Costo de oportunidad (servicios suspendidos)**
- **Pérdida de confianza de tus clientes en tu reputación**
- **Poco o ningún apoyo del marco legal cuando hay pérdidas económicas por fraude telefónico (los detalles, desde luego, varían de país a país)**

Entendiendo los Ataques

Para entender como proteger nuestros sistemas tenemos que entender el objetivo de los ataques comunes y sus mecanismos:

- **Fraude Telefónico**
- **Negación de Servicio**
- **Muchos otros: Intercepción de llamadas, secuestro de registro, etc …**

Fraude Telefónico

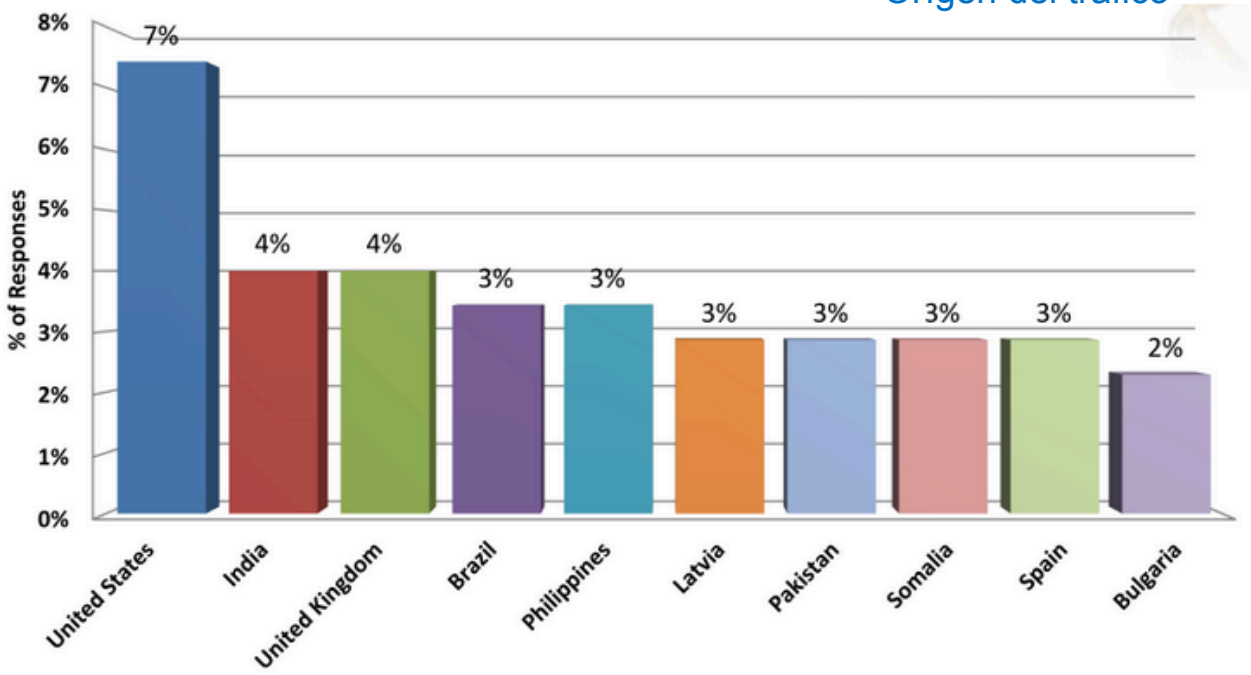
El objetivo es hacer llamadas usando tu PBX hacia destinos con un costo alto controlados directa o indirectamente por el perpetrador del ataque.

- **África suele ser un destino clave**

- **Con frecuencia los ataques se registran en fines de semana**

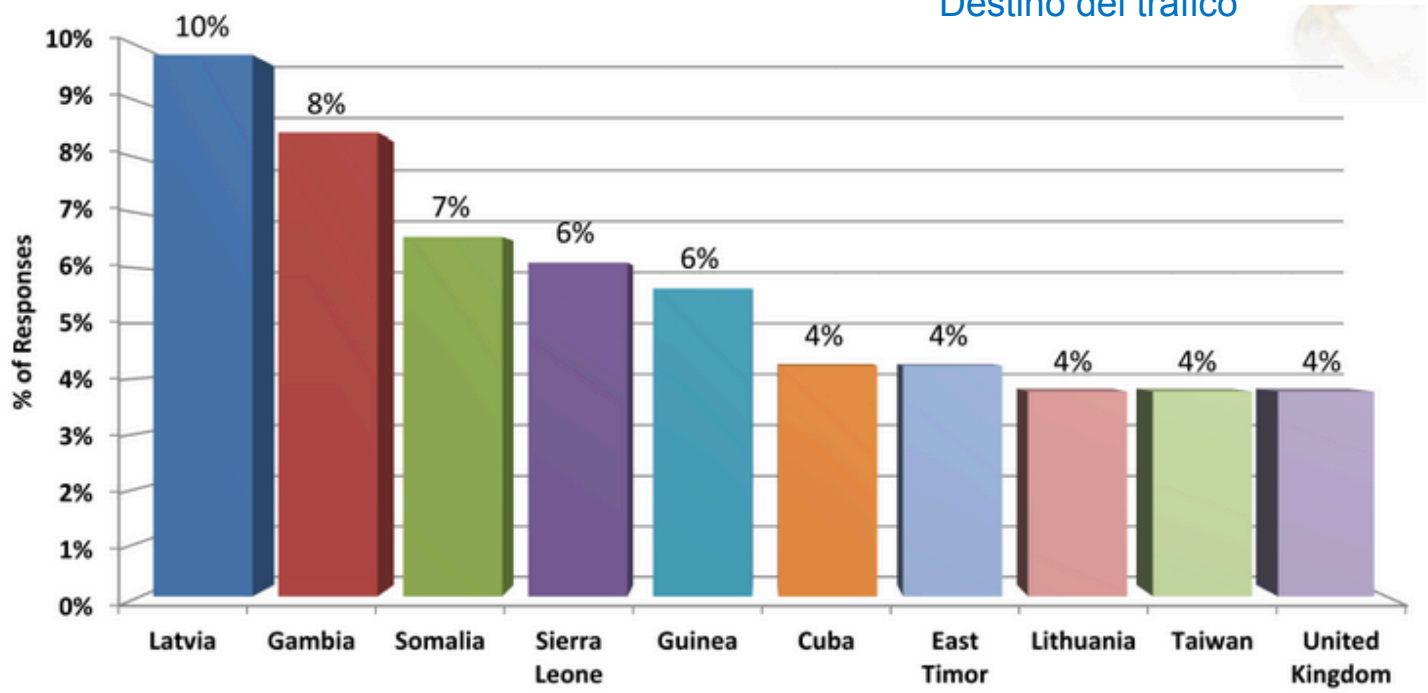
Fraude Telefónico

Orígen del tráfico



Fuente: Encuesta CFCA 2013

Fraude Telefónico



Fuente: Encuesta CFCA 2013

Negación de Servicio

El objetivo es evitar que usuarios legítimos del servicio puedan accederlo. La motivación puede ser el simple gusto de romper sistemas, o bien, tratar de probar un punto o extorsionar.

- **Paquetes malformados pueden provocar un “crash” del sistema**
- **Otro método es acabar con los recursos del sistema (memoria, CPU, descriptores de archivos, etc) enviando muchas peticiones**

El ABC de un Ataque

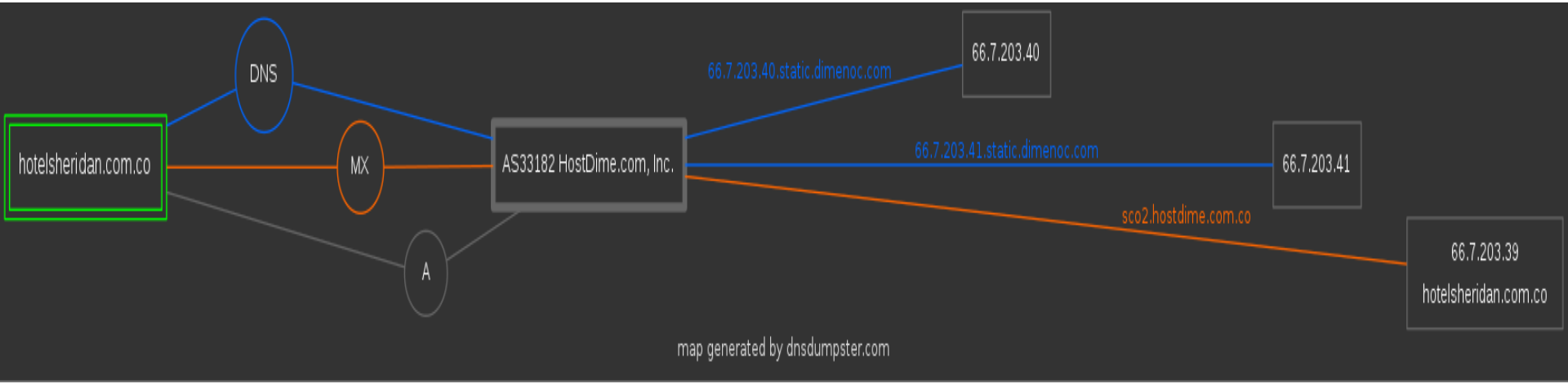
- **Footprinting (Obtener la mayor información posible sobre la red)**
  - **Uso de whois, nslookup, google, dnsdumpster.com**
- **Enumeración (enumerar hosts y cuentas)**
  - **nmap, svmap, svwar**
- **Explotación**
  - **svcrack, tftptheft, etc**

El ABC de un Ataque

- **El uso de sipvicious ha permitido hacer ataques a sistemas VoIP de manera relativamente sencilla usando:**
- **svmap para encontrar sistemas escuchando por tráfico SIP**
- **svwar para buscar extensiones válidas**
- **svcrack para encontrar passwords válidos**

Ejemplo de footprinting

Mapa DNS del hotel del evento:



Ejemplo de enumeración

Puertos abiertos en el servidor de correo del hotel:

```
# nmap 66.7.203.39

Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-08 05:42 UTC
Nmap scan report for sco2.hostdime.com.co (66.7.203.39)
Host is up (0.039s latency).
Not shown: 978 filtered ports
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    closed ssh
25/tcp    open   smtp
26/tcp    closed rsftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
993/tcp   open   imaps
995/tcp   open   pop3s
3300/tcp  closed unknown
3306/tcp  open   mysql
5432/tcp  open   postgresql
8080/tcp  open   http-proxy
30000/tcp closed unknown
30718/tcp closed unknown
30951/tcp closed unknown
31038/tcp closed unknown
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

Ejemplo de enumeración

Salida del comando svmap de sipvicious:

```
C:\sipvicious>svmap.py 10.0.0.1/16 -v
INFO:root:start your engines
INFO:DrinkOrSip:10.0.2.1:5060   -> 10.0.2.1:5060  -> Asterisk PBX
INFO:DrinkOrSip:10.0.2.20:5060  -> 10.0.2.20:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.21:5060  -> 10.0.2.21:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.22:5060  -> 10.0.2.22:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.23:5060  -> 10.0.2.23:5060 -> Grandstream BT100
WARNING:root:caught your control^c - quiting
INFO:root:we have 5 devices

| SIP Device          | User Agent                  |
-------------------------------------------------
| 10.0.2.1:5060       | Asterisk PBX                |
| 10.0.2.20:5060      | Grandstream BT100 1.0.6.7   |
| 10.0.2.20:5060      | Grandstream BT100 1.0.6.7   |
| 10.0.2.20:5060      | Grandstream BT100 1.0.6.7   |
| 10.0.2.20:5060      | Grandstream BT100 1.0.6.7   |

INFO:root:Total time: 0:00:04.384883
```

Fuente: infosecwriters.com

Ejemplo de enumeración

Salida del comando svwar de sipvicious:

```
C:\sipvicious>svwar.py 10.0.2.1 -e 123 -v
INFO:root:start your engines
INFO:TakeASip:Ok SIP device found
INFO:TakeASip:extension '123' exists - requires authentication
INFO:root:we have 1 extensions
| Extension | Authentication |
-------------------------------
| 123       | reqauth        |

INFO:root:Total time: 0:00:03.115869
```

Fuente: infosecwriters.com

Ejemplo de un ataque

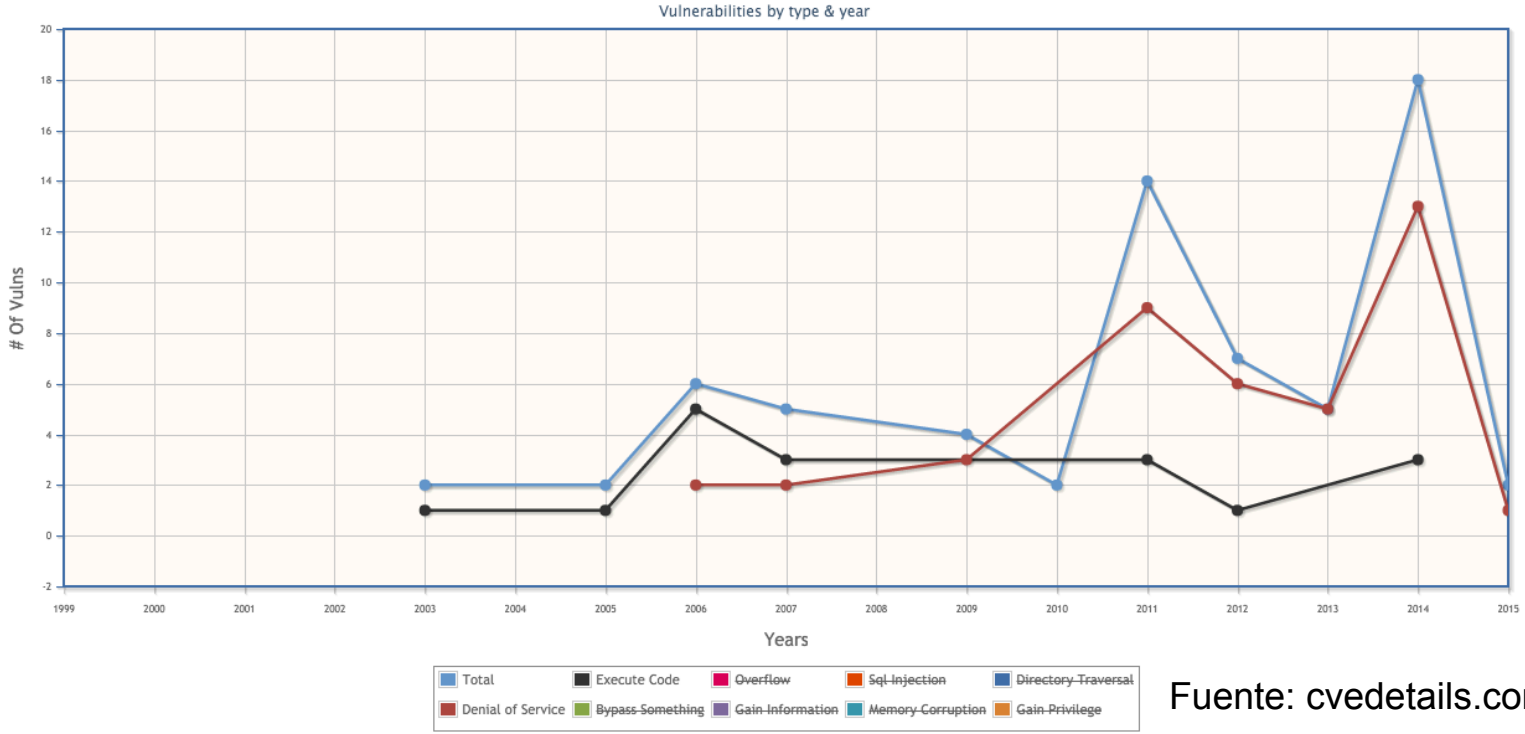
Salida del comando svcrack de sipvicious:

```
C:\sipvicious>svcrack.py 10.0.2.1  -u 123  -d dictionary.txt
INFO:root: scan started at 2021-07-21 13:01:32.23143
INFO:ASipOfRedWine:The password for 123 is vagrant
INFO:root:we have 1 cracked users
| Extension | Password |
------------------------
| 123       | vagrant  |

INFO:root:Total time: 0:00:32.145588
```

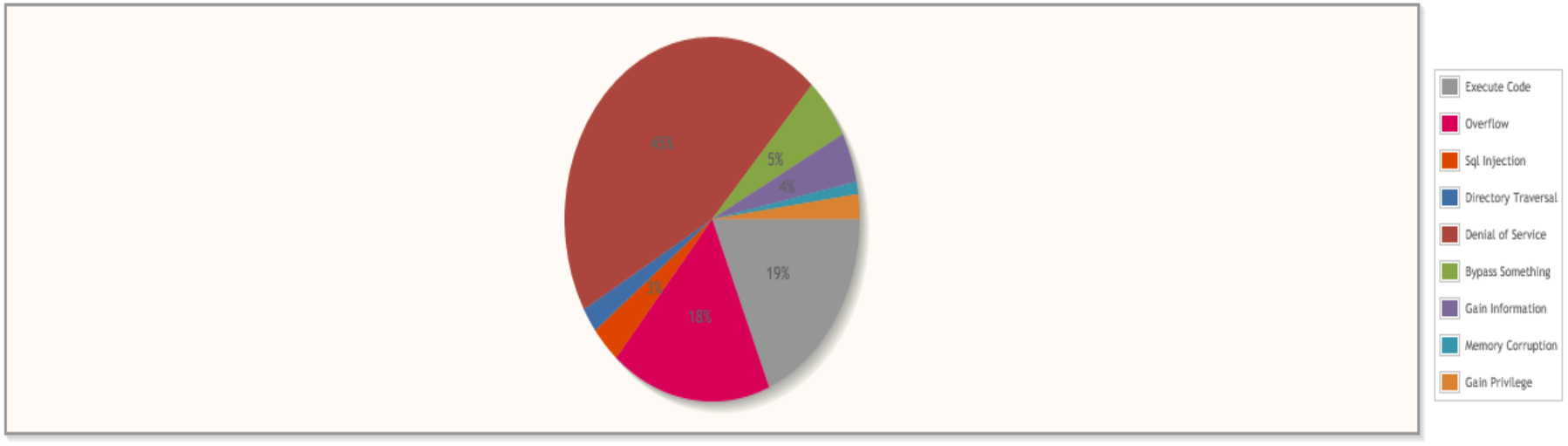
Fuente: infosecwriters.com

Vulnerabilidades en Asterisk



Fuente: cvedetails.com

Vulnerabilidades en Asterisk



Fuente: cvedetails.com

Vulnerabilidades en Asterisk

Importante mantenerse al tanto de las vulnerabilidades publicadas y actualizar frecuentemente:

http://www.asterisk.org/downloads/security-advisories

Vulnerabilidades en Asterisk

Asterisk Project Security Advisory - AST-2015-001

Product	Asterisk
Summary	File descriptor leak when incompatible codecs are offered
Nature of Advisory	Resource exhaustion
Susceptibility	Remote Authenticated Sessions
Severity	Major
Exploits Known	No
Reported On	6 January, 2015
Reported By	Y Ateya
Posted On	9 January, 2015
Last Updated On	February 11, 2015
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2015-1558

Vulnerabilidades en Asterisk

Asterisk Project Security Advisory - AST-2014-019

Product	Asterisk
Summary	Remote Crash Vulnerability in WebSocket Server
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	30 October 2014
Reported By	Badalian Vyacheslav
Posted On	10 December 2014
Last Updated On	December 22, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-9374

Seguridad Básica General

- **IP Firewall (ej. Lista blanca de IPs y puertos permitidos)**
- **Actualizaciones de seguridad frecuentes en todo el software**
- **Contraseñas fuertes para todos los servicios**

Seguridad Básica en Asterisk

- **Solo incluye módulos que necesitas en modules.conf (esto minimiza la superficie de ataque)**
- **Usa nombres de usuario diferentes a las extensiones**
- **Allowguest=no en sip.conf**
- **Usa SIP TLS/SRTP siempre que sea posible**

Seguridad Básica en Asterisk

- **Usa fail2ban para bloquear varios intentos fallidos de autenticación**
- **Elastix y FreePBX incluyen fail2ban**
- **Usa alwaysauthreject=yes en sip.conf [general] (versiones recientes de Asterisk tienen esto por defecto)**

Seguridad Básica en Asterisk

[Aug 22 15:17:15] NOTICE[25690] chan_sip.c: Registration from '"123"<sip:123@127.0.0.1>' failed for '203.86.167.220:5061' - No matching peer found
[Aug 22 15:17:15] NOTICE[25690] chan_sip.c: Registration from '"1234"<sip:1234@127.0.0.1>' failed for '203.86.167.220:5061' - No matching peer found
[Aug 22 15:17:15] NOTICE[25690] chan_sip.c: Registration from '"12345"<sip:12345@127.0.0.1>' failed for '203.86.167.220:5061' - No matching peer found

Filtros

```
exten => _X.,1,Dial(SIP/${EXTEN})
```

Filtros

exten => _X.,1,Dial(SIP/${EXTEN})

Qué sucede si ${EXTEN} es “1234&DAHDI/g1/01123230160081” ?

Filtros

exten => _X.,1,Dial(SIP/${EXTEN})

Qué sucede si ${EXTEN} es “1234&DAHDI/g1/01123230160081” ?

Al expandir ${EXTEN} el comando resultante es:

exten => _X.,1,Dial(SIP/1234&DAHDI/g1/01123230160081)

El resultado es una llamada a Sierra Leone ☺

Filtros (evitando “dialplan injection”)

- **Filtra variables como ${EXTEN} en tu plan de marcado**
- **Piensa de donde vienen tus variables y filtra sus valores**
- **Use patrones de marcado estrictos**

Filtros (evitando “dialplan injection”)

Patrones estrictos:

```
exten => _XXXX,1,Dial(SIP/${EXTEN})
exten => _XXXXXX,1,Dial(SIP/${EXTEN})
```

Filtro explicito:

```
exten => _X.,1,Set(NUM=${FILTER(0-9),${EXTEN})})
exten => _X.,n,Dial(SIP/${NUM})
```

ACLs

- **Asterisk te permite definir listas de control de acceso. Usalas!**
- **Una vez definida puedes usarla en distintos modulos como sip, iax, manager (AMI), etc**
- **Prefiere ACLs nombradas (acl.conf) en lugar de permit/deny directamente en sip.conf**

Control de Llamadas

- **Limita el número de llamadas concurrentes por usuario y globalmente**
- **Usa ${GROUP_COUNT} para especificar limite por dispositivo y/o grupo**

Método Viejo:

- **Habilita callcounter=yes en sip.conf**
- **Usa call-limit en sip.conf por cada dispositivo**
- **Usa maxcallnumbers y [callnumberlimits] en iax.conf**

Control de Llamadas

```
exten => _X.,1,Set(GROUP(users)=${CHANNEL(peername)})

same => n,GotoIf($[${GROUP_COUNT(${CHANNEL(peername)})} > 2]?denied:continue)

same => n(denied),NoOp(Demasiadas llamadas)

same => n,Hangup()

same => n(continue),NoOp(Continuacion de la llamada …)
```

Técnicas Avanzadas

Uso de Kamailio / OpenSIPs

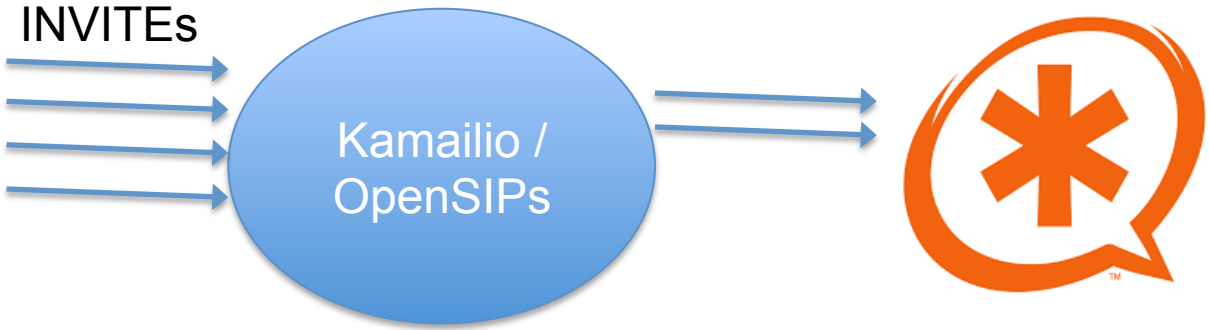
- **El módulo pike permite limitar número de mensajes SIP por IP y bloquear ‘flooding’**

- **Puedes definir ciertas IP o dejarlo abierto a cualquier IP que mande un mensaje**

Técnicas Avanzadas

Uso de Kamailio / OpenSIPs

Limitando numero de mensajes INVITE



Técnicas Avanzadas

PSAD (Port Scan Attack Detector)

- **Psad analiza los logs de iptables para detectar el escaneo de puertos y otros patrones sospechosos**
- **Opcionalmente psad puede bloquear la actividad sospechosa**
- **Usa este método para tomar acciones proactivas antes de que se inicie un ataque**
- **Usualmente se puede usar en combinación con snort y fwsnort**

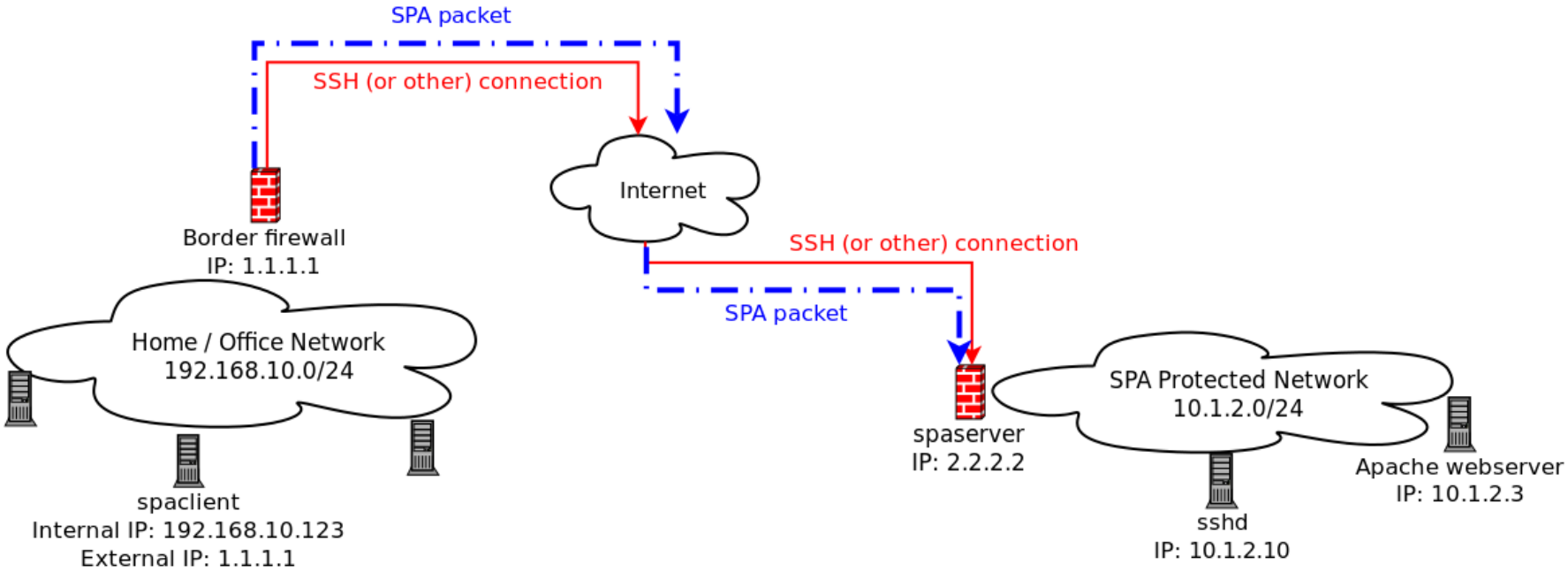
Técnicas Avanzadas

fwknop

- **Autenticación por paquete único (Single Packet Authorization)**
- **Evita completamente el escaneo de servicios públicos**
- **Esto permite la conexión a clientes móviles sin exponer la existencia de los servicios al resto del mundo**
- **Requiere de configuración en el servidor y un cliente que envie el paquete encriptado de autorización para abrir el puerto**

Técnicas Avanzadas

fwknop



Ideas Finales

- **Entiende las configuraciones generadas por herramientas como FreePBX y Elastix**
- **Audita tus sistemas frecuentemente**
- **Considera el uso de equipo externo de seguridad VoIP, como Elastix SIP Firewall, Sangoma SBC, etc.**

Mas gente muere cada año a causa de puercos que debido a tiburones, lo que muestra que tan buenos somos evaluando riesgos

Bruce Schneier

Gracias.

SANGOMA


SANGOMA
WANPIPE
The sky's the limit!
Drivers & Utilities
Because it must work.
SANGOMA
NetBorder EXPRESS
400
Vega 400
IP telephony gateway
5000
Vega 5000
IP telephony gateway
SANGOMA
TDMX
TX
RX
ETH
SMART
RS-232
POWER
+5V, 2A

SANGOMA