Seguridad yAsterisk

NOTA:

La siguiente información es meramente informativa.
Callmyway no se hace responsable de los resultados o veracidad de los mismos.

Seguridad y Asterisk

- Asterisk: Configuración descuidada
- Endureciendo Asterisk
- Protección de Privacidad

Asterisk Configuración Descuidada

- Seguridad en el Dial plan
- SIP.conf
- IAX2.conf
- Manager.conf
- Problemas de Facturación

Seguridad en el Dial Plan

- - Salto entre Extensiones
- - Protecciones basadas en el CallerID
- - _.
- - El Contacto Demo
- - Cuentas de Usuario en el dial plan
- - Mucho cuidado con el contexto por defecto
- - Límite las llamadas simultaneas

Salto entre Extensiones

- El usuario puede alcanzar CUALQUER extensión bajo el siguiente contexto:

[internal]

exten => intro,1,Background(question);

exten => 1,spanish,Goto(Spanish)

exten => 2,english,Goto(English)

exten => _XX.,1,Dial(ZAP/g1/${EXTEN});

Protección basada en el CallerID

```
exten =>
    _X.,1,GotoIf($[“${CALLERIDNUM}”=“32134”?3);
exten => _X.,2,Hangup();
exten => _X.,3,Dial(${EXTEN});
```

- Cuando no se encuentra explicitamente definida para cada usuario/canal en zapata.conf, sip.conf, iax.conf, entonces el usuario puede escoger su propio CallerID!

Uso inapropisado de _.

- _. Se acopla con TODO!

(incluyendo: fax, colgado, invalido, timeout,….)

Ejemplo:

exten => _.,1,Playback(blah);

exten => _.,2,Hangup;

➔ Causando un “FAST LOOP”.

(cambiado en CVS-head)

Context de demo

- No es un riesgo real
- Pero… Alguien podría jugar con su sistema y utilizar su ancho de banda, realizar llamadas de broma a Digium.

Acceso de los usuarios al dialplan

- - AMP y otros GUI's (Interfaces Graficos de Usuario) podrían permitir al usuario cambiar el dial plan en su propio contexto. ie.: PBX hospedada

- - Goto / GotoIf / dial(Local/…) -> Saltar entre diferentes contextos.
- - System -> podría hacer cualquier cosa

Contexto por defecto

- Ejemplo:

[default]
Include outgoing;
Include internal;

PELIGRO: Las llamadas invitadas iran al contexto por defecto!!!!!

Contexto de USO:

- Toda llamada tiene dos extremos, el contexto utilizado es el contexto definido para dicho usuario/canal en el archivo de configuración para dicho protocolo.

ie:

- Llamada Zap a SIP:

El contexto establecido en zapata.conf es usado

- Llamada SIP a IAX:

El contexto utilizado es sip.conf

Contexto de USO:

- En sip.conf, zapata.conf, iax2.conf…

Un contexto por defecto es definido, si no existe un contexto especifico definido para un canal o usuario, entonces el contexto por defecto es utilizado!

Limite las llamadas simultaneas

- Generalmente usted no desea que ciertos usuarios no realicen llamadas simultaneas multiples..

- Ejemplo: Servicios pagados / tarjetas telefónicas / llamadas al PSTN

Solucion: setgroup, checkgroup (no confie en el incominglimit.)

exten => s,1,SetGroup(${CALLERIDNUM})

exten => s,2,CheckGroup(1)

Solo funciona si el CallerID no puede ser falsificado !!!!

Considere utilizar el accountcode para esto.

Sip.conf

- Default context
- Bindport, bindhost, bindip
- [username] vs username=
- Permit, deny, mask
- Insecure=yes, very, no
- User vs peer vs friend
- Allowguest
- Autocreatepeer
- Pedantic
- Ospauth
- **Realm**
- Md5secret
- User authentication logic
- Username= vs [username]

Bindport, bindhost,bindip

- Si usted utiliza SIP únicamente para llamadas internas, no configure bindip=0.0.0.0, más bien limitelo a la IP interna.

- Cambiar el bindport hacia uno que no sea el puerto 5060 podría salvarle de barridas de escaneo de puerto hacia este puerto.

Permit, deny, mask

- Bloquee todo, luego permita por usuario lo permitido y sus rangos.

(Multiple es permitido)

SIP.conf – opcion insegura

Insecure = …

- No: la opcion por defecto siempre pregunta por autenticación
- Si: Aceptar un peer basado únicamente en su dirección.
- insecure=very ; permitir servidores registrados llamar sin reautenticar y validar únicamente por dirección IP
- insecure=port; no importa si el portnumber es diferente de cuando se registraron
- insecure=invite; cada invite es aceptado.

User vs Peer vs Friend en SIP

- USER: nunca registra, solo realiza llamadas
- PEER: puede registrarse + puede realizar llamadas.

[user1]
type=user
[user1]
type=peer

Con type=friend si los otros paramentros son identicos!!!

Allowguest =…

- True: usuarios sin autenticar utilizaran en el contexto por defecto segun se define en sip.conf
- False: usuarios sin autenticar obtendran un mensaje de “permission denied error”.
- OSP: para permitir a acceso de invitado para tráfico VoIP desde un servidor OSP.

autocreatepeer

- La opción autocreatepeer permite, si puesta en Yes (sí) a cualquier SIP UA (User Agent) a registrarse en su PBX Asterik como peer . Esta configuración peer estará basada en las opciones globales. El nombre del peer se basará en el usuario del contacto: El campo del header del URL

  Este es un riesgo de seguridad muy alto si usted no cuenta con buen control de acceso a su servidor.

Pedantic

- La opcion por defecto para pedantic=no
- Si se habilita (yes), podría permitir un “denial of service” o DOS al enviar una gran cantidad de invites, causando muchos (y lentos) DNS lookups.

Ámbito (Realm)

- Realm=Asterisk; Ámbito de la autenticación implicita;

Por defecto “Asterisk“;

Los ambitos (realms) deberían ser globalmente únicos de acuerdo a la especificación RFC 3261;

Establezca este según su nombre único de servidor o dominio.

¿Como se realiza la autenticación?

- Se busca en el FROM del header SIP por el username:

-> busque en sip.conf por un type=user con el usuario
Si lo encuentra -> verifique el md5
Si no lo encuentra:

-> busque el sip.conf por un type=peer con el usuario
-> busque el sip.conf por una IP (registrada) donde la solicitud viene de:
if insecure=very, no se realizan más verificaciones
if insecure=port, si desea autenticarlos, aún en el caso que se encuentren llamadando de un puerto diferente del que se han registrado. (Se utiliza para NAT TRAVERSAL en donde no se utiliza el mismo puerto todo el tiempo).
de cualquier otro modo, verifica el md5 + allow/deny.

- Si el peer no se encuentra ? Permitimos el “allow guest access” (allowguest=true ?)
- SI? OK, el allow se envia al contexto por defecto, si NO, se rechaza.

Secret vs md5secret

- Con SIP todos los passwords son encriptados bajo el md5 al enviarse los paquetes, pero se almacenan en un archivo plano en sip.conf (esto aplica para Asterisk)

- [user]
- Secret=blabla

Secret vs md5secret

- echo - n "<user>:<realm>:<secret>" | md5sum
- Ejemplo:

echo -n "user:asterisk:blabla" | md5sum

e1b588233e4bc8645cc0da24d8cb848d

[user]

md5secret=e1b588233e4bc8645cc0da24d8cb848d

Username= vs [username]

- [username] es para autenticar un cliente que se esta conectando al asterisk.

Username=… es para que su servidor Asterik se autentique a otro servidor SIP.

Iax.conf

- auth=texto,md5,rsa
- Logica de autenticación de usuarios
- Context por defecto
- [username] vs username=
- Permit, deny, mask
- Bindport, bindhost, bindip
- User vs peer vs friend

iax.conf - auth

- Plaintext: las claves con enviadas en texto plano
- Md5: encrypta la clave (password) utilizando md5
- RSA: utiliza una llave pública
- AES: utiliza una llave privada.

User vs Peer vs friend

- USER: solo puede aceptar llamadas
- PEER: solo puede realizar llamadas
- FRIEND: puede realizar ambas

[user1]
type=user
[user1]
type=peer

Es permitido!!!

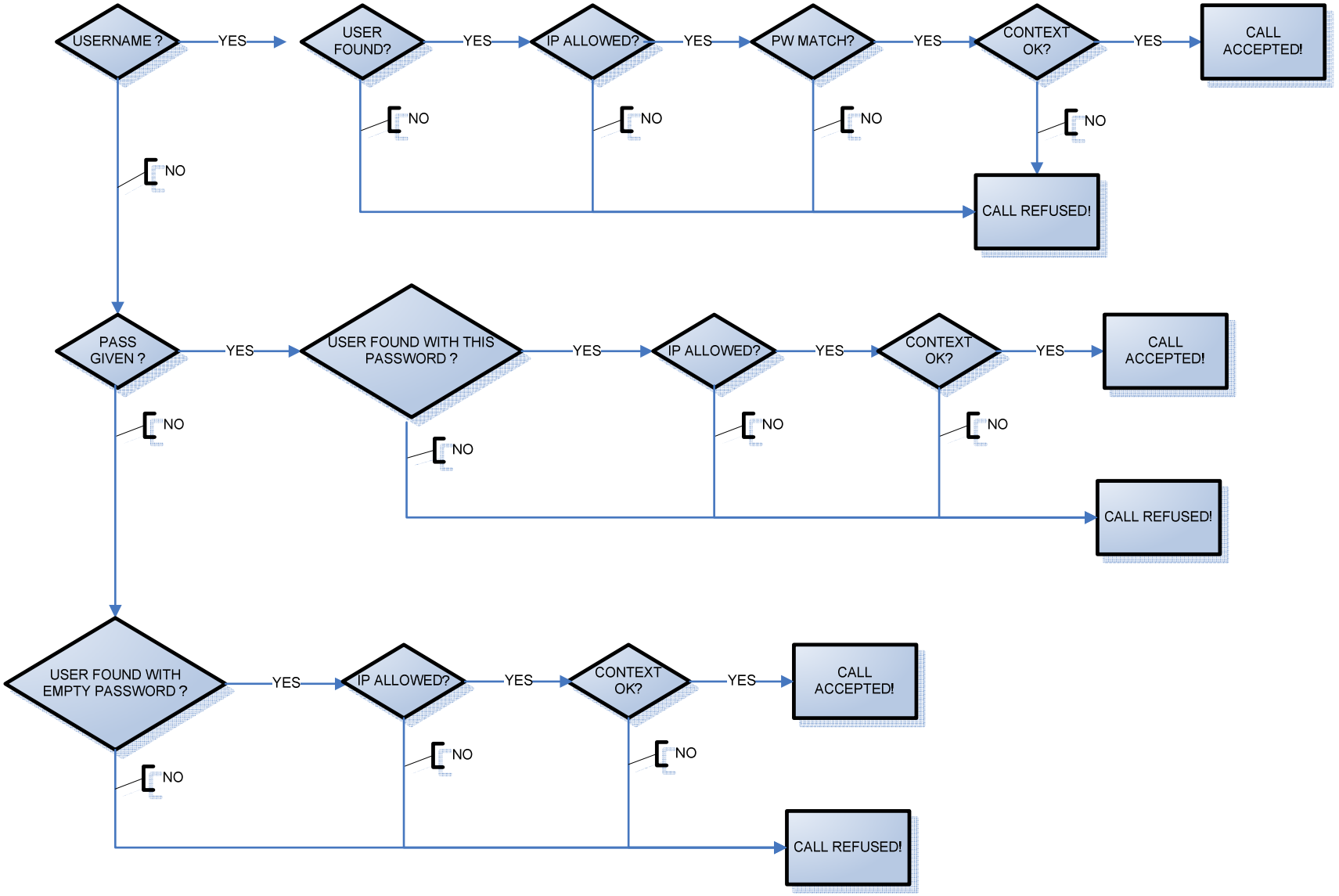
Como se realiza la autenticación?

- En iax2: (encabezado-cvs!!)

Pseudocodigo:
Viene un usuario ?
-> sí -> comparelo contra los usuarios en iax.conf, iniciando de abajo hacia arriba.
encontro el usuario ?
-> sí : esta en el IP in allowed / disallowed list ?
si –> encontró el password ?
si -> el contexto requerido calza con una linea del contexto?

-> si -> viene un password ?
-> si : Asterisk buscara de abajo hacia arriba por un usuario con esa clave,
-> si el contexto calza o no hay contexto especificado y el host se encuentra en el “allowed list” (allow / deny) entonces la llamada es aceptada.

-> no: Asterisk buscará de abajo hacia arriba por algun usuario sin clave.
-> si el contexto calza o no hay contexto especificado y el host se encuentra en el “allowed lists” (allow / deny) entonces la llamada es aceptada.



- Agregue cuando menos una entrada en iax.conf sin clave para forzar los “nosecret” a un contexto especifico.
- Si usted utiliza tiempo real (realtime), no utilice ningun usuario sin password y sin permit/deny.

Manager.conf

```
[general]
enabled = yes
port = 5038
bindaddr = 0.0.0.0

[zoa]
secret = blabla
deny=0.0.0.0/0.0.0.
permit=221.17.246.77/255.255.255.0
permit=127.0.0.1/255.255.255.0
read = system,call,log,verbose,command,agent,user
write = system,call,log,verbose,command,agent,user
```


call my way

Manager.conf

- No se utiliza encripcion, hasta la clave se almacena en texto plano.

- No lo habilite en una IP pública.
- Puede utilizar http://www.stunnel.org/
- Vigile con programas de administración con acceso directo al interface del administrados.
- Limite los privilegios por usuario (especialmente los del sistema!!!).

call my way

Seguridad Asterisk

- Asterisk: Configuracion descuidada
- Endureciendo Asterisk
- Protección de Privacidad

Endureciendo Asterisk

- Asterisk no como un “root user”
- Instale Asterisk en CHROOT
- Instale Asterisk en una CARCEL (in a JAIL)
- Instale Asterisk con permisos limitados de lectura y escritura (read / write)
- ZAPTEL kernel modules
- Asterisk firewalling / shaping / NAT
- Tty9
- Linux hardening
- Remote logging
- Tripwire
- Limite los procesos de sistema que corren en el servidor

call my way

Asterisk como no root (root user)

NOTA: Si no esta seguro de los resultados de los siguientes comandos, consultar a algún técnico antes de ejecutarlos.

```
adduser --system --home /var/lib/asterisk --no-create-home Asterisk
chown -r asterisk:asterisk /var/lib/asterisk
chown -r asterisk:asterisk /var/log/asterisk
chown -r asterisk:asterisk /var/run/asterisk
chown -r asterisk:asterisk /var/spool/asterisk
chown -r asterisk:asterisk /dev/zap
chown -r root:asterisk /etc/asterisk
chmod -r u=rwX,g=rX,o= /var/lib/asterisk
chmod -r u=rwX,g=rX,o= /var/log/asterisk
chmod -r u=rwX,g=rX,o= /var/run/asterisk
chmod -r u=rwX,g=rX,o= /var/spool/asterisk
chmod -r u=rwX,g=rX,o= /dev/zap
chmod -r u=rwX,g=rX,o= /etc/asterisk
chown asterisk /dev/tty9
su asterisk -c /usr/sbin/safe_asterisk
or
Asterisk -U asterisk -G asterisk
```

Asterisk con permisos limitados de escritura y lectura (read / write permissions)

- Instale Asterisk sin permisos de escritura para sus archivos de configuración (config) y que corra como un “non root”

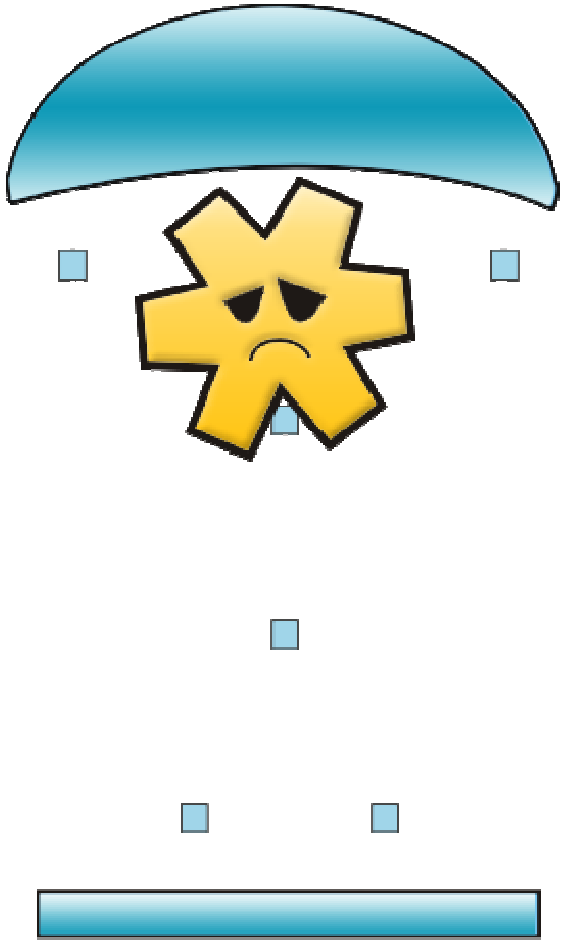
- En el indeseado caso que alguien ingrese a travez de su Asterik, su dial plan es vulnerable mediante el CLI o el administrador.

Asterisk en chroot

- Cambiar el directorio visibles a asterisk a otro que no sea la raiz, ejemplo: /foo/bar
- Es de poca utilidad si asterisk corre como root y perl o gcc se encuentran disponibles.

Asterisk en una carcel

- Cambios en el directorio raiz (root) visibles a Asterik.
- Limite a una lista los comandos / programas que cualquier usuario ene esta carcel pude ejecutar.
- Expanción de chroot.



Módulos Zaptel kernel

- Zaptel es únicamente un módulo, no se puede poner en el kernel.
- A los hackers le gusta esconderse en un módulo, hacer “backdor” en algun módulo, compilarlo, cargarlo en memoria y remueve cualquier trazo del mismo en el disco.
- Uster puede realizar una verificación md5 de los módulos Zapatel en el kernel.

Firewalling / shaping / NAT

- Bloquee todos excepto los puertos que realmente necesita. (5060, 4569, …)

- Los puetos RTP tambien (en rtp.conf)

Nota: No esta mal verificar si su ISP bloquea el rango de puerto en el rango definido en RTP.conf

Limite el acceso a tty9

- safe_asterisk abre una consola en tty9.

Esta no requiere una clave y provee acceso "root" a cualquiera que por ahí pase.

(al utilizar el commando !command en el CLI (Command line interface)).

- Remueva el comando, o no utilice "safe_asterisk"

Endureciendo Linux

- GRsec (2.6.x)
- Openwall (2.4.x)
- Remueva todo lo que no necesita.

Acceso Remoto

- Remote syslog
- Instale todos los “log files” en un servidor remoto.

Tripwire

- Realiza comprobaciones de todos los archivos importantes en el servidor y verifica por cambios que usted no realizó.

Limite los procesos del servidor

- Un servidor Asterisk debe de ser únicamente:

- OS + ASTERISK.
- Sin Base de datos
- Sin APACHE
- Sin PHP

(Si realmente los necesita y no cuenta con suficientes servidores, no lo instale en una IP pública e instale un Firewall!!!)

Seguridad Asterisk

- Asterisk: Configuracion descuidada
- Endureciendo Asterisk
- Protección de Privacidad

Privacidad en Asterisk

- Encrypción
- Monitoreo
- Falsificación de CallerID
- CallingPRES

Encripción de llamadas - SIP

- SRTP -> método para encriptar paquetes de voz.
- TLS -> método para encriptar paquetes de señalización.

➔Ambos no se encuentran soportados por asterisk.

Encripción de llamadas – Solución General

- Envíe sus paquetes mediante un VPN o un tunel.

- Utilice únicamente tuneles UDP para evitar retrasos.

Se conoce que trabajen:

➔IPSEC, VTUN, OPENVPN.

Encripción de llamadas – Solución mediante tunnel

- ➔Ventaja, la encripción es cara en recursos de CPU y solo se puede realizar en una maquina poderosa y dedicada.
- ➔ Desventaja: no trabaja en “hardphones” o ATA’s sin agregar un servidor adicional delante de ellos.