

# Seguridad en BGP

LACNIC IV  
Santiago de Chile, Chile

José A. Domínguez <[jad@ns.uoregon.edu](mailto:jad@ns.uoregon.edu)>

# Problemas de BGP

- Corre en TCP y hereda todos los problemas de TCP
  - IP Spoofing
  - Session Hijacking

# Problemas de BGP

- Posibilidad de inyección de información errónea
  - Pretendiendo ser un peer de BGP legítimo
  - Distribuyendo información errónea por un peer de BGP legítimo
- La mayoría de los casos debido a problemas de configuración

# Resultados de Inyección Información Errónea

- Si remueve información de un prefijo, este quedará fuera de servicio
- Si cambia la ruta al prefijo, tráfico sigue:
  - un camino sub-óptimo
  - un camino que no cumple con las políticas de enrutamiento
  - Un camino que descarta los paquetes

# Posibles Ataques a BGP

## 1) Eavesdropping

Es posible debido a los datos de las actualizaciones de BGP pueden ser capturados debido a que la información no es encriptada.

En la mayoría de los casos encriptación no es un requisito de las políticas.

# Posibles Ataques a BGP

## 2) Replay

El protocolo no provee protección contra la reproducción del tráfico de una sesión.

La única protección es ofrecida por el procesamiento de los números de secuencia en TCP

# Posibles Ataques a BGP

- 3) Inserción de Mensajes
- 4) Borrado de Mensajes
- 5) Modificación de Mensajes

El protocolo no provee protección contra ninguno de estos ataques. Sin embargo TCP provee protección a través del procesamiento de los números de secuencia. Una adición a BGP que utiliza "TCP MD5 Signature Option" ayuda a reducir la posibilidad de estos ataques cuando se utiliza en la configuración de los peers.

# Posibles Ataques a BGP

## 6) Hombre en el Medio (Man-in-the-middle)

Puesto que BGP no requiere autenticación de los peers es muy fácil ejecutar este ataque. En conexiones punto-a-punto es un poco más difícil pero en puntos de intercambio es muy sencillo. Las posibilidades se pueden reducir cuando se utiliza una clave para la sesión con "TCP MD5 Signature Option".

# Posibles Ataques a BGP

## 7) Disrupción de Servicio (Denial of Service)

Aunque en los anteriores casi siempre se puede crear un disrupción del servicio a prefijos específicos, estos casi siempre tienen un alcance reducido. Sin embargo, alguien podría inyectar todos los prefijos del Internet como /24s y causar una sobrecarga en los routers (incidente del AS7007, Florida Internet Exchange, debido a una configuración errónea y la falta de filtros por Sprint en 4/1997)

# Vulnerabilidades y Riesgos

- BGP no tiene mecanismos internos que:
  - garanticen la integridad y autenticidad de los peers y de los mensajes recibidos
  - validen la autoridad de un AS para anunciar informaciones del NLRI
  - Aseguren la autenticidad y validez los atributos de camino de un AS

# Vulnerabilidades de los Mensajes de BGP

- Existen ataques específicos que pueden ser ejecutados a través de los siguientes mensajes:
  - OPEN
  - KEEPALIVE
  - NOTIFICATION
  - UPDATE
- Estos ataques requieren que las sesiones de BGP puedan ser secuestradas
- Ver [draft-murphy-bgp-vuln-02](#) para información para información más detallada

# Vulnerabilidades a Través de Otros Protocolos

- BGP corre encima de TCP y por lo tanto es vulnerable a:
  - TCP SYN (SYN Flooding)
  - TCP SYN ACK
  - TCP ACK
  - TCP RST/FIN/FIN-ACK
- Ver [draft-murphy-bgp-vuln-02](#) para información para información más detallada

# Que Se Puede Hacer Hoy En Día?

- Restringir conexión a peers autorizados
  - Restricción al puerto 179
  - Uso de passwords para la sesión
- Controlar los prefijos que se anuncian
- Controlar los prefijos que se reciben

# Registros de Enrutamiento

- Usar los registros de enrutamiento para definir las políticas de entrada y salida que incluyen los prefijos que se aceptarán y enviarán.
- Fuentes:
  - Servidor Específico del Proveedor
  - Routing Assets Database (RADB)  
(<http://www.radb.net>)

# Registros de Enrutamiento

- Maintainer Object:

**mntner:** MAINT-AS3582  
**descr:** University of Oregon  
**admin-c:** DMM65  
**tech-c:** JAD77  
**upd-to:** netstaff@ns.uoregon.edu  
**auth:** PGPKEY-98A02F16  
**auth:** PGPKEY-A099D8A7  
**auth:** PGPKEY-FAE5AEBB  
**notify:** netstaff@ns.uoregon.edu  
**mnt-by:** MAINT-AS3582  
**changed:** jad@ns.uoregon.edu 20020307  
**source:** RADB

# Registros de Enrutamiento

- AS SET:

<b>as-set:</b>	<b>AS-UONET</b>
<b>descr:</b>	<b>ASes announced by UONET (AS3582)</b>
<b>members:</b>	<b>AS3582</b>
<b>admin-c:</b>	<b>DMM65</b>
<b>tech-c:</b>	<b>JAD77</b>
<b>notify:</b>	<b>jad@ns.uoregon.edu</b>
<b>notify:</b>	<b>nethelp@ns.uoregon.edu</b>
<b>mnt-by:</b>	<b>MAINT-AS3582</b>
<b>changed:</b>	<b>jad@ns.uoregon.edu 20010111</b>
<b>source:</b>	<b>RADB</b>

# Registros de Enrutamiento

- Route Object:

<b>route:</b>	<b>128.223.0.0/16</b>
<b>descr:</b>	<b>UONet University of Oregon Computing Center Eugene, OR 97403-1212 USA</b>
<b>origin:</b>	<b>AS3582</b>
<b>mnt-by:</b>	<b>MAINT-AS3582</b>
<b>changed:</b>	<b>jad@ns.uoregon.edu 19960222</b>
<b>source:</b>	<b>RADB</b>

# Registros de Enrutamiento

- Contact Person:

<b>person:</b>	<b>Jose A. Dominguez</b>
<b>address:</b>	<b>Computing Center University of Oregon 1225 Kincaid Street Eugene, OR 97403-1212</b>
<b>phone:</b>	<b>+1 541 346-1685</b>
<b>fax-no:</b>	<b>+1 541 346-4397</b>
<b>e-mail:</b>	<b>jad@ns.uoregon.edu</b>
<b>nic-hdl:</b>	<b>JAD77</b>
<b>notify:</b>	<b>jad@ns.uoregon.edu</b>
<b>mnt-by:</b>	<b>MAINT-AS3582</b>
<b>changed:</b>	<b>jad@ns.uoregon.edu 20001108</b>
<b>source:</b>	<b>RADB</b>

# Registros de Enrutamiento

- POLÍTICA

```
aut-num:      AS3582
as-name:      UONET
descr:        University of Oregon
admin-c:      DMM65
tech-c:       JAD77
import:       from AS689
              action pref=400;
              accept NOT ANY
import:       from AS4222
              action pref=400;
              accept AS-OPEN-SOUTH AND
              NOT {0.0.0.0/0}
```

# Registros de Enrutamiento

**export:** to AS689  
announce AS-UONET

**export:** to AS4222  
announce AS-UONET

**notify:** nethelp@ns.uoregon.edu

**mnt-by:** MAINT-AS3582

**changed:** jad@ns.uoregon.edu 20030331

**source:** RADB

# Registros de Enrutamiento

- Puedes utilizar RtConfig para generar las configuraciones

```
@RtConfig set cisco_access_list_no = 100
```

```
@RtConfig set cisco_map_first_no = 10
```

```
@RtConfig set cisco_map_increment_by = 10
```

```
@RtConfig set cisco_max_preference = 1600
```

```
router bgp 3582
```

```
neighbor 198.32.162.4 remote-as 4222
```

```
neighbor 198.32.162.4 peer-group oix-embgp-peer
```

```
neighbor 198.32.162.4 description OPEN South
```

```
@RtConfig set cisco_prefix_acl_no = 100
```

```
@RtConfig set cisco_aspath_acl_no = 100
```

```
@RtConfig set cisco_map_name = "AS4222-EXPORT"
```

```
@RtConfig export AS3582 198.32.162.1 AS4222 198.32.162.4
```

```
@RtConfig set cisco_map_name = "AS4222-IMPORT"
```

```
@RtConfig import AS3582 198.32.162.1 AS4222 198.32.162.4
```

# Registros de Enrutamiento

- Y despues correr:

```
RtConfig    -h rpsl.merit.edu  
            -cisco_use_prefix_lists  
            -cisco_force_tilda  
            -supress_martian  
            < source_file  
            > config_file
```

# Registros de Enrutamiento

```
router bgp 3582
neighbor 198.32.162.4 remote-as 4222
neighbor 198.32.162.4 peer-group oix-embgp-peer
neighbor 198.32.162.4 description OPEN South
!
no ip prefix-list pl105!
router bgp 3582
neighbor 198.32.162.4 route-map AS4222-IMPORT in
!
ip prefix-list pl105 deny 0.0.0.0/0 ge 32
ip prefix-list pl105 deny 127.0.0.0/8 le 32
ip prefix-list pl105 deny 10.0.0.0/8 le 32
ip prefix-list pl105 deny 172.16.0.0/12 le 32
ip prefix-list pl105 deny 192.168.0.0/16 le 32
ip prefix-list pl105 deny 192.0.2.0/24 le 32
ip prefix-list pl105 deny 128.0.0.0/16 le 32
```

# Registros de Enrutamiento

```
ip prefix-list pl105 deny 191.255.0.0/16 le 32
ip prefix-list pl105 deny 192.0.0.0/24 le 32
ip prefix-list pl105 deny 223.255.255.0/24 le 32
ip prefix-list pl105 deny 224.0.0.0/3 le 32
ip prefix-list pl105 deny 169.254.0.0/16 le 32
ip prefix-list pl105 permit 157.246.0.0/16
ip prefix-list pl105 permit 158.165.0.0/16
ip prefix-list pl105 permit 163.41.0.0/16
ip prefix-list pl105 permit 167.128.0.0/16
ip prefix-list pl105 permit 192.135.183.0/24
ip prefix-list pl105 permit 192.220.64.0/18
ip prefix-list pl105 permit 198.98.8.0/22
ip prefix-list pl105 permit 198.98.12.0/24
ip prefix-list pl105 permit 198.140.208.0/24
ip prefix-list pl105 permit 198.237.0.0/19 ge 20 le 20
```

# Registros de Enrutamiento

```
ip prefix-list pl105 permit 198.237.48.0/20
ip prefix-list pl105 permit 198.237.96.0/20
ip prefix-list pl105 permit 198.237.120.0/21
ip prefix-list pl105 permit 198.237.127.0/24
ip prefix-list pl105 permit 198.237.128.0/20
ip prefix-list pl105 permit 199.79.32.0/20
ip prefix-list pl105 permit 204.87.204.0/24
ip prefix-list pl105 permit 206.99.0.0/19
ip prefix-list pl105 deny 0.0.0.0/0 le 32
!
no route-map AS4222-IMPORT
!
route-map AS4222-IMPORT permit 10
  match ip address prefix-list pl105
  set local-preference 1200
```

# Registros de Enrutamiento

- Para más información ver:
  - RFC2622
  - RFC2725
  - Internet Routing Registry Daemon (IRRd)  
(<http://www.irrd.net/>)

# Configurando BGP

! Nuestro AS es 3582

**router bgp 3582**

!

! No Espere por la sincronización del IGP

**no synchronization**

!

! Desactivar la sumarización automática de nuestros anuncios

**no auto-summary**

! Si tenemos varios enlaces desde el router hacia el mismo AS

! Entonces tratamos de balancear el tráfico por destino. El

! Límite es 6 caminos.

**maximum-paths 2**

# Configurando BGP

!  
! Permitir que la sesión se mantenga aunque  
! se pierdan algunos mensajes keepalives  
**no bgp fast-external-falover**

!  
! Monitorear todos los cambios en BGP a través de syslog  
**bgp log-neighbor-changes**

!  
! Configurar los parámetros para dampening de las rutas  
! utilizando la lista de NUNCA-ACEPTE y las recomendaciones  
! en RIPE-229  
**bgp dampening route-map FLAP-DAMPENING**

# Configurando BGP

!

! Anunciar nuestro bloque de una manera que no incremente  
! el uso del CPU. Hay que tratar de evitar la distribución de  
! IGP debido a que puede introducir inestabilidades en BGP.  
! Redistribución de una ruta estática es más estable pero  
! requiere que el CPU monitoree las tablas de enrutamiento  
! por posibles cambios. El uso de una instrucción network es  
! más económica en términos de CPU y más estable.

**network 128.223.0.0 mask 255.255.0.0 nlrri unicast multicast**

# Configurando BGP

! Definimos nuestro peer

**neighbor 198.32.163.2 remote-as 3701**

!

! Evitar un retiro completo de todos los prefijos anunciados

! cuando se hace un "clear ip bgp aaa.bbb.ccc.ddd". Debe notarse que

! esto mantiene una copia de la tabla antes de que las políticas se

! apliquen. En teoría doblando la necesidad de memoria

**neighbor 198.32.163.2 soft-reconfiguration inbound**

!

! Escriba un descripción del dueño/propósito de la sesión

**neighbor 198.32.163.2 description eBGP con 3701**

!

! Configurar un password para autenticar/validar la sesión

! y los mensajes del peer

**neighbor 198.32.163.2 password algobiendifical**

# Configurando BGP

! Forzar la version a 4 desabilita el tener que negociarla  
! durante el proceso de conexión y acelera el establecimiento  
! de la sesión

**neighbor 198.32.163.2 version 4**

!

! Bloquear todos los anuncios de prefijos que no deberían  
! Ser anunciados en Internet. Usar un "prefix-list" porque  
! Tienen menor impacto en el CPU y son más fáciles de  
! modificar. La lista de prefijos es definida más adelante.

**neighbor 198.32.163.2 prefix-list NUNCA-ACEPTE in**

!

! Anunciar solo los prefijos que han sido especificados por  
! nosotros y para los cuales tenemos autoridad. Esto ayuda a  
! evitar a convertirse en un proveedor de tránsito y además  
! Es lo que se debe hacer ;-)

**neighbor 10.10.5.1 prefix-list MIS-PREFIJOS out**

# Configurando BGP

! Para protegernos contra errores o problemas internos de  
! nuestro peer (o alguien con quien nuestro peer tiene un  
! acuerdo de intercambio o transito) que puedan sobrecargar  
! nuestro router o las tablas de BGP, vamos a limitar el número  
! de prefijos que aceptamos. Cuando IOS ve que los anuncios  
! han llegado al 75% del límite comienza a enviar mensajes a  
! los logs. Se puede modificar el porcentaje por el cual  
! comenzamos a recibir mensajes si lo agregamos al final de la  
! línea. Por ejemplo, `maximum prefix 130000 90`, causará que  
! IOS envíe mensajes cuando el peer anuncia 90% del  
! límite.

**`neighbor 198.32.163.2 maximum-prefix 125000`**

# Configurando BGP

!

! Este es nuestro peer interno

```
neighbor 128.223.253.23 remote-as 3582
```

!

! Cambiar la descripción y la clave de la sesión. El resto de los  
! comandos es común.

```
neighbor 128.223.253.23 description iBGP con 128.223.253.23
```

```
neighbor 128.223.253.23 password otropassworddifícil
```

```
neighbor 128.223.253.23 soft-reconfiguration inbound
```

```
neighbor 128.223.253.23 version 4
```

```
neighbor 128.223.253.23 next-hop-self
```

```
neighbor 128.223.253.23 prefix-list NUNCA-ACEPTE in
```

```
neighbor 128.223.253.23 maximum-prefix 130000
```

!

! Usar la interfase de loopback para iBGP. Esto ayuda a incrementar la  
! estabilidad de la sesión.

```
neighbor 128.223.253.23 update-source Loopback0
```

# Configurando BGP

! Agregar rutas estáticas para nuestro prefijo apuntando hacia  
! null, para el loopback de iBGP. Además hay que agregar rutas  
! estáticas para los prefijos más específicos que se requieran  
!

**ip route 128.223.0.0 255.255.224.0 Null0**

**ip route 128.223.253.23 255.255.255.255 192.168.50.2**

**ip route 128.223.175.0 255.255.255.0 192.168.50.5**

**ip route 128.223.140.128 255.255.255.128 192.168.50.8**

# Configurando BGP

- ! Debemos restringir quien se conecta al puerto 179 (BGP). Solo
- ! permitiremos las conexiones desde nuestros peers. Cualquier otro
- ! intento será registrado en los logs.
- ! Este ACL debe ser aplicado a las interfaces externas o este
- ! segmento deberá ser agregado a un ACL existente
- !

```
ip access-list extended inbound-filter
permit tcp any any established
deny ip 128.223.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 0.0.0.0 0.255.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
```

# Configurando BGP

```
permit tcp host 198.32.163.2 host 198.32.163.1 eq 179  
permit tcp host 198.32.163.2 eq bgp host 198.32.163.1  
deny tcp any host 198.32.163.1 eq 179
```

! Por lo menos queremos un registro de los intentos de  
! conexión. También podríamos bloquearlo por completo

```
permit tcp any any eq 179 log
```

# Configurando BGP

! La lista de prefijos MIS-PREFIJOS nos previene de anunciar  
! otros prefijos a excepción del espacio asignado.

!

**ip prefix-list MIS-PREFIJOS description AS3582**

**ip prefix-list MIS-PREFIJOS seq 5 permit 128.223.0.0/16**

**ip prefix-list MIS-PREFIJOS seq 100 deny 0.0.0.0/0 le 32**

# Configurando BGP

! La lista de prefijos NUNCA-ACEPTE previene el aceptar  
! actualizaciones de prefijos obviamente erróneos. La lista está  
! basada en las asignaciones hechas por IANA, incluyendo los  
! prefijos que no han sido asignados y prefijos que han sido  
! designados para usos especiales. Estos prefijos nunca  
! deberían ser vistos en los anuncios de NLRI's. Para  
! información más detallada ver RFC1918 y  
! <http://www.iana.org/assignments/ipv4-address-space>  
!

```
ip prefix-list NUNCA-ACEPTE description Lista de Rechazos  
ip prefix-list NUNCA-ACEPTE seq 5 deny 0.0.0.0/8 le 32  
ip prefix-list NUNCA-ACEPTE seq 10 deny 1.0.0.0/8 le 32  
ip prefix-list NUNCA-ACEPTE seq 15 deny 2.0.0.0/8 le 32  
ip prefix-list NUNCA-ACEPTE seq 20 deny 5.0.0.0/8 le 32  
ip prefix-list NUNCA-ACEPTE seq 25 deny 7.0.0.0/8 le 32
```

# Configurando BGP

....

**ip prefix-list NUNCA-ACEPTE seq 495 deny 192.168.0.0/16 le 32**

**ip prefix-list NUNCA-ACEPTE seq 500 deny 197.0.0.0/8 le 32**

**ip prefix-list NUNCA-ACEPTE seq 505 deny 223.0.0.0/8 le 32**

**ip prefix-list NUNCA-ACEPTE seq 510 deny 224.0.0.0/3 le 32**

**! Aquí también podemos definir el prefijo más largo que vamos a  
! aceptar. Algunos ISPs no aceptan nada mayor de /24 pero tu  
! puedes determinar tus propias políticas.**

**ip prefix-list NUNCA-ACEPTE seq 999 permit 0.0.0.0/0 le 25**

# Configurando BGP

**! La siguiente configuración para dampening ayuda  
! a minorizar los efectos de dampening en los  
! prefijos más cortos e históricamente más estables  
! y los bloques que contienen los servidores root de  
! DNS. Los prefijos mas largos son castigados por  
! periodos de tiempo mas largos debido a que estos  
! son la fuente de un mayor porcentaje de las  
! inestabilidades de las tablas de enrutamiento  
! globales. A prefijos más largos, menor agregación  
! y menor bloque de direcciones. Esta configuración  
! está basada en las recomendaciones de RIPE-229**

# Configurando BGP

! La lista PREFIJOS-LARGOS es para prefijos de /24 o más  
**ip prefix-list PREFIJOS-LARGOS description Prefijos >= /24**  
**ip prefix-list PREFIJOS-LARGOS seq 5 permit 0.0.0.0/0 ge 24**  
!

! La lista PREFIJOS-MEDIANOS es para prefijos /22 y /23  
**ip prefix-list PREFIJOS-MEDIANOS description Prefijos /22 y /23**  
**ip prefix-list PREFIJOS-MEDIANOS seq 5 permit 0.0.0.0/0 ge 22 le 23**  
!

! La lista PREFIJOS-CORTOS es para prefijos menores de /22  
**ip prefix-list PREFIJOS-CORTOS description Prefijos <= 21**  
**ip prefix-list PREFIJOS-CORTOS seq 5 permit 0.0.0.0/0 le 21**

# Configurando BGP

! La lista ROOTSERVERS es para prevenir castigar los prefijos donde  
! están los rootservers

```
ip prefix-list ROOTSERVERS description Bloques de DNS rootservers
ip prefix-list ROOTSERVERS seq 5 permit 198.41.0.0/24
ip prefix-list ROOTSERVERS seq 10 permit 128.9.0.0/16
ip prefix-list ROOTSERVERS seq 15 permit 192.33.4.0/24
ip prefix-list ROOTSERVERS seq 20 permit 128.8.0.0/16
ip prefix-list ROOTSERVERS seq 25 permit 192.203.230.0/24
ip prefix-list ROOTSERVERS seq 30 permit 192.5.4.0/23
ip prefix-list ROOTSERVERS seq 35 permit 192.112.36.0/24
ip prefix-list ROOTSERVERS seq 40 permit 128.63.0.0/16
ip prefix-list ROOTSERVERS seq 45 permit 192.36.148.0/24
ip prefix-list ROOTSERVERS seq 50 permit 193.0.14.0/24
ip prefix-list ROOTSERVERS seq 55 permit 198.32.64.0/24
ip prefix-list ROOTSERVERS seq 60 permit 202.12.27.0/24
```

# Configurando BGP

! Ahora creamos la política usando un route-map

! Perdona los ROOTSERVERS

```
route-map FLAP-DAMPENING deny 10
```

```
match ip address prefix-list ROOTSERVERS
```

! Castiga los /24 a un máximo de 60 minutos

```
route-map FLAP-DAMPENING permit 20
```

```
match ip address prefix-list PREFIJOS-LARGOS
```

```
set dampening 30 750 3000 60
```

# Configurando BGP

! Castiga los prefijos /22 y /23 a un máximo de 45  
! minutos

```
route-map FLAP-DAMPENING permit 30  
match ip address prefix-list PREFIJOS-MEDIANOS  
set dampening 15 750 3000 45
```

! Castiga los prefijos menores que /22 a un máximo  
! de 30 minutos

```
route-map FLAP-DAMPENING permit 40  
match ip address prefix-list PREFIJOS-CORTOS  
set dampening 10 1500 3000 30
```

# Configurando BGP

```
set dampening <half-life> <reuse-limit>  
<suppress-limit> <max-suppress>
```

## Para más información:

- RFC2439 BGP Route Flap Damping (Proposed Standard)  
(<ftp://ftp.ietf.org/rfc/rfc2439.txt>)
- Cisco BGP Case Studies: Route Flap Damping  
(<http://www.cisco.com/warp/public/459/16.htm>)
- ISI/RSd Configuration: Route Flap Damping  
(<http://www.isi.edu/div7/ra/RSd/doc/dampen.html>)
- RIPE-229  
(<http://www.ripe.net/ripe/docs/routeflap-damping.html>)

# En qué se está Trabajando?

- Para tratar de solucionar el resto de los problemas de seguridad en BGP, dos propuestas están siendo desarrolladas:
  - S-BGP (BBN Technologies)
  - SOBGP (IETF)

# Secure BGP (SBGP)

- **Para validar la autenticidad e integridad de las actualizaciones de BGP que se reciben y para verificar la identidad y autoridad de quien envía el mensaje se usan:**
  - **Dos PKIs basadas en certificados X.509 v3**
    - **Asignación de Direcciones (1 tipo de certificado)**
    - **Asignación de ASNs y Relación de los Routers (3 tipos de certificados)**
  - **Un nuevo atributo transitivo llamado “Attestation”**
    - **Router**
    - **Prefijo**
  - **IPSec**

# Secure BGP (SBGP)

- Para validar un ruta recibida desde  $AS_n$  ,  $AS_{n+1}$  necesita:
  - 1 “address attestation” de cada una de las organizaciones dueñas de un bloque(s) de direcciones en el NLRI
  - 1 certificado de asignación de direcciones de cada una de las organizaciones dueñas de un bloque(s) de direcciones en el NLRI
  - 1 “route attestation” de cada router con SBGP (o su ASN) a través del camino ( $AS_n$  a  $AS_1$ ), donde el “route attestation” generado y firmado por router x (o  $AS_x$ ) especifica el NLRI y el  $AS\_PATH$  desde  $AS_{x+1}$  hacia  $AS_1$
  - 1 certificado por cada router con SBGP a través del camino ( $AS_n$  a  $AS_1$ ) para verificar las firmas en los “route attestations”

# Secure BGP (SBGP)

- Si un router no entiende SBGPe el atributo de "attestation" es ignorado
- Existe una implementación inicial en gateD como prueba de concepto
- Un IETF draft
  - draft-clynn-s-bgp-protocol-00a.txt

# Secure Origin BGP (soBGP)

- Crea un nuevo mensaje de BGP denominado "Security Message" (tipo 6)
- Tres tipos de certificados
  - Certificado de Entidad
  - Certificado de Política
  - Certificado de Autorización
- La capacidad de intercambiar mensajes de seguridad deberá ser negociada al inicio de la sesión

# Secure Origin BGP (soBGP)

- Todavía no hay implementaciones
- Dos IETF drafts han sido generados:
  - draft-ng-sobgp-bgp-extensions-00.txt
  - draft-white-sobgp-bgp-extensions-00.txt

# Recursos Recomendados

- Secure BGP Project (S-BGP)  
<http://www.net-tech.bbn.com/sbgp>
- IETF Inter-domain Routing WG  
<http://www.ietf.org/html.charters/idr-charter.html>
- Secure BGP Template  
(<http://www.cymru.com/Documents/secure-bgp-template.html>)
- BGP Expert (<http://www.bgpexpert.com/resources.php>)