(In)Seguridad en IPv6

O peligros del IPv6 en redes Ipv4

@hugo_glez

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Precaución:

La plática no contendrá “profundizaciones técnicas”, es un tema que estoy explorando/trabajando y busco **colaboradores**

¿Me debería interesar?

Muchos sistemas traen IPv6 activado por defecto.

Solaris
Linux
Win ..
MAC

Agenda

- Reflexiones
- ¿Qué es IPv6?
- Diferencias IPv4
- Problemas de IPv6 en redes IPv4
- Tools
- Demo
- Conclusiones

Reflexiones de la seguridad IPv6

- Tenemos menos experiencia con IPv6.
- Las implementaciones de IPv6 son menos maduras que las de IPv4.
- Los productos de seguridad (firewalls, ids) tienen menos soporte para IPv6
- La complejidad de la migración ... *********
- Recursos humanos menos preparados

¿Qué es IPv6?

- El Internet Protocol version 6 (IPv6) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.
- Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

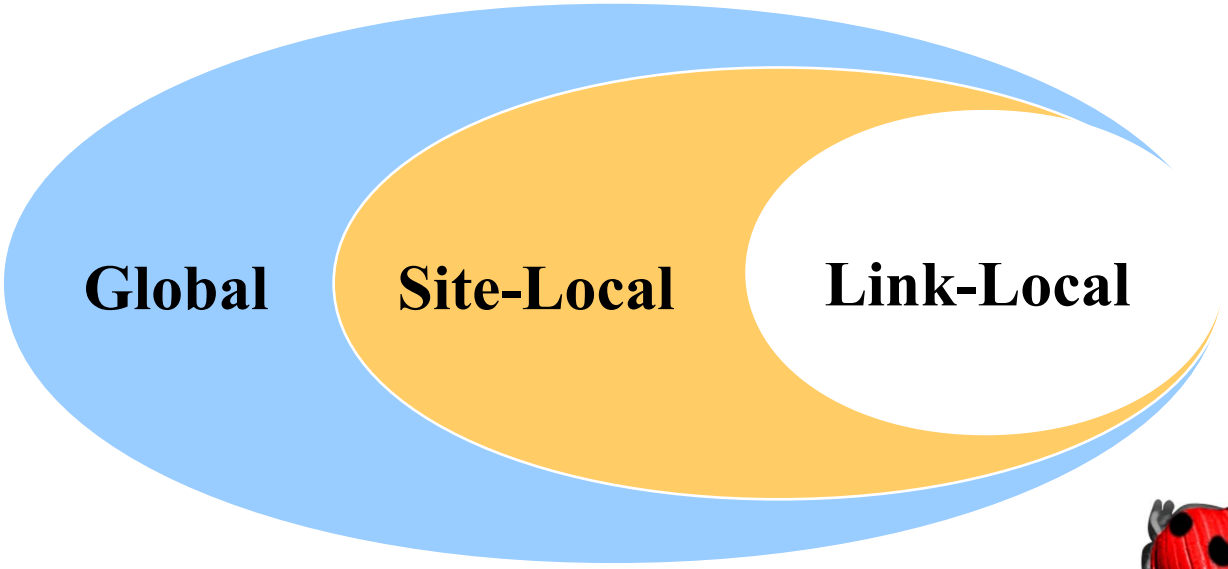
Ventajas

- Mayor número de direcciones 2 **64
- IPSec
- Ruteo global, todos los dispositivos con dirección podrían ser alcanzables
- Mobile ipv6
- Autoconfiguración

Direcciones

- fe80::92cf:15ff:fe5f:747a
- ff02::1:2

- Multicast
- Unicast
- Anycast



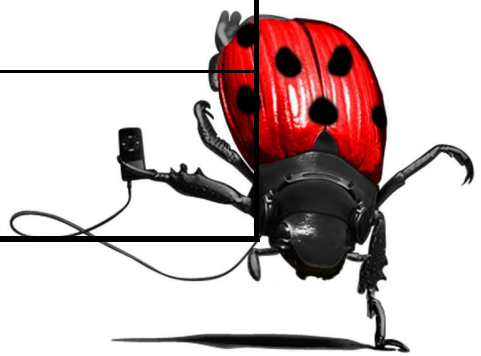
- No Broadcast !!

Métodos de migración

- Dual stack
- NAT-PT
  - 6to4
  - 4to6
- Tunneling

Comparaciones

	IPv4	IPv6
Addressing	32 bits	128 bits
Address resolution	ARP	ICMPv6 NS/NA (+ MLD)
Auto-configuration	DHCP & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (optional) (+ MLD)
Fault Isolation	ICMPv4	ICMPv6
IPsec support	Optional	Mandatory (to "optional")
Fragmentation	Both in hosts and routers	Only in hosts



IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options				Padding

IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

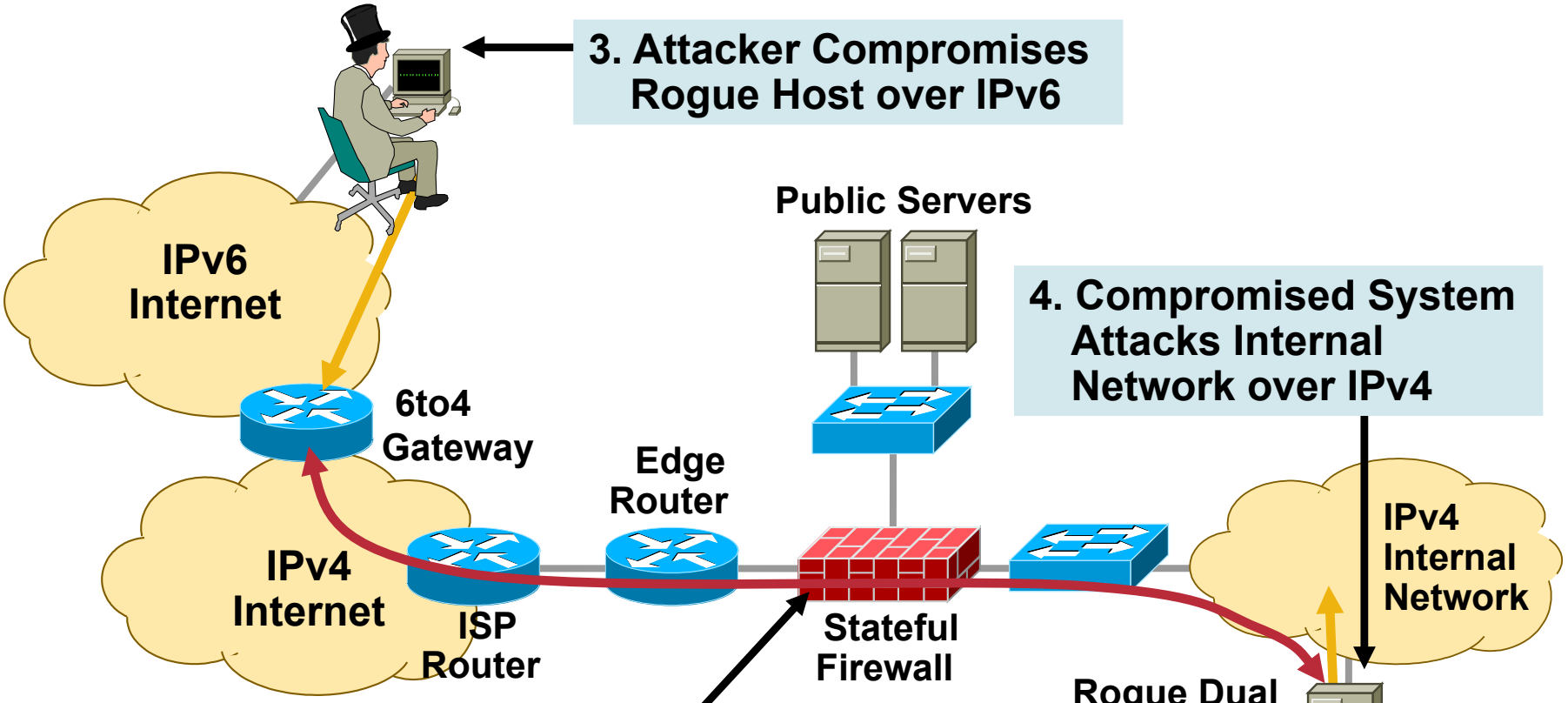
Legend

- —Field's Name Kept from IPv4 to IPv6
- —Fields Not Kept in IPv6
- —Name and Position Changed in IPv6
- —New Field in IPv6

Problemas

- "Tunneling"
  - Los firewalls, ids, ... no saben de IPv6
  - Teredo

IPv6 Attack Against IPv4



Note That This Tunneling Can Be Benign in Origin Whereas Other Tunnels (Like GRE) Tend to Require an Active Participant Inside and Outside

2. Firewall Permits Outbound IP Protocol 41

1. Rogue Device Establishes 6to4 Tunnel to IPv6 Internet

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Problema

- Information disclosure pasiva
  - Los dispositivos Apple anuncian su presencia y otra información.
  - Su dirección Ipv4
  -
  - Tcpdump -nni eth0 'ip6'

06:54:51.752524 IP6 fe80::cabc:c8ff:fe36:c1a1.5353 > ff02::fb.5353: 0*- [0q] 4/0/3 (Cache flush) PTR Jose-Mansurs-iPad.local., (Cache flush) PTR **Jose-Mansurs-iPad.local., (Cache flush) AAAA fe80::cabc:c8ff:fe36:c1a1, (Cache flush) A 172.28.53.99 (256)**

06:54:29.359739 IP6 fe80::92cf:15ff:fe5f:747a.546 > ff02::1:2.547: dhcp6 solicit

06:54:51.164693 IP6 fe80::5a55:caff:fe17:1caf.5353 > ff02::fb.5353: 0 [2q] [2n] [1au] ANY (QM)? **iPhone-de-Julio-Alexander.local. ANY (QM)? iPhone-de-Julio-Alexander.local. (122)**

Problemas

- MiTM
  - Fake router AV con mayor prioridad ó dhcp6 server
  - DNS ...
  - Tunneling
  - Proxy SSL

Problemas

- DoS
  - Fake router AV
  - Black hole
  - Flooding
  - Smurf attack

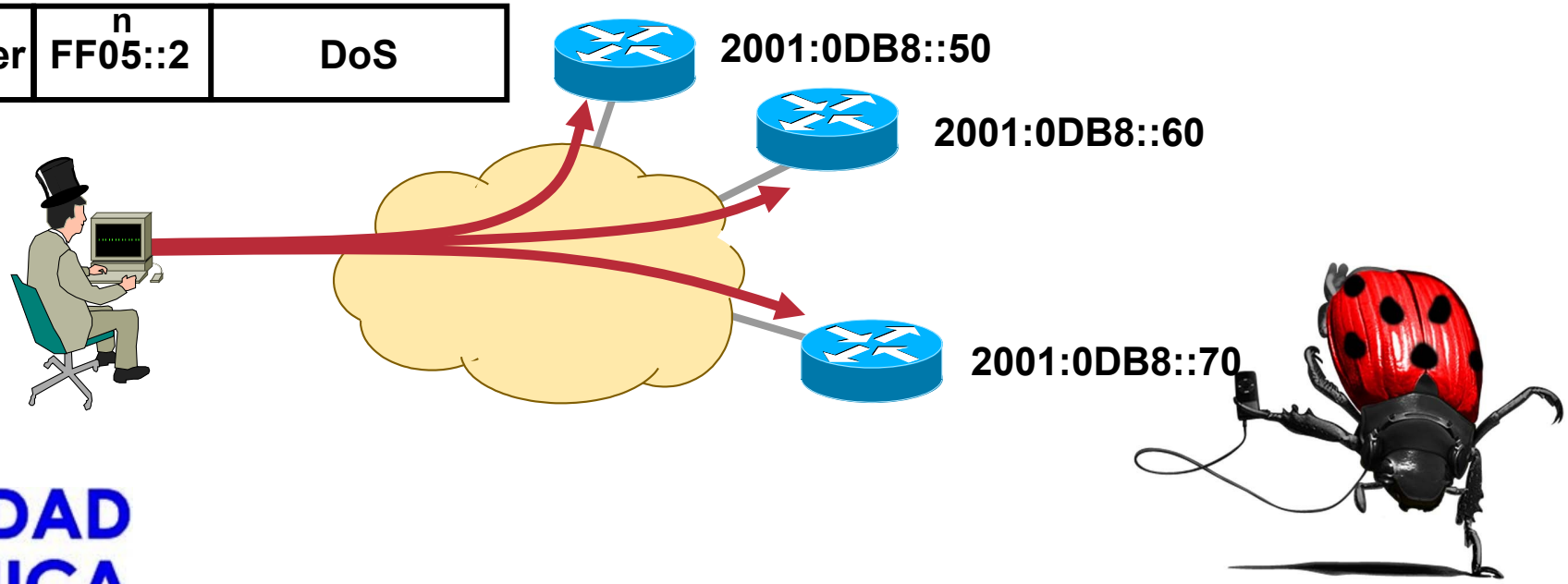
Reconocimiento

- Se necesitan DNS's
- Al no haber NAT se necesitan DNS's dinámicos
- Se usarán “posiblemente” direcciones fáciles de recordar para los DNS
  - ::10 , ::20, ::FOOD
- Relacionadas con las MAC, buscar por las NIC más comunes.

- No es posible usar nmap para escanear la red
  - Escuchar arp
  - Formar direcciones locales
  - Escanear el host de manera individual
- Tools
  - alive6, te dice todos los clientes con soporte ipv6

- Ahora hay direcciones multicast para ciertos recursos
  - FF05::2 routers FF05::1:3 dhcpservers

Source	Destination	Payload
Attacker	FF05::2	DoS



Attack suite

Www.thc.org/thc-ipv6

Van Houser

The Hackers Choice

Tools

- THC-IPv6
  - parasite6
  - Alive6
  - Dnsdic6
  - fake_router6
  - Redir6
  - Toobig6
  - Trace6
  - flood_router6
- Denial6
- flood_advertise6
- Rsmurf6
- Sendpees6
- thcping6

Demo

@hugo_glez

hugo.gonzalez@acm.org

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Conclusiones

- Ipv6 superficio de ataque.
- Redes ipv4 por todos lados, pero ... muchos clientes con capacidades Ipv6 habilitadas.
-
- Deshabilita IPv6 si no la utilizas
- Ipv6 ya viene en camino.

Fuentes

- van Houser
- Fernando Gont

Gracias a todos !