



Something Old Is New Again

Merike Kaeo

merike@doubleshotsecurity.com

www.doubleshotsecurity.com



Internet Evolution

- Networking Stuff [data link and network layer]
 - Bridging vs Routing
 - Switching
 - VLANs
- Applications – Isn't this what we really care about?
 - Email/Web were the beginning
 - Web 2.0 / P2P is the now and the future
- Cloud Computing – Someone else may be running the infrastructure that house your applications
- Where does Security fit in?



What Are Security Goals?

- Controlling Data Access
- Controlling Network Access
- Ensuring Network Availability
- Protecting Information In Transit
- Preventing Intrusions
- Responding To Security Breaches
- Privacy? – Related but Orthogonal



Causes of Security Related Issues

- Protocol error
 - No one gets it right the first time
- Software bugs
 - Is it a bug or feature ?
- Active attack
 - Target control/management plane
 - Target data plane
 - More probable than you think !
- Configuration mistakes
 - Most common form of problem

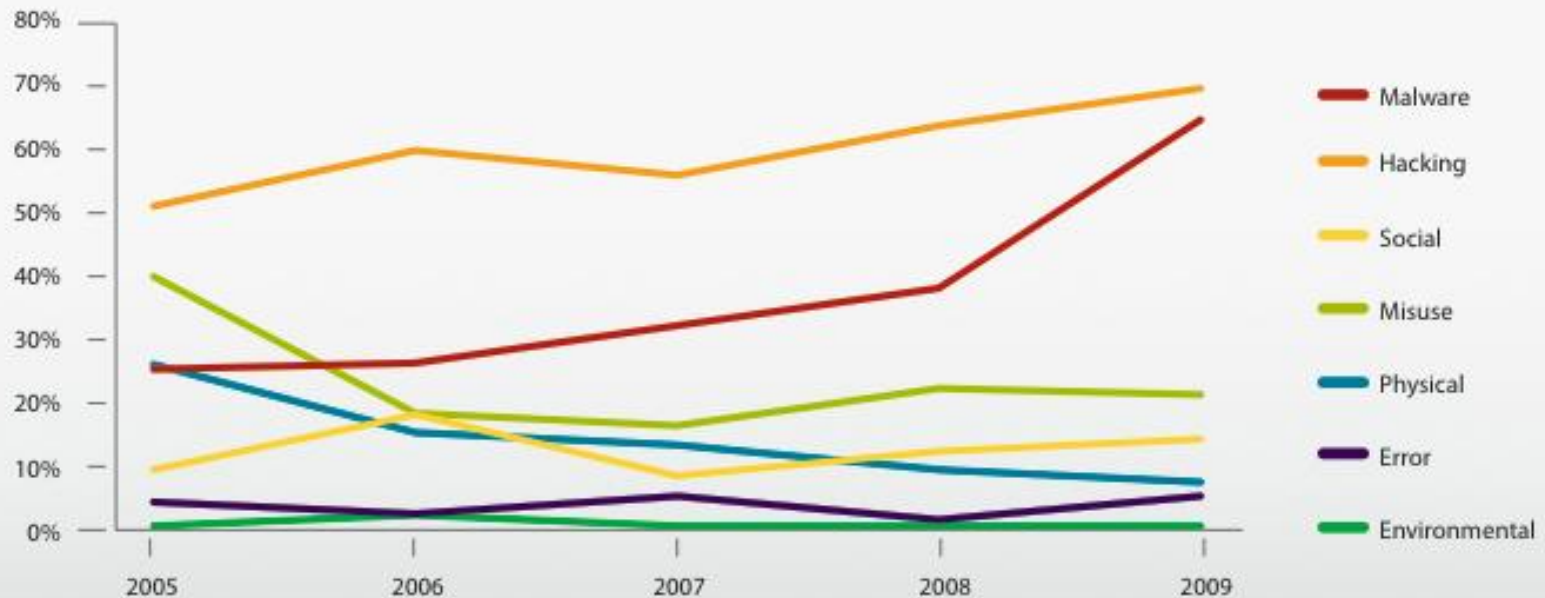


Realities of Current Security Issues

The following data re Security Breaches is from:

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

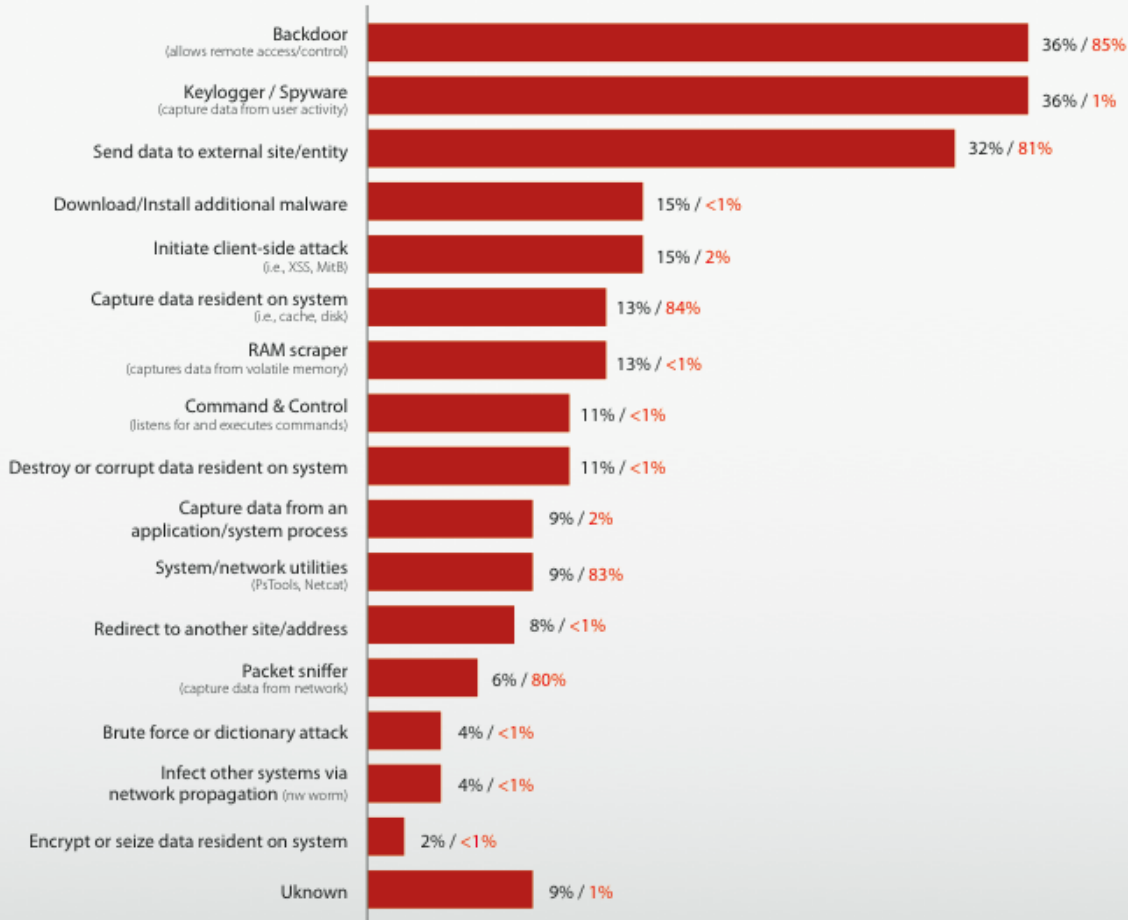
Figure 16. Threat action categories over time by percent of breaches (Verizon cases)





Data Breaches - Malware

Figure 19. Malware functionality by percent of breaches within Malware and percent of records

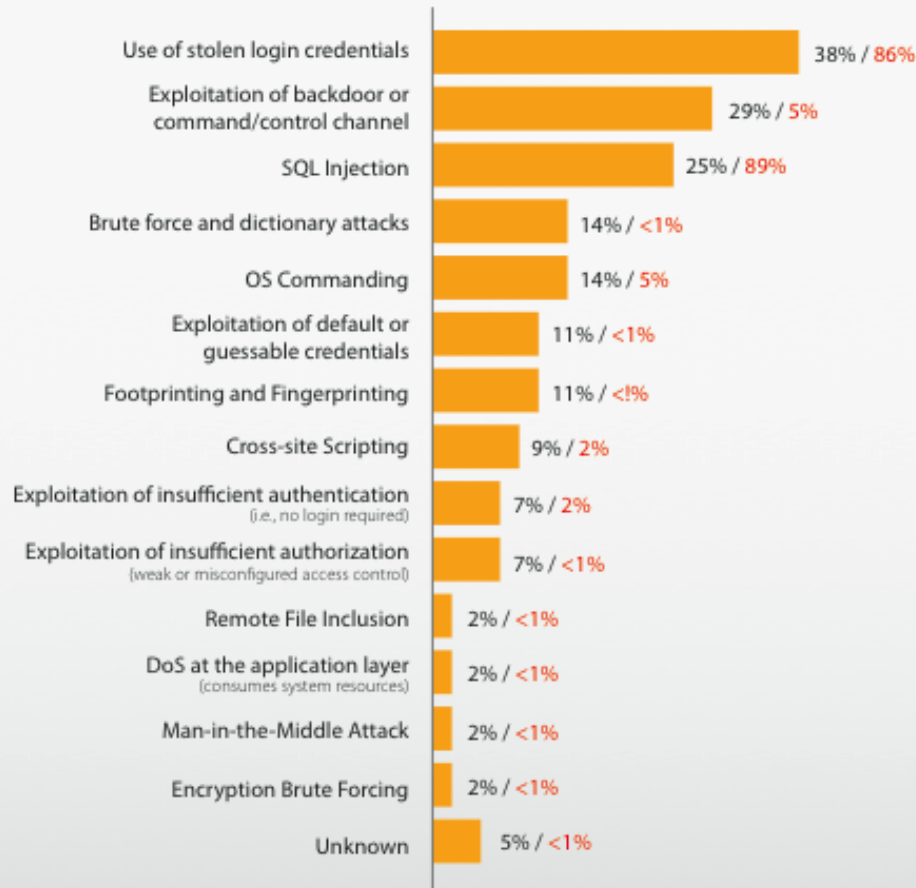


Malware is any software developed for compromising or harming information assets.



Data Breaches - Hacking

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records

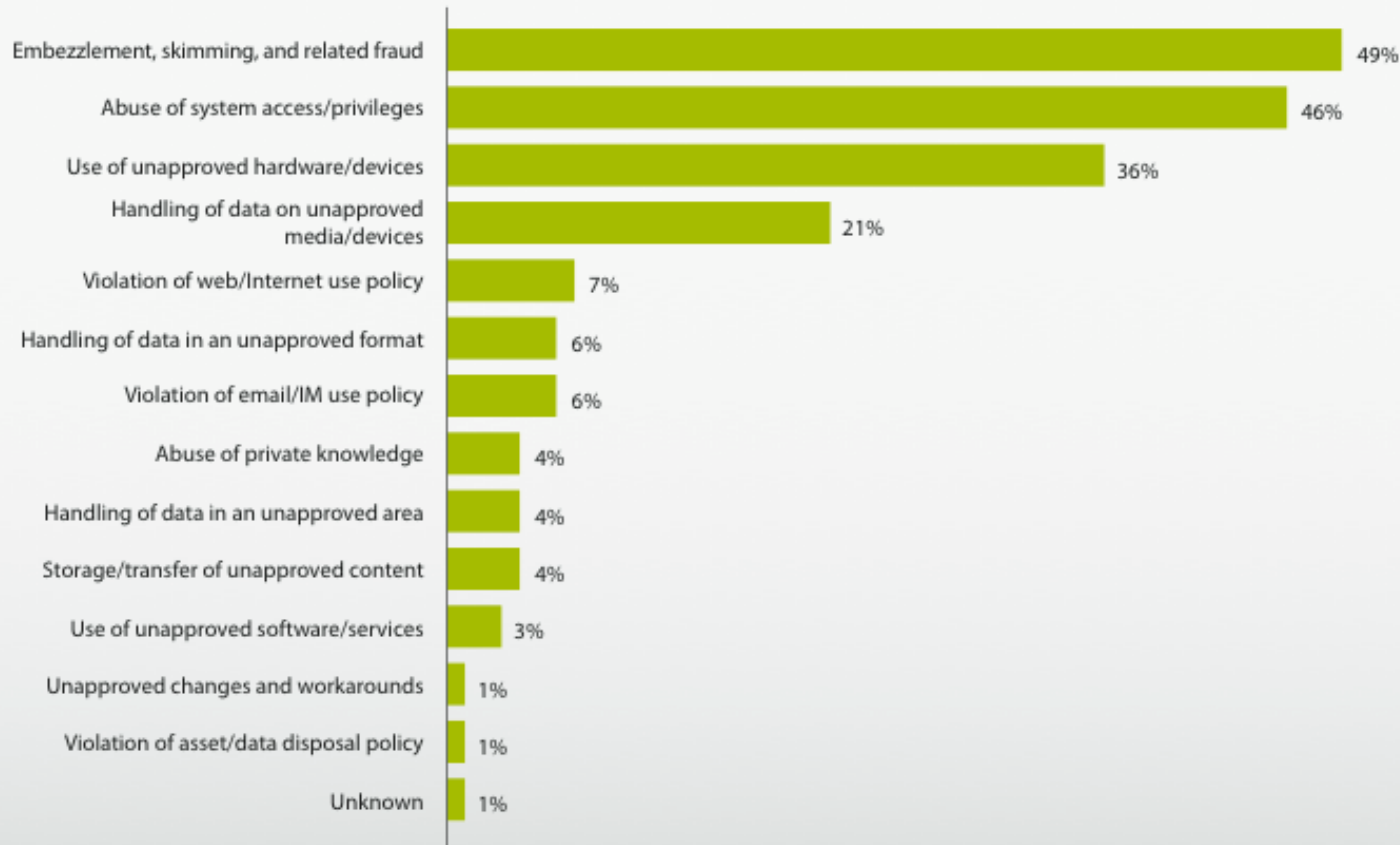


Hacking is any activity where someone attempts to intentionally access or harm information assets without authorization by bypassing logical security mechanisms.



Data Breaches - Misuse

Figure 25. Types of misuse by percent of breaches within Misuse



Misuse is using any organizational resources or privileges for any purpose that is contrary to that which was intended. It can be deliberate or unintentional.



Security Services

- User Authentication / Authorization
- Device Authentication / Authorization
- Access Control (Packet Filtering)
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation



What Is The Same / What Is Different

- Same for IPv4 and IPv6
 - Security Properties
 - Security Services
- Different for IPv6 Architectures
 - Protocol Operation
 - More Automation
 - Scalable Mobile Hosts
 - Potential Application Integration



What About Cloud Computing?

- New Jargon (more confusion)
- Trust Models are Different
 - You trust a 3rd party with your data and not your IT department
- What Is Still Same
 - Security properties
 - Security services

Accountability Is Important

- *Controlled Access and Audit Enforcement*
- *Are the individual VMs hardened?*

TRUST but VERIFY



Operational Security Considerations

- Is automation advantageous or a security risk?
- How will IPv4/IPv6 content be accessible?
 - Is NAT a security feature or a simple way of getting access to the global Internet (without paying for it)?
 - Where is an address translation capability required?
- Network vs host-based security mitigation?
- What technologies need to be made easier to deploy to be operationally viable?



Architecture Considerations

- Addressing / Naming
 - What subnet boundaries make sense
 - your own network infrastructure
 - filtering considerations
 - Endpoint Identifier management
 - address automation vs obscurity vs auditability
 - DNS and DHCPv6 Considerations
- Native Routing vs Tunnels
- Management
- Security (Is This A Last Consideration In Practice?)

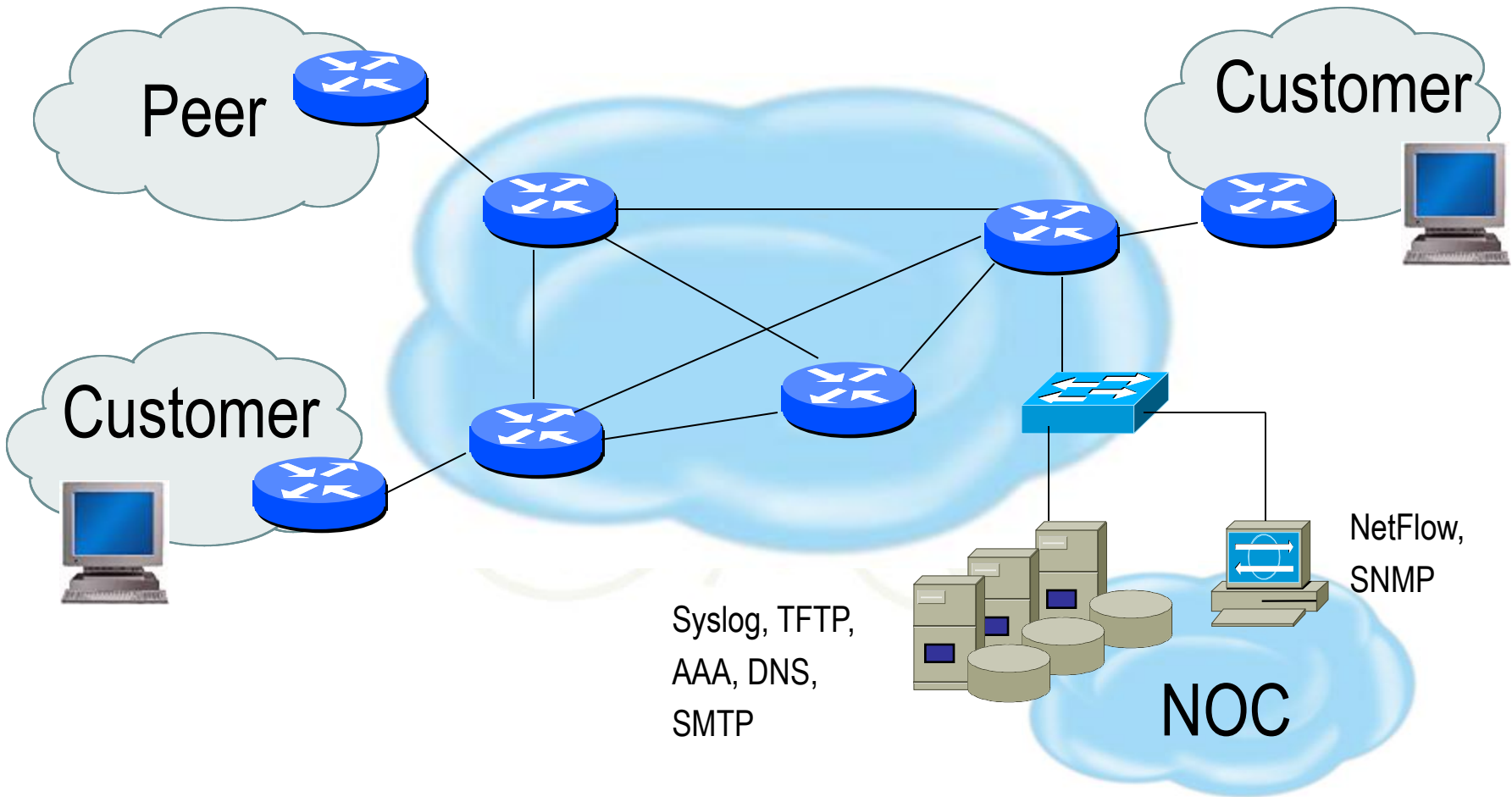


IPv6 Security Enhancements

- **Fragmentation**
 - Prohibited by intermediary devices
 - Overlapping fragments are not allowed
 - Devices must drop reassembled packets that are less than 1280 bytes
- **Broadcasts**
 - Removes concept of dedicated broadcasts
 - Specific language to avoid ICMPv6 broadcast amplification attacks
- **IPsec**
 - Defined into the base protocol spec



Infrastructure Security





Fundamental Issues

- What is meant by *Securing The Network* ?
- Design security into IPv6 networks that do not blindly mimic the current IPv4 architectures
 - Don't break working v4 infrastructure
 - Don't re-architect current problems and place limitations on IPv6 capabilities
- Requires some thought to policy
 - Where are you vulnerable today ?
 - What new application capabilities are possible with IPv6?
 - New risk assessment will help (re)define appropriate security policy
- Security policy will dictate which security measures to implement

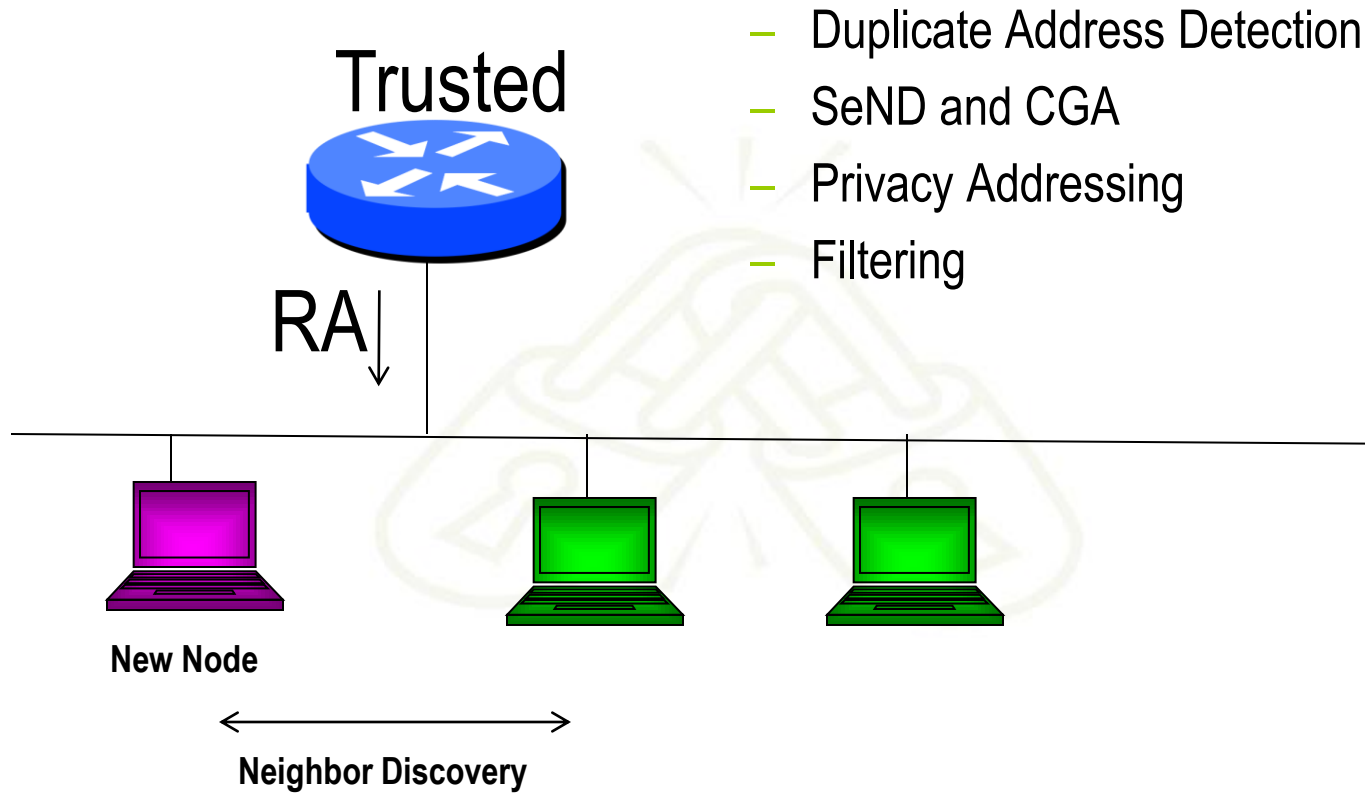


IPv6 Security Theory vs Reality

- IPv6 has security built-in
 - Mostly based on mandate to implement IPsec
 - IPsec use was never fully defined in IPsec specs
 - Early implementations made it up
 - Configuration is still difficult and often operationally not optimal
 - IPv6 conformance testing doesn't necessarily require it
- IPv6 needs IPv4 security feature parity
 - Yes and No 😊

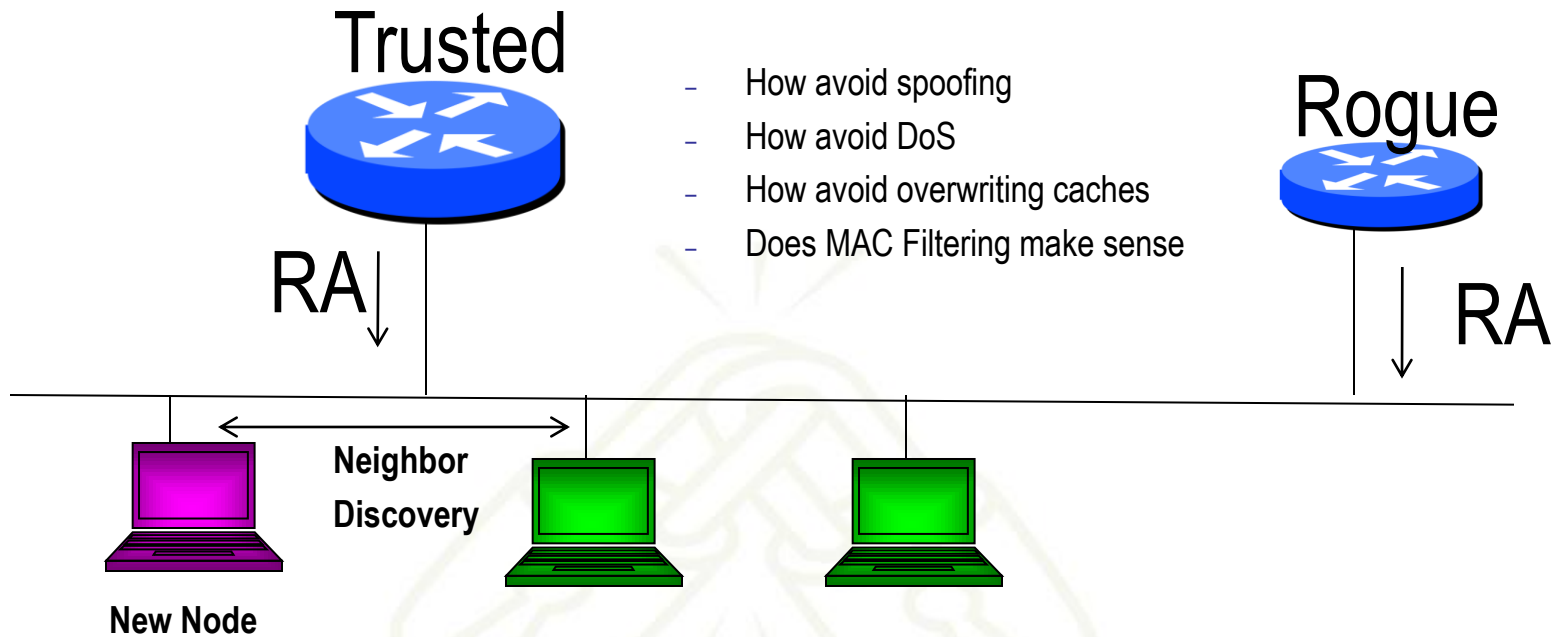


Node Initialization Security (Theory)





Node Initialization Security (Practice)



- How avoid spoofing
- How avoid DoS
- How avoid overwriting caches
- Does MAC Filtering make sense

- Host behaviors vary and need to be understood
- SeND and CGA not widely used (yet?)
- Layer 2 mitigation techniques wip for vendors
- <http://www.kb.cert.org/vuls/id/472363>



Node Global Addressing Security (Theory)

- Static addressing can be used
- Stateful Autoconfiguration
 - Requires use of a server to give hosts information
- Stateless Autoconfiguration
 - Requires no manual configuration of hosts
 - Minimal (if any) configuration on routers
- Privacy Addresses (rfc4941)
- Router Advertisements vs DHCPv6



Node Global Addressing Security (Practice)

- Statically defined addresses used for critical devices
- Privacy addresses are used by default by Vista
 - How do you correlate IPv6 address to log info?
- Router Advertisement
 - Relying on unauthenticated broadcast packet to determine where host should send traffic to
- DHCPv6
 - Can send requests to local LAN before get an RA message telling you to do so. This requires manual configuration on host



Better RA/DHCPv6 Filtering Needed

- Networks with visitors have shown a serious problem with rogue RA and DHCP servers
 - Networks with visitors that use either RA or DHCPv6 for address assignment will have the exact same problem if someone comes along with a rogue server
- Features needed to limit where RA messages and DHCPv6 messages can be sent from
 - Allow RA messages only from routers, and DHCPv6 responses only from DHCPv6 servers
- Some Ethernet equipment has the ability to filter on Ethernet source/destination
 - Only allow messages to the all routers multicast address to go to the switch interfaces that have routers on them
 - Only allow messages to the all DHCPv6 servers multicast address to go to the switch interfaces that have DHCPv6 servers or relays on them



Packet and/or Route Filtering in IPv6

- In theory, certain addresses should not be seen on the global Internet
- In practice, they are and filters aren't being deployed (even when capability available)



```
ipv6 access-list extended DSL-ipv6-Outbound  
permit ipv6 2001:DB8:AA65::/48 any  
deny ipv6 any any log
```

```
interface atm 0/0  
ipv6 traffic-filter DSL-ipv6_Outbound out
```



General Firewall BCP (same for IPv6 and IPv4 networks)

- Explicitly deny all traffic and only allow what you need
- The default policy should be that if the firewall doesn't know what to do with the packet, deny/drop it
- Don't rely only on your firewall for all protection of your network
- Implement multiple layers of network protection
- Make sure all of the network traffic passes through the firewall
- Log all firewall exceptions (if possible)



Ingress IPv6 Packet Filters To Consider

- Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Reject the packets which contain relevant special-use prefix in the **source** address field
 - `::1/128` : loop back address
 - `::/128` : unspecified address
 - `::/96` : IETF reserved address; IPv4-compatible IPv6 address
 - `::ffff:0:0/96` : IPv4-mapped IPv6 address
 - `::/8` : reserved
 - `fc00::/7` : unique-local address
 - `ff00::/8` : multicast address
 - `2001:db8::/3` : documentation addresses



Ingress IPv6 Packet Filters To Consider (2)

- Reject the packets which contain relevant special-use prefix in the **destination** address field
 - `::1/128` : loop back address
 - `::/128` : unspecified address
 - `::/96` : IETF reserved address; IPv4-compatible IPv6 address
 - `::ffff:0:0/96` : IPv4-mapped IPv6 address
 - `::/8` : reserved
 - `fc00::/7` : unique-local [`fc00::/16`] and site-local [`fc00::/10`] address
 - `2001:db8::/32` : documentation address
- Reject the packets which have your own prefix in the source address field
- Reject packets that use the routing header Care must be taken not to reject ICMPv6 packets whose source address used with Duplicate Address Detection is the unspecified address (`::/128`). If all of ICMPv6 is accepted, then there is no problem although ordering of the filters needs to be carefully thought through.



Egress IPv6 Packet Filters To Consider

- Permit sending all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Deny sending the packets which contain special-use prefix in the source address field
 - `::1/128` : loop back address
 - `::/128` : unspecified address
 - `::/96` : IETF reserved address; IPv4-compatible IPv6 address
 - `::ffff:0:0/96` : IPv4-mapped IPv6 address
 - `::/8` : reserved
 - `fc00::/7` : unique-local address
 - `ff00::/8` : multicast address
 - `2001:db8::/32` : documentation address
- Deny sending packets that use the routing header [unless using mobility features]
- Deny sending packets with destination address in the 6to4 reserved address range (`2002::/16`) if not supporting 6to4 services (i.e. relays) and not providing transit services
- Deny sending packets with destination address in the Teredo address range (`2001::/32`) if not running a Teredo relay or offering a Teredo transit service
- Multicast address should only be in source address field.



Allow Following ICMPv6 Through Firewall

- ICMPv6 type 1 code 0: no route to destination
- ICMPv6 type 2: packet too big (required for PMTUD)
- ICMPv6 type 3: time exceeded
- ICMPv6 type 4: parameter problem (informational when IPv6 node has problem identifying a field in the IPv6 header or in an extension header)
- ICMPv6 type 128: echo request
- ICMPv6 type 129: echo reply



Allow Following ICMPv6 To/From A Firewall

- ICMPv6 type 2: packet too big – firewall device is not allowed to fragment IPv6 packets going through it and must be able to generate this message for correct PMTUD behavior
- ICMPv6 type 4: parameter problem
- ICMPv6 type 130-132: multicast listener messages – in IPv6 a routing device must accept these messages to participate in multicast routing
- ICMPv6 type 133-134: router solicitation and advertisement – needed for IPv6 autoconfiguration
- ICMPv6 type 135-136: neighbor solicitation and advertisement – used for duplicate address detection and layer2-to-IPv6 address resolution



Need Better IPv6 Extension Header Filtering

- Carry the additional options and padding features that are part of the base IPv4 header
- Extension headers are optional and placed after the base header
- There can be zero, one, or more Extension Headers between the IPv6 header and the upper-layer protocol header
- Ordering is important

➤ Currently Defined IPv6 Extension Headers:

- Hop-by-Hop Options (0)
- Routing Header (43)
- Fragment Header (44)
- ESP Header (50)
- Authentication Header (51)
- Destination Options (60)

➤ Other Extension Header Values:

- TCP upper-layer (6)
- UDP upper-layer (17)
- ICMPv6 (58)
- No Next Header Present (59)



Routing Header: RFC 2460 Text

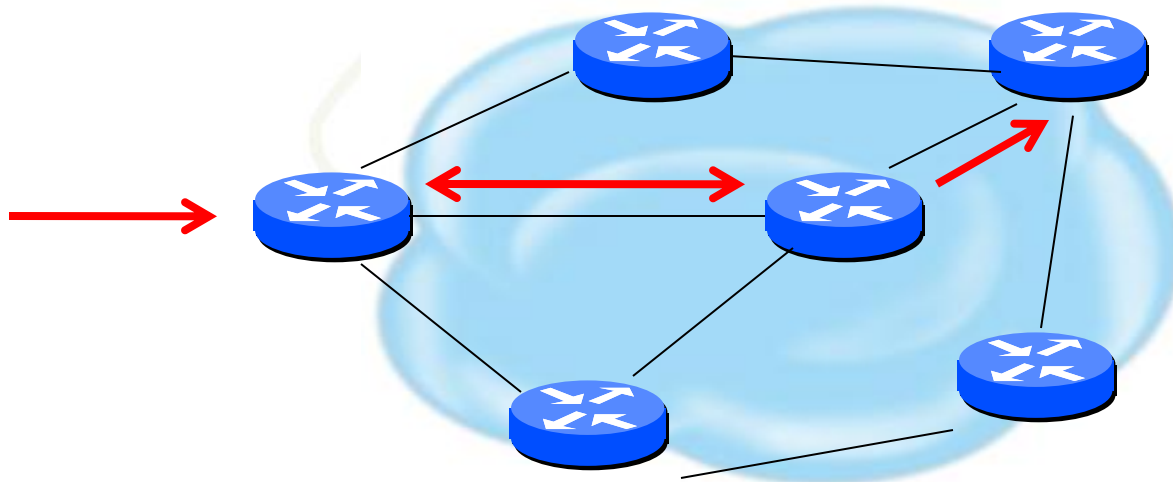
- The routing header is used by an IPv6 source to list one or more intermediate **nodes** to be “visited” on the way to packet’s destination.
- Each extension header should occur at most once, except for the destination options header which should occur at most twice.
- IPv6 nodes must accept and attempt to process extension headers **in any order** and **occurring any number of times** in the same packet.



Routing Header Issue

A single RH of Type 0 may contain multiple intermediate node addresses, and the same address may be included more than once in the same RH0.

If the routing header contains a repetition of a pair of addresses of the form A B A B A B ... If this A B pair were repeated 3 times then a single packet directed at A would traverse the path A B 3 times, and B A twice. If such packets were generated at a total rate of 1 Mbps then the path between A and B would experience a total of 5Mbps of traffic.





Routing Header Processing

- Disabling processing still allows all other hosts to be used for attack
- Dropping is required for ISP's
- RFC 5095 – Deprecation of RH0
- Until rfc5095 implemented:
 - Use ingress filtering for RH0 traffic
 - RH Type 2 is required for mobility so have to ensure that only RH0 traffic is blocked



Cisco and RH0 Filtering

- To disable processing of all types routing headers on 12.2(15)T and up one can use:

```
no ipv6 source-route
```

Note that this will still forward these packets on to other hosts which can be vulnerable. This statement also affects perfectly valid Routing Headers of Type 2 which are used by Mobile IPv6.

- If possible upgrade to 12.4(2)T or higher and block only the Type 0 Routing Header (note interface specific config):

```
Router(config)#ipv6 access-list deny-sourcerouted
Router(config-ipv6-acl)#deny ipv6 any any routing-type 0
Router(config-ipv6-acl)#permit ipv6 any any
Router(config)#interface Ethernet0
Router(config-if)#ipv6 source-route
Router(config-if)#ipv6 traffic-filter deny-sourcerouted in
```



Cisco IPv6 NetFlow

- Netflow IPv6 support from 12.4 IOS releases
- Uses Netflow v9
- Activate per interface

`ipv6 flow ingress`

`ipv6 flow egress`

- Show status

`show ipv6 flow cache`





IPv6 Filtering References

- RFC 4890 'Recommendations for Filtering ICMPv6 Messages in Firewalls'
- RFC 5156 'Special-Use IPv6 Addresses'
- <http://www.space.net/~gert/RIPE/ipv6-filters.html>
- <http://www.cymru.com/Bogons/v6top.html>
- NSA Router Security Configuration Guide Supplement – Security for IPv6 Routers

Many filtering recommendations are not uniform and that while similarities exist, a definitive list of what to deny and what to permit does not exist. Any environment will need to determine what is most suitable for them by using these references as guidelines.



BGP Prefix Filtering (same for IPv6 and IPv4 networks)

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is most ISPs are not:
 - Filtering Comprehensively
 - Filtering their customer's prefixes
 - Filtering prefixes going out of their network.

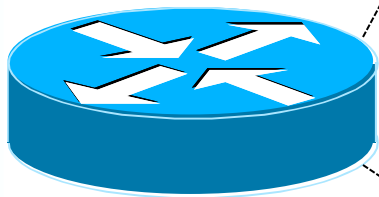


BGP IPv6 Prefix Filters To Consider

- Special-use prefixes
 - `::/0` exact : default route
 - `::1/128` : loop back address
 - `::/128` : unspecified address
 - `::/96` : IPv4-compatible IPv6 address
 - `::ffff:0:0/96` : IPv4-mapped IPv6 address
 - `::/8` or longer : reserved
 - `fe80::/10` or longer : link-local address
 - `fc00::/7` or longer : unique-local address
 - `ff00::/8` or longer : multicast range (RFC3513)
 - `fe00::/9` or longer : multicast range (RFC3513)
 - `2001:db8::/32` or longer : documentation address
- Your own prefix
- The 6bone prefix (`3ffe::/16`)
- The 6to4 reserved address range (`2002::/16`) if not supporting 6to4 services (i.e. relays) and not providing transit services
- The Teredo address range (`2001::/32`) if not running a Teredo relay or offering a Teredo transit service



Simple IPv6 Bogon Prefix Filter Example



```
ipv6 prefix-list ipv6-special-use-pfx deny 0::/0 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 0::1/128 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 0::/128
ipv6 prefix-list ipv6-special-use-pfx deny 0::/96
ipv6 prefix-list ipv6-special-use-pfx deny 0::ffff:0:0/96
ipv6 prefix-list ipv6-special-use-pfx deny 0::/8 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fe80::/10 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fc00::/7 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fe00::/9 le 128
ipv6 prefix-list ipv6-special-use-pfx deny ff00::/8 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 2001:db8::/32 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 3ffe::/16 le 128
```

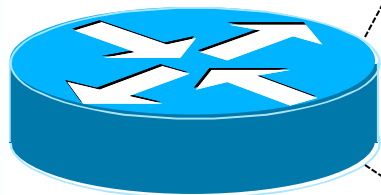


BGP Prefix Filters (RIR Allocations)

- APNIC
 - <ftp://ftp.apnic.net/stats/apnic/delegated-apnic-latest>
- RIPE NCC
 - <ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest>
- ARIN
 - <ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest>
- LACNIC
 - <ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest>
- AfriNIC
 - <ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest>



IPv6 RIR Allocation Prefix Filter Example (Needs Constant Updating)



```
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0500::/30 ge 48 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0678::/29 ge 48 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001::/16 ge 35 le 35
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001::/16 ge 19 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2003::/18 ge 19 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2400::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2600::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2610::/23 ge 24 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2620::/23 ge 40 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2800::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2A00::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2C00::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0DF0::/29 ge 40 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:43F8::/29 ge 40 le 48
```



Prefix Filter Bogons and RIR Blocks

- Templates available from the Bogon Project:
 - <http://www.cymru.com/Bogons/index.html>
- Cisco Template
 - <ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/>
- Juniper Template
 - <http://www.qorbit.net/documents.html>



IPv6 Tunneling Considerations

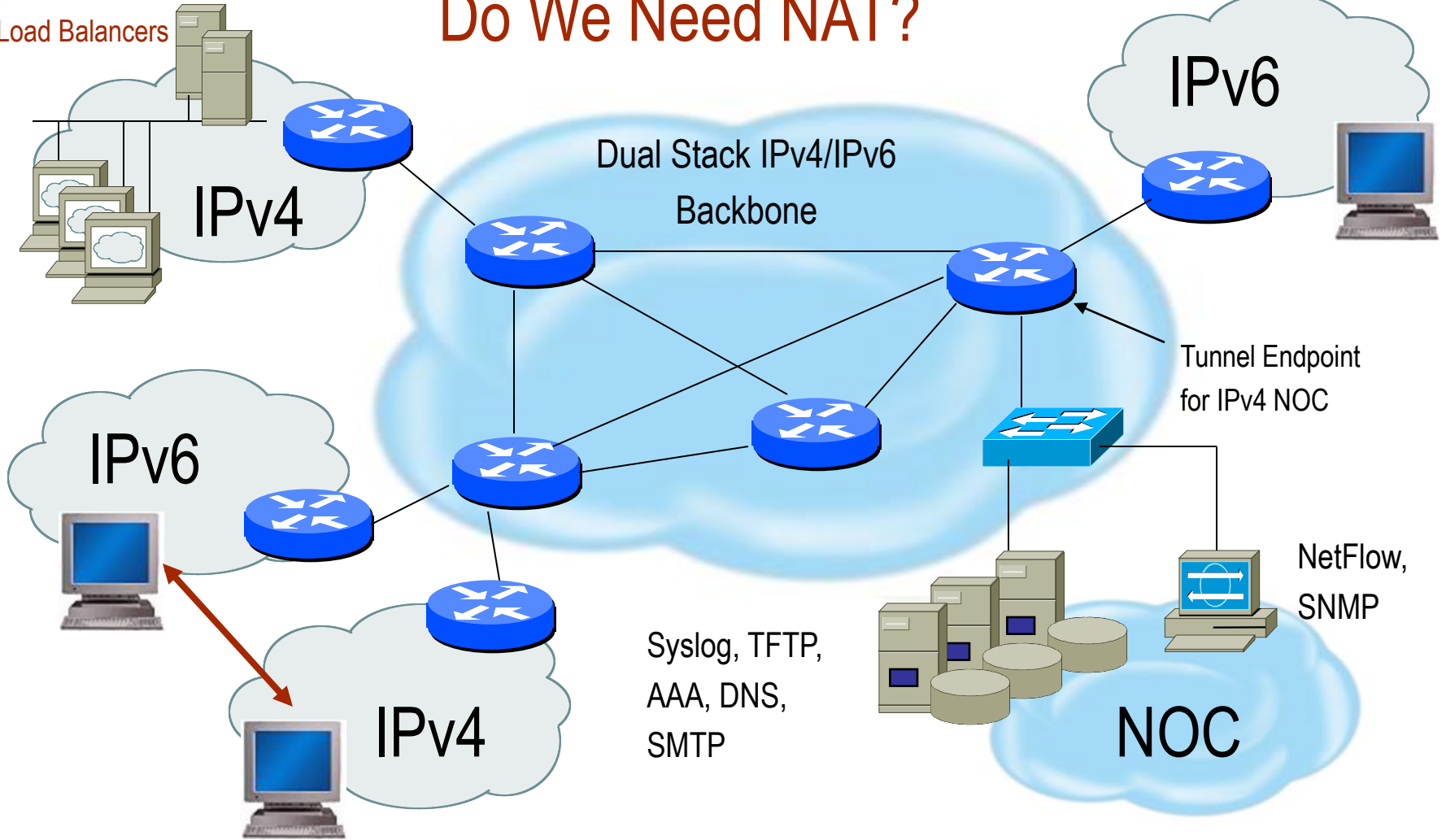
- Manually configured tunnels are not scalable
- Automated tunnels require more diligence to provide effective security services
- Look at IETF Softwire Working Group
 - <http://www.ietf.org/html.charters/softwire-charter.html>
 - RFC 5619 (softwire-security-requirements)
- Deployments of 6to4, 6rd, Dual-Stack Lite, ISATAP and Teredo all require layered security models
 - Perform ingress firewall sanity checks
 - Log and audit tunneled traffic
 - Provide authentication where possible
 - Use IPsec where appropriate



Network Address Translation

Do We Need NAT?

Load Balancers





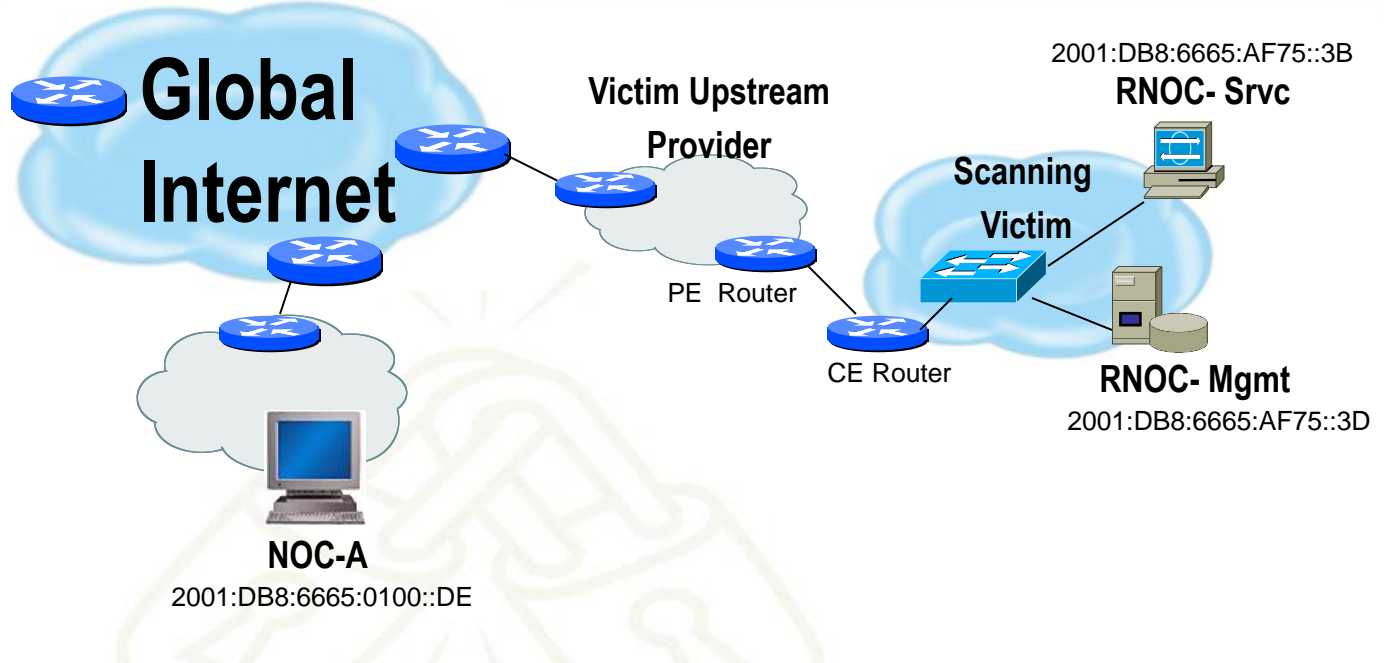
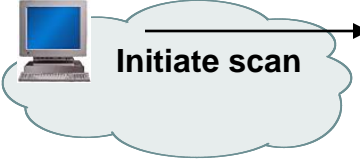
IPsec in IPv6 Environments

- Bootstrapping credentials
 - Ship all devices with some embedded certificates and trusted roots
- Where useful
 - BGP/OSPFv3/ISIS Authentication
 - Syslogv6 / Radius (server-to-router)
 - TFTP / SNMP / Netflow
- Interoperable defaults
 - Have until widespread deployment of IPv6
 - Window of opportunity closing



Protecting Against Scanning Attacks

Attacker



Protocol	Port
tcp	21
tcp	22
tcp	23
tcp	25
tcp	135
tcp	139
tcp	1433
tcp	2967
udp	1026
udp	1027
udp	1434

IPsec Security Policy Database

From	To	Protocol	Dst Port	Policy
2001:DB8:6665:0100::DE	2001:DB8:6665:01C8::3B	TCP / UDP	53 (DNS)	ESP: SHA1, AES-256
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3B	TCP	25 (SNMP)	ESP: SHA1, AES-256
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3D	UDP	1812/1813 (RADIUS)	ESP: SHA1, AES-128
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3D	UDP	514 (Syslog)	ESP: SHA1, 3DES
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::/48	TCP / UDP	ANY	ESP: SHA1



Vendor Specific Deployment Issues

- Lack of interoperable defaults
 - A default does NOT mandate a specific security policy
 - Defaults can be modified by end users
- Configuration complexity
 - Too many knobs
 - Vendor-specific terminology
- Good News: IPv6 support in most current implementations



IPv6 IPsec Concerns

- Are enough people aware that IKEv2 is not backwards compatible with IKEv1?
 - IKEv1 is used in most IPv6 IPsec implementations
 - Will IKEv2 implementations first try IKEv2 and then revert to IKEv1?
- Is IPsec implemented for IPv6?
 - Some implementations ship IPv6 capable devices without IPsec capability....this needs to change
- OSPFv3
 - All vendors 'IF' they implement IPsec used AH
 - Latest standard to describe how to use IPsec says MUST use ESP w/Null encryption and MAY use AH



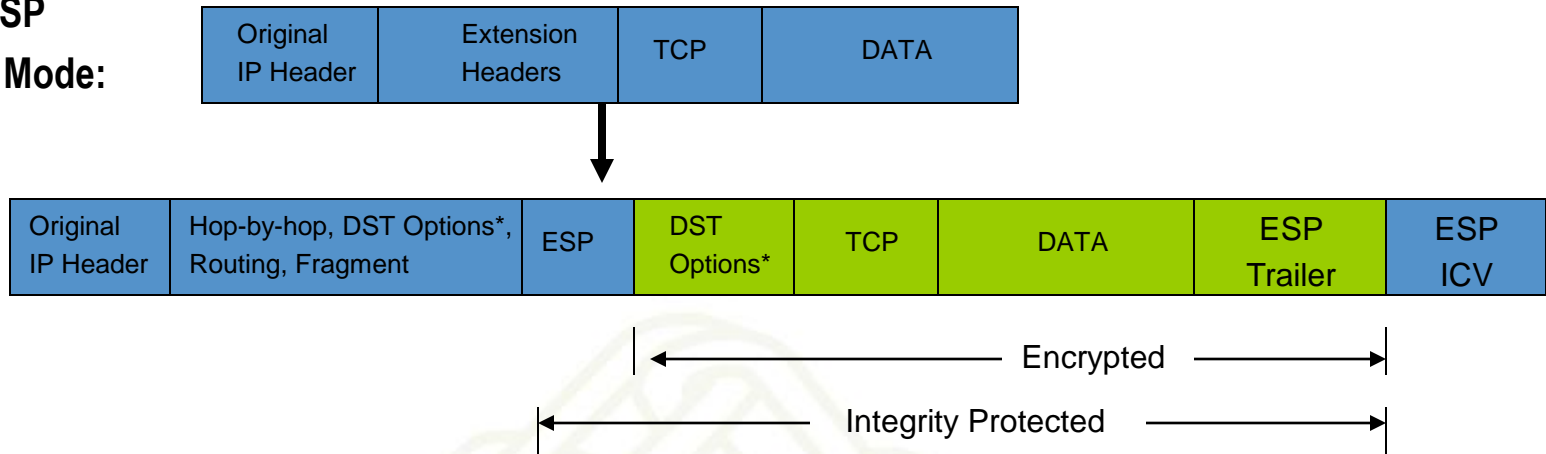
IPv6 IPsec Concerns (cont)

- What is transport mode interoperability status?
 - Will end user authentication be interoperable?
- PKI Issues
 - Which certificates do you trust?
 - How does IKEv1 and/or IKEv2 handle proposals with certificates?
 - Should common trusted roots be shipped by default?
 - Who is following and implementing pki4ipsec-ikecert-profile (rfc4945)
- Have mobility scenarios been tested?
 - Mobility standards rely heavily on IKEv2
- ESP – how determine if ESP-Null vs Encrypted

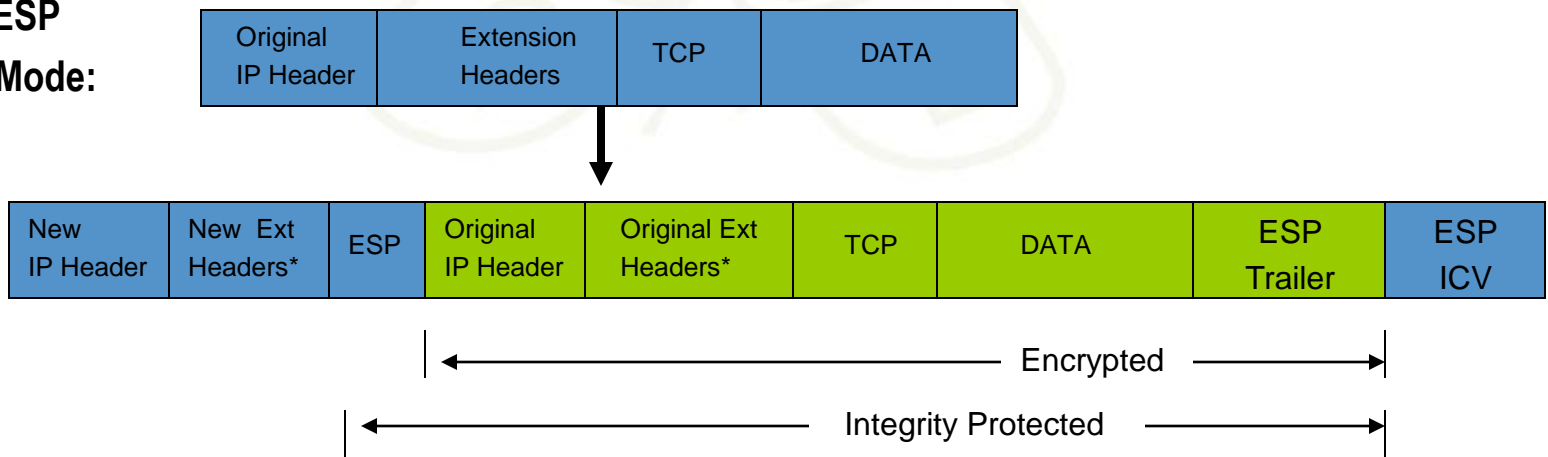


IPv6 IPsec ESP

IPv6 ESP Transport Mode:

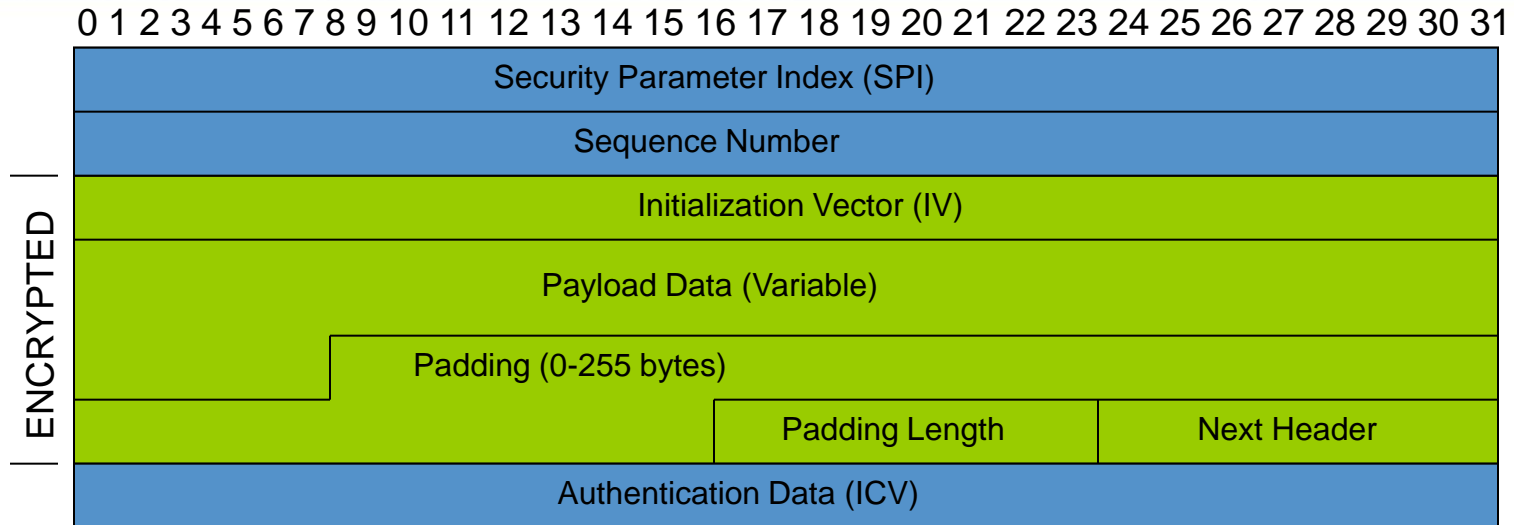


IPv6 ESP Tunnel Mode:





ESP Header Format



- SPI:** Arbitrary 32-bit number that specifies SA to the receiving device
- Seq #:** Start at 1 and must never repeat; receiver may choose to ignore
- IV:** Used to initialize CBC mode of an encryption algorithm
- Payload Data:** Encrypted IP header, TCP or UDP header and data
- Padding:** Used for encryption algorithms which operate in CBC mode
- Padding Length:** Number of bytes added to the data stream (may be 0)
- Next Header:** The type of protocol from the original header which appears in the encrypted part of the packet
- Auth Data:** ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)



Vendor A

IKE Phase 1
SHA1
RSA-SIG
Group 1
Lifetime 86400 Sec
Main Mode

IKE Phase 2
PFS
Group 1

Vendor B

IKE Phase 1
MD5
Pre-Share Key
Group 5
Lifetime 86400 Sec
Main Mode

IKE Phase 2
PFS
Group 5

Vendor C

IKE Phase 1
SHA1
Pre-Share Key
Group 2
Lifetime 86400 Sec
Aggressive Mode

IKE Phase 2
PFS
Group 2



Terminology Issues

IKE Phase 1

IKE Phase 1 SA

IKE SA

ISAKMP SA

Main Mode

DH Key Length

DH Group

Modp #

Group #

IKE Phase 2

IKE Phase 2 SA

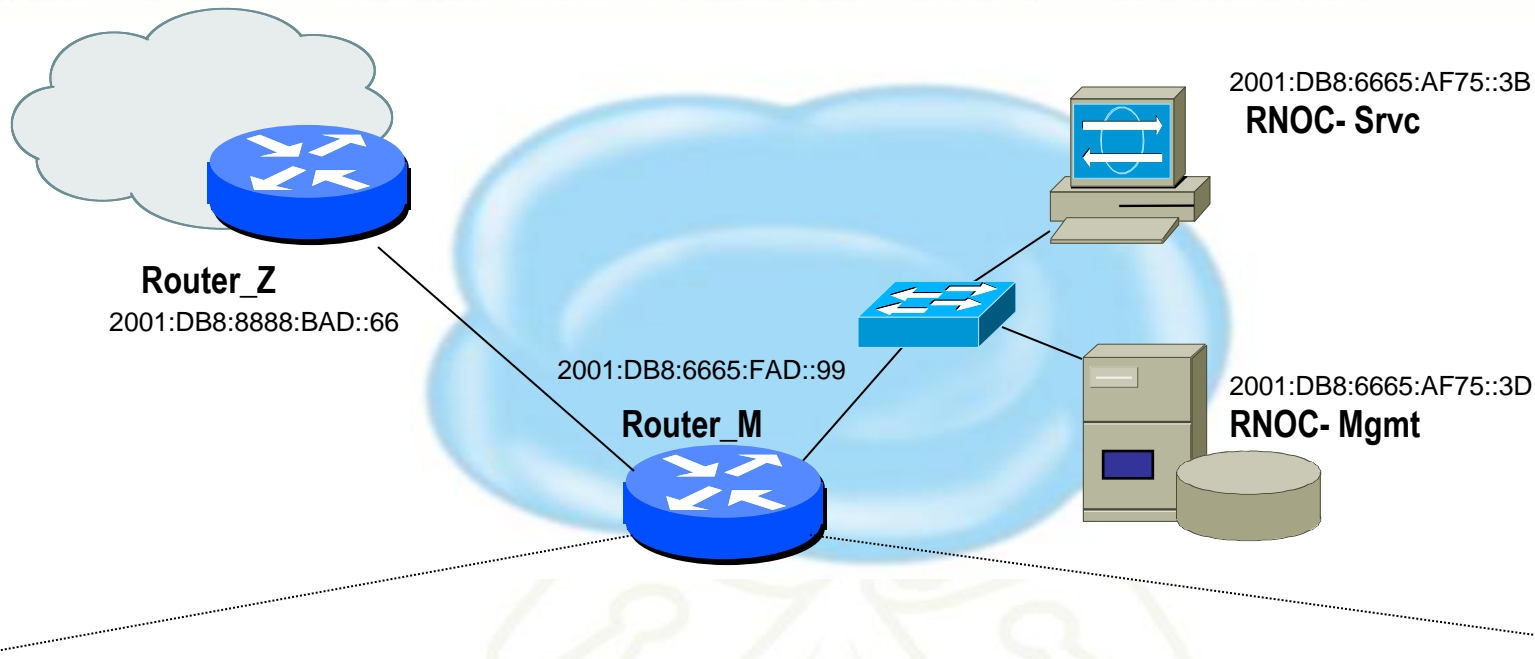
IPsec SA

Quick Mode

Configuration complexity
increased with vendor specific
configuration terms



Potentially Easy Configuration



```
Syslog server 2001:DB8:6665:AF75::3D authenticate esp-null sha1 pre-share 'secret4syslog'  
TFTP server 2001:DB8:6665:AF75::3D authenticate esp-null aes128 pre-share 'secret4tftp'  
BGP peer 2001:DB8:8888:BAD::66 authenticate esp-null aes128 pre-share 'secret4AS#XXX'
```



Latest IETF Work related IPv6 Security

- CPE Device Issues / Concerns
 - draft-ietf-v6ops-cpe-simple-security-12.txt
 - draft-ietf-v6ops-ipv6-cpe-router-07.txt
- Router Advertisements
 - draft-ietf-v6ops-ra-guard-08.txt
- SeND / CGI
 - draft-ietf-savi-send-03.txt
 - RFC 5909 (security ND proxy problem statement)
 - draft-ietf-csi-hash-threat-09
 - Draft-ietf-csi-proxy-send-04.txt
 - Draft-ietf-csi-send-cert-06.txt
 - Draft-ietf-csi-dhcpv6-cgs-ps-04.txt



Latest IETF Work related IPv6 Security

- Tunneling Protocols
 - draft-gont-6man-teredo-loops-00.txt
 - draft-ietf-v6ops-tunnel-loops-00.txt
 - draft-ietf-v6ops-tunnel-security-concerns-02.txt
- General
 - draft-gont-6man-flowlabel-security-00.txt
 - draft-ietf-6man-node-req-bis-05
 - IPsec from 'MUST' to 'SHOULD'
- IPsec
 - RFC 5739 (IPv6 Configuration in IKEv2)



Summary: Use Hybrid Security Model

- Defense in Depth
 - Security services in network infrastructure
 - Security services on end host
- Provides gradual move to native v6
 - Add IPv6 capability in places that require dual-stack
 - If services can support native IPv6, deploy native
- Maintains existing policy controls
- Performance vs management tradeoff



End Host IPv6 Security Guidelines

- **Basic Principles**
 - Address assignment is performed in a reliable manner and cannot be spoofed
 - Traffic sourced from or destined to an end-host can be protected from modification, deletion or spoofing
 - Malicious behavior can be detected and mitigated
- **Addressing recommendations**
 - Use stateless auto-configuration when low probability that spoofing can occur
 - Use DHCPv6 if need to have control over addresses
 - Use standard but non-obvious static addresses for critical systems
- **Hardening the host**
 - Restrict access to the client or server to authenticated and authorized individuals
 - Monitor and audit access to the client and server
 - Turn off any unused services on the end node
 - Use host firewall capabilities to control traffic that gets processed by upper layer protocols
 - Use virus scanners to detect malicious programs
- **Protecting traffic between hosts**
 - Use IPsec



Conclusions

- Fundamental issues for security remain same but new jargon created for evolving technologies
- Understand operational requirements for network protocols: IPv4 vs IPv6
- Understand trust delegations for in-house or outsourced IT (private vs public cloud networks)
- Understand what certain protocols will buy you in terms of risk mitigation vs operational headache
- Distributed security management is essential
- How well do YOU know the valid traffic that is traversing YOUR network?