



# Security with IPv6 Explored

**U.S. IPv6 Summit 2003**

December 8-11, 2003

Renée Esposito – Booz Allen Hamilton

Richard Graveman – RFG Security

# IPv6 Security: Outline

1 Internet Security

2 IPv6: Core Protocols

3 Protocol Security: IPsec and IKE

4 Firewalls for IPv6

5 Security and IPv6 Transition

6 Summary

# Security and the Internet

- “When we first turned on extensive logging on our gateway host, it was much like moving into a new house with a tin roof in a hail-prone neighborhood under several large oak trees during acorn season. ... We diligently chased down evil-doers and helped secure numerous open systems. ... Some corporate machines were secured as well.”
- “Getting hacked is seldom a pleasant experience”
  - Bellovin and Cheswick, *Firewalls and Internet Security*

# Scope

- This talk covers
  - IPv6 protocol security
    - And methods to hinder IPv6-based denial of service attacks
  - Host and router system security only as related to IPv6
  - IPv6 firewalls
  - Security of IPv6 transition strategies
- It does not cover
  - Overall security architecture
  - Physical, environmental, or personnel security
  - General system security
  - Network applications, buffer overflows, viruses, worms, spam, ...
  - DHCPv6, IPv6 Routing, QoS, Flows, Timers, Multicast Keying, DNS

# What Do We Want from Security?

- We assume an adversary may get complete access to our communications channels (i.e., we're on the Internet):
  - Read, write, replay, modify, reorder, rearrange, truncate, reroute, spoof headers and addresses, etc.
  - Try to “take control of” routers and hosts
  - Launch additional attacks from compromised systems
- We want:
  - To know who's sending what we get
  - To know who's reading what we send
  - To know that no one else has tampered with it
  - To keep the network working reasonably well
  - To control our own equipment
    - Contents and operation; software and data

# IPv6 and the “Black Hat World”

- IPv6 has been found running today without administrators' knowledge
  - Can be enabled on many platforms (XP, 2000, Linux, etc.)
    - Intentionally or otherwise
  - Can provide a stealth network for intruders
    - Harder to scan
    - Evades many intrusion detection systems
    - Has been caught in “honeypots”
  - Attacks on IPv6 can compromise co-existing IPv4 networks
- Precautions
  - Block protocol 41
  - Handle Teredo as a “dangerous UDP port” at IPv4 firewalls
  - Look for Router Advertisements and Neighbor Discovery packets

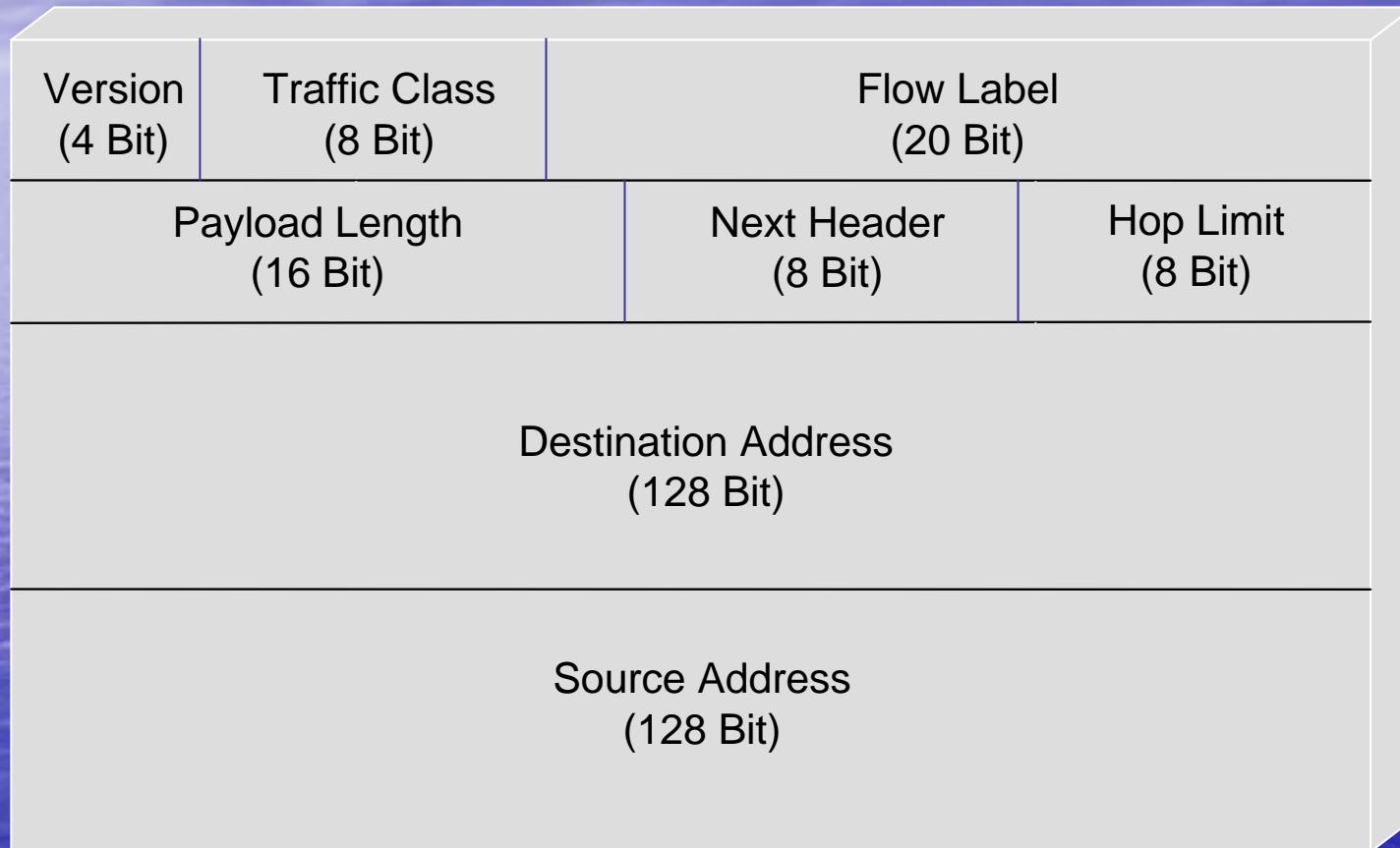
# IPv6 Security: Outline

- 1 Internet Security
- 2 IPv6: Core Protocols
- 3 Protocol Security: IPsec and IKE
- 4 Firewalls for IPv6
- 5 Security and IPv6 Transition
- 6 Summary

# IPv6 Core Protocols: Introduction

- IPv6 can offer end-to-end connectivity to all hosts
  - That, in itself, is scary to some who are used to NATs
- IPv6 header is simpler
  - But IPv6 extensions are much more flexible
- IPv6 does much more than IPv4 at Layer 3
  - Some old favorites like ARP disappear
  - Stateless Auto-Configuration is new
- IPv6 promotes Mobile IP

# IPv6 Core Protocols: IPv6 Header Format



# IPv6 Core Protocols: IPv6 Extension Headers

- Order of Extension Headers when more than one is used in same packet:
  - IPv6 Header
  - Hop-by-hop Options Header
  - Destination Options Header (*every* Routing Header destination)
  - Routing Header
  - Fragment Header
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP) Header
  - Destination Options Header (*last* Routing Header destination)
  - Upper-Layer Header



# IPv6 Core Protocols: Addressing

- Unicast, Multicast, Anycast
  - Broadcast dropped; Multicast essential
- Link local and site local scoping
  - Link local makes a lot of sense
  - Site local makes a lot less sense (today)
- Some good news
  - Address and port scanning a subnet can be a lot harder

# IPv6 Core Protocols: Address Generation and Renumbering

- Auto-Configuration
  - “Getting on a LAN” may imply having “insider privileges”
  - Need to look at different cases
    - Enterprise, in the building
    - Public WiFi
    - *Ad hoc* networking
- Effects of self-generated addresses
  - RFC 2462 addresses can be “stolen” by others
  - RFC 3041 addresses cannot have pre-established IPsec keys
- Subnet renumbering
  - Need to track multiple prefixes simultaneously
  - Need to map permissions from old to new addresses
  - draft-bellovin-ipv6-accessprefix-01 proposes a way to retrieve a list of privileged prefixes with an ICMPv6 Router Advertisement

# IPv6 Core Protocols: IPv6 Anycast Security

- Reserved anycast addresses may provide an attacker with a well-known target
  - Globally reachable anycast only defined for routers
- No authorization mechanism exists for destination anycast addresses
  - Spoofing and masquerade possible
- IPsec hard to set up in advance
  - IPsec security associations need destination address

# IPv6 Core Protocols: Site-Local Addresses

- IETF deprecated site-local addresses in March 2003
  - Intuitively, sites are hard to define
  - Site boundaries may not match security, reachability, QoS, administrative, and funding boundaries
  - The same addresses (e.g., FEC0::1) can exist in many sites
  - A multi-homed host can belong to a site per interface
  - Developers have to handle site identifiers along with addresses
  - Multi-sited routers have to remember arrival interface
  - Addresses can leak in application layer data
- Replacement architecture will have unambiguous addresses and more flexible scope rules
  - Firewalls will need to implement the new design and block the old-style FEC0::/10 addresses

# IPv6 Core Protocols: ICMPv6

- Capabilities implemented with ICMPv6
  - Address auto-configuration
  - Router and prefix discovery
  - Neighbor reachability and address resolution
  - Duplicate address detection
  - Router renumbering
  - Redirect
  - PMTU discovery
  - Echo request and echo reply
  - Error notifications
- Examples of security questions
  - Are Router Advertisements coming from an authorized router?
  - Are there security requirements for Neighbor Advertisements?
  - Are redirects coming from the router to which the packet was actually sent?

# IPv6 Core Protocols: Neighbor Discovery

- Neighbor Discovery lacks mechanism for determining authorized neighbors
- Attacks:
  - Redirection, duplicate address detection, advertisement and parameter spoofing, denial of service
- Defenses:
  - The “hop count 255 trick” has limited value
  - IPsec Authentication Header (AH) or Encapsulating Security Payload (ESP) “works” with manual keying

# IPv6 Core Protocols: Summary of ICMPv6 Security

- IPv6 RFCs say:
  - “Use IPsec AH for IPMCv6”
- Begs the question, how?
  - Need addresses, which may not be determined
  - Need a Security Association and keys
    - Manual set up: how many?
    - Automatically generated: need to run UDP
- Chicken and egg problem

# IPv6 Core Protocols: Mobile IP Issues

- Goals: roaming, address anonymity, location privacy
- Authenticated, dynamic registration (binding) is needed
  - Between the Mobile Node and the Home Agent
- Current draft specifies IPsec ESP and IKE (plus alternative) for:
  - Binding updates and binding acknowledgements
  - Return routability messages: “Home Test Init” and “Home Test”
  - ICMPv6 between the Home Agent and Mobile Node (e.g., prefix discovery)
  - User traffic (optional)
  - Need to work around lack of global PKI, IKE-IPsec overhead, ...
    - See draft-ietf-mobileip-mipv6-ha-ipsec-06, draft-ietf-mobileip-ipv6-24, and draft-perkins-mobileip-precfg-kbm-00
- Firewalls need to control use of routing and home address headers

# Summary: IPv6 Core Protocols

- Some things are brand new
  - Subnet renumbering
  - Site-local and link-local addresses
  - Address generation (auto-configuration)
  - Anycast
  - Duplicate address detection
- Some things are likely to become more common
  - End-to-end connectivity
  - Multicast
  - Use of clocks and timers (at Layer 3, not just TCP)
  - Host multi-homing
- Some things are just different
  - Flows (QoS)
  - Fragmentation
  - ICMPv6
  - Subnet scanning attacks
  - Packet filtering methods

For the most part, IPv6 is like IPv4, only more so



# IPv6 Security: Outline

- 1 Internet Security
- 2 IPv6: Core Protocols
- 3 Protocol Security: IPsec and IKE
- 4 Firewalls for IPv6
- 5 Security and IPv6 Transition
- 6 Summary

# Protocol Security: IPsec

- The big change in IPsec from IPv4 to IPv6 is that IPsec is **mandatory** in IPv6 implementations
- IPsec can provide authentication, integrity, confidentiality, and replay detection for *any* IP datagram
  - Provided ...

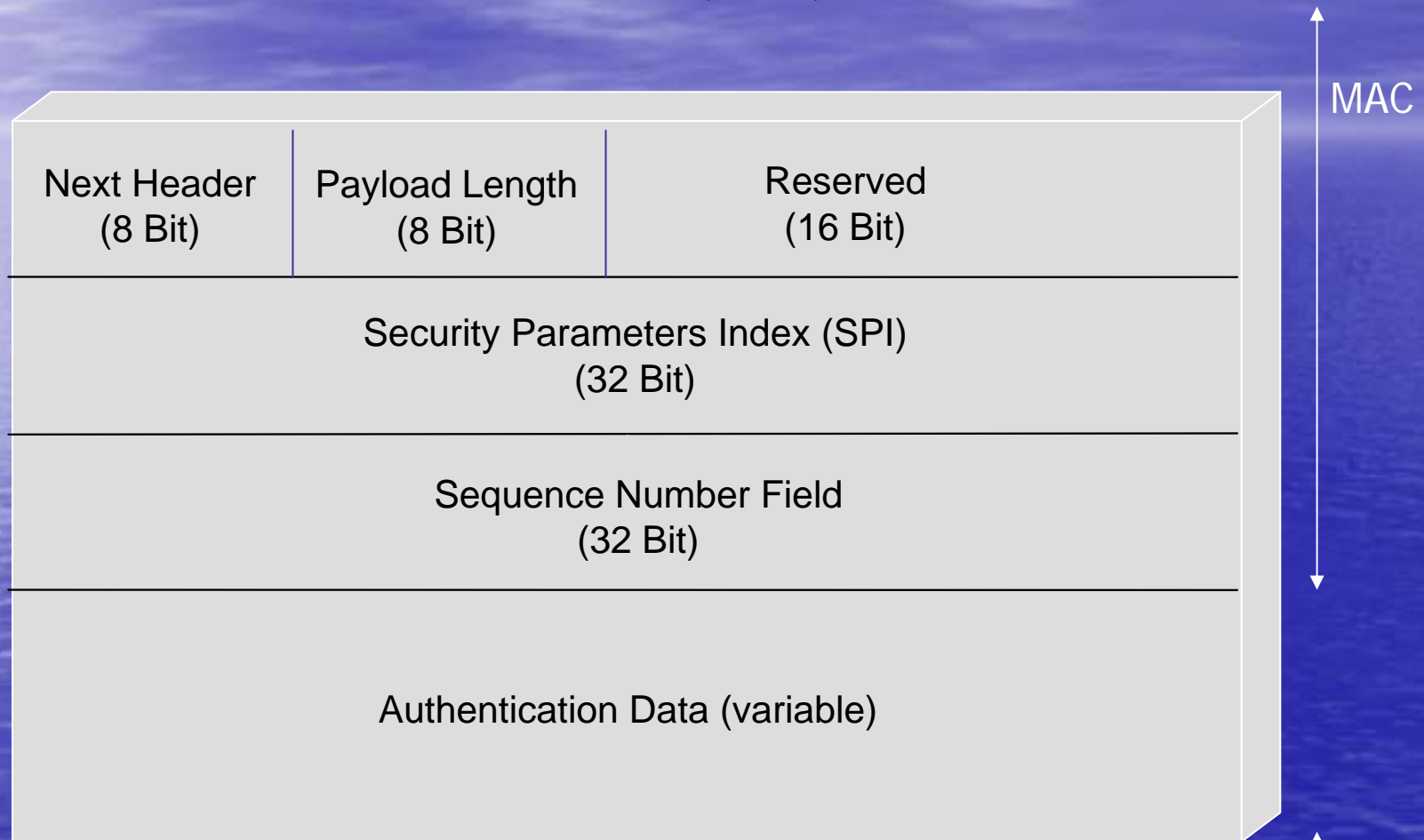
# Protocol Security: IPsec

- Provided we can trust identities and implement it correctly on a secure platform
- IPsec provides an extraordinarily sound protocol security infrastructure, but
  - Details matter
  - Implementing IPsec is somewhat difficult
  - We have to figure out how to use it, case by case
  - Changes in IPsec are still in the works
- “If you think cryptography is the solution to your problem, you don’t know what your problem is.”
  - Roger Needham

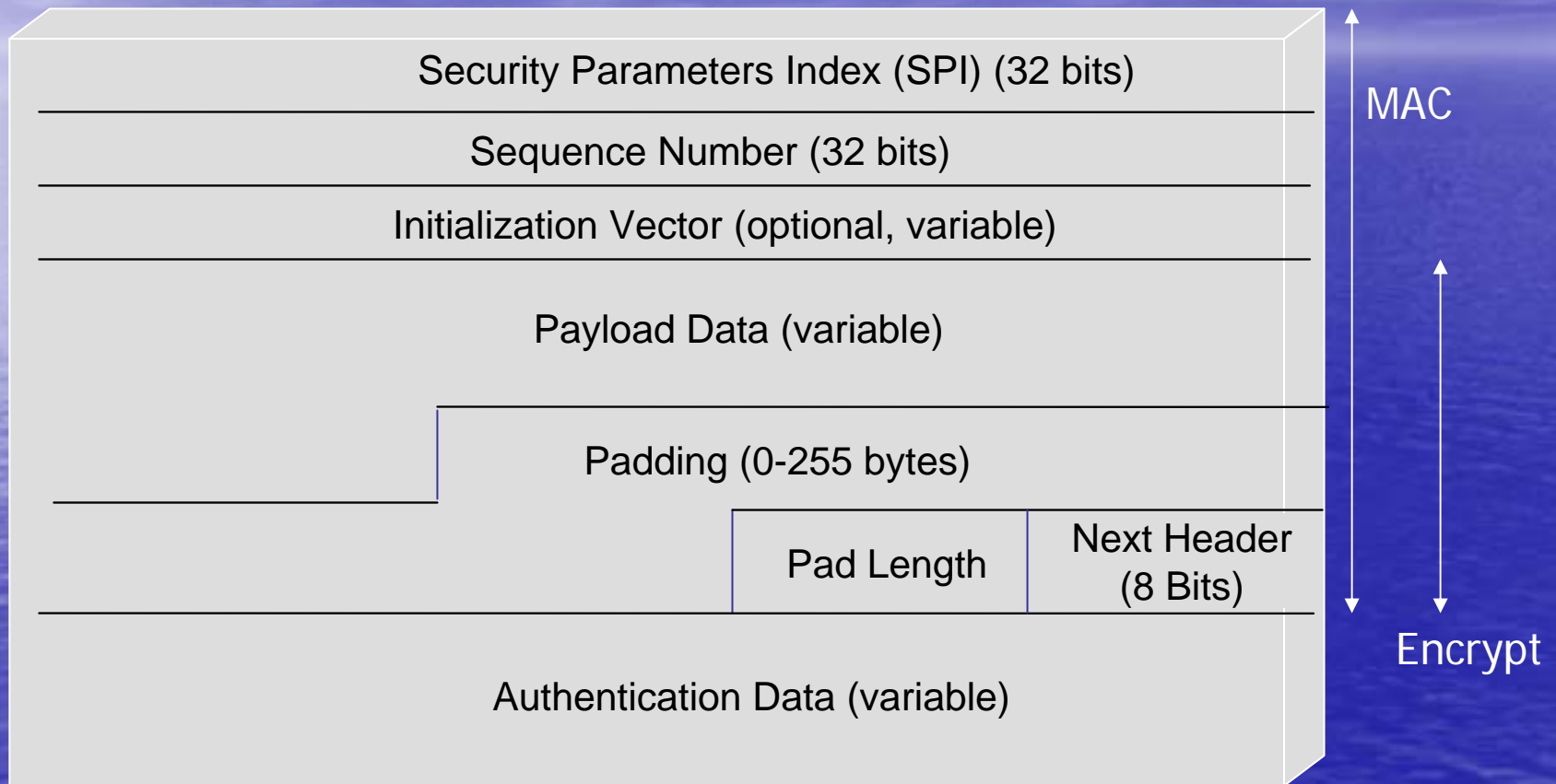
# IPsec and IKE: Where Do they Live?

- IPsec: architecture and two extension headers
  - RFC 2401: Security Architecture
  - RFC 2402: Authentication Header
    - Message origin authentication and connectionless integrity
    - Replay detection
  - RFC 2406: Encapsulating Security Payload
    - Everything in AH plus confidentiality
- Key management for IPsec: IKE (Internet Key Exchange)
  - RFCs 2407, 2408, 2409
    - Entity authentication
    - Security Association (SA) negotiation
    - Key exchange
- All of these RFCs will be revised in the next year (or so)

# IPsec: Authentication Header (AH) Format



# IPsec: Encapsulating Security Payload (ESP) Packet Format

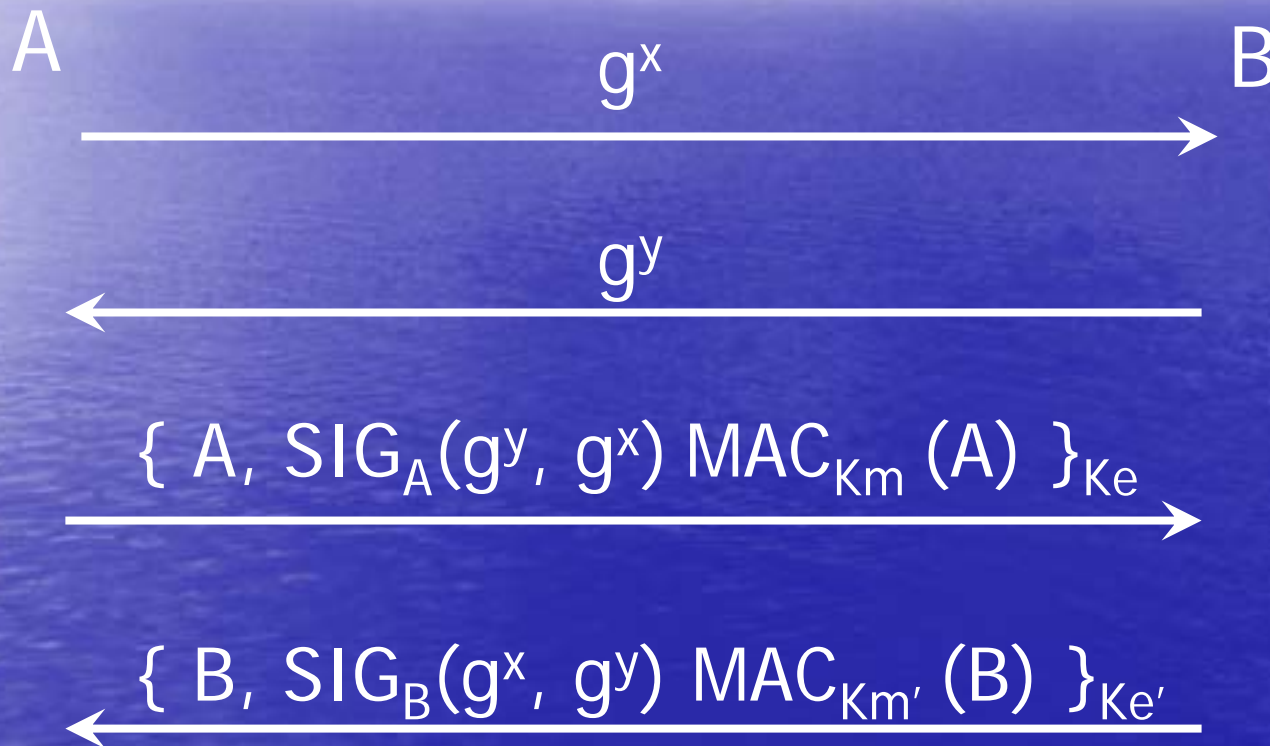


# IPsec: Security Associations

- Contain all the parameters needed to specify
  - When and how the source applies security
  - When and how the destination verifies security
- Named by a destination address, protocol, and Security Parameters Index
- Usually configured in pairs
  - One in each direction

# IPsec: IKEv2 Key Exchange Protocol

IKEv2 adds nonces, directional protection, etc.



# IPsec: Current Revisions

- IKE v2
  - Problems fixed, simpler, fewer options
  - Four-message sign-and-MAC protocol, formal security analysis
  - New transforms
  - One document for protocol, one for the transforms
- ESP, AH, and RFC2401bis
  - 64-bit (implicit) sequence numbers
  - Arbitrary padding
  - Dummy packets: Protocol 59
  - New processing model and definition of security association
  - Virtual IDs to support VPNs
- Thorny topics
  - Legacy authentication
  - PKI

# IPsec: IKE and ICMPv6

- ICMPv6 can be end-to-end, any-to-end, or link local
- ICMPv6 can be Unicast, Multicast, or Anycast; IKE is Unicast only
- IKE can only run if UDP is already enabled
- See draft-arkko-icmpv6-ike-effects-02 for the following table:

– Dest. Unreachable	Any-to-End	May use IKE
– Packet Too Big	Any-to-End	May use IKE
– Time Exceeded	Any-to-End	May use IKE
– Parameter Problem	End-to-End	May use IKE
– Echo Request	End-to-End	May use IKE
– Echo Reply	End-to-End	May use IKE
– Redirect	Link Local	May use IKE
– Router Solicit	Link Local	Must Not use IKE
– Router Advert.	Link Local	Must Not use IKE
– Neighbor Solicit	Link Local	Must Not use IKE
– Neighbor Advert.	Link Local	Must Not use IKE
– Router Renumb.	End-to-End	May use IKE

# IPsec: Manual Keying and Neighbor Discovery

- Neighbor discovery uses many destination address types
  - ICMPv6 message types overloaded
  - Destination may be Multicast (M), Unicast (U), or Anycast (A)

1 Router and Prefix Discovery	133->M; 134->MU
2 Address Auto-Configuration	135->MUA; 136->MU
3 Duplicate Address Detection	135->MUA; 136->MU
4 Address Resolution	135->MUA; 136->MU
5 Neighbor Reachability Detection	135->MUA; 136->MU
6 Redirect	137->U
  - Attacks and consequences vary case by case
- Need Security Associations for:
  - Each node's Unicast and solicited node Multicast addresses
    - Known ahead of time (not RFC 3041 addresses)
  - The "All Nodes" and "All Routers" Multicast addresses
  - See draft-arkko-manual-icmpv6-sas-02

# IPv6 Security: Outline

- 1 Internet Security
- 2 IPv6: Core Protocols
- 3 Protocol Security: IPsec and IKE
- 4 Firewalls for IPv6
- 5 Security and IPv6 Transition
- 6 Summary

# Firewalls for IPv6: Role of Firewalls

- Firewalls **solve different problems** from IPsec
  - Enforce uniform policy at perimeter
  - Stop outsiders from performing dangerous operations
  - Provide a choke point and scalable, centralized control
- End-to-end connectivity, tunneling, and encryption may conflict with this policy
  - Traffic that cannot be checked at the firewall can bring unpleasant things to your desktop
  - IPsec is like SSL, only more powerful in this respect
- The tunneling problem has no satisfactory solution
  - “We’ll run it on Port 80, so it gets through the firewall”

# Firewalls for IPv6: Changing the Model

- The perimeter security model is changing
  - Clear boundaries do not exist
  - Users are being forced to run safe(r) computers
    - Passwords on start up and wake up
    - Virus protection
    - Personal firewalls
    - SSL, IPsec VPNs, PGP, encrypted hard drives, WiFi security
    - Patches and updates
- Firewalls themselves are changing too
  - Location
    - Network or end system (personal firewall)
  - Control
    - Administrator or end user

# IPv6 Firewalls: Packet Filtering

- Packet filtering uses rules based on:
  - Source and destination addresses
  - Protocol
  - Source and destination ports
  - Other fields like Traffic Class or Flow Label
- Source and destination addresses are the easiest part, but
  - IPv6 hosts typically have many addresses
  - IPv6 sub-networks can be renumbered
  - Some IPv6 addresses have restricted scope
- IPv6 makes it harder to apply RFC 2827 consistently
  - To prevent denial of service attacks with spoofed source addresses
  - Especially with RFC 3041 addresses

# IPv6 Firewalls: Extension Headers

- Processing IPv6 extension headers is more work
  - Routing and fragmentation headers may trigger an access decision
  - May get stuck on an unknown extension header
    - Should a firewall send an “unrecognized header” ICMP?
    - ... discard the packet?
    - Note that the RFCs are unclear on firewall or middlebox actions
  - Unknown destination options are a bit easier to handle
    - TLV format
    - Still need to define policy for unknown types

# IPv6 Firewalls: RH and HA Processing

- Many IPv4 firewalls prohibit source routing
- IPv6 Routing Header (RH) and Home Address (HA) rewrite addresses
  - Needed for mobile IPv6, TE, and multi-homing
  - Want to recognize legitimate MobileIP addresses and route optimizations
- RH and HA can turn any host behind a firewall into a router
  - May enable an unauthorized Web server
  - May break denial of service protections
- What does this mean?
  - Want to characterize what RH and HA are doing
    - Mobile IP: allow only one RH “segment left,” only if policy and use correspond
    - Demand secure Binding Updates or an authenticated packet before accepting HA
    - TE: decide which routers are configured to handle TE
- Internet defined in the RFCs  $\neq$  Internet accessed by enterprises

# IPv6 Firewalls: Fragmentation

- Some IPv4 firewalls prohibit fragmentation
- Extension headers make it harder to determine whether the upper layer protocol number is in a fragment
  - Cisco FRAGMENT keyword matches all non-initial segments and initial segments if the upper layer cannot be determined

# IPv6 Firewalls: ICMPv6 issues

- ICMPv6 needs additional attention
  - CISCO ACLs by default allow Neighbor Discovery, Neighbor Advertisement, and Neighbor Solicitation but deny others
- "Hop count 255" may be defeated by tunneling
- Is a reasonable policy-based approach to Redirects possible?
  - Note the increased use of host multi-homing

# IPv6 Firewalls: IPsec ESP

- No reasonable solution to accessing encrypted content at the border exists
  - The ipsec WG rejected an ESP-like transform that left the upper layer header in the clear
    - Another attempt is in the works
  - A proposal to use the Flow Label bits has other drawbacks
- Consider using host-based, administratively controlled firewalls

# IPv6 Firewalls: Peer-to-Peer Services

- IPv6 without NAT makes peer to peer potentially more usable
- Firewalls usually take an “outbound only” stance, except for well-known servers
- Possible approaches:
  - Reserved range of high-numbered ports
  - End-system firewalling
  - IETF midcom WG’s pinholing

# IPv6 Security: Outline

- 1 Internet Security
- 2 IPv6: Core Protocols
- 3 Protocol Security: IPsec and IKE
- 4 Firewalls for IPv6
- 5 Security and IPv6 Transition
- 6 Summary

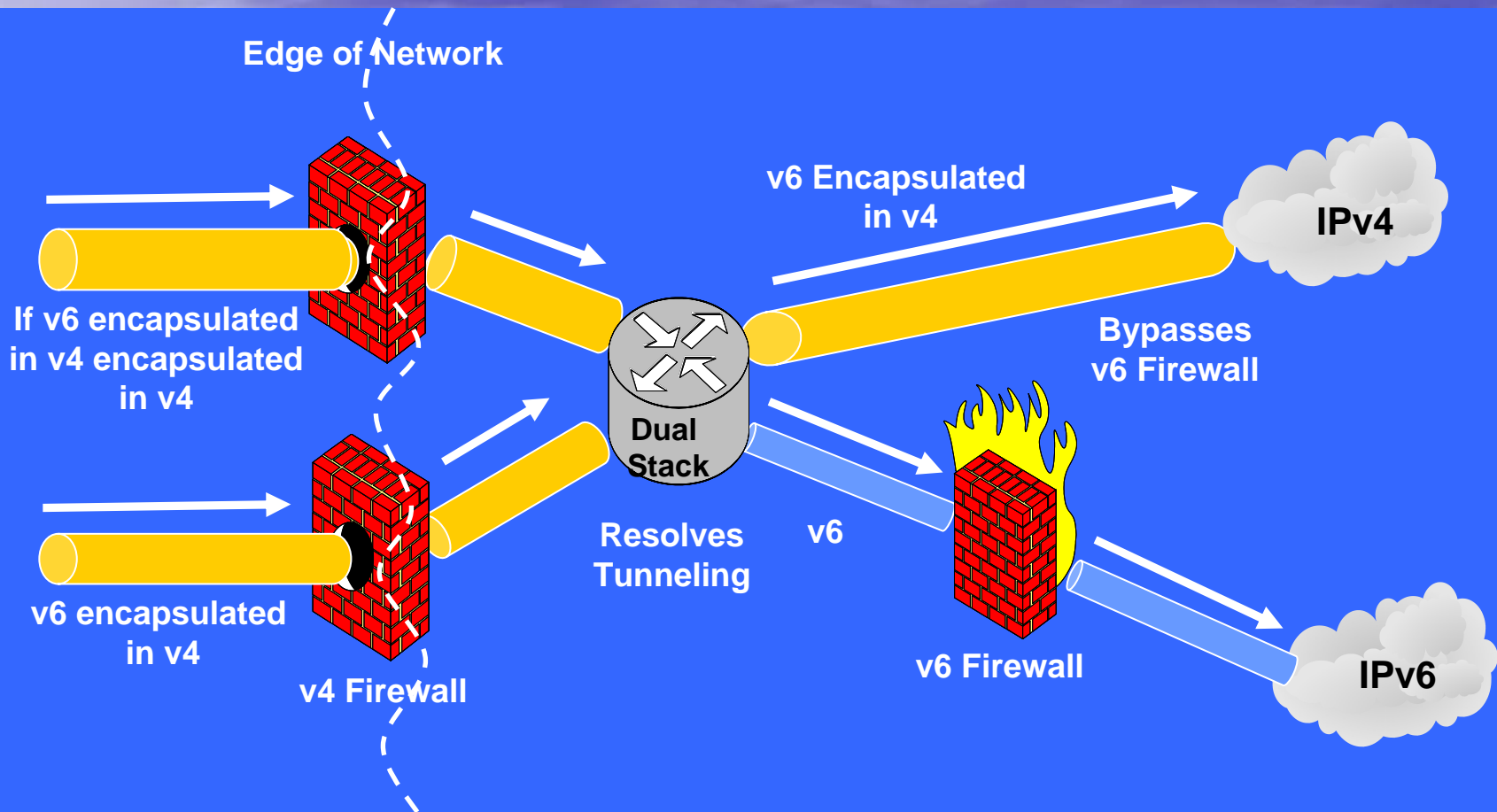
# Security and IPv6 Transition

- Two original IPv6 goals were
  - Security
  - Transition
- “Secure transition” only recently received attention
- Main transition components
  - Dual stack
  - Tunneling
  - Translation
- Many variations
  - Security issues similar
  - Some differences in the details

# Transition Strategies

- Various encapsulation (tunneling) proposals
  - SIT
  - 6over4 (RFC 2529)
  - 6to4 (RFC 3056)
  - ISATAP
  - Teredo (UDP port 3544)
- Main security issues:
  - Do not mistakenly configure a back door around firewall
  - Do not let the IPv6 network open attacks on the IPv4 network
    - After decapsulating, enforce address-interface consistency (anti-spoofing) and firewall rules
    - Requires careful configuration
  - Do not provide a hiding place for DoS attacks

# IPv6 Transition Strategy



# General Tunneling Security Issues

- Typically, a loose approach is taken to IPv6 service piloting
- Tunneling can break the perimeter defense
  - Automatic tunneling accepts packets from “everywhere”
    - Consider some access control or firewall functionality
    - For example, treat addresses the way stateful UDP filtering works
  - Tunnel exit should decrement hop count
- Ambiguities exist with IPv4-mapped IPv6 addresses
  - Applies to RFC 2373 ::ffff:a.b.c.d addresses in general
- Some IPv6 pieces are only partially deployed or immature
  - DNS, routing, applications
- Enabling IPv6 may open routers to bugs, inefficiencies, or instabilities
- IPsec can be deployed between routers and relay routers
  - With manual keying or with IKE

# IPv6 Security: Outline

- 1 Internet Security
- 2 IPv6: Core Protocols
- 3 Protocol Security: IPsec and IKE
- 4 Firewalls for IPv6
- 5 Security and IPv6 Transition
- 6 Summary

# IPv6 Security: Summary

- The IETF is still working on IPv6 security for ICMPv6, IPv6 firewalls, mobility, transition, etc.
- Hackers, today, are turning on stealth IPv6 networks after intrusions
- Increased use of IPsec depends in part on PKI and user authentication
- The “standard bag of tricks” for IPv6 firewalls has not been invented yet
- Security analysis must be a part of any service provider’s or enterprise’s IPv6 transition plan
- The Internet defined by the IETF does not always match the Internet deployed and used by today’s enterprises