Security in IPv6

Security in IPv6

- Basic Security Requirements and Techniques
  - Confidentiality
    - The property that stored or transmitted information cannot be read or altered by an unauthorized party
  - Integrity
    - The property that any alteration of transmitted or stored information can be detected

Security in IPv6

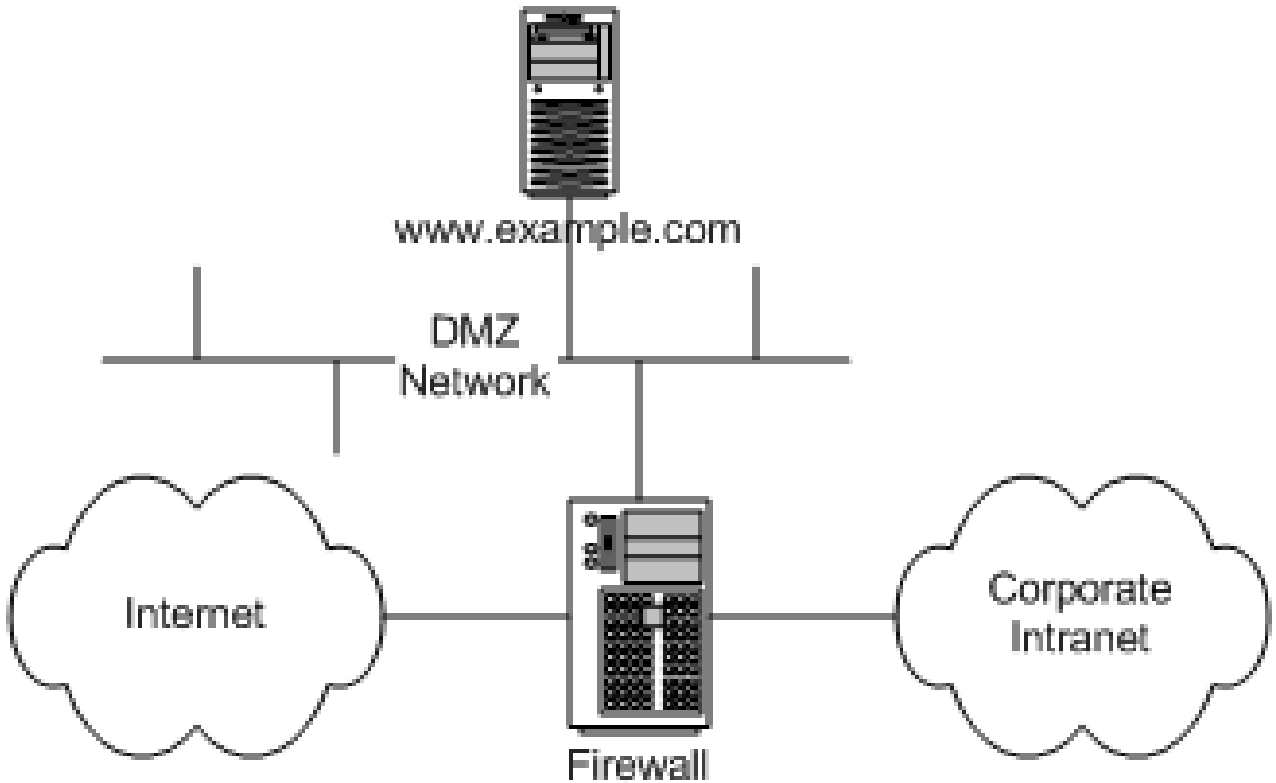
- Current Solutions
  - Internet adoption grew
    - Applications were designed and operated “ad hoc” security solutions
      - Provides semi-trusted and semi-secure Internet access
      - Don’t address fundamental issues
      - Mostly concerned with fighting symptoms

Native6 Inc.

Security in IPv6

- Current Solutions
  - Packet Filters and Firewalls
    - Filters traffic based on predefined rules
      - IP address
      - port numbers
      - virus patterns
    - May determine “unusual” behavior

Security in IPv6 - example



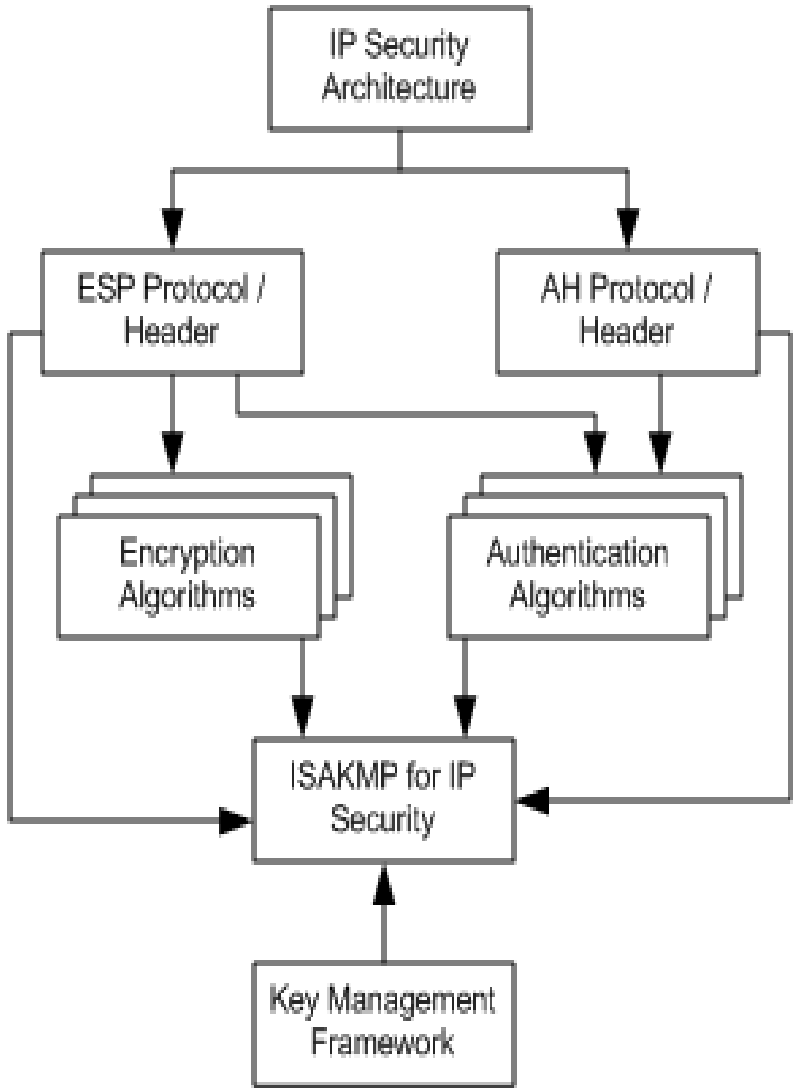
Security in IPv6

- The IPSEC framework
  - A formally defined standard (RFC 2401)
  - Contains 6 distinct elements
    - Description of security requirements and mechanisms on the network layer
    - Security element for encryption (RFC 2406)
    - Security element for authentication (RFC 2402)
    - Concrete cryptographic algorithms for encryption and authentication
    - Definition of Security policy and Security associations between partners
    - IPSEC key management
      - ISAKMP - RFC 2408 - Internet Security Association and Key Management Protocol

Security in IPv6

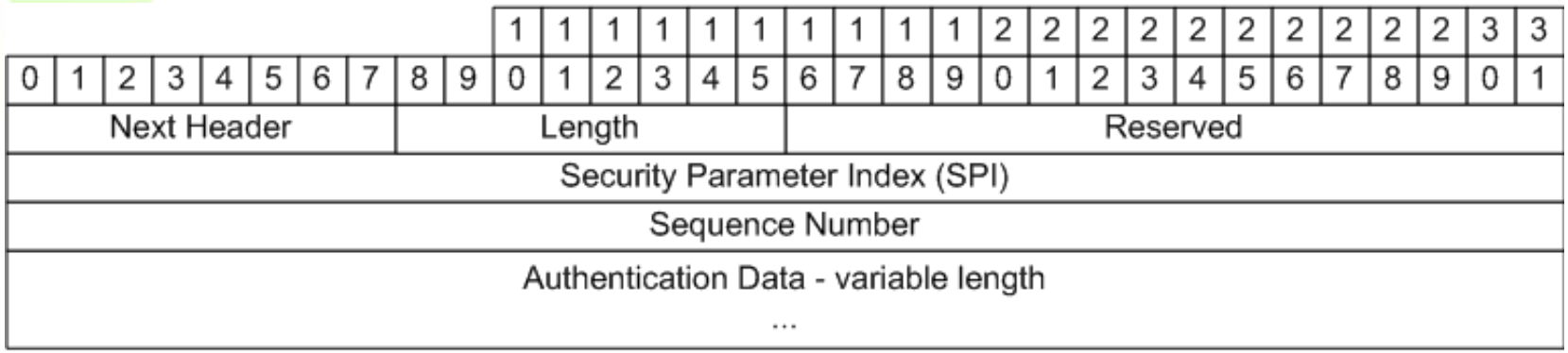
Source: "IPv6 Essentials", O'Reilly Press, 2002

The IPSEC framework



Security in IPv6

- Authentication in IPv6
  - Extension Header type 51 provides integrity and authentication for end to end data



Native6 Inc.

Security in IPv6

- Authentication in IPv6
  - Next Header
  - Length of Payload in x32 bits
  - Reserved
  - SPI - Indicates which checksum algorithm has been used
  - Sequence Number - Prevents replay attacks
    - Not to exceed 232 to prevent replay.
      - Re-negotiation should occur
      - It is know that packets may arrive out of order
  - Authentication Data - variable length
    - A cryptographically secure checksum over the payload and possibly other fields

Security in IPv6

- Authentication in IPv6
  - Cryptographical checksum is also known as a message digest or hash. Uses rules
    - IP Header, version, class, and flow label are excluded from the computation. Hop Limit is assumed to contain zero
    - All Extension Headers that change en-route are computed as a sequence of zero
    - If Routing Extension Header is present the IPv6 destination address is set to the final destination
    - IPv6 implementations MUST support
      - Keyed message digest No. 5 (MD5)
      - requires “key”
      - considered theoretically breakable
      - Secure Hash Algorithm No. 1 (SHA-1)

Security in IPv6

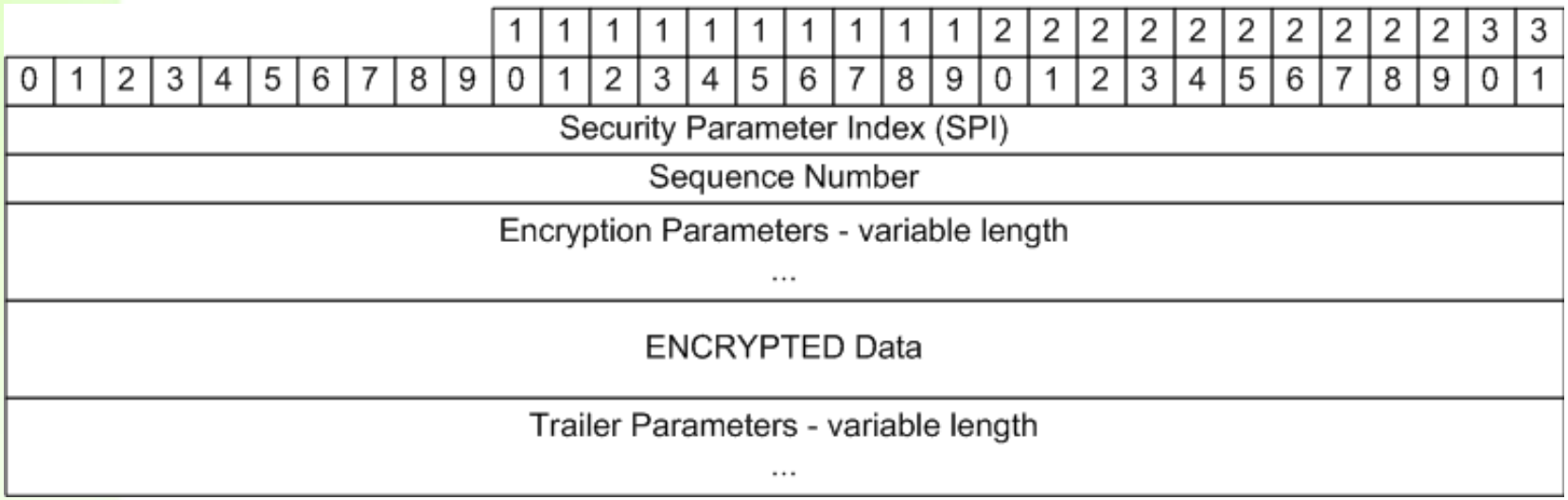
- Authentication in IPv6
  - Payload Authentication
    - Transport mode authenticates all end to end payload plus selected headers (described previously)
      - Payload Length
      - Next Header
      - Extension headers (not listed previously)
      - Upper layer headers and data
      - Some IP header fields are not protected
      - Will not work with NAT environment

Security in IPv6

- Authentication in IPv6
  - Header and Payload Authentication
    - Accomplished by creating a tunnel between 2 gateways
      - Gateway may be a router
      - May be a VPN implementation
    - Wraps the original packet in a new packet
    - Applies checksum to entire packet

Security in IPv6

- Encryption in IPv6
  - Extension Header type 50 provides integrity and confidentiality



Security in IPv6

- Encryption in IPv6
  - SPI - Indicates which encryption algorithm has been used
  - Sequence Number - Prevents replay attacks
    - Not to exceed 232 to prevent replay.
      - Re-negotiation should occur
      - It is know that packets may arrive out of order
  - Encryption Parameters - variable length
    - Depends on the encryption algorithm used
  - Encrypted Data

Security in IPv6

- Encryption in IPv6
  - Trailer
    - Contains Optional authentication information to protect the encrypted data and the sequence number
    - Padding (for 64 bit alignment)
    - Next Header value (in the encrypted packet)
  - IPv6 specification contains one encryption algorithm that must be supported by every implementation
    - DES-CBC (Data Encryption Standard in Cipher Block Chaining Mode)
  - Other stronger algorithms may be negotiated using corresponding SA and SPI
    - Government export controls

Security in IPv6

- Encryption in IPv6
  - Payload encryption
    - Transport mode encrypts all end to end extension headers and payload
      - Extension headers must not be looked at in path

Security in IPv6

- Encryption in IPv6
  - Header and Payload encryption
    - Accomplished by creating a tunnel between 2 gateways
      - Gateway may be a router
      - May be a VPN implementation
    - Wraps the original packet in a new packet
    - Applies checksum to entire packet

Security in IPv6

- Encryption in IPv6
  - Combining Authentication and Encryption
    - It was originally intended to use both
    - But increased IPv6 packet size was not good
    - Decided to included AH functionality in ESP

Security in IPv6

- IPSEC may solve many issues on the Internet
  - FTP, Telnet, DNS, and SNMP
- However other issues exist
  - IPSEC tunnels break through firewalls or NAT
  - Tunneled IPSEC traffic may contain malicious data
  - QOS doesn't work in IPSEC
  - Mobility issues
    - Dynamic IP addresses cause IPSEC to fail

Native6 Inc.

Security in IPv6

- IPv6 deployment slowed due to IPv4 workarounds
  - NAT and CIDR
  - SSL
  - SSH
  - S/MIME, PGP
- IPSEC deployment issues
  - lack of public key infrastructure
  - lack of vendor/IPv6 adoption

Native6 Inc.

Questions?