

IP Security Overview

- **IP Packets have no inherent security**
 - Relatively easy to
 - forge contents of IP packets
 - modify contents of IP packets
 - inspect the contents of IP packets in transit
- **Therefore, there is no guarantee that IP datagrams received:**
 - are from the claimed sender (source address in the IP header)
 - contain the original data that the sender placed in them
 - were not inspected by a third party while the packet was being sent from source to destination

IPSec is a means to limit the spoofing of routers

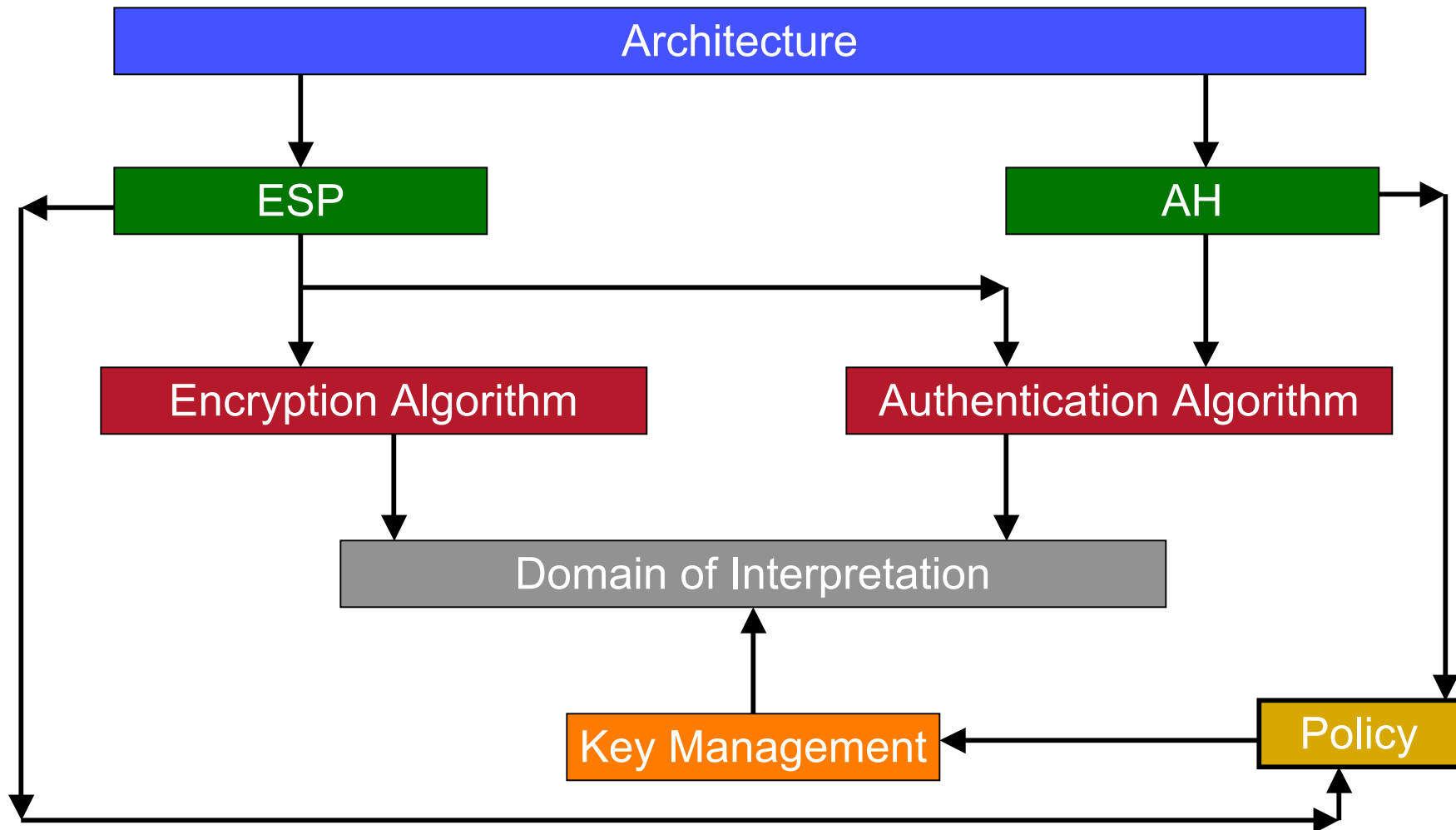


IPSec

- **IPSec is a method of protecting IP datagrams.**
- **This protection takes the form of**
 - data origin authentication
 - connectionless data integrity authentication
 - data content confidentiality
 - anti-replay protection
 - limited traffic flow confidentiality
- **Protection via Encapsulating Security Payload (ESP) or Authentication Header (AH)**
 - Ultimate security dependent upon the cryptographic algorithm applied
 - Symmetric key cryptography used – why?



IPSec Overview



IPSec Roadmap, Doraswamy and Harkins



COMP 6370 – IPSec – Lecture 13



IPSec Architecture

- **Defined by RFC 2401**
- **The IPSec protocols, AH and ESP can be used to protect an entire IP payload or the upper layer protocols of an IP payload.**
 - AH used for authentication
 - ESP used for encryption
- **Two different modes of IPSec**
 - Transport mode to protect upper-layer protocols
 - Tunnel mode to protect entire IP datagrams



Transport Mode

- **AH and ESP intercept the packets moving from the transport layer into the network layer.**
 - When security is **NOT** enabled, TCP and UDP flow into IP which adds an IP header
 - When security is enabled, TCP / UDP flow into the IPsec component
 - When **both** AH and ESP are used, ESP is applied first – why?



Packet format with AH and ESP



Tunnel Mode

- IPsec in Tunnel mode is normally used when the ultimate destination of the packet is **different** from the security termination point.
 - ex. security termination point may be a router rather than a host.
 - also used when a router provides security services for packets it is forwarding
 - In the case of tunnel mode, IPsec encapsulates an IP packet with IPsec headers and adds an outer IP header



IPsec tunneled mode packet format



Transforms

- **Transformation applied to the data to secure it.**
 - includes algorithm, key sizes, derivations
 - specific information required in order for different implementations to interoperate
- **IKE – Internet Key Exchange**
 - establishes shared security parameters and authenticated keys
 - i.e. security associations (SAs) between IPSec peers
 - Actual negotiated parameters come up in the Domain of Interpretation (DOI)
- **Policy**
 - Necessary but not sufficient for interoperability
 - Determines transforms, representations and implementation



IPSec Implementation

- Can be implemented in end hosts, gateways / routers or both
- **Advantages of OS-level integration**
 - Efficiency: IPSec can use network services in the OS such as user context (sockets)
 - Ease of Implementation: Network connections, HTTP connections – all can be configured from the host
 - All IPSec modes are supported
- **BUMP-in-the-Stack (BITS) network level integration**
 - Supports multiple OSs
 - Duplicated functionality causing unnecessary complications
 - Allows firewall vendors to integrate with their products



Security Associations

- **SAs form the basis for IPSec**
 - contract between two communicating entities
 - determine the protocols used for securing packets
- **SAs are one-way, i.e. simplex**
 - If two hosts are communicating, host A will have an SAout and an SAin
- **SAs are protocol specific**
 - Each host builds a separate SA for AH and ESP
- **Security policy database**
 - Works in conjunction with the security association database
- **Security Parameter Index**
 - 32-bit entity that is used to uniquely identify an SA at the receiver
 - SPI passed to AH and ESP headers using a tuple <spi,dst,protocol>

