

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

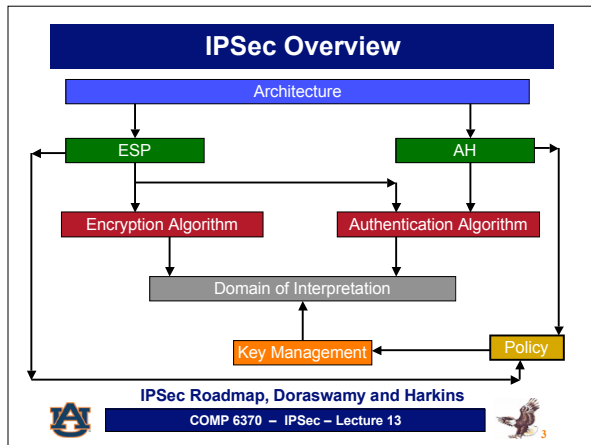
IPSec is a means to limit the spoofing of routers

COMP 6370 – IPSec – Lecture 13

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?

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

COMP 6370 – IPSec – Lecture 13

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?

IP Header	AH Header	ESP Header	TCP Payload
-----------	-----------	------------	-------------

Packet format with AH and ESP

COMP 6370 – IPSec – Lecture 13

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

(Outer)IP Header	ESP	IP Header	Network Payload
------------------	-----	-----------	-----------------

IPSec tunneled mode packet format

COMP 6370 – IPSec – Lecture 13

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



COMP 6370 – IPSec – Lecture 13



7

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



COMP 6370 – IPSec – Lecture 13



8

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>



COMP 6370 – IPSec – Lecture 13



9