CSCI 7000-001 — Network-level Security: IPSec Basic Architecture

October 18, 2001

References:

- RFC 2401 (`http://www.ietf.org/rfc/rfc2401.txt`)

1 Premise

General principle: *security in distributed systems should be implemented at the highest level possible.*
However

- many systems still rely on network-level security
- many systems rely on authentication based on the network-level source address
- many systems do not implement any form of encryption for confidentiality

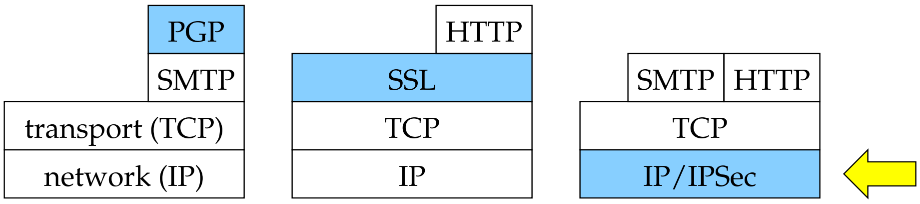
therefore, it would be good to have some network-level security.

2 IP-level security overview: goals

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. In particular:

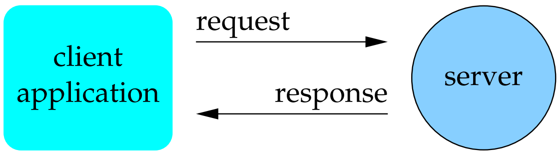
- access control
- connectionless integrity
- data origin authentication
- protection against replays (a form of partial sequence integrity)
- confidentiality (encryption)

- limited traffic flow confidentiality.



These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

3 How IPSec applies to network traffic



- applications are oblivious to the IPSec
- so who decides where, when, and how to apply security?

For each packet, an IPSec implementation decides whether to

- discard that packet
- bypass IPSec security services, or
- afford IPSec security services

4 Security Policy Database (SPD)

The decision is based on a *security policy*, stored in a Security Policy Database (SPD).

The SPD contains an ordered list of policy entries. Each entry is defined by one or more *selectors*, and an indication whether the traffic matching this policy will be bypassed, discarded, or subject to IPsec processing.

- source address
- destination address
- protocol
- source port
- destination port
- user id
- ...

5 How IPSec provides security

IPsec uses two protocols to provide traffic security:

- *Authentication Header (AH)* provides connectionless integrity, data origin authentication, and an optional anti-replay service.
- *Encapsulating Security Payload (ESP)* provides
  - confidentiality (encryption), and limited traffic flow confidentiality, and optionally
  - data origin authentication, and an anti-replay service

Both AH and ESP, indirectly, provide access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

6 Summary of mapping of services to protocols

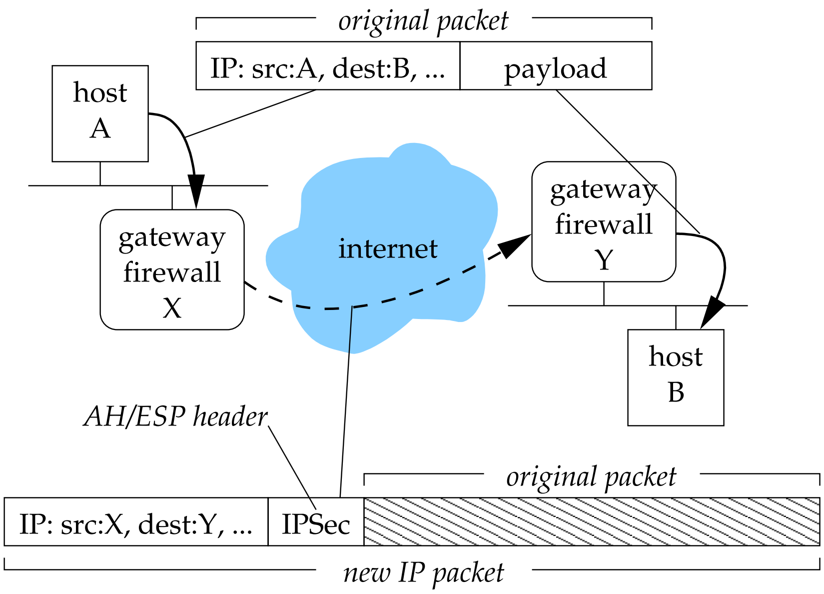
	AH	ESP authentication	ESP authentication + encryption
access control	•	•	•
connectionless integrity	•		•
data origin authentication	•		•
rejection or replayed packets	•	•	•
confidentiality		•	•
limited traffic flow confidentiality		•	•

7 Transport and tunnel modes

Both AH and ESP can function in either

- *transport mode* provides security for upper-level protocols (such as TCP or UDP) by authenticating and/or encrypting the payload
- *tunnel mode* provides security for the whole IP packet by encapsulating (tunneling) that packet into another IP packet.

8 Virtual private networks with tunnel mode



9 Security association (SA)

- key concept appearing in both authentication and confidentiality mechanisms of IPSec
- *one-way* relation
- between a *sender* and a *receiver*

a security association is identified by

- *security parameter index (SPI)*: a key that identifies a set of parameters for this association, stored in the Security Association Database
- *destination address* (currently only unicast addresses)
- *security protocol identifier*: AH or ESP

10 Some comments

- key exchange and cipher negotiation is outside the scope of the basic architecture
- policy definition is outside of the scope of IPSec
- policy implementation reduces to network management