# Internet Security

Comer's
chapter 32 (4th ed.)
chapter 28 (3rd ed.)



# Contents

- Internet Protocol Security
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Security Association (SA)
  - Key Management (with IKE)
- Firewalls
- Virtual Private Network (VPN)

# Security Services

- Confidentiality
- Integrity
- Availability

- Access Control
- Authentication and Authorization
- Non-repudiation



# Introduction to Cryptology

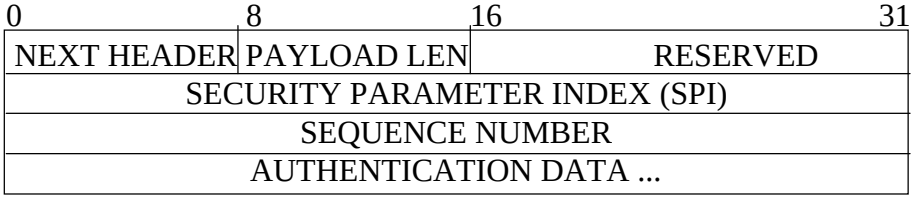
- Symmetric and public key cryptography
- Digital signature
- Cryptographic hash functions
- Message Authentication Code (MAC)
- Random number generators

# IP Security (IPsec)

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Transport and tunneling mode
  - between two hosts, two security gateway or security gateway and host
- Authentication of data origin, integrity and/or confidentiality, anti-replay service
- Works with both IPv4 and IPv6

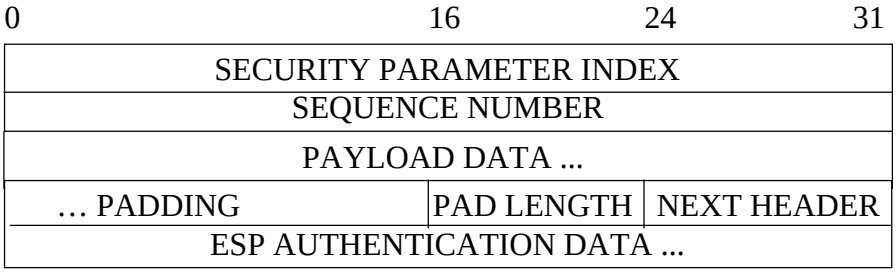


# Authentication Header




- Connectionless integrity and data origin authentication
- Authenticate the non-changeable fields of IP header and data in the datagram

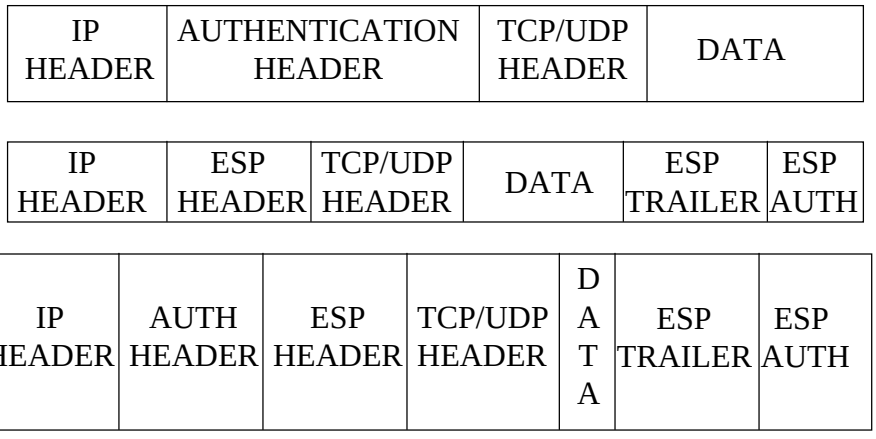
# Encapsulating Security Payload




- Connectionless integrity, data origin authentication, and/or confidentiality
- Header and trailer

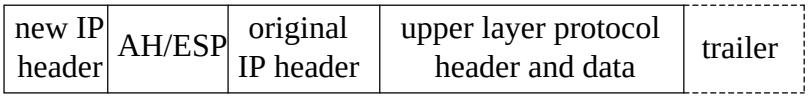


# Datagram Structure



# IPsec Tunneling

- Tunneling is used when another end or both ends of a connection is/are (acts as) a security gateway
- New IP header is formed and the whole original IP datagram is protected by selected SA






# Security Association (SA)

- SA defines the security services used
  - which depend on the security protocol, chosen algorithms and mechanisms
  - that protect communication to one direction between two endpoints
- There may be several SAs for one connection
- SA identifier: Security Parameter Index (SPI), IP destination address and security protocol identifier

# Security Association Management and Key Exchange for IPsec

- Use of IPsec requires agreement of SA and cryptographic keys
  - authentication algorithms
  - encryption algorithms
  - used keys and their delivery mechanisms
- Security Policy of an organization defines common goals that must be followed

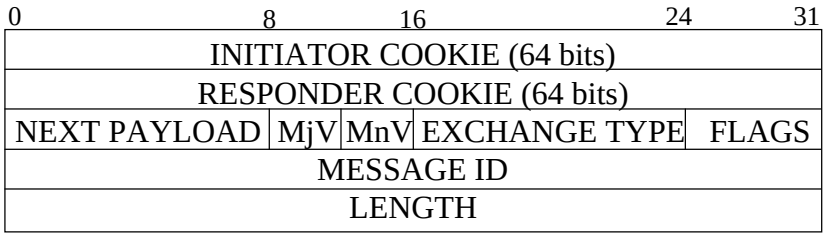


# Internet Security Association and Key Management Protocol (ISAKMP)

- A generic framework for negotiating and maintaining SAs and keys
  - can use certificates for authentication/authorization
  - can protect identity of communicating peers
- Does not bind to use specific algorithms or mechanisms

# ISAKMP (continued..)

- Header, 13 payloads and 5 exchanges
- Two phases
  - ISAKMP SA negotiation
  - Protocol specific SA negotiation






# Domain of Interpretation (DOI)

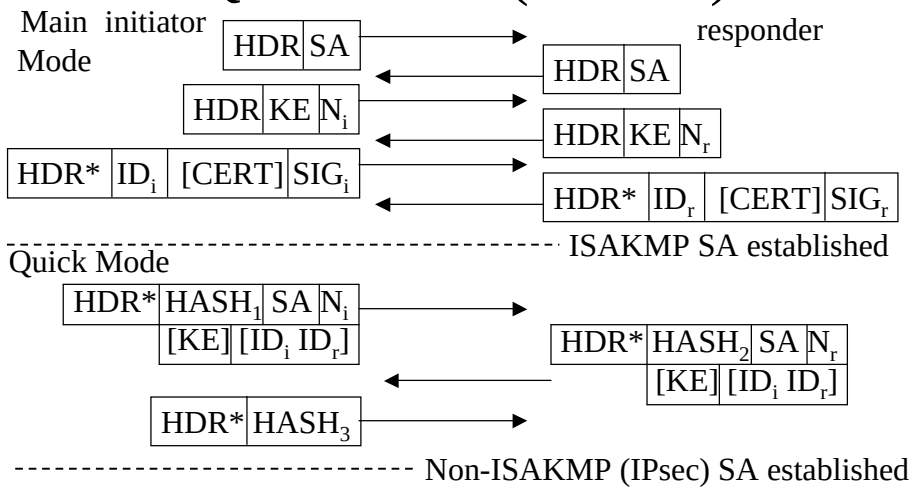
- Used in Security Association negotiation
  - naming scheme for protocol identifiers
  - interpretation of some fields of ISAKMP
  - syntax for attributes
  - additional types
- DOI for IPsec is defined in RFC 2407
- ISAKMP acts as a DOI for itself

# Internet Key Exchange (IKE)

- Standard for key and SA management protocol for IPsec
- Uses Diffie-Hellman key exchange
- Phase one negotiation: two modes
  - Authentication with signatures, two kinds of public key encryption, or pre-shared key
- Phase two: SA for IPsec
  - Quick Mode



# IKE: Main Mode (Phase 1) and Quick Mode (Phase 2)



# SA and Security Policy Databases

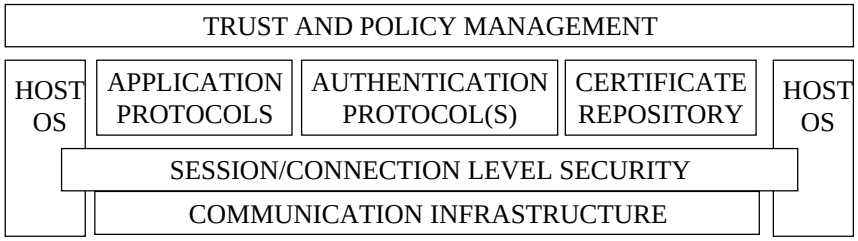
- Security Association Database (SAD)
  - Used SAs for every connection
- Security Policy Database (SPD)
  - Offered security services
  - Managing security for all traffic



# Trust Management

- Public Key Infrastructure (PKI) provides authenticated keys in an untrusted network
- Certificates are signed documents
  - X.509 (identity certificates)
  - SPKI (authorization certificates)
- Trusted Third Parties (TTP)
- Kerberos

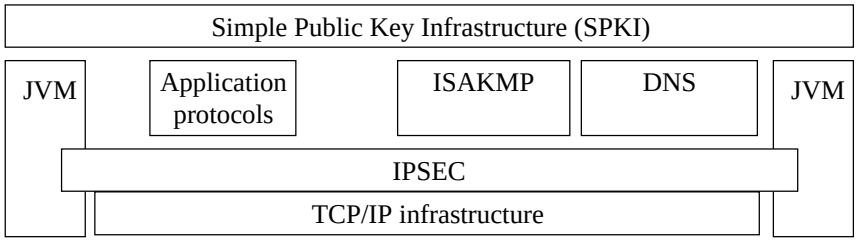
# Architecture for Internet Security




- Pekka Nikander's Doctoral Thesis



# TeSSA Architecture

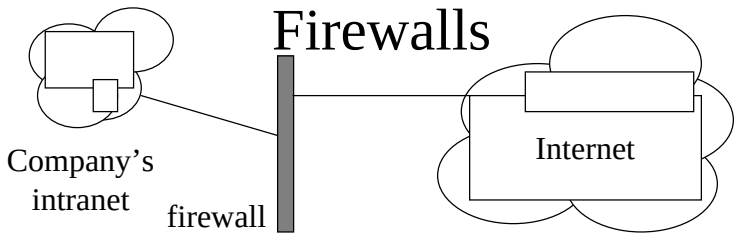



- Implementation of Nikander's architecture
- Prototypes done in TeSSA-project at TML/HUT (several master's thesis)

# Firewalls and VPN



## Firewalls




- Separate the network to "inside" and "outside" networks
  - implement access control policy
  - hide structure of intranet
- Usually vendor-specific implementations

# Network Layer Firewalls

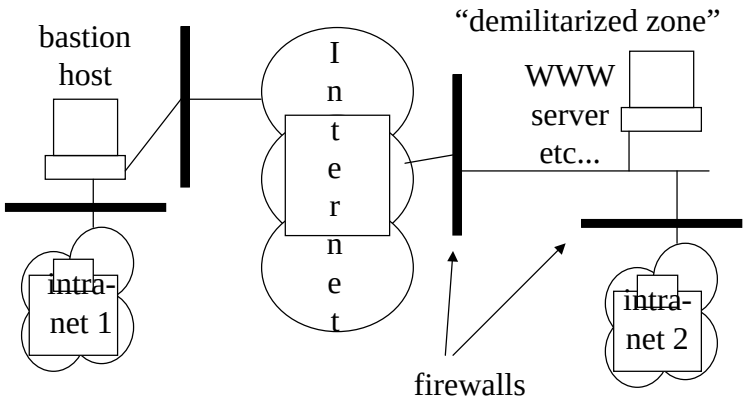
- Also called Packet filter firewalls
- Access decision is based on addresses and ports of TCP/IP packets and protocols
- Block all datagrams except some specific addresses, ports and protocols
- Efficient and simple
- Can be implemented by routers



# Application Layer Firewalls

- Proxy-based firewalls
- Understand used applications
- More complex but allow more flexibility
- Access control and Logging
- Can also implement other services like NAT

# Firewall Architectures






# Surveillance

- Purpose is to notice problems and attempts to break in the system
- Monitoring
  - Active: for example, sending mail to administrator
  - Passive: writing a log

# Virtual Private Network (VPN)

- Internet is used to connect private networks of an organization
  - does not use reserved private channels to interconnect parts
- Tunneling and encryption
  - confidentiality and privacy
- Several vendor-specific solutions available



# Summary

- Internet is not trustworthy
- Several techniques to provide security
- IPsec provides authentication and confidentiality
- Firewalls provide access control
- Virtual Private Networks (VPN) provide trusted network connection through Internet

# References

- Comer chapter 32 and 20
- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: Handbook of Applied Cryptography
- Pekka Nikander: An Architecture for Authorization and Delegation in Distributed Object-Oriented Agent Systems



# References - RFCs

- 2401- Security Architecture for the Internet Protocol
- 2402 - IP Authentication Header
- 2406 - IP Encapsulating Security Payload (ESP)
- 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
- 2408 - Internet Key Exchange and Key Management Protocol (ISAKMP)
- 2409 - The Internet Key Exchange (IKE)
- 2411 - IP Security Document Roadmap

# More courses

- Tik-110.401 Fundamentals of information security
- Tik-110.451 The development process of information security
- Tik-110.452 Special course in practical security of information systems
- Tik-110.501 Seminar on network security
- Tik-110.502 Fundamentals of cryptology
- Tik-110.554 Seminar on corporate security
- Tik-79.159 Cryptography and data security