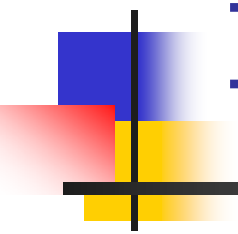
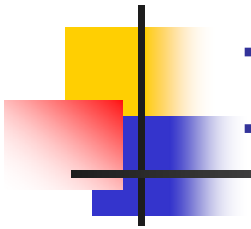


ISAKMP

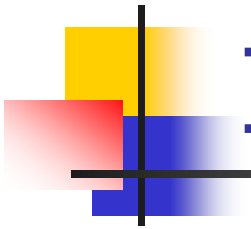
Internet Security Association and Key Management Protocol

Artur Hecker, ENST Paris
Paris, 01/24/2002



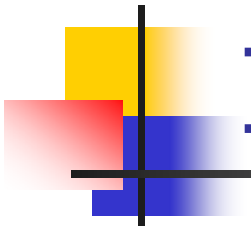
ISAKMP: Intentions

- Intended to support the SA management for security protocols at all layers (IPSEC, TLS, OSPF, etc.)
- Centralizes the SA management and reduces the amount of duplicated functionality



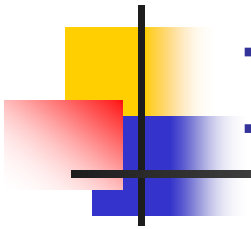
ISAKMP: Overview

- Defined in RFC 2408
- Cleanly separates the two points:
  - Security Association (SA) and key management
  - key exchange protocol (not defined here)
- Builds a framework for:
  - Transferring key and authentication data
  - Negotiation, establishment, modification and deletion of SAs



ISAKMP: Motivation

- Growing number of complex VPNs:
  - One security requirement within the VPN and many others for communications outside
- Mobility
  - Limited bandwidth
  - Need for authentication



ISAKMP: Requirements

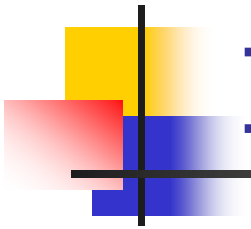
- Linkage of authentication and key exchange within one protocol, linkage of the SA establishment with this protocol
- Usage of strong authentication with digital signatures based on PK-cryptography

ISAKMP: Basic run – 2 phases

Phase 1: ISAKMP SA establishment

- Initial protocol exchange:
  - Agreement upon basic set of security attributes
  - Provides protection for subsequent exchanges
  - Indicates the auth-method and key exchange to be performed within ISAKMP
  - Can be skipped if the basic set already exists
- Authentication+key (material) exchange
- Generation of required keys

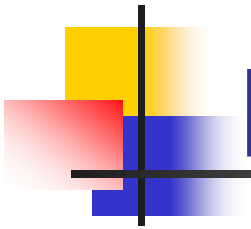
Phase 2: Protocol SA establishment



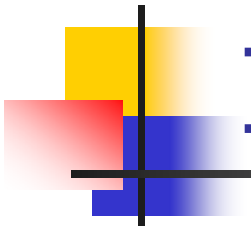
ISAKMP: Why 2 phases?

1. Amortization of the costs of the first phase across several second phase negotiations
2. First channel provides security properties for the second phase. The security can be adjusted in the second phase.
3. Reduced cost of the ISAKMP management: no re-auth for each error

ISAKMP: Key exchange protocol

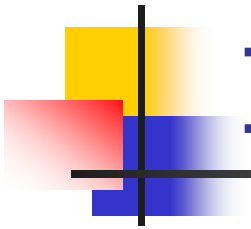


- Is not defined in ISAKMP, possibility: IKE
- Requirements:
  - Key generation vs. transport
  - Perfect forward secrecy (PFS)
  - Computational overhead
  - Key escrow
  - Key strength
- Negotiated and supported by ISAKMP



ISAKMP: Protection (1/2)

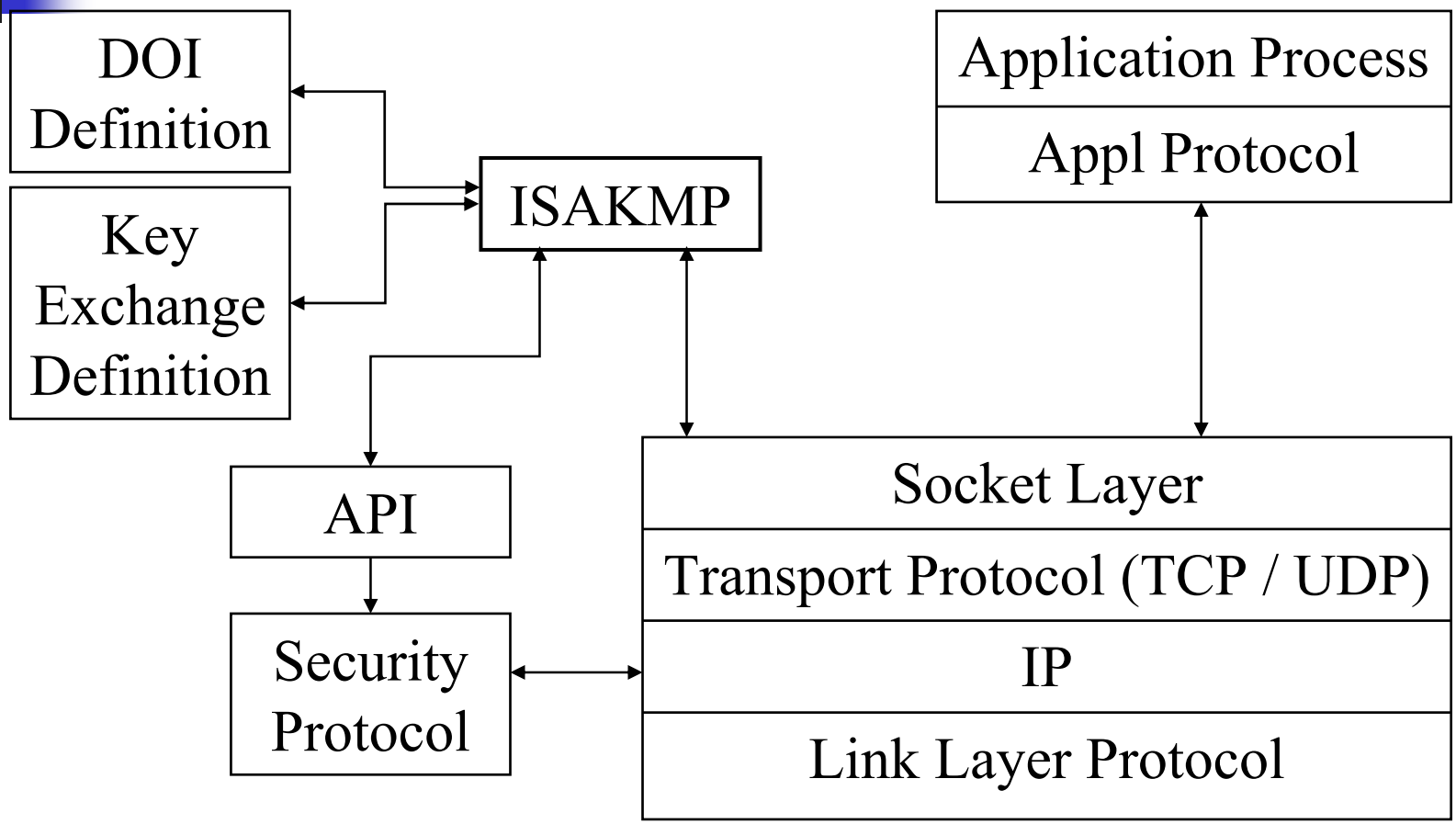
- Denial of Service
  - Cookie exchange (using only fast operations)
  - Aggressive memory management in the FSM
  - Absolute protection impossible!!!
- Connection Hijacking
  - Authentication linked with key and SA exchanges
- Multicast communications
  - Planned as a future extension



ISAKMP: Protection (2/2)

- Man-in-the-Middle
  - Exchange linking against message insertion
  - No partial SA creation
  - FSM design against reflection back to sender
  - Time variant material against replaying
  - Strong authentication
  - Detection of redirection and modification

ISAKMP: Placement



ISAKMP: Cookies

- So-called Anti-Clogging Tokens (ACT)
- Three generation rules:
  1. Depend on the specific parties
  2. No other entity can generate the same cookie so it will be accepted by the entity
  3. The generation function must be fast
- Example:

cookie := md5(IPsrc, IPdst, UDPsrc, UDPdst, RndVal, timestamp)

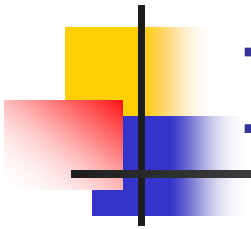
ISAKMP: Fixed header format

1 64

Initiator Cookie				
Responder Cookie				
Next Payload	MjVer	MnVer	Exchange Type	Flags
Message ID				
Length				

Next Payload (1 byte): The format of the next payload
Major/Minor Version (4 bit) : ISAKMP protocol version
Exchange Type (1 byte): Type of exchange being used
Flags (1 byte): Specific options set for the exchange

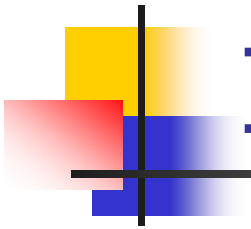
ISAKMP: Payload types



- Each payload type has its own header
- Header chaining with the "general header"
- Exact header formats defined in the RFC (3.4-3.16)
- Header processing rules in the RFC (5)

1. Security Association
2. Proposal
3. Transform
4. Key Exchange
5. Identification
6. Certificate
7. Certificate Request
8. Hash
9. Signature
10. Nonce
11. Notification
12. Delete
13. Vendor ID

-- Private USE (128-255)



ISAKMP: Conclusions

- Well-designed protocol aimed to the future
- Contains all the features needed for Internet's massive growth
- Flexible through negotiation
- Able to establish SAs for multiple protocols
- Can be used with arbitrary transports
- Follows the design principles of IPv6