IPsec

Protocol security - where?

Application layer: (+): easy access to user credentials, extend without waiting for OS vendor, understand data; (-): design again and again; e.g., PGP, ssh, Kerberos

Transport layer: (+): security mostly seamlessly, but difficult to get credentials; e.g., TLS

Network layer: (+): reduced key management, fewer application changes, fewer implementations, VPNs; (-) non-repudiation, multi-user machines, partial security in “middle boxes”

Data link layer: (+): speed; (-): hop-by-hop only

Documents

Document Roadmap	RFC 2411
Architecture	RFC 2401
IP Authentication Header (AH)	RFC 2402
IP Authentication Using Keyed MD5	RFC 1828
IP Encapsulating Security Payload (ESP)	RFC 2406
The Oakley Key Determination Protocol	RFC 2412
Internet Sec. Assoc. and Key Mmgt. P. (ISAKMP)	RFC 2408
The Internet Key Exchange (IKE)	RFC 2409
HMAC: Keyed-Hashing for Message AuthenticationA	RFC 2104

IPSec services

- IPv4 and IPv6 unicast
- access control
- connectionless integrity
- data origin authentication
- protection against replays (partial sequence integrity)
- confidentiality (encryption)
- limited traffic flow confidentiality.
- todo: NAT, multicast

Architecture

Authentication header (AH): access control, integrity, data origin authentication, replay protection

Encapsulating Security Payload (ESP): access control, confidentiality, traffic flow confidentiality.

Key management protocols: IKE = OAKLEY + ISAKMP, . . .

- for any upper-layer protocol
- no effect on rest of Internet
- algorithm-independent, but default algorithms

Architecture

- between host and/or security gateways
- security gateway = router, firewall, ...
- security policy database (SPD) ➠ IPsec, discarded, or bypass
- negotiate compression (why?)
- *tunnel mode* or *transport mode*
- granularity: single host-host tunnel vs. one per TCP connection

Implementation

- native IP implementation
- bump in the stack (BITS): beneath IP layer
- bump in the wire (BITW)

Security Assocation (SA)

- simplex
- AH *or* ESP
- identified by
  - Security Parameter Index (SPI),
  - IP destination address,
  - security protocol (AH or ESP) identifier.
- transport mode: two hosts
  - AH or ESP after IPv4 options, before UDP/TCP
  - IPv6: after base header and extensions, before/after destination options
  - mostly for higher-layer protocols (but: AH also some IP header parts)
- tunnel mode: one or two security gateways

- outer header ➠ tunnel endpoint
- security header between outer and inner
- traffic hiding; ESP payload padding

Nested Security Associations

AH *and* ESP ➠ two SAs (“SA bundle”):

- transport adjacency: AH, then ESP
- both tunnel endpoints the same
- one endpoint the same
- neither the same

Security Policy Database

- map to Security Assocation Database (per packet or per SPD entry)
- discard, bypass or apply to *inbound* or *outbound*
- ordered list of filters (stateless firewall)
- example: “use ESP in transport mode using 3DES-CBC with explicit IV, nested inside of AH in tunnel mode using HMAC-SHA-1.”
- selectors:
  - destination IP address: address, range, address + mask, wildcard
  - source IP address
  - name (for BITS/BITW hosts): user id, X.500 DN, system name, opaque, ...
  - data sensitivity label
  - transport layer protocol

- source/destination ports

- per socket setup or per packet (BITS, BITW, gateway)

Security Association Database (SAD)

- inbound: outer destination address
- IPsec protocol (AH or ESP)
- SPI (32-bit value)

Examples of Implementations

- end-to-end security (H1* == H2*)
- VPN (H1 – SG1* == SG2* – H2)
- e2e + VPN (H1* – SG1* == SG2* – H2*)
- remote access (H1* == SG2* – H2*)

Locating a Security Gateway

- where's the gateway? authentication?
- currently done manually
- alternatives: SLP, multicast, DHCP, ...

Authentication header (AH)

protocol 51:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   |  Payload Len  |          RESERVED             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Security Parameters Index (SPI)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sequence Number Field                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+          Authentication Data (variable, typ. 96 b)            |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Authentication Header: Transport Mode

IPv4:

```
---------------------------------
|orig IP hdr  |    |     |      |
|(any options)| AH | TCP | Data |
---------------------------------
|<------- authenticated ------->|
except for mutable fields
```

IPv6:

```
------------------------------------------------------------
|             |hop-by-hop, dest*, |    | dest |     |      |
|orig IP hdr  |routing, fragment. | AH | opt* | TCP | Data |
------------------------------------------------------------
|<---- authenticated except for mutable fields ----------->|
```

Authentication Header: Tunnel Mode

IPv4:

```
------------------------------------------------
| new IP hdr* |    | orig IP hdr*  |    |      |
|(any options)| AH | (any options) |TCP | Data |
------------------------------------------------
|<- authenticated except for mutable fields -->|
|            in the new IP hdr                 |
```

IPv6:

```
---------------------------------------------------------------
|            | ext hdrs*|    |            | ext hdrs*|   |    |
|new IP hdr*|if present| AH |orig IP hdr*|if present|TCP|Data|
---------------------------------------------------------------
|<-- authenticated except for mutable fields in new IP hdr ->|
```

Authentication

- replay prevention: if seq. no. cycles, new SA; sliding window ➠ reject lower than left window edge
- immutable or predictable IP header fields: version, IH length, total length, identification, protocol, source, destination (source route ➠ predictable)
- set mutable fields to zero: TOS, flags, fragment, TTL, header checksum
- AH header, with zero ICV
- upper-layer data

Encapsulating Security Payload (ESP)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
|               Security Parameters Index (SPI)                 | ^Auth.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          | |erage
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
~                                                               ~ |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |     Padding (0-255 bytes)                     | |erage*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|                 Authentication Data (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ESP for IPv4

```
-------------------------------------------------
|orig IP hdr  | ESP |     |       |   ESP    | ESP|
|(any options)| Hdr | TCP | Data  | Trailer  |Auth|
-------------------------------------------------
                    |<----- encrypted ---->|
              |<------ authenticated ----->|
```

ESP

- DES in CBC mode [MD97]
- HMAC with MD5 (RFC 2104)
- HMAC with SHA-1
- NULL Authentication algorithm
- NULL Encryption algorithm

Keyed Authentication (RFC 2104)

- keyed MAC (message authentication codes)
- works with any iterated hash
- prf(key, msg) = $H((K \oplus opad)|H((K \oplus ipad)|text))$
- note: double hash, avoids continuation problem of $H(K—m)$
- replace fixed IV of iterated hash by random (key) IV
- outer pad (opad) = 0x5c, ipad = 0x36 (Hamming distance!) to $B = 64$ bytes
- may truncate hash – no less secure

Internet Key Exchange (IKE)

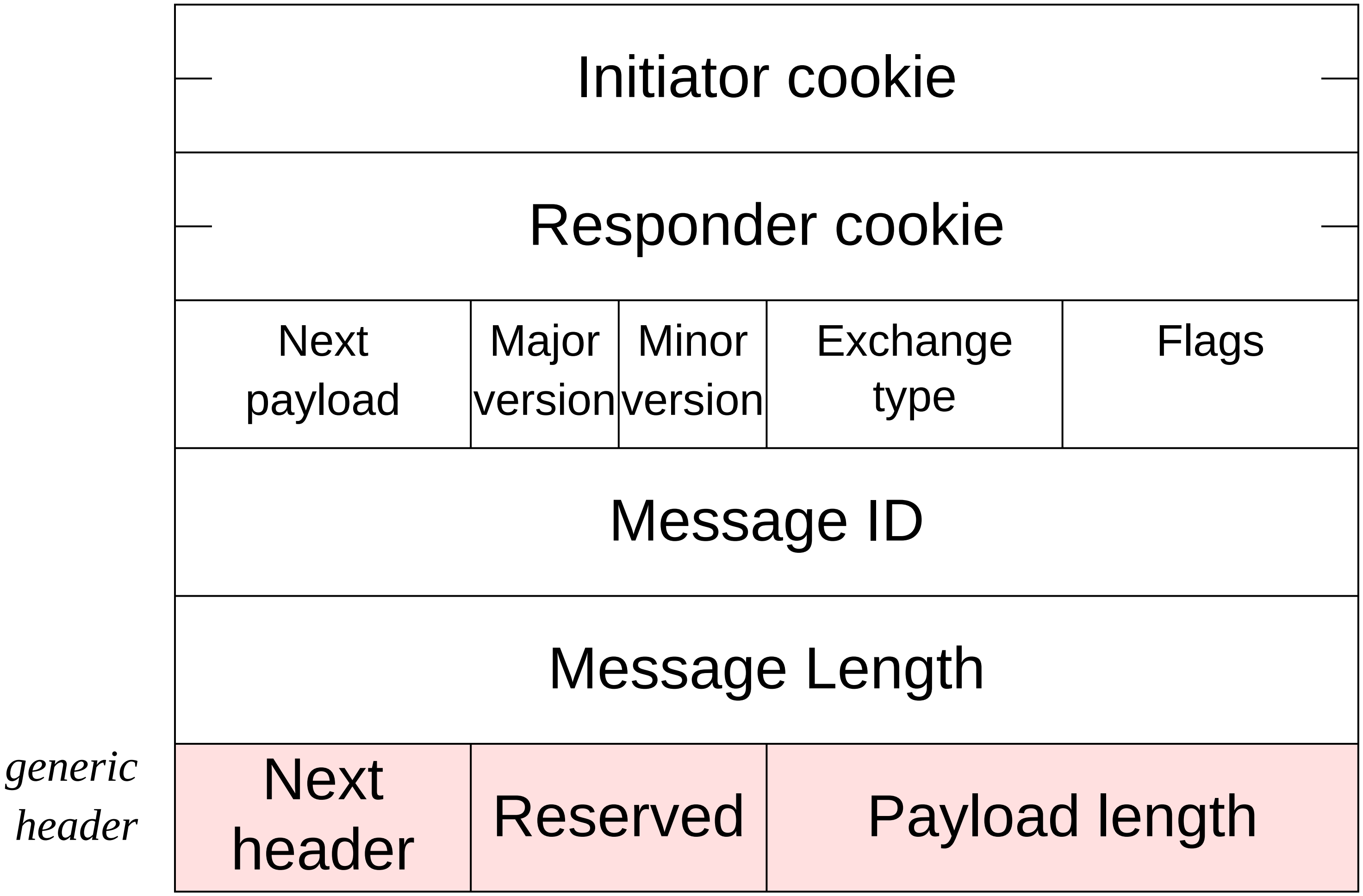
- IKE = ISAKMP + Oakley
- "negotiate and provide authenticated keying material for security associations in a protected manner"
- VPN, remote ("roaming") user
- perfect forward secrecy (PFS): compromise of key ➠ only single data item (➠ D-H)
- DOI = domain of interpretation ➠ roughly, "name space" for algorithms (RFC 2407)
- ISAKMP phases, Oakley modes:

Phase 1: ISAKMP peers establish bidirectional secure channel using *main mode* or *aggressive mode* $\longrightarrow$ ISAKMP SA

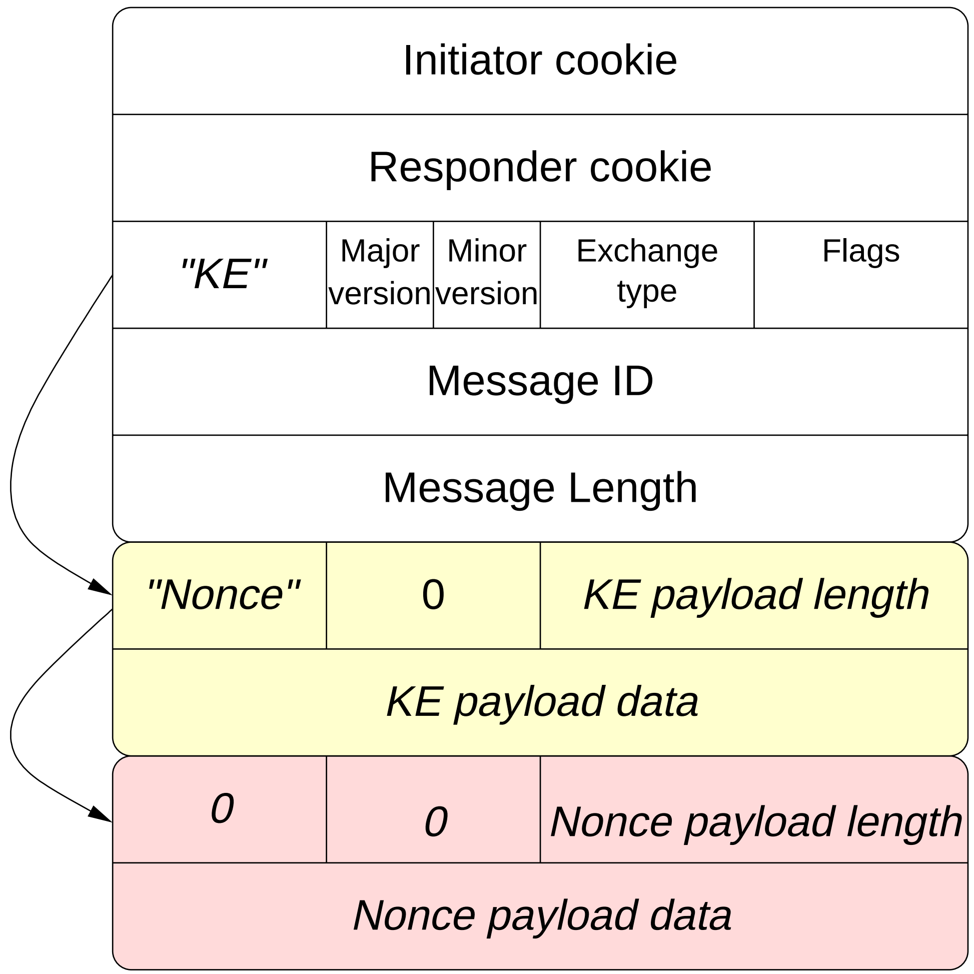
Phase 2: negotiation of security services for IPsec (maybe for several SAs) using *quick mode*

- can have multiple Phase 2 exchanges, e.g., to change keys

ISAKMP


Initiator cookie
Responder cookie
Next payload
Major version
Minor version
Exchange type
Flags
Message ID
Message Length
generic header
Next header
Reserved
Payload length

ISAKMP example



Phase 1 ISAKMP exchange

all based on ephemeral Diffie-Hellman exchange

Main mode: 6 messages = negotiate policy (2 msg.), D-H + nonces (2), authenticate D-H (2)

Aggressive mode: 3 messages = negotiate policy, exchange D-H public values, identities, authenticate responder (2 msg.), authenticate initiator

typically uses UDP (port 500), may use other protocols

Policy proposals

Allow AND (same number) and OR (different numbers); transforms are always OR

Proposal 1	AH	
	Transform 1: HMAC-SHA	
	Transform 2: HMAC-MD5	
Proposal 2	ESP	
	Transform 1: 3DES with HMAC-SHA	
Proposal 3	ESP	
	Transform 1: 3DES with HMAC-SHA	
Proposal 3	PCP	
	Transform 1: LZS	
	Transform 2: Deflate	

ISAKMP Attacks

Connection hijacking: linking authentication, key exchange, SA exchange

Man-in-the-Middle: linking ➠ no insertion; deletion ➠ no creation; reflection; modification

ISAKMP Identification

#	Operation	I-C.	R-C.	Message ID	SPI
1	Start ISAKMP SA negotiation	X	0	0	0
2	Respond ISAKMP SA negotiation	X	X	0	0
3	Init other SA negotiation	X	X	X	X
4	Respond other SA negotiation	X	X	X	X
5	Other (KE, ID, etc.)	X	X	X/0	NA
6	Security Protocol (ESP, AH)	NA	NA	NA	X

ISAKMP Message

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                          Initiator                            !
!                            Cookie                             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                          Responder                            !
!                            Cookie                             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  Next Payload ! MjVer ! MnVer ! Exchange Type !     Flags     !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                          Message ID                           !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                            Length                             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ISAKMP Payloads

NONE	0
Security Association (SA)	1
Proposal (P)	2
Transform (T)	3
Key Exchange (KE)	4
Identification (ID)	5
Certificate (CERT)	6
Certificate Request (CR)	7
Hash (HASH)	8
Signature (SIG)	9
Nonce (NONCE)	10
Notification (N)	11
Delete (D)	12
Vendor ID (VID)	13
RESERVED	14–127
Prive Use	128–255

Anti-Clogging Token (”Cookie”) Creation

- The cookie must depend on the specific parties;
- It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity.
- The cookie generation function must be fast to thwart attacks intended to sabotage CPU resources.

➠ hash over the IP source and destination address, the UDP source and destination ports and a locally generated secret random value.

ISAKMP

- encrypted flag ➠ SA(ic,rc)
- commit: done with phase, detect losses
- authentication

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
! Next Payload  !   RESERVED    !         Payload Length        !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IKE Keys

SKEYID =

signatures	prf($N_i \| N_r$, g^{xy})	
public key	prf($h(N_i \| N_r), C_i \| C_r$)	$C_{i,r}$: initiator or responder cookie
pre-shared	prf(shared key, $N_i \| N_r$)	