Security in IP networks

Markus Peuhkuri

2005-03-15

Lecture topics

- Reminder: levels
- Security in IP networks
- WLAN security
- Mobile IP security

Because IPsec is (still, after more than 10 years) much in work progress, this presentation is based on current internet-drafts by IPsec working group. If you study some other material from IPsec, make sure that you check chapter "Differences from RFC..." from current RFCs/i-ds.

Where to locate confidentiality and integrity protection

- Link layer
  - all communication protected on protected links
  - intermediate nodes must be trusted
  - popular on wireless links
  - problems on high-speed links
    ⇒ usable on edge
  - GSM, WEP, PPP Encryption[5]
- Network layer
  - end-to-end encryption (if not a tunnel mode)
  - all communication between hosts protected
  - OS modifications needed
  - applications may work as is
  - IPsec
- Transport layer
  - underlying protocol provides retransmissions
    - no possibility to recover if invalid data injected. For example, if attacker can monitor link, it is trivial to inject data into TCP stream. If encryption is not broken, then TLS will detect invalid data. When valid data arrives, then TCP would consider it as retransmission and drops that data.
      ⇒ possible to DoS
    - difficult on datagram services: TLS not usable with UDP
  - applications may need to be adapted
  - faster to deploy
  - TLS
- Application layer: see lecture 5

IPsec

- Provides
  - confidentiality
  - integrity
  - authentication
  - replay protection
- Two modes

  transport mode transport protocol and payload encapsulated

  tunnel mode original IP datagram encapsulated
- Two protocols

  ESP Encapsulating Security Payload

  AH Authentication Header
- Three databases

  SPD Security Policy Database — contains policies for incoming and outgoing traffic

  SAD Security Association Database — established SAs

  PAD Peer Authorization Database — link between e.g. IKE and SPD
- Integrated into IP implementation or

  BITS bump-in-the-stack: additional software for host IP stack to implement IPsec

  BITW bump-in-the-wire: a gateway (router, firewall) in network implements IPsec on behalf of hosts

Security policy database

- Like firewall rules
- Policy determines how a packet is processed

  discard packet is dropped

  bypass packet is delivered as is

  protect IPsec protection is applied
- All traffic is processed
- Rules derived for new SAD entry
- Selector can be one or more of
  - source or destination address
  - next protocol / header
  - transport layer field (port, ICMP code)
  - name: data originator or destination
- Longest match applied

Security association database

- Contains parameters of defined SAs
  - security parameter index (SPI)
    - inbound: find right SA
    - outbound: record right SPI to packet
  - sequence number counter (64-bit, may be also 32-bit if negotiated with interoperability to older implementations)
  - sequence counter overflow: is rollover permitted or should report to audit log
  - anti-replay window: what sequence numbers are valid. Contains a 64-bit counter and a bit-map used to determine whether an inbound AH or ESP packet is a replay. Anti-replay protection can be disabled.
  - AH parameters: key, algorithm if used
  - ESP encryption, integrity or combined mode parameters
  - SA lifetime: bytecount and/or time interval (soft and hard; entire packet must be delivered in hard lifetime or discarded)
  - IPsec protocol mode: tunnel or transport
  - statefull fragment checking flag
  - bypass flags for DF bit and DSCP values (in tunnel mode)
  - path MTU value, if known
  - tunnel endpoint IP addresses

Key management

- Manual mode
- Automatic mode
  - IKEv2
  - multiple keys needed
- IKEv2
  - based on Diffie-Hellman key exchange
  - mutual authentication
  - SA establishment
    - in pairs for both directions

normal mode 6 messages needed (phase 1)
aggressive mode 3 messages: does not protect identity
quick mode used for re-keying in phase 2 (3 messages)

ICMP messages

- Informal messages according to SPD
- Error messages problematic
  - unauthenticated sources
    $\Rightarrow$ possibility of attack
    - changes in routing, MTU to too small
  - must react on some, e.g. Fragmentation needed
- Also "secure side" is problematic
  - compromised host
- Should set according to local policy

IPsec modes

- Original datagram:

IP header	TCP header	payload

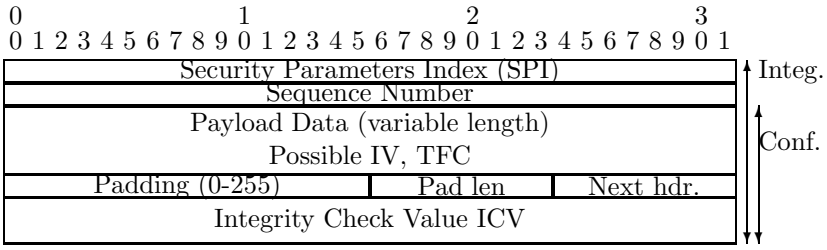
- Transport mode: transport protocol and payload encapsulated

IP header	*IPsec header*	TCP header	payload
	← ..... Protected by ESP ..... →		
← ..... Protected by AH ..... →			

- Tunnel mode: original IP datagram encapsulated

tunnel IP header	*IPsec header*	IP header	TCP header	payload
	← ..... Protected by ESP ..... →			
← ..... Protected by AH ..... →				

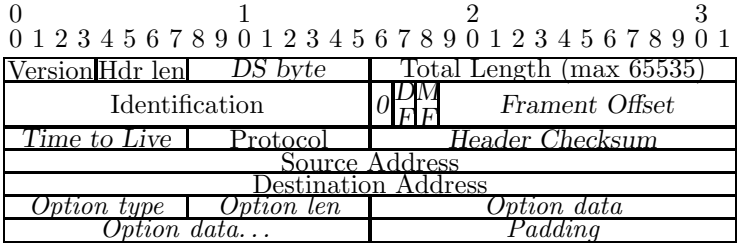
Encapsulating Security Payload



- Provides set of
  - confidentiality
  - data origin authentication
  - connectionless integrity
  - anti-replay service (partial sequence integrity)
  - traffic flow confidentiality (limited)

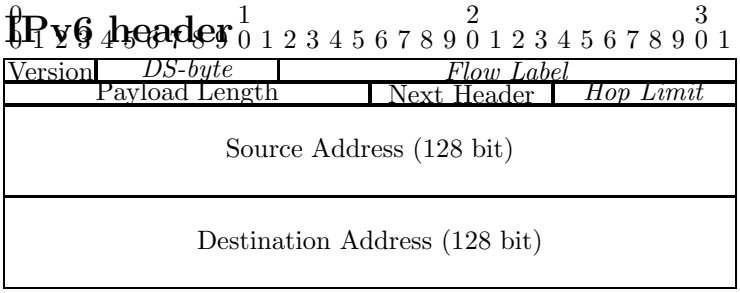
  All services ESP provides are optional. ESP may provide confidentiality without integrity, integrity without confidentiality (using NULL encryption [2]) or both. One should note, however, if confidentiality is used without integrity, it makes some attacks on confidentiality possible.
- IV transmitted in payload: because use of IV is algorithm-specific, its transmission must be specified when use of cipher algorithm is defined. For example in AES-CBC, IV uses 16 first octets.
- Padding needed to fill blocksize
- Traffic Flow Confidentiality (TFC) Padding
  - provides larger variability to padding
  - hides packet length distribution
  - encapsulated data must know its length: thus it is not possible to use with TCP. With IP, UDP and ICMP it is possible.
- Integrity check value optional
  - if integrity not used
  - if combined confidentiality and encryption algorithm
- Encryption before integrity: integrity calculated from encrypted data.
- Anti-replay uses SPI
  - 64-bit counter, top 32 not transmitted on wire
- Fragmentation after ESP (if needed)
- Also possible to transmit over UDP [4]

IPv4 header

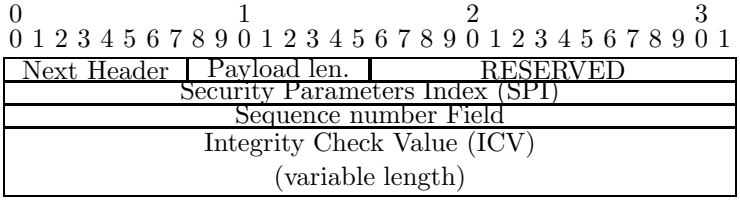


- Some fields are *mutable* i.e. modified by network
- Mutable fields set to zero

IPv6 header



Authentication Header



- Provides
  - connectionless integrity
  - data origin authentication
  - replay protection
- Why not ESP with NULL encryption?
  - protects as much as possible from IP header
  - payload visible for network devices
  - export regulations
- Mutable fields set to zero
  - end-to-end IPv6 options included

Issues with IPsec

- Key exchange DoS
  ⇒ use of cookies: sufficiently secure values that are fast to verify
- Overhead by additional headers
  - VoIP with 40-byte payload, 40-byte IP+UDP+RTP header
    ⇒ IPsec(3DES+SHA): 134 byte packet, 68 % increase
  - use of packet compression [6]. This does, however, help with voice data as it is probably compressed anyway.

- Not usable with performance enhancement proxies (PEP)
- Traffic classification more difficult, as it is not possible to see transport layer protocol fields
- Issues with firewalls

Wireless LANs

- Gained popularity in last few years
  - increase in bandwidth: 1 Mbit/s → 54 Mbit/s →
  - dropped costs: 1000s €→ sub-50 €
- Easy to deploy (in small scale)
- Provides convince

WLAN security

- WEP protection weak
  - in many cases, not even used: the problem is that there may not be clear indicator if traffic is protected or not. If traffic is not protected, it works as well or even better than if protected.
  - invalid use of RC4, shared, manual secret (see lecture on cryptology for details)
- WPA and 802.11i will help (802.1X)
- Attacks on WLAN
  - war-driving: searching for (open) networks
  - passive attacks on encryption
  - fake access point
  - man-in-middle, ARP poisoning
  - traffic analysis: padding uses precious bandwidth
- Possible to eavesdrop from long distance
  - even bluetooth access to phone 1.6 km apart: bluetooth phone had transmission power less than 1 mW; WLANs have max. 100 mW.

DoS Attacks on WLAN

- Attacks on MAC layer
  - reserving channel with CLS frames
    ⇒ other systems cannot access for 32 ms
  - fake deassociate messages
    ⇒ other systems lose connectivity (temporally)
- Attacks on radio
  - short pulses cause bit errors on frames
    ⇒ frames must be discarded
  - OFDM vulnerable on noise on pilot signal IEEE 802.11g
    ⇒ cannot estimate channel
- Difficult to protect from, solving need special tools

Protecting from traffic analysis

- Data content hidden with encryption
- Traffic flow hidden with mixing, padding, bandwidth limits
  - remailers[1]
  - onion routing[3]
- Additional traffic problematic with wireless edge
- Simple tunnelling hides destination

Dare I use open access point

- Found open WLAN, could I check email?
- Threats using open AP
  - may be unlawful: this is a quite difficult question and the right answer varies by country
  - traffic may be recorded
  - captive portal asks for credit card number, should I trust?
- Threats providing open AP
  - may end responsible for misbehaving guests
  - may be against ISP AUP (Acceptable Usage Policy)

Providing mobility

- IEEE802.11 WLAN has mobility support
  - does not extend more than few APs
    $\Rightarrow$ not scalable for large networks
- Do mobility on network layer
  $\Rightarrow$ IP mobility
- Mobility on application layer
  - in HTTP-type use change of address does not matter
  - connections does not last long
  - SIP can provide mobility
  - using DNS to update address: this may result performance problems in DNS system

IP mobility

- IPv4 does not provide good infrastructure for mobility
- IPv6 has tools
  - autoconfiguration
  - large address space
  - routing headers
  - IPsec
- Mobility components

  MN mobile node
  HA home agent
  CN correspondent node
  home link MN's home network
  CoA care of address, MN's address on foreign network

Moving around network

- When a MN connects to new network (has a new CoA)
  1. informs HA about new CoA (authenticates)
  2. HA tunnels all traffic directed to MN to CoA
  3. MN tunnels sent traffic to HA
  4. HA sends traffic to CN

  $\Rightarrow$routing not optimal: "triangle routing"
  - reverse tunnelling (MN $\rightarrow$ HA) needed because of ingress filtering: only packets that have a source address belonging to that network, are allowed to pass. The MN can only use CoA.
- Routing optimisation
  - MN sends BU (Binding Update) to CN
  - MN $\leftrightarrow$ CN communication with help of Mobile IP routing header

Security of routing optimisation

- Possibility to
  - steal addresses
  - attack on confidentiality, integrity
  - flooding attacks
  - reflection attacks
- CN must make sure that
  - both MN home address and CoA are valid: return routability. This security model assumes that network routing is trustworthy for those parts of network that participate on this exchange. This results "current fixed IPv4 network equivalent security".

  1. MN requests RO with two messages to CN
     (a) one from CoA
     (b) one via HA
  2. CN calculates challenge, and sends
     (a) one directly to CoA
     (b) one to MN home address
  3. MN sends BU based on challenge

Summary

- IPsec application-independent way to provide security
- Mostly used in tunnel mode to build VPNs
- WLAN: a network that extends to outside of corporate walls
- Without global trusted PKI, Mobile IP must take care with routing optimisation

References

[1] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, 1981.

[2] R. Glenn and S. Kent. The NULL Encryption Algorithm and Its Use With IPsec. Request for Comments RFC 2410, Internet Engineering Task Force, November 1998. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2410.txt`.

[3] David Goldschlag, Michael Reed, and Paul Syverson. Onion routing. *Commun. ACM*, 42(2):39–41, 1999.

[4] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, and M. Stenberg. UDP Encapsulation of IPsec ESP Packets. Request for Comments RFC 3948, Internet Engineering Task Force, January 2005. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc3948.txt`.

[5] G. Meyer. The PPP Encryption Control Protocol (ECP). Request for Comments RFC 1968, Internet Engineering Task Force, June 1996. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc1968.txt`.

[6] A. Shacham, B. Monsour, R. Pereira, and M. Thomas. IP Payload Compression Protocol (IPComp). Request for Comments RFC 3173, Internet Engineering Task Force, September 2001. (Internet Proposed Standard) (Obsoletes RFC2393). URL:`http://www.ietf.org/rfc/rfc3173.txt`.