Security in IP networks

TkL Markus Peuhkuri

2008-04-22

Lecture topics

- Reminder: levels
- Security in IP networks
- WLAN security
- Mobile IP security
- After this lecture, you should
  - know components of IPSec
  - know protocols used in IPSec
  - know *not* to use WEP on WLAN

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[7]
- 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. The mode used to implement IPSec VPNs.
- 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 a new SAD entry
- Selector can be one or more of
  - source or destination address(es)
  - 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 a 32-bit value if negotiated with interoperability to older implementations)
  - sequence counter overflow: is a rollover permitted or should one to be reported to a 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 a hard lifetime or discarded)
  - IPSec protocol mode: tunnel or transport
  - statefull fragment checking flag
  - bypass flags for DF bit and DSCP, ECN 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
  - 4 messages
  - fixed problems with IKE
    - vulnerability to DoS: stateless cookies
    - adds two messages
  - mutual authentication
  - SA establishment
    - in pairs for both directions
    - two messages needed
    - re-keying can be initiated by either one

ICMP messages

- Informal messages according to SPD
- Error messages are problematic
  - unauthenticated sources
    $\Rightarrow$ possibility of attack
    - changes in routing, forcing MTU to too small

  - must react on some, e.g. fragmentation needed
- Also the "secure side" is problematic
  - a compromised host
- Should set according to local policy

IPSec modes

- Original datagram:

IP header	TCP header	payload

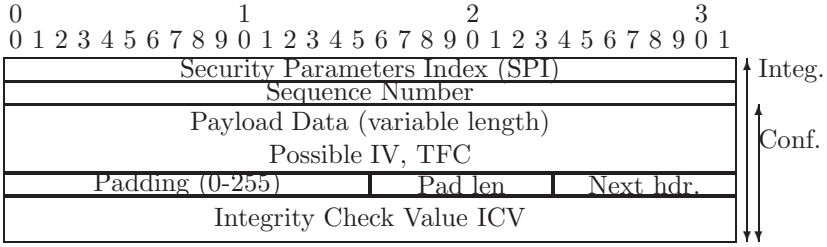
- Transport mode: transport protocol and payload encapsulated

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)

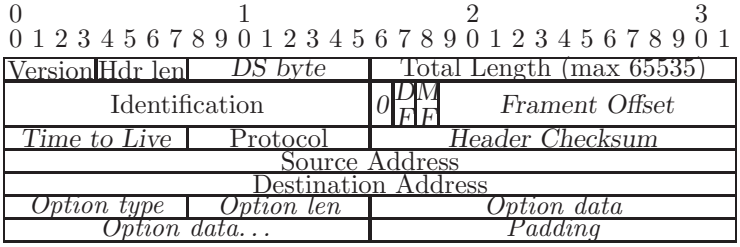
  All services ESP provides are optional. ESP may provide confidentiality without integrity, integrity without confidentiality (using NULL encryption [4]) or both. One should note, however, if confidentiality is used without integrity, it makes some attacks on confidentiality possible.

Encapsulating Security Payload

- IV transmitted in payload: because use of IV is an algorithm-specific variable, its transmission must be specified when use of a 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 in transport mode. With IP, UDP and ICMP it is possible.

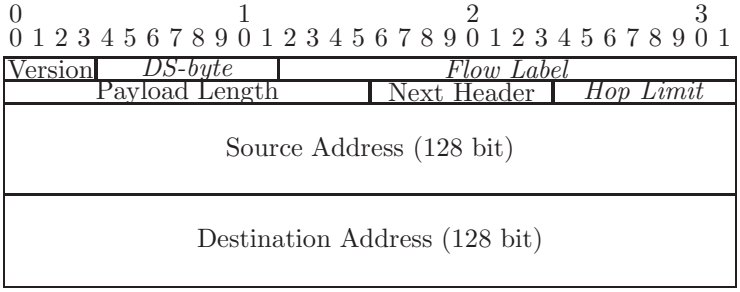
- Integrity check value is optional
  - if integrity is not used
  - if combined confidentiality and encryption algorithm is used
- Encryption before integrity: integrity calculated from encrypted data.
- Anti-replay uses SPI
  - a 64-bit counter, top 32 bits are not transmitted on wire
- Fragmentation after ESP (if needed)
- Also possible to transmit over UDP [6]
  - communicating through NAT and firewalls
  - by default port 4500, but may use other. For example some vendors have different ports like 2746.

IPv4 header

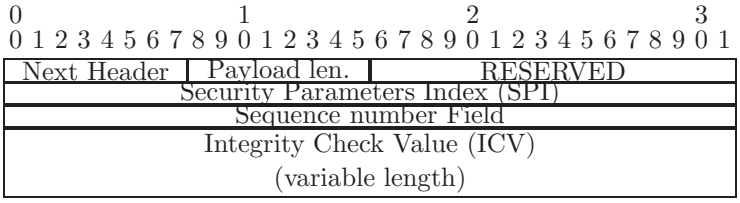


- Some fields are *mutable* i.e. modified by network
- Mutable fields set to zero

IPv6 header



Authentication Header



- Provides
  - connectionless integrity
  - data origin authentication
  - replay protection

Authentication Header

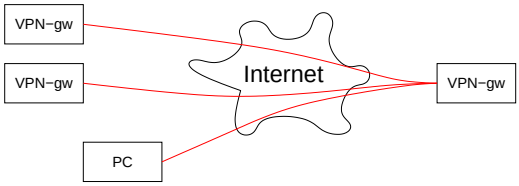
- Why not ESP with NULL encryption?
  - protects as much as possible in the IP header
  - payload visible for network devices
  - export regulations
- Mutable fields set to zero
  - end-to-end IPv6 options included

Issues with IPSec

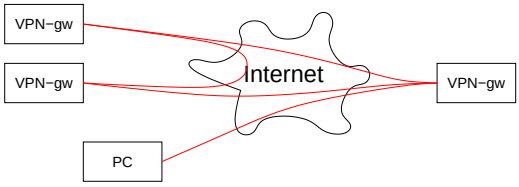
- Key exchange DoS
  ⇒ use of cookies in IKEv2: sufficiently secure values that are fast to verify
- Overhead by additional headers
  - VoIP with 40-byte payload, 40-byte IP+UDP+RTP header
    ⇒ IPSec(3DES+SHA): 134 byte packet, 68 % increase
  - use of a packet compression [8]. This does not, however, help with voice data as it is probably compressed anyway.
- Not usable with performance enhancement proxies (PEP)
- Traffic classification is more difficult, as it is not possible to see transport layer protocol fields
- Issues with firewalls

VPNs between sites

- Hub-and-spoke: central location
  - one VPN for each branch office
  - easiest to build and maintain
  - good if little or no traffic between branch offices

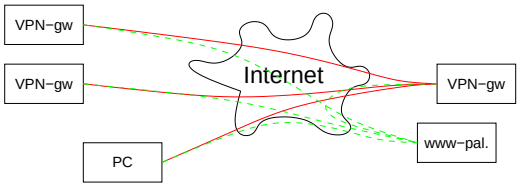


- Multipoint connections
  - direct connections with sites
    - between all (full mesh)
    - only selected
  - need dynamic routing
  - best performance (VoIP)

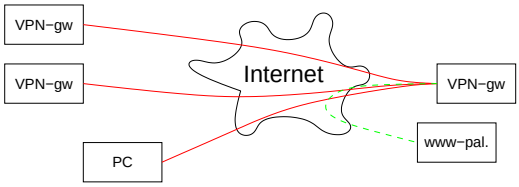


VPN traffic and other traffic

- Only intra-site traffic uses VPN (split tunnelling)
  - the best performance
  - Internet traffic directly to ISP network
  - possible security hole



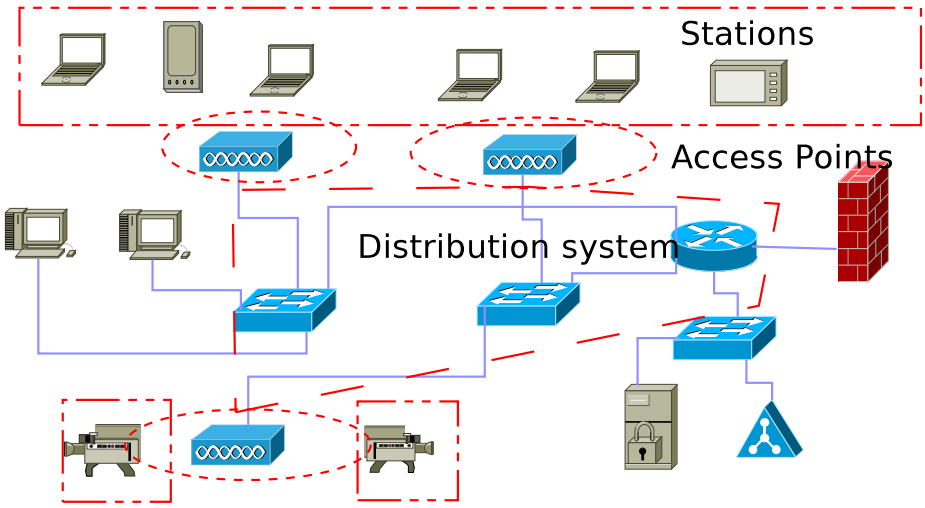
- All traffic using VPN
  - central management of security (firewalls, IDS, . . .)
  - needs performance on central office
  - according to Finnish Vahti rules



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 a small scale)
- Provides convenient network access
  - faster than mobile networks
  - no hassle with cables (except power cord)

WLAN components



WLAN security

- Problems with wireless access
  - not easy to physically secure network
  - can attacked be from a long distance
    - even bluetooth access to an unmodified phone 1.6 km apart: bluetooth phone had transmission power less than 1 mW; WLANs have max. 100 mW.
- 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 (WPA2) will help (802.1X)
  - possible to use individual keys, for example by using EAP-TLS authentication with RADIUS

WPA2 (802.11i) security

- Robust Secure Network (RSN)
- Good algorithms, used right way

  TKIP upgrade for old devices (WPA)
  - confidentiality: RC4 with per-packet key mixing, makes FMS attack [3] useless
  - integrity: Michael Message Integrity Code
  - replay protection
  - active attack protection

  CCMP AES with CCM (Counter with CBC-MAC) [10]
  - confidentiality: CTR (counter mode) turns block cipher to stream cipher
  - integrity and authentication: CBC-MAC
  - 48-bit packet number
- Management frames not protected. There is work on IEEE 802.11w working group to implement authentication for management frames.

Key generation for WPA

- Two modes: WPA2 equipment sertification may be only personal profile, or enterprise profile (that includes also personal mode)

  personal uses PSK (Pre-shared Key)

  enterprise uses EAP (Extensible Authentication Protocol) [1]
- EAP makes possible to use multiple authentication methods
  - method must provide keying material[9]
  - using TLS tunnels to protect authentication

  EAP-TLS need certificates for clients and authentication server: to deploy, one needs some PKI authentication infrastructure like Active Directory

  EAP-TTLS no need for client certificates, easy integration with RADIUS using inner (TLS-protected) authentication method. (EAP Tunneled TLS)

  PEAP similar to EAP-TTLS. There are actually multiple versions about PEAP, but the most supported version is PEAPv0/EAP-MSCHAPv2 and PEAPv1/EAP-GTC does not have native support on Windows.

  EAP-SIM using GSM SIM card

Attacks on WLAN

- War-driving: searching for (open) networks
- Passive attacks
  - WEP encryption
  - weak passwords in WPA-PSK, LEAP (Lightweight Extensible Authentication Protocol)
  - traffic analysis
- Active attacks
  - abuse of management frames (deassosiate messages)
  - replay attacks, for example retransmitting ARP frames and learning new IVs for WEP if there is not enough traffic otherwise.
  - fake access point
  - man-in-middle, ARP poisoning

DoS Attacks on WLAN

- Attacks on MAC layer
  - reserving channel with CLS frames
    $\Rightarrow$ other systems cannot access transmission channel for 32 ms
  - fake deassociate messages
    $\Rightarrow$ other systems lose their connectivity (temporally)
- Attacks on radio
  - short pulses cause bit errors on frames
    $\Rightarrow$ frames must be discarded
  - OFDM vulnerable on noise on pilot signal (IEEE 802.11g)
    $\Rightarrow$ devices cannot estimate channel properties
- 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[2]
  - onion routing[5]
- Additional traffic problematic at the wireless edge
- A simple tunnelling hides destination

Dare I use open access point

- Found an 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 a credit card number, should I trust?
- Threats providing open AP
  - one may end responsible for misbehaving guests
  - may be against ISP AUP (Acceptable Usage Policy)

Providing mobility

- IEEE802.11 WLANs have a mobility support
  - does not extend more than few APs
    $\Rightarrow$ not scalable for large networks
  - 11i provides pre-authentication and PMKSA (Pairwise Master Key Security Assosiation) that helps somewhat
  - IEEE 802.11r should improve
- Do mobility on network layer
  $\Rightarrow$ IP mobility
- Mobility on application layer
  - in HTTP-type use change of address does not matter. In some cases authentication be depend on the IP address used by client.
  - 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 a network

- When a MN connects to a 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 is 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
  - security much improved thanks to IEEE 802.11i
  - open access has its uses
- Without global trusted PKI, Mobile IP must take care with routing optimisation

References

[1] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, and Ed. *Extensible Authentication Protocol (EAP)*, June 2004. RFC 3748. URL:`http://www.ietf.org/rfc/rfc3748.txt`.

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

[3] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In *Eighth Annual Workshop on Selected Areas in Cryptography*. Springer, 2001.

[4] R. Glenn and S. Kent. *The NULL Encryption Algorithm and Its Use With IPsec*, November 1998. RFC 2410. URL:`http://www.ietf.org/rfc/rfc2410.txt`.

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

[6] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, and M. Stenberg. *UDP Encapsulation of IPsec ESP Packets*, January 2005. RFC 3948. URL:`http://www.ietf.org/rfc/rfc3948.txt`.

[7] G. Meyer. *The PPP Encryption Control Protocol (ECP)*, June 1996. RFC 1968. URL:`http://www.ietf.org/rfc/rfc1968.txt`.

[8] A. Shacham, B. Monsour, R. Pereira, and M. Thomas. *IP Payload Compression Protocol (IPComp)*, September 2001. RFC 3173. URL:`http://www.ietf.org/rfc/rfc3173.txt`.

[9] D. Stanley, J. Walker, and B. Aboba. *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*, March 2005. RFC 4017. URL:`http://www.ietf.org/rfc/rfc4017.txt`.

[10] D. Whiting, R. Housley, and N. Ferguson. *Counter with CBC-MAC (CCM)*, September 2003. RFC 3610. URL:`http://www.ietf.org/rfc/rfc3610.txt`.