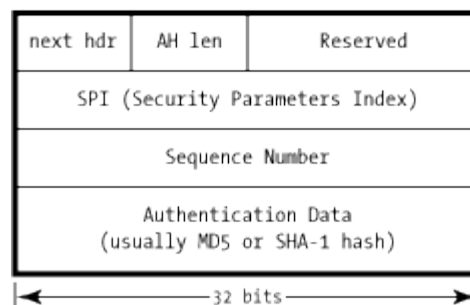


IPSec

Acknowledgement: All the figures in this lecture note are from Steve Friedl's [Unixwiz.net](http://www.unixwiz.net) *Tech Tips: An Illustrated Guide to IPsec*. Thank Steve Friedl for allowing us to use his figures.

- ❖ Motivation: how to protect communication between two computers?
 - Approach 1: when we write programs, we implement data encryption. We have to do this for every program.
 - Approach 2: we build the encryption/authentication logic on top of layer 4 (TCP). SSL (Secure Socket Layer) took this approach.
 - Approach 3: we build the encryption/authentication logic on top of layer 3 (IP). This is the approach of IPSec. IPsec is a suite of protocols for securing network connections.
- ❖ Philosophy:
 - Many IP stacks are implemented so that layer 4 (e.g. TCP) and below are implemented in the OS, and anything above is implemented in a user space.
 - SSL's philosophy: it is easier to deploy something if you don't have to change the OS. It requires the applications to interface to SSL instead of TCP.
 - IPSec's philosophy: implementing security within the OS automatically causes all applications to be protected without the application having to be modified.
- ❖ Two IPSec headers: AH vs. ESP
 - AH: Authentication Header. Protocol Type = 51 (this is one of the fields in IP header)
 - ESP: Encapsulating Security Payload (Protocol Type = 50)
- ❖ Two modes of applying IPSec protection to a packet
 - Transport mode: end-to-end communication
 - Tunnel mode: firewall to firewall, or endnode to firewall, where data are only protected along part of the path between endpoints.
 - Tunnel mode can be used instead of transport mode.
- ❖ AH: Authentication Header

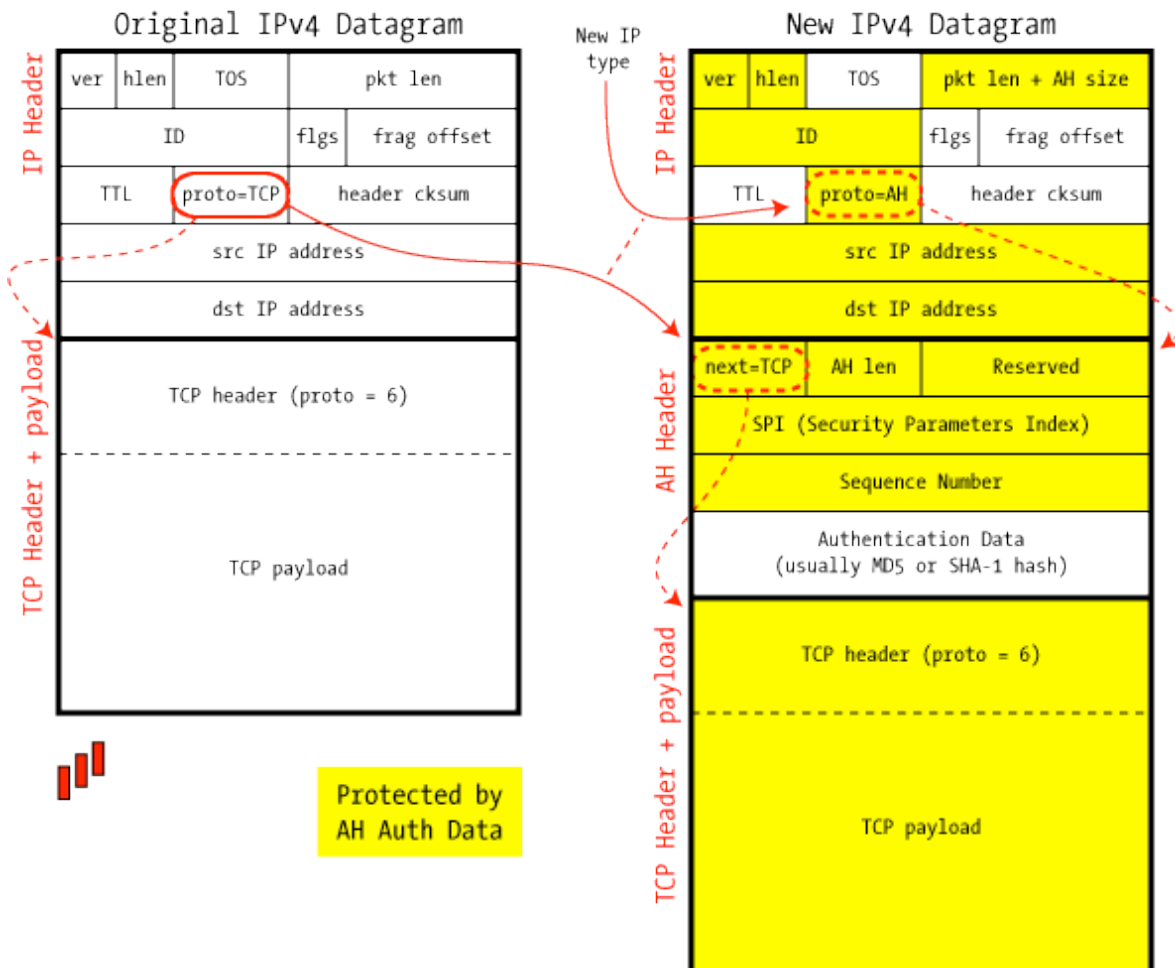
IPSec AH Header



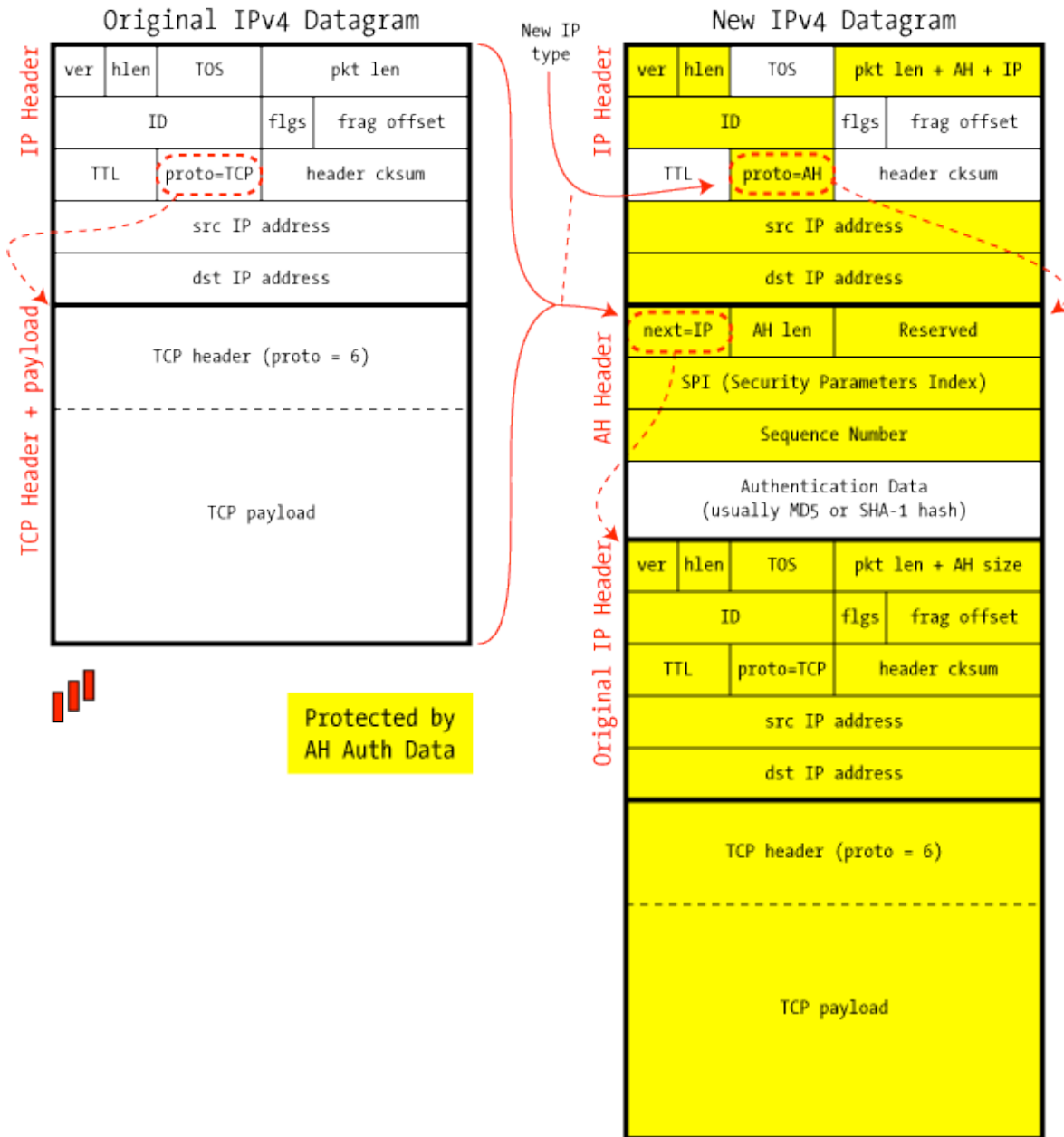
- AH is used to authenticate — but not encrypt — IP traffic

- *Authentication* is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum)
- **Next header:** Identifies the protocol type of the transferred data (not that this type information is supposed to be in the original IP header, however, because of the IPsec, the protocol type field in the original IP header is changed to 50 (for ESP) or 51 (for AH).
- **AH len:** Size of AH packet.
- **Reserved:** This field is reserved for future use and must be zero.
- **Security Parameters Index:** Identifies the security parameters.
- **Sequence Number:** This is used to prevent the replay attack. This field is included in the authentication data, so modification can be detected.
- **Authentication Data:**
 - Integrity on IP data part, plus immutable IP header part.
 - Mutable IP header part: tos, flags, fragment offset, ttl, header checksum.
 - The mutable fields are set to zero during the integrity computation.
 - AH header part is also included in the integrity computation, with the authentication data field filled by zero during the computation.

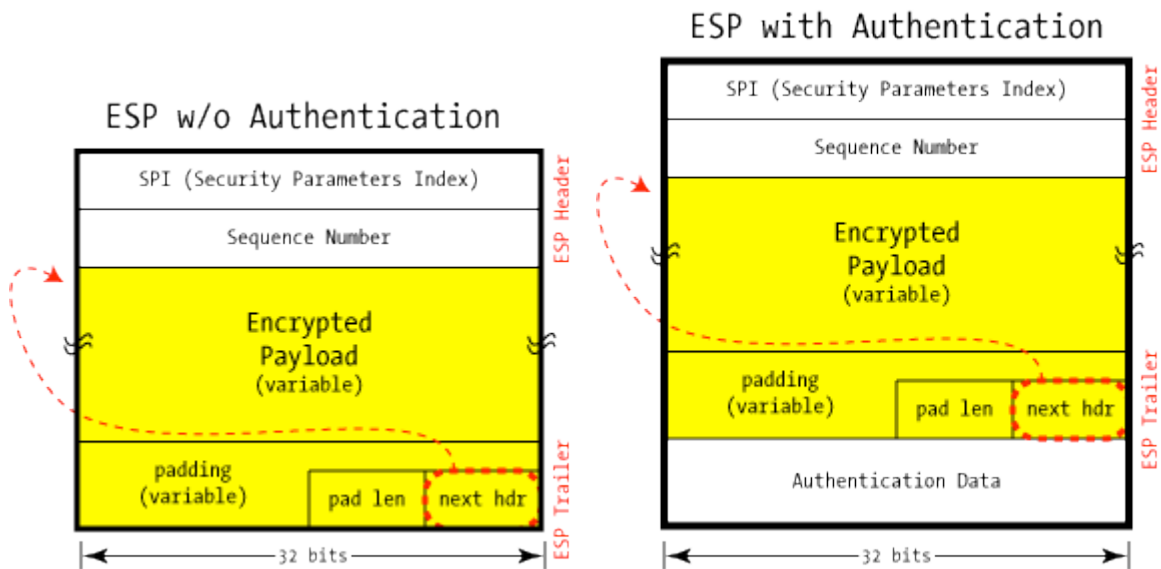
IPSec in AH Transport Mode



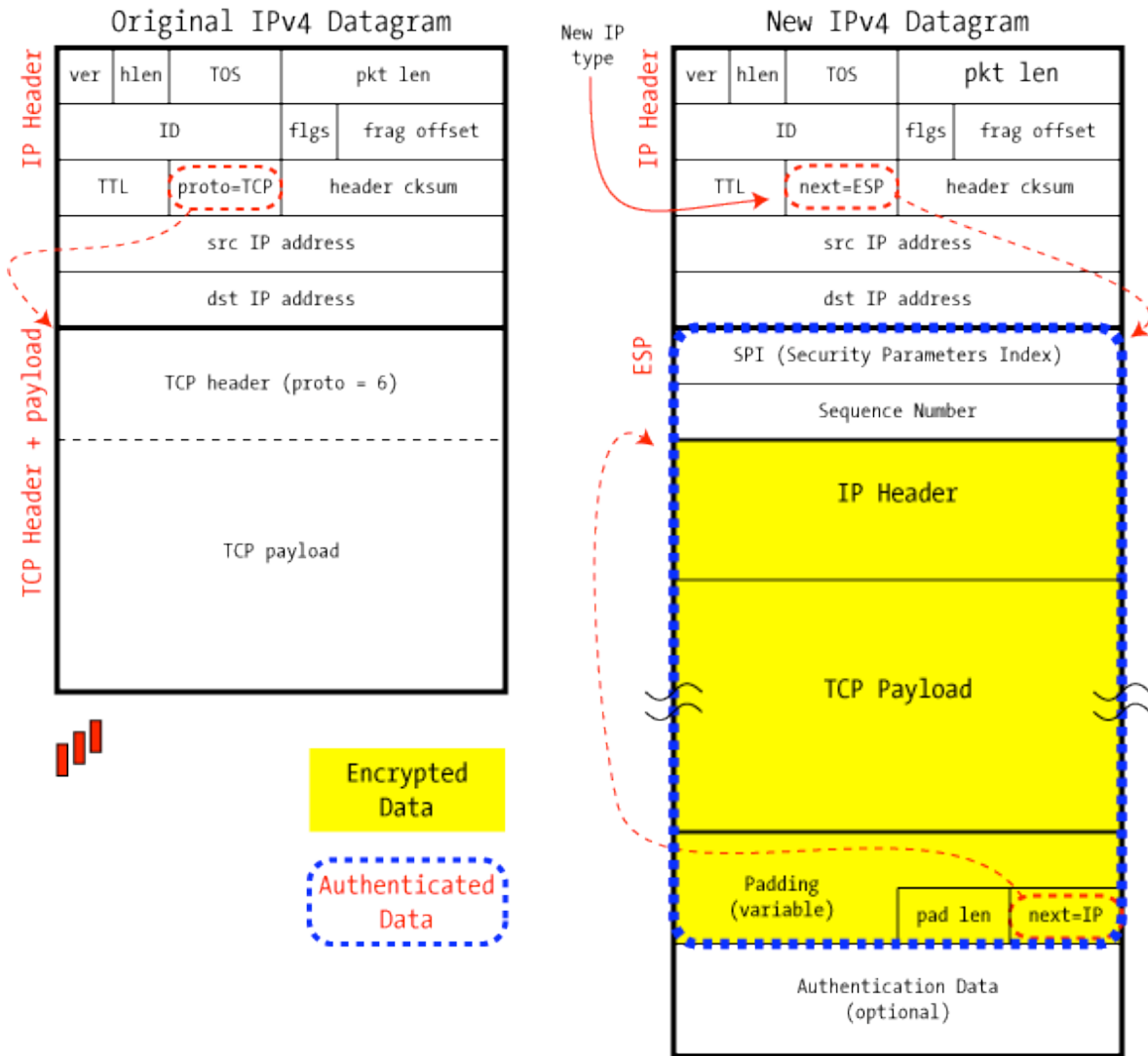
IPSec in AH Tunnel Mode



- ❖ ESP: Encapsulating Security Payload
 - Provide encryption and/or integrity protection
 - Integrity beyond the IP header.
 - Encryption beyond the IP header: makes the firewall difficult.
 - ESP surrounds the payload it's protecting.
 - It's possible to use ESP without any actual encryption (to use a NULL algorithm).
 - The authentication is optional.
 - Unlike AH, however, this authentication is *only for the ESP header and encrypted payload*: it does not cover the full IP packet.



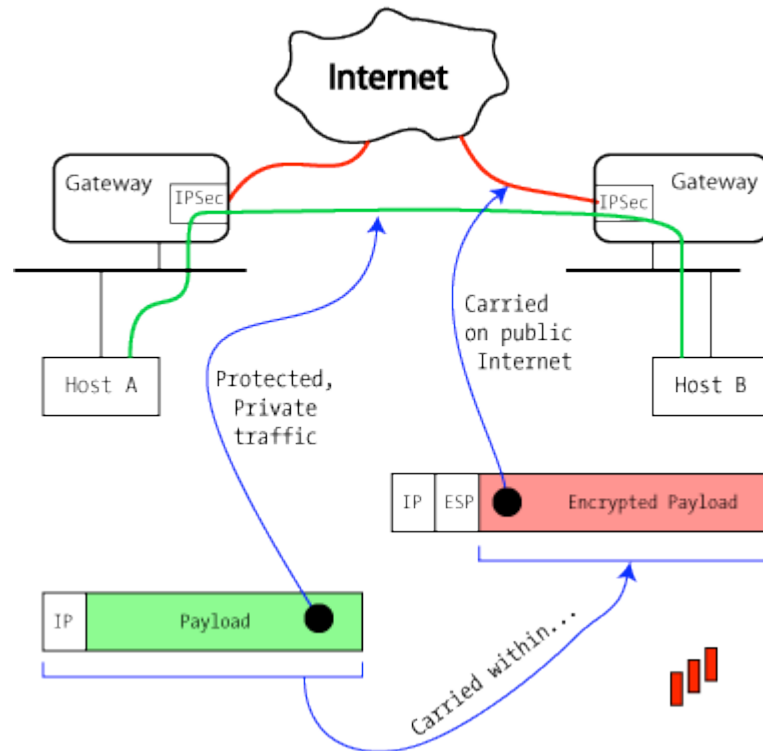
IPSec in ESP Tunnel Mode



- ❖ Key Management
 - Manual configuration: one party generates a set of secrets, and conveys them to all the partners. All parties install these secrets in their appropriate Security Associations.
 - IKE (Internet Key Exchange): exists to allow two endpoints to properly set up their Security Associations, including the secrets to be used. IKE uses the ISAKMP (Internet Security Association Key Management Protocol) as a framework to support establishment of a security association compatible with both ends.
- ❖ Building a Virtual Private Network (VPN) using IPSec
 - The goal of VPN is to join two trusted networks across an untrusted intermediate network, as is by stringing a very long Ethernet cable between the two.
 - Commonly used to connect branch offices with company headquarters, allowing all users to share sensitive resources without fear of interception.

- ESP (with Authentication) + Tunnel mode
- Transparent to end users.

Virtual Private Network



❖ Impact of IPsec over NAT

- NAT (Network Address Translation) solves the IP address space problem.
- IPsec tunnel mode: NAT wants to update the IP address inside the encrypted (or authenticated) data, but it doesn't have the key.
- IP addresses: NAT needs to update the IP address (for the tunnel mode, this IP address is the one inside the tunnel).
 - For AH: NAT does not know how to recomputed the authentication data
 - For ESP: NAT does not even know the IP address, nor can it conduct encryption.
- TCP/UDP checksum: IP address is included in the computation of the TCP or UDP checksum. NAT changes the IP address, but cannot modify the checksum encrypted/authenticated by IPsec.
- TCP/UDP port: NAT sometimes changes the port numbers, but the port numbers are encrypted/authenticated by IPsec.
- IPv6 proponents hates NAT, they now like IPsec because IPsec makes NAT fail.

❖ Impact of IPsec over Firewalls

- IPsec encrypts information on which firewalls like to base decisions, such as PORT fields in the TCP header.

- ❖ Some politics between IP, IPsec and IPv6
 - 1992, IAB (Internet Architecture Board) recommended replacing IP with the CLNP packet format, a format similar to IP, but had larger addresses.
 - If CLNP is adopted, the Internet would certainly be better off than it is now.
 - Some very vocal IETF members wanted to invent their own header format. The new format is known as IPv6. They have been designing it for so long (10 years).
 - IPv6 specification says that IPsec is a mandatory feature of IPv6.
 - IPv6 proponents hoped that IPsec would be the motivator for moving to IPv6.
 - However, IPsec designers designed IPsec for both IP versions.