Network Security

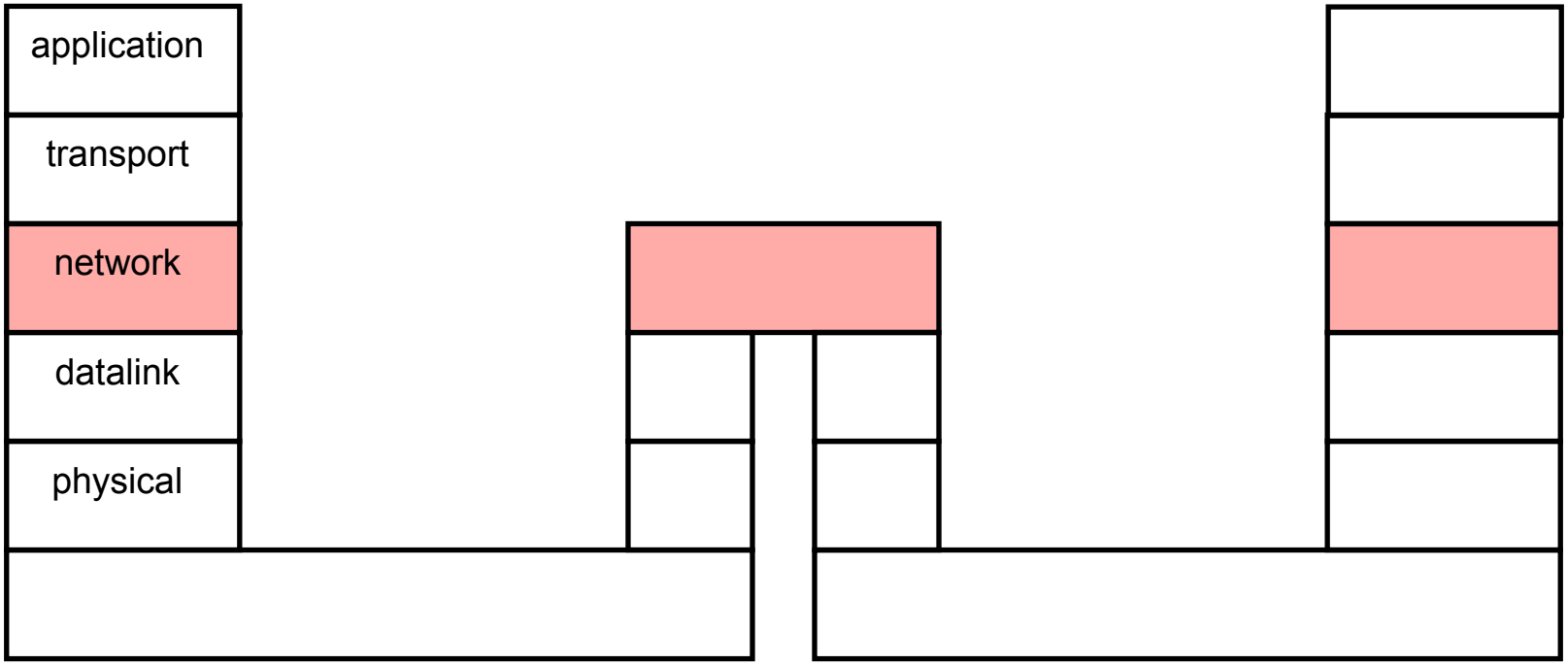
Lecture 3

Design and Analysis of Communication Networks (DACS)

University of Twente

The Netherlands

Security protocols



Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

Contents

- **IPSec overview**
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

IP Security (IPSec)

- Authentication
- Data confidentiality
- Data integrity

- Key management

- IPv4: option / IPv6: included

IPSec protocols

1) Authentication Header (AH)

- Authentication
- Access control
- Replay protection
- Integrity
- Non-repudiation (depends on algorithm)

2) Encapsulating Security Payload (ESP)

- Confidentiality
- Authentication (depends on algorithm)
- Access control
- Replay protection
- Integrity (depends on algorithm)
- Non-repudiation (depends on algorithm)

3) Internet Key Exchange (IKE)

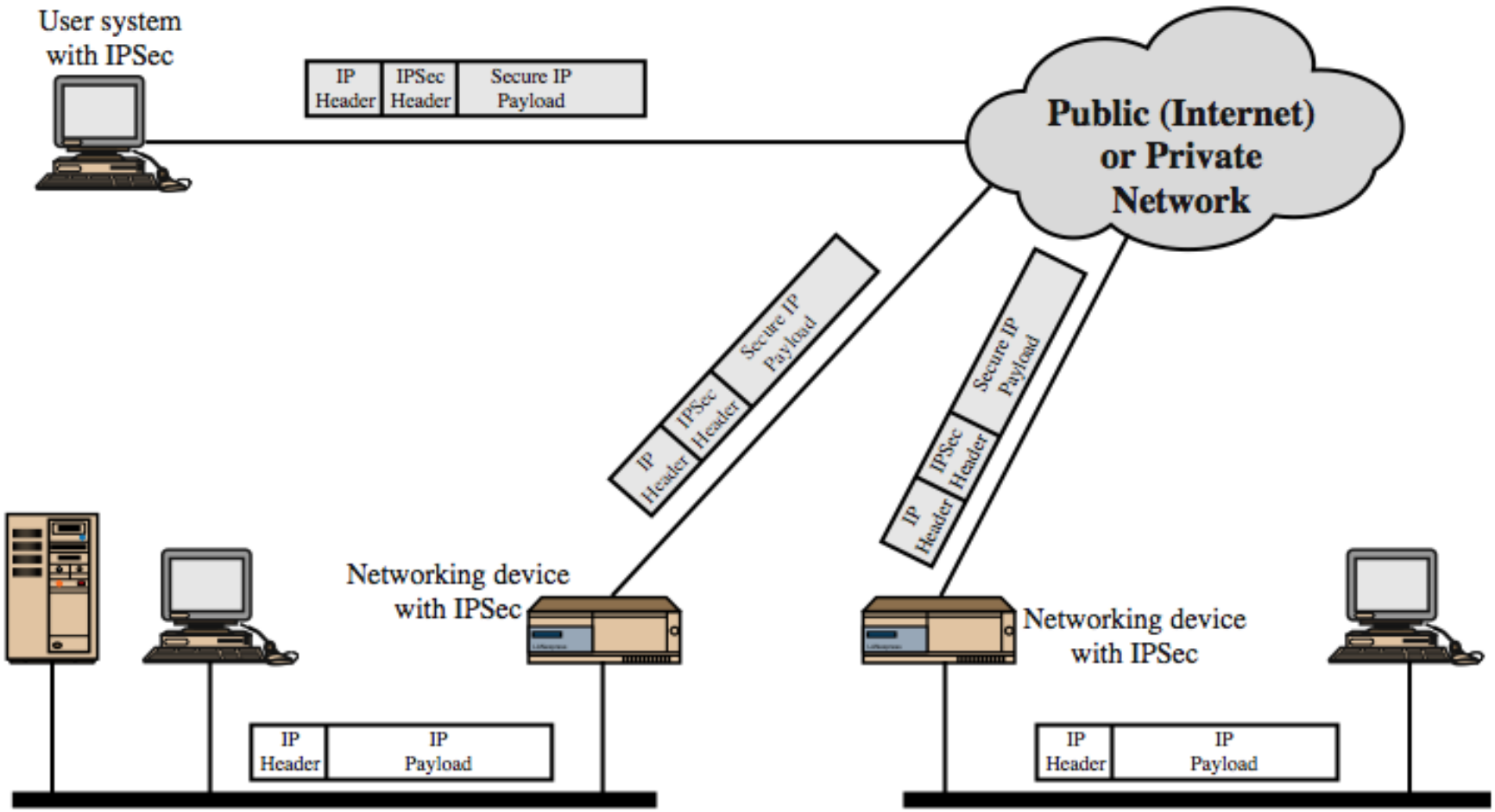


Figure 6.1 An IP Security Scenario

Contents

- IPSec overview
- **IPSec in practice**
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

Encryption in practice

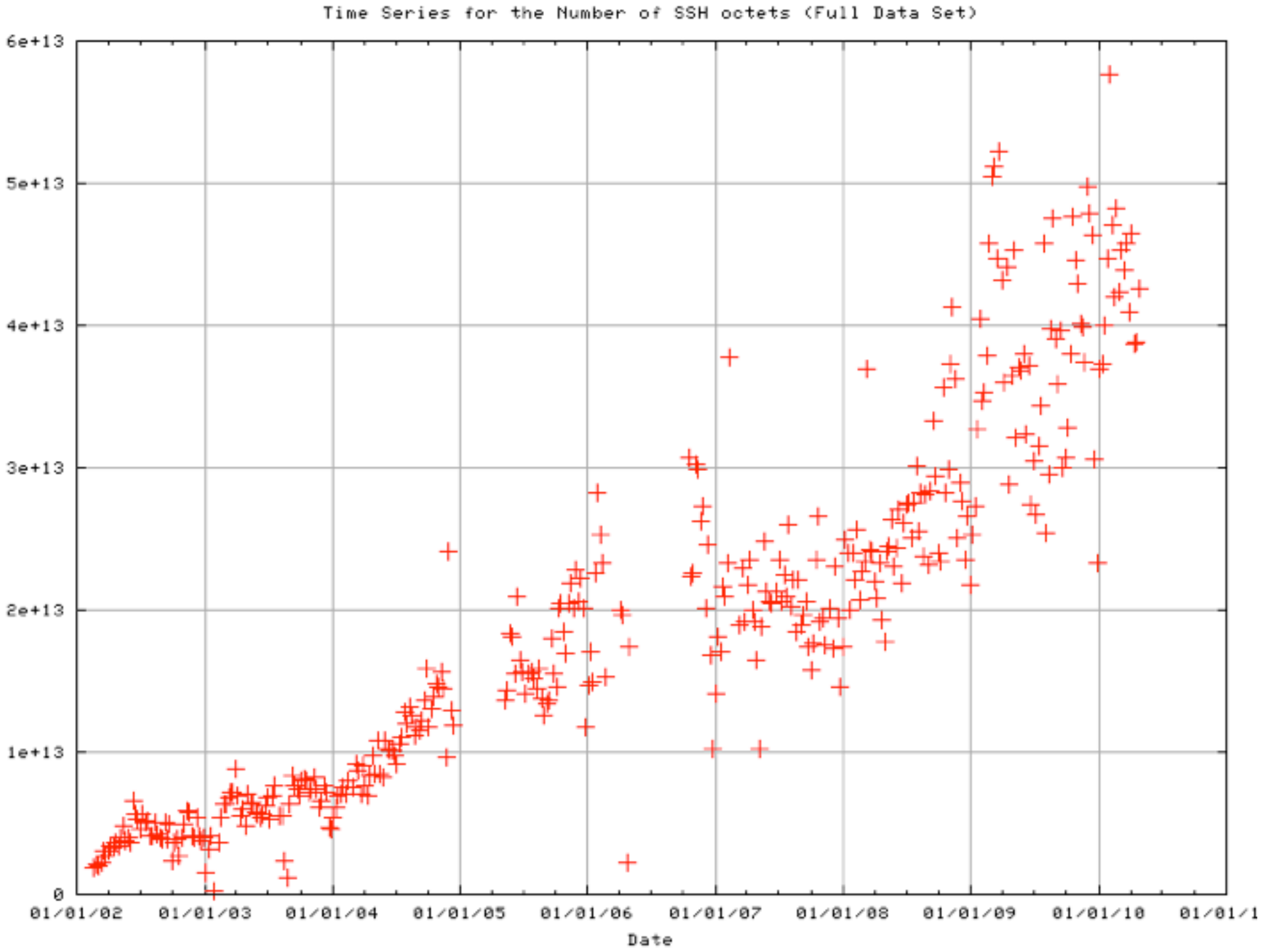
Traffic type	Octets		Packets	
SSH	2,33%	42,55T	1,98%	47,95G
HTTPS	2,63%	48.02T	3,61%	87,32G
IPsec ESP	0,28%	5.131T	0,34%	8.255G
IPsec AH	0,00%	83,91G	0,01%	181.4M
IPsec IKE	0,00%	16,98G	0,00%	61,63M

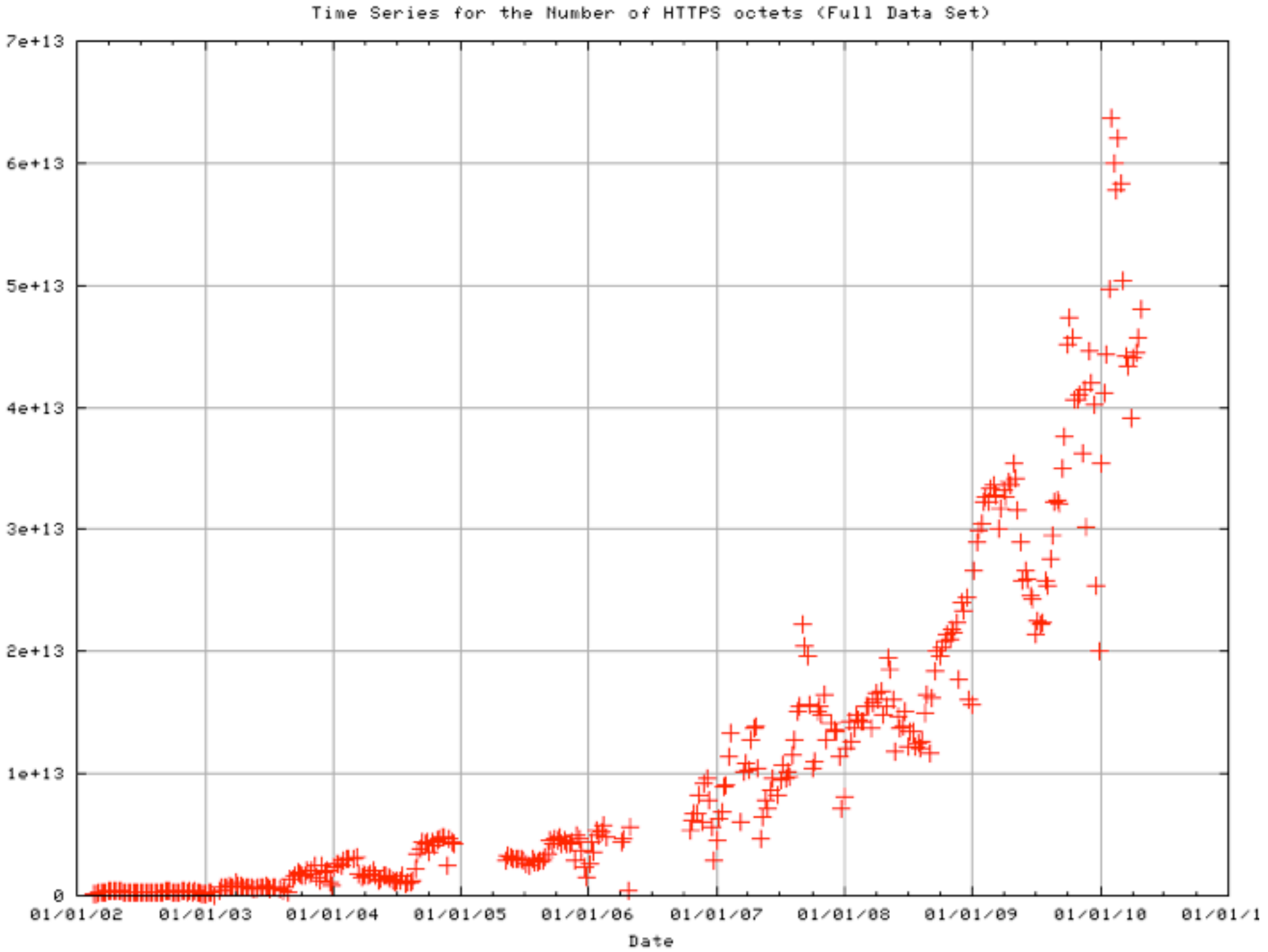
- *Source: http://netflow.internet2.edu/weekly/20100426/*

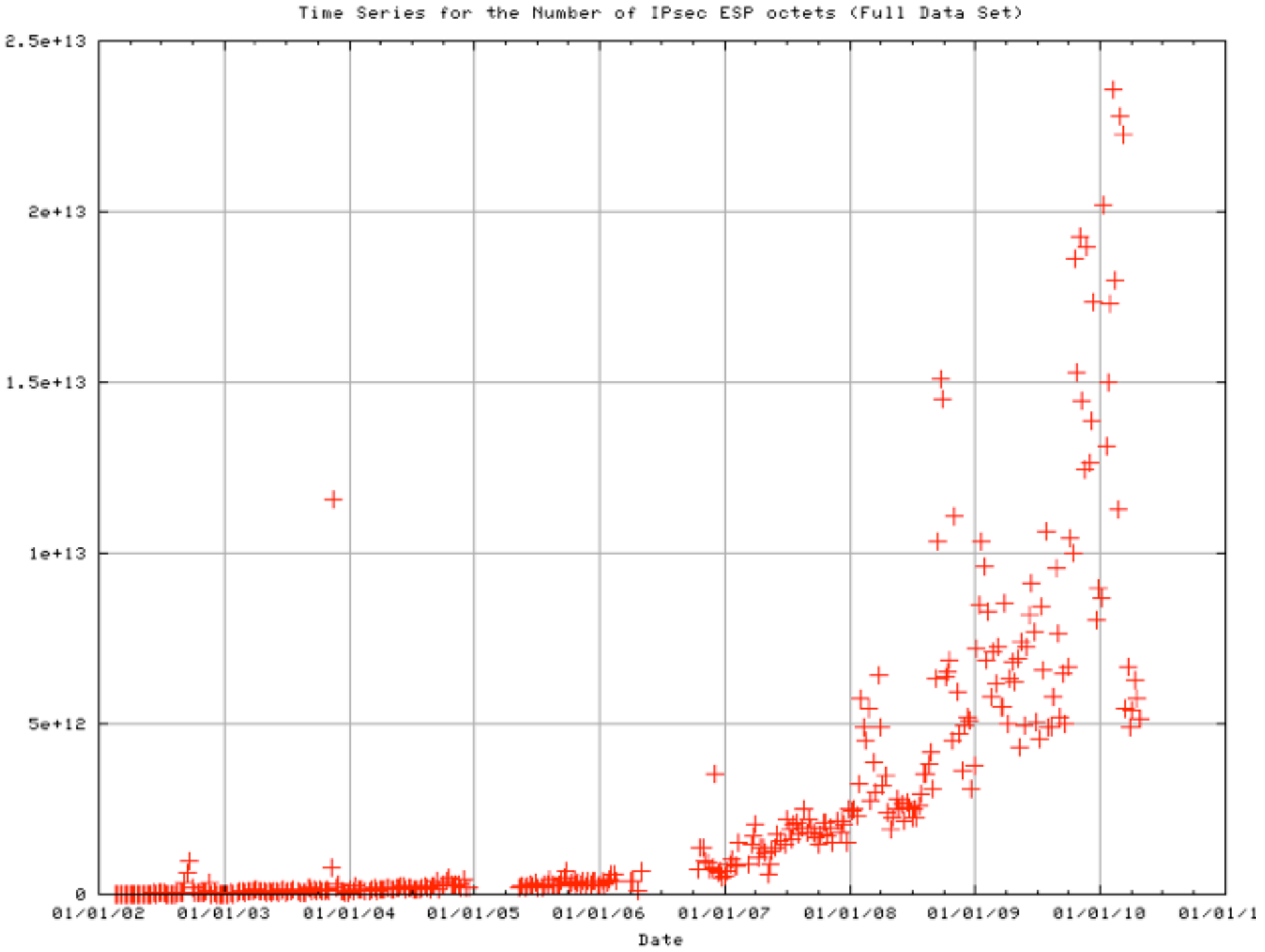
Encryption in practice

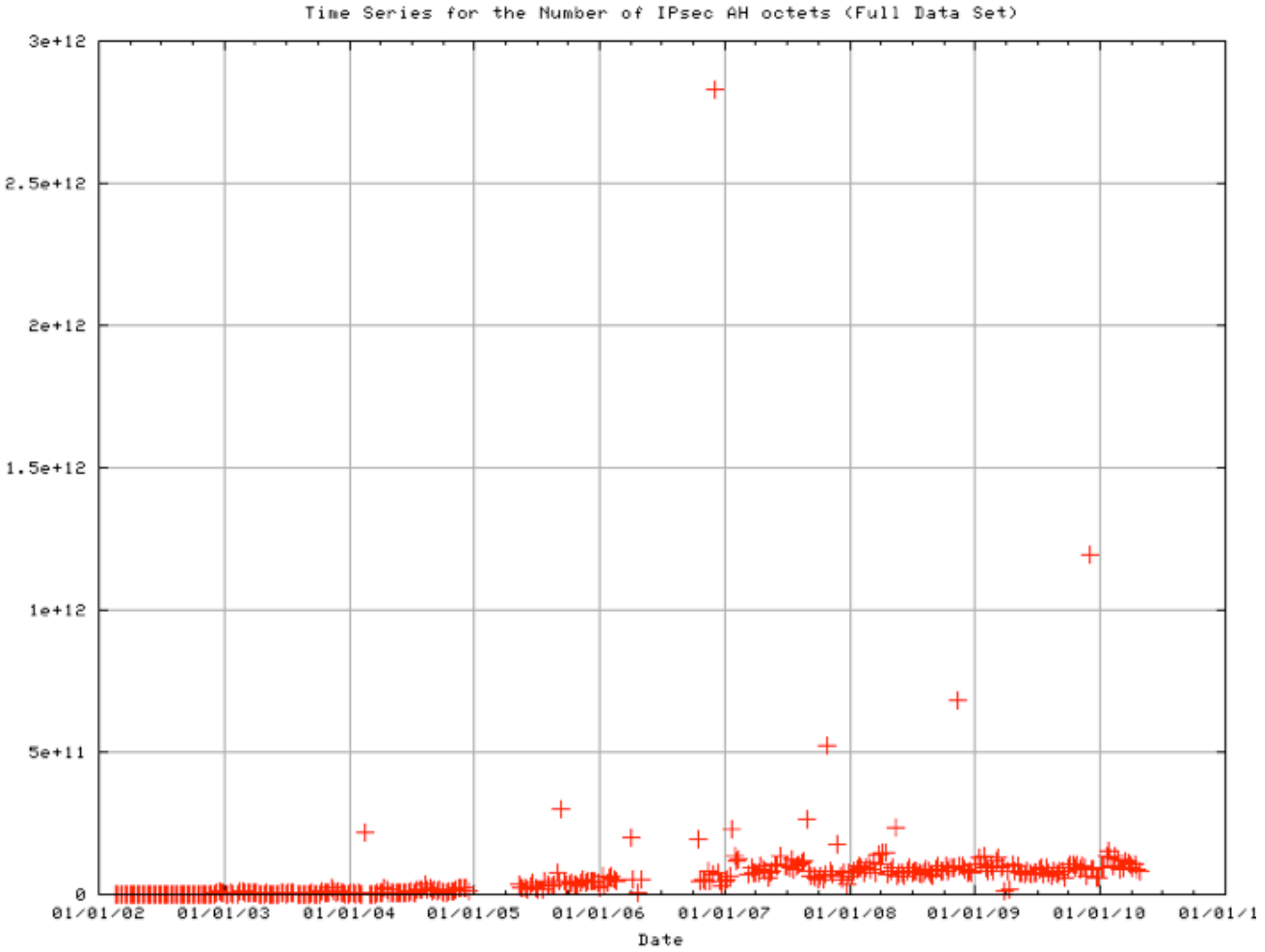
Traffic type	Octets		Packets	
SSH	3,42%	17.45T	3,51%	20.98G
HTTPS	1,11%	5.677T	1,67%	10.00G
IPsec ESP	0,14%	696.9G	0,20%	1.211G
IPsec AH	0,01%	54.20G	0,01%	89.35M
IPsec IKE	0,00%	1.174G	0,00%	5.818M

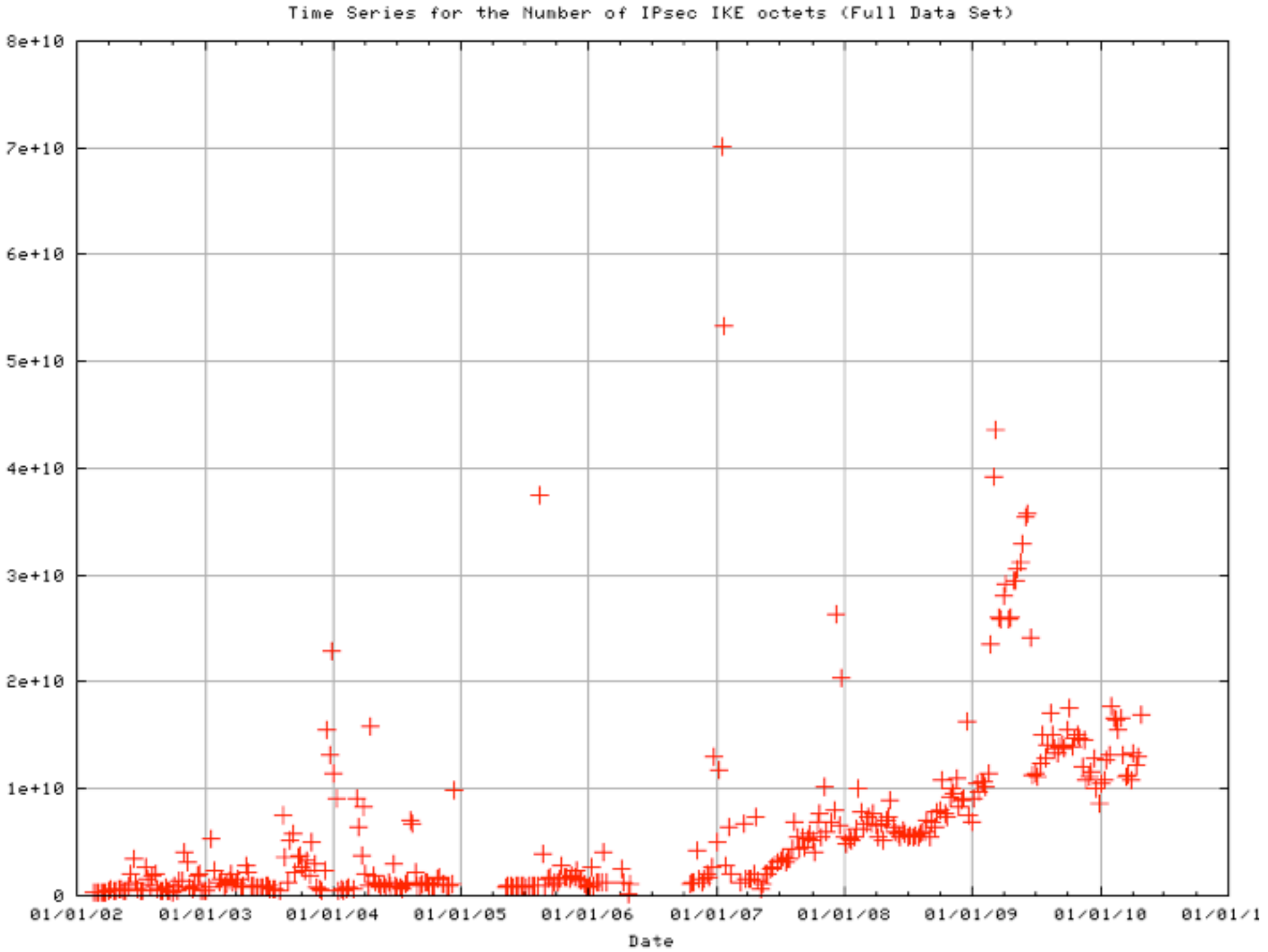
- *Source: http://netflow.internet2.edu/weekly/20060506/*


Time Series for the Number of SSH octets (Full Data Set)
6e+13
5e+13
4e+13
3e+13
2e+13
1e+13
0
01/01/02
01/01/03
01/01/04
01/01/05
01/01/06
01/01/07
01/01/08
01/01/09
01/01/10
01/01/1
Date


Time Series for the Number of HTTPS octets (Full Data Set)
7e+13
6e+13
5e+13
4e+13
3e+13
2e+13
1e+13
0
01/01/02
01/01/03
01/01/04
01/01/05
01/01/06
01/01/07
01/01/08
01/01/09
01/01/10
01/01/1
Date


Time Series for the Number of IPsec ESP octets (Full Data Set)
2.5e+13
2e+13
1.5e+13
1e+13
5e+12
0
01/01/02
01/01/03
01/01/04
01/01/05
01/01/06
01/01/07
01/01/08
01/01/09
01/01/10
01/01/1
Date


Time Series for the Number of IPsec AH octets (Full Data Set)
3e+12
2.5e+12
2e+12
1.5e+12
1e+12
5e+11
0
01/01/02
01/01/03
01/01/04
01/01/05
01/01/06
01/01/07
01/01/08
01/01/09
01/01/10
01/01/1
Date


Time Series for the Number of IPsec IKE octets (Full Data Set)
8e+10
7e+10
6e+10
5e+10
4e+10
3e+10
2e+10
1e+10
0
01/01/02
01/01/03
01/01/04
01/01/05
01/01/06
01/01/07
01/01/08
01/01/09
01/01/10
01/01/1
Date

Contents

- IPSec overview
- IPSec in practice
- **IPSec standardization**
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

IPSec components

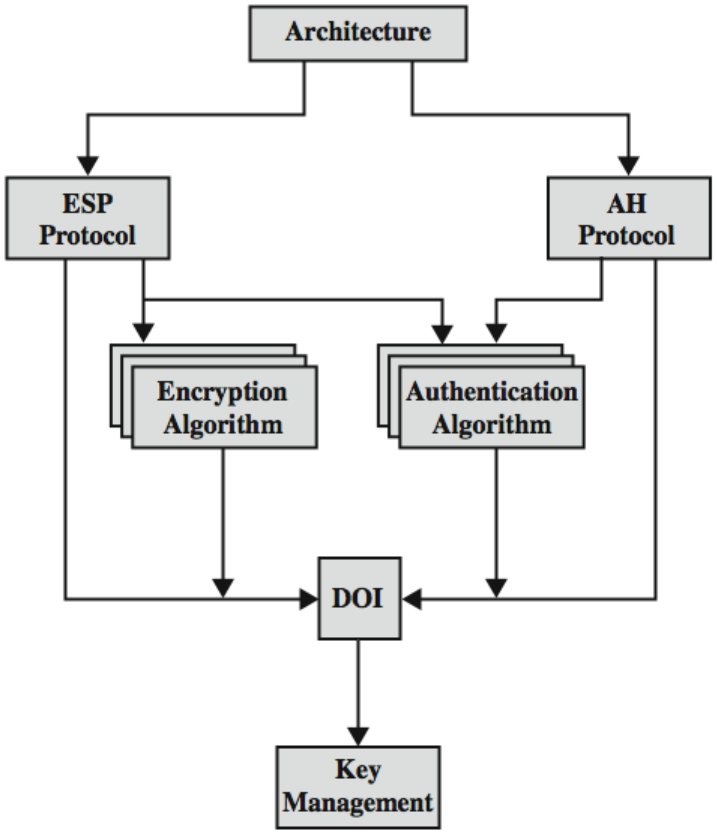


Figure 6.2 IPSec Document Overview

- The ESP DES-CBC Transform (RFC 1829) (19291 bytes)
- IP Encapsulating Security Payload (ESP) (RFC 1827) (30278 bytes) obsoleted by RFC 2406
- IP Authentication using Keyed MD5 (RFC 1828) (9800 bytes)
- IP Authentication Header (RFC 1826) (30475 bytes) obsoleted by RFC 2402
- Security Architecture for the Internet Protocol (RFC 1825) (56772 bytes) obsoleted by RFC 2401
- HMAC: Keyed-Hashing for Message Authentication (RFC 2104) (22297 bytes)
- HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085) (13399 bytes)
- Security Architecture for the Internet Protocol (RFC 2401) (168162 bytes)
- The NULL Encryption Algorithm and Its Use With IPsec (RFC 2410) (11239 bytes)
- IP Security Document Roadmap (RFC 2411) (22796 bytes)
- IP Authentication Header (RFC 2402) (52831 bytes)
- The OAKLEY Key Determination Protocol (RFC 2412) (118649 bytes)
- The ESP CBC-Mode Cipher Algorithms (RFC 2451) (26400 bytes)
- The Use of HMAC-MD5-96 within ESP and AH (RFC 2403) (13578 bytes)
- The Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404) (13089 bytes)
- The ESP DES-CBC Cipher Algorithm With Explicit IV (RFC 2405) (20208 bytes)
- IP Encapsulating Security Payload (ESP) (RFC 2406) (54202 bytes)
- The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407) (67878 bytes)
- Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408) (209194 bytes)
- The Internet Key Exchange (IKE) (RFC 2409) (94949 bytes)
- The Use of HMAC-RIPEMD-160-96 within ESP and AH (RFC 2857) (13544 bytes)
- More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) (RFC 3526) (19166 bytes)
- On the Use of Stream Control Transmission Protocol (SCTP) with IPsec (RFC 3554) (20102 bytes)
- The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec (RFC 3566) (24645 bytes)
- The AES-CBC Cipher Algorithm and Its Use with IPsec (RFC 3602) (30254 bytes)
- The AES-XCBC-PRF-128 algorithm for IKE (RFC 3664) (6711 bytes)
- Using AES Counter Mode With IPsec ESP (RFC 3686) (43777 bytes)
- A Traffic-Based Method of Detecting Dead IKE Peers (RFC 3706) (30196 bytes)
- IPsec-NAT Compatibility Requirements (RFC 3715) (43476 bytes)
- Negotiation of NAT-Traversal in the IKE (RFC 3947) (0 bytes)
- UDP Encapsulation of IPsec Packets (RFC 3948) (0 bytes)
- IP Encapsulating Security Payload (ESP) (RFC 4303) (114315 bytes)
- Internet Key Exchange (IKEv2) Protocol (RFC 4306) (250941 bytes)
- IP Authentication Header (RFC 4302) (82328 bytes)
- Extended Sequence Number (ESN) Add. to Ipsec DOI for Internet Security Association &Key Management Protocol (ISAKMP (RFC 4304) (9243 bytes)
- Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) (RFC 4309) (28998 bytes)
- Cryptographic Algorithms for use in the Internet Key Exchange Version 2 (IKEv2) (RFC 4307) (12980 bytes)
- Cryptographic Suites for IPsec (RFC 4308) (13127 bytes)
- Security Architecture for the Internet Protocol (RFC 4301) (262123 bytes)
- Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (RFC 4305) (17991 bytes)
- The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) (RFC 4106) (23399 bytes)

IETF Active security WGs

- btns — Better-Than-Nothing Security
- dkim — Domain Keys Identified Mail
- emu — EAP Method Update
- inch — Extended Incident Handling
- isms — Integrated Security Model for SNMP
- kitten — Kitten (GSS-API Next Generation)
- krb-wg — Kerberos WG
- ltans — Long-Term Archive and Notary Services
- msec — Multicast Security
- openpgp — An Open Specification for Pretty Good Privacy
- pki4ipsec — Profiling Use of PKI in IPSEC
- pkix — Public-Key Infrastructure (X.509)
- sasl — Simple Authentication and Security Layer
- secsh — Secure Shell
- smime — S/MIME Mail Security
- syslog — Security Issues in Network Event Logging
- tls — Transport Layer Security

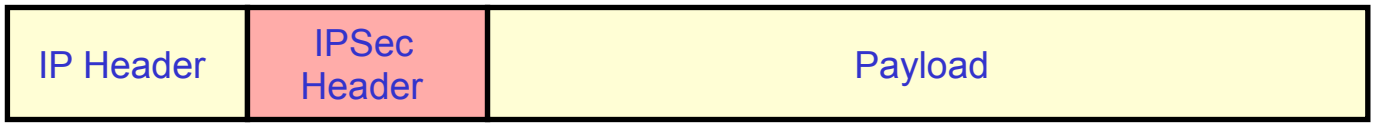
Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- **IPSec modes: transport – tunnel**
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

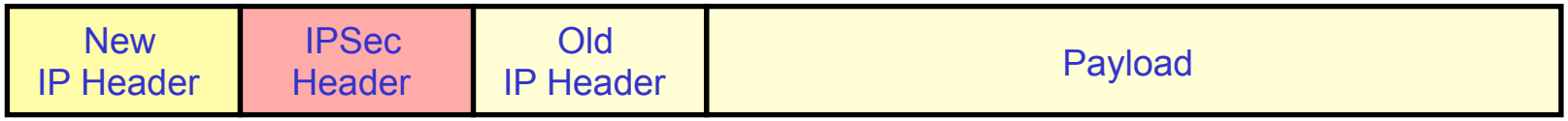
Transport and Tunnel mode

Original IP packet

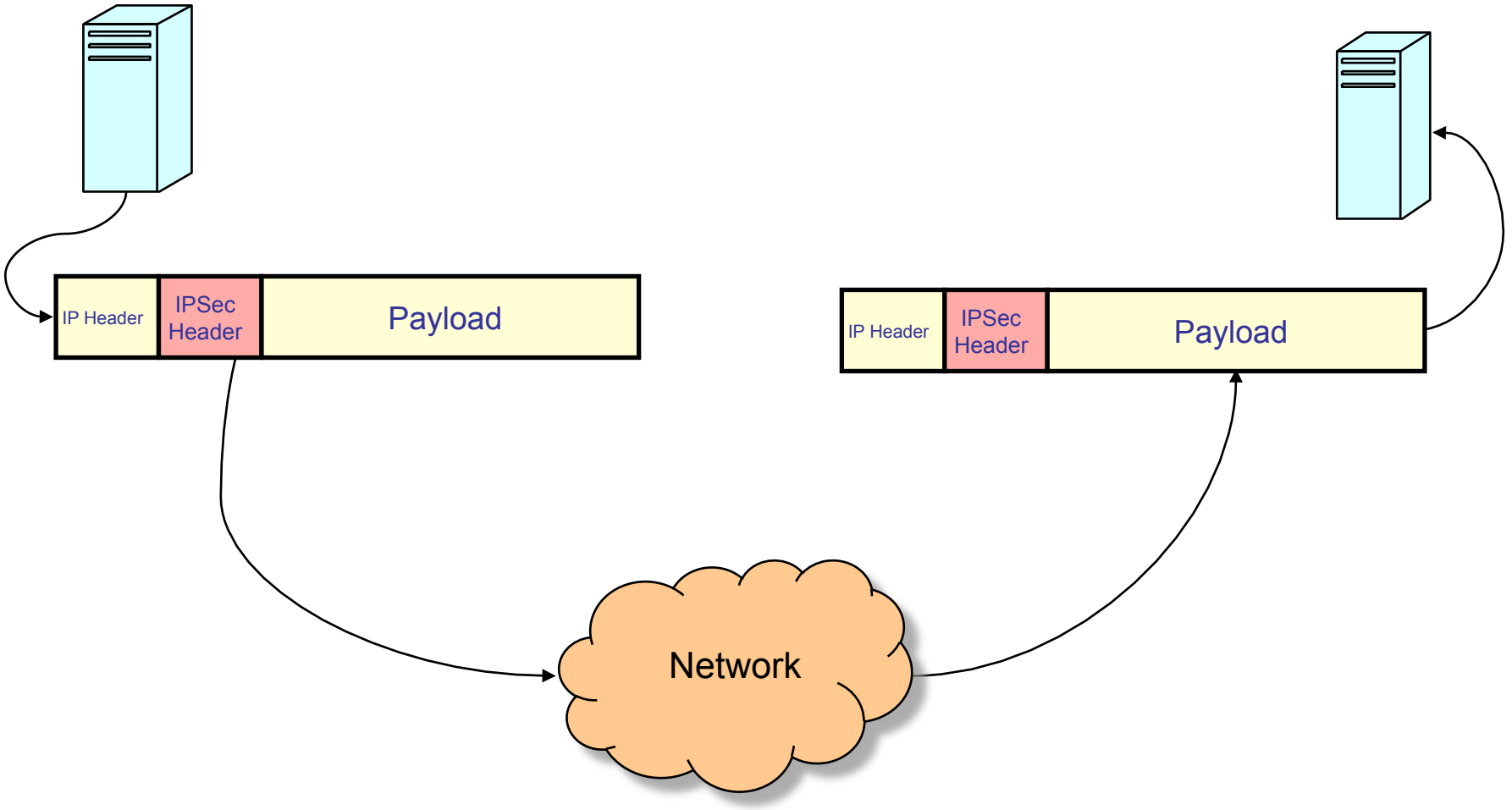
Transport mode



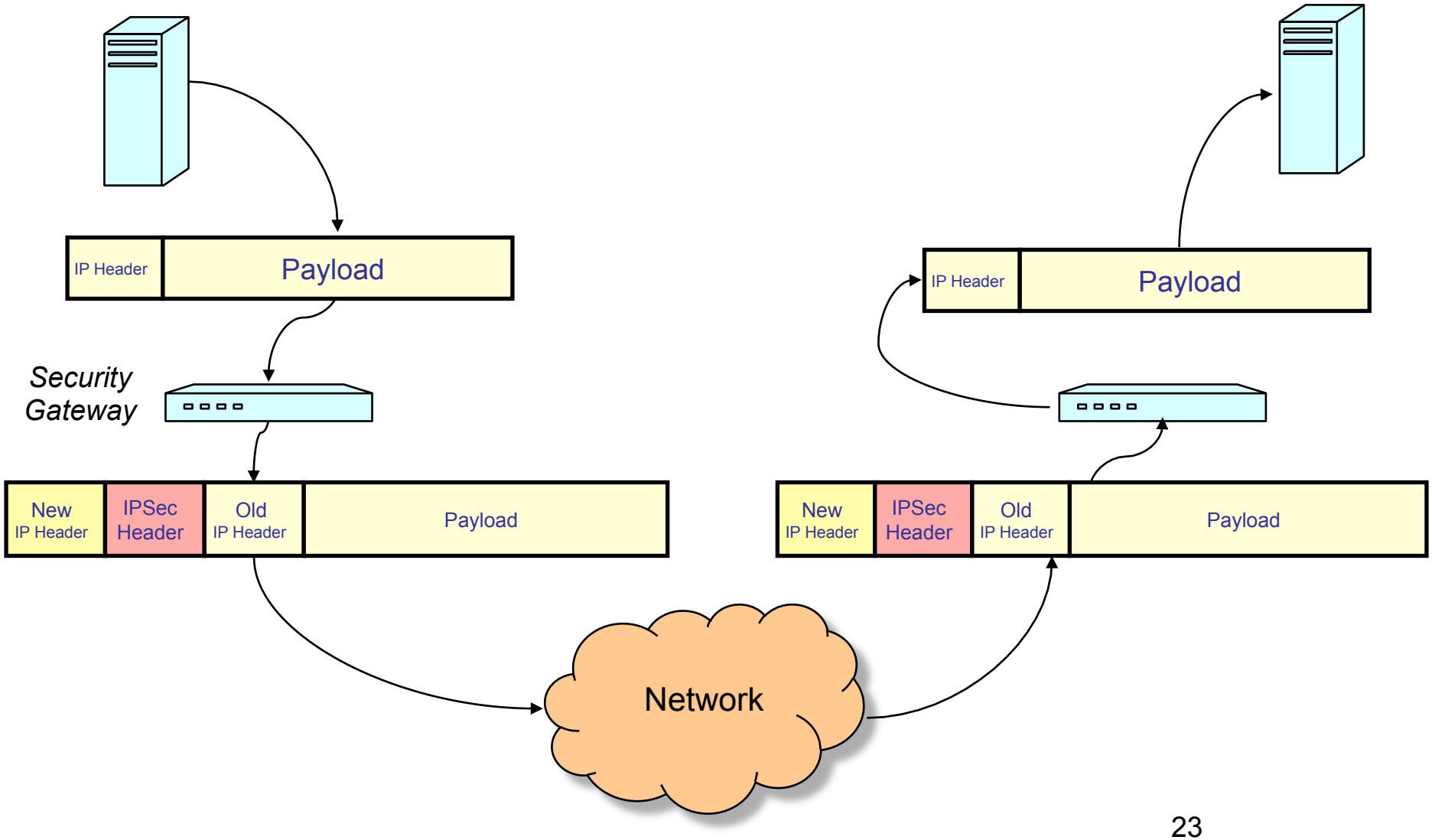
Tunnel mode



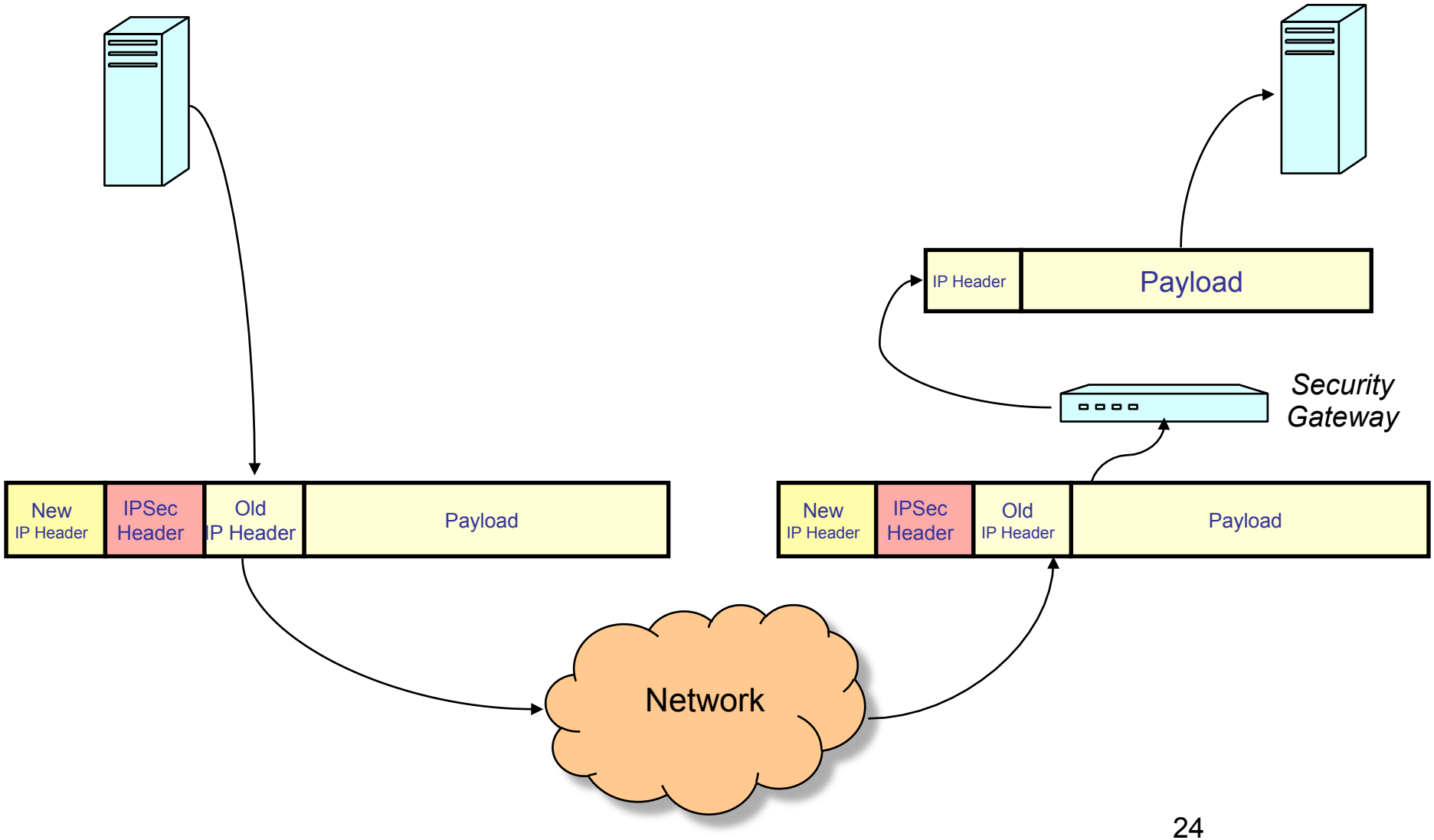
Transport mode



Tunnel mode


IP Header
Payload
Security
Gateway
New
IP Header
IPSec
Header
Old
IP Header
Payload
Network
IP Header
Payload
New
IP Header
IPSec
Header
Old
IP Header
Payload

Tunnel mode


New
IP Header
IPSec
Header
Old
IP Header
Payload
Network
New
IP Header
IPSec
Header
Old
IP Header
Payload
Security
Gateway
IP Header
Payload

Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- **IPSec AH**
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- Summary

AH and ESP Functionality

	Transport mode	Tunnel mode
AH	Authenticates IP payload plus selected portions of IP header	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload	Encrypts inner IP packet
ESP with Authentication	Encrypts IP payload. Authenticates IP payload but not IP header	Encrypts and Authenticates inner IP packet

IPSec AH header

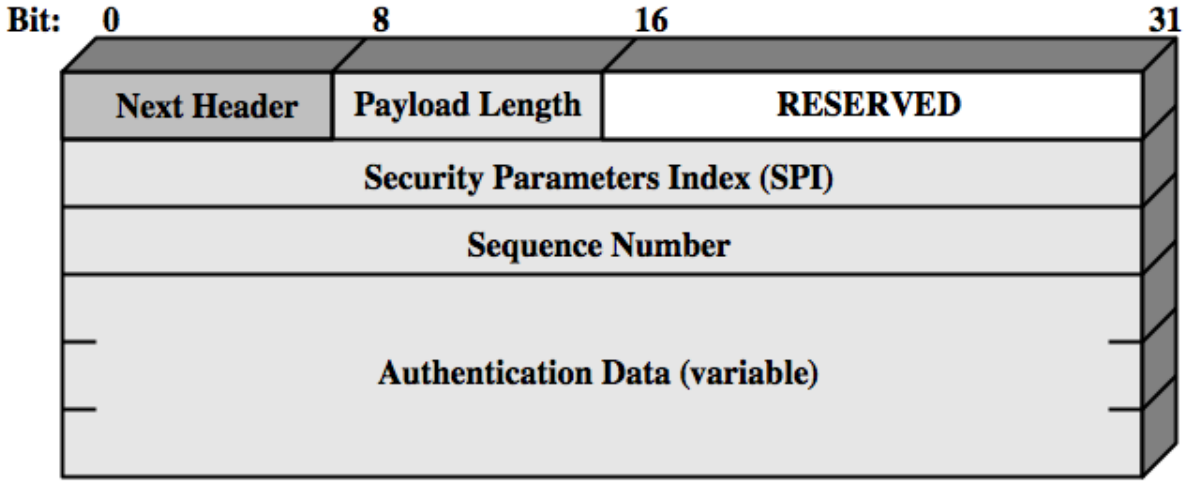


Figure 6.3 IPSec Authentication Header

Note that Security Associations (SAs) are 1 way;
for full duplex communication two SAs must be established.
SPI is therefore different for both directions

Question

- How can replay be detected?

Replay protection

- Uses Sequence number and window

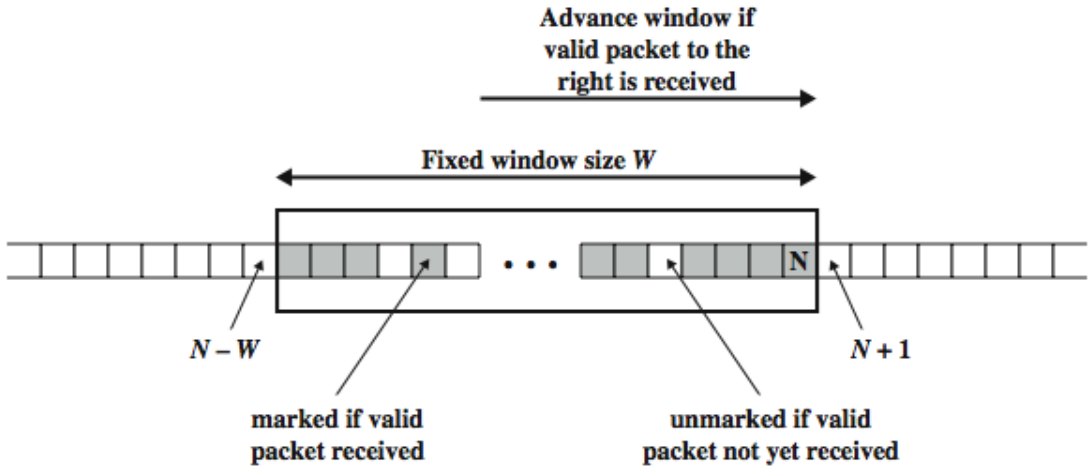


Figure 6.4 Anti-Replay Mechanism

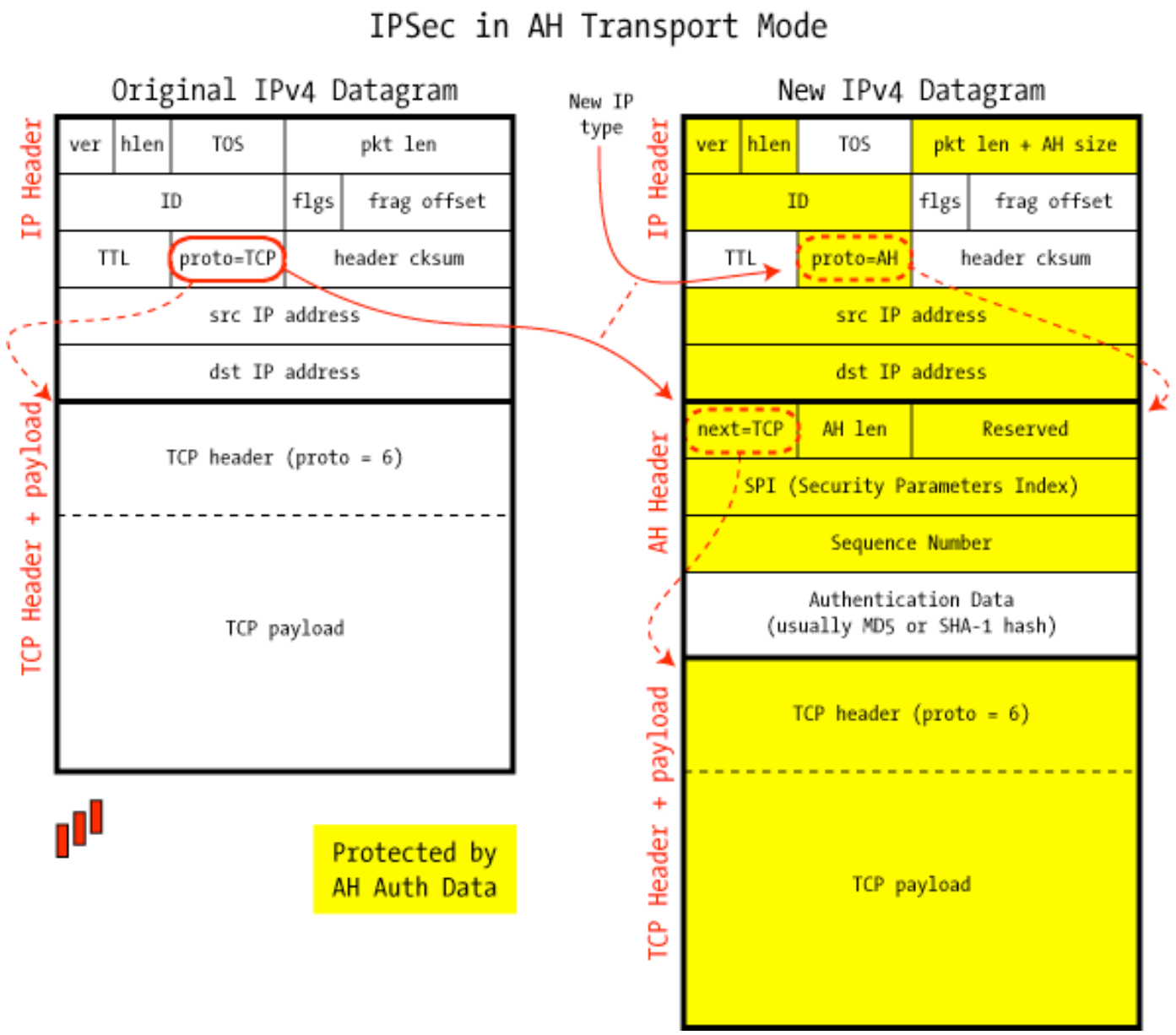
Integrity Check Value

- Implementations must support:
- HMAC-MD5-96
- HMAC-SHA-1-96

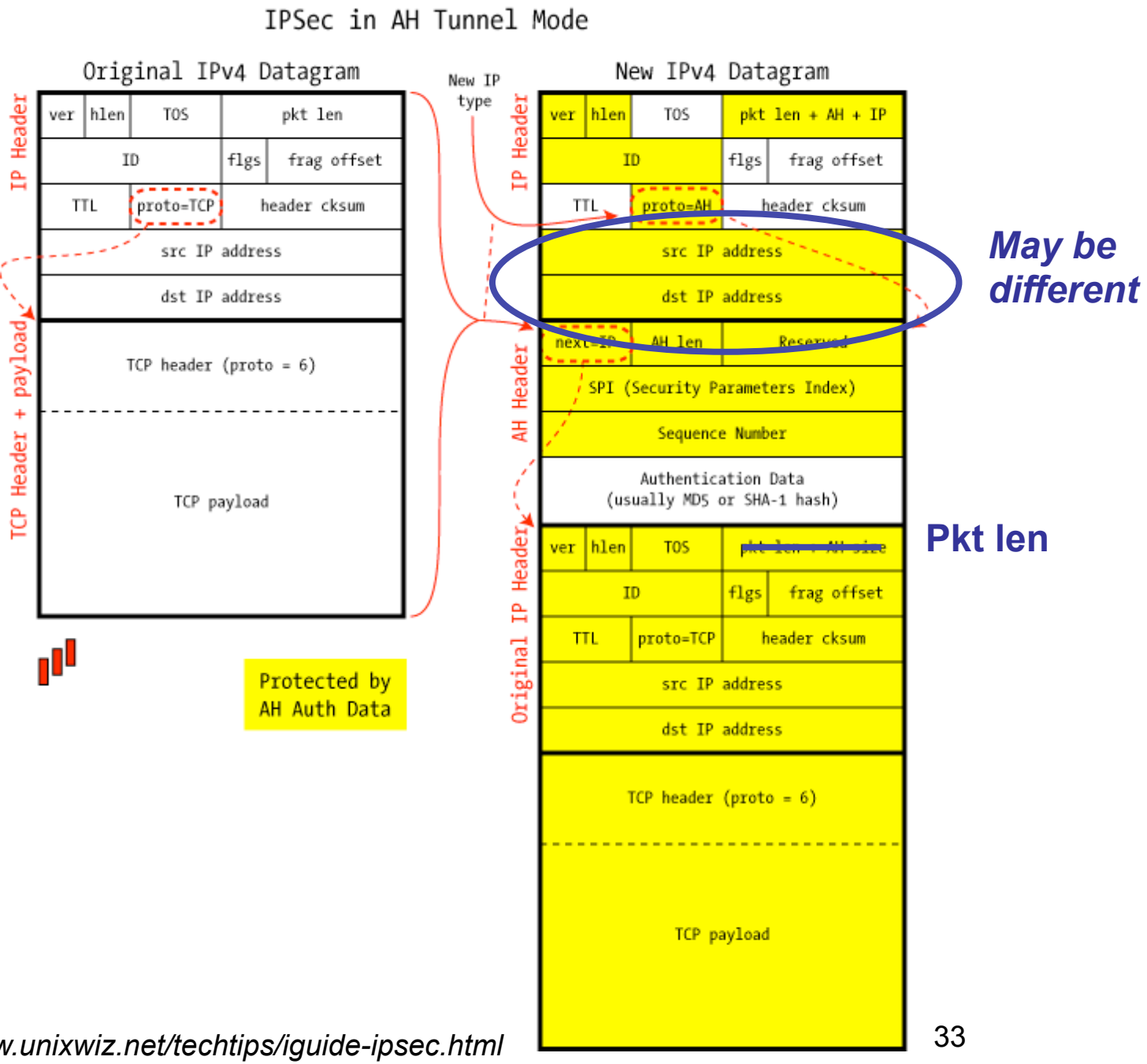
- The Integrity Check Value is calculated over the IP data and the IP header fields that do not change in transit

Question

- The Integrity Check Value is calculated over the IP data and most of the IP header.
- Which IP header fields should be included, which not?
- *IP Version number?*
- *IP Source and Destination addresses?*
- *IP Time To Live (TTL) Field?*
- *IP header length?*
- *IP total packet length?*
- *IP header checksum?*
- *IP Type of Service*



Source: http://www.unixwiz.net/techtips/iguide-ipsec.html

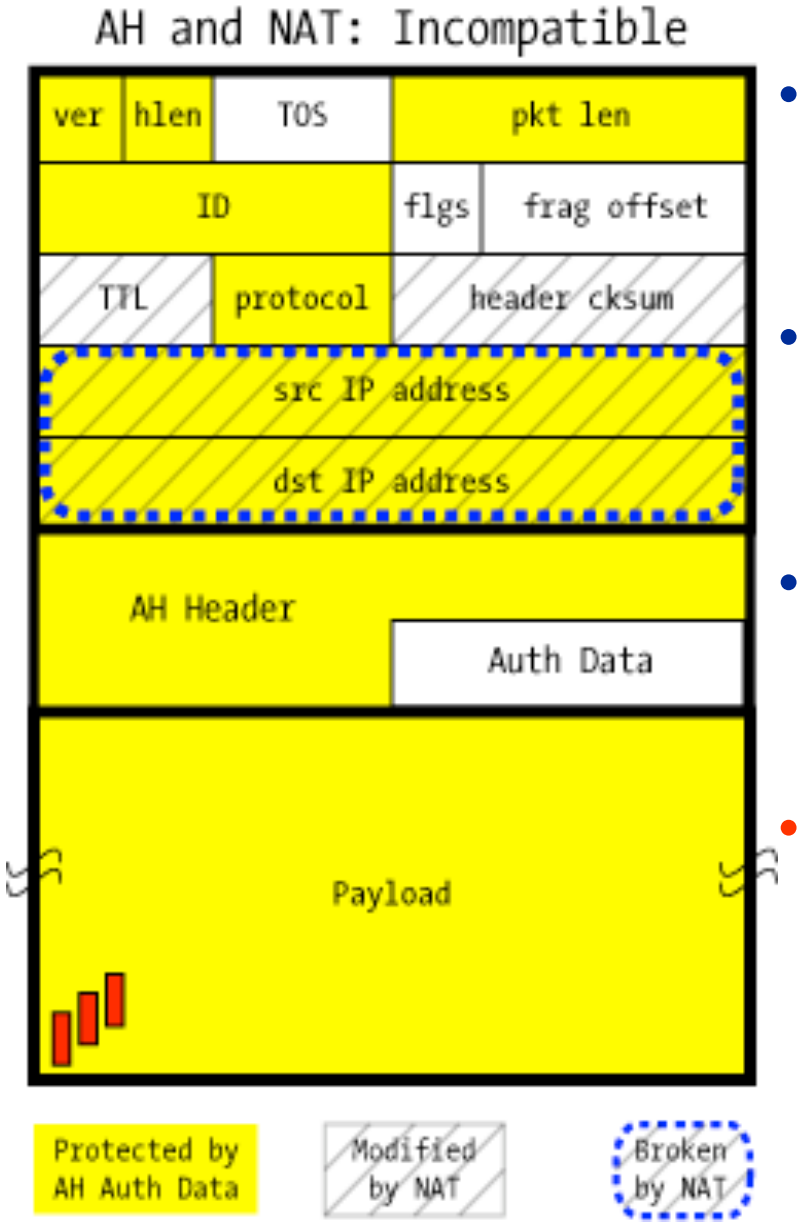


Source: *http://www.unixwiz.net/techtips/iguide-ipsec.html*

Question

- Can IPSec AH operate over NATs?

- *Yes*
- *No*
- *Depends whether NAT is at sender or receiver side*
- *Depends whether transport or tunnel mode is used*



- NAT (Network Address Translation) changes IP address
- NAT does not know the secret key to update the Auth Data
- Same holds for PAT (Port Address Translation)
- **IPSec AH (both transfer & tunnel mode) can not work over NATs**

Source: http://www.unixwiz.net/techtips/iguide-ipsec.html

Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- **IPSec ESP**
- IPSec and VPNs
- IPSec key management
- Summary

IPSec ESP header (+ payload)

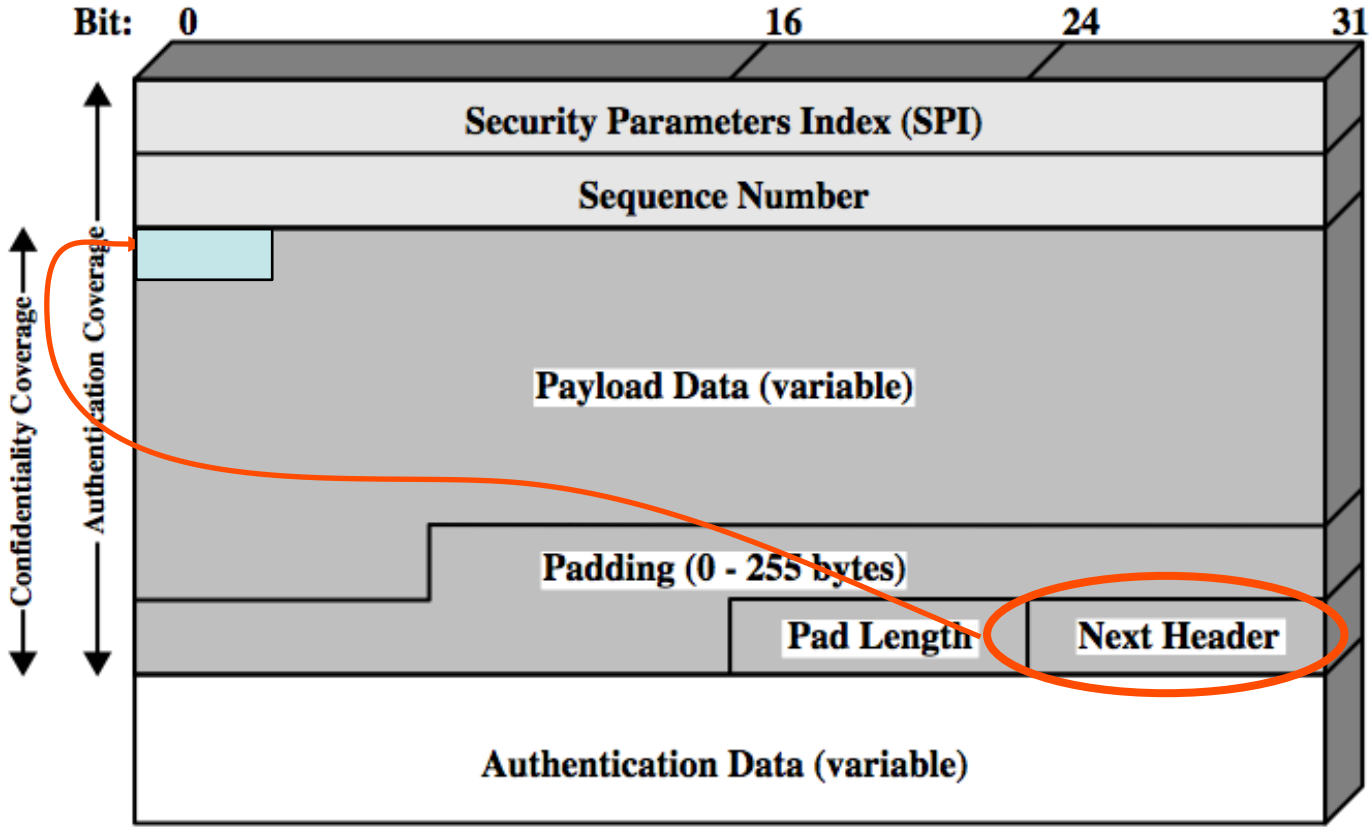


Figure 6.7 IPSec ESP Format

Encryption and Authentication Algorithms

- Implementations must support:
- DES-CBC (Cipher Block Chaining) mode (*encryption*)
- HMAC-MD5-96 (*authentication*)
- HMAC-SHA-1-96 (*authentication*)

- Optional:
- Triple DES
- RC5
- AES
- Blowfish
- IDEA
- Triple IDEA
- …

ESP Authentication

- Only the ESP header and encrypted payload are authenticated
- This is different from AH
  (although security is not really weakened)

- Note that outsiders may not even be able to determine if authentication is used. Only the destination knows the meaning of the SPI field

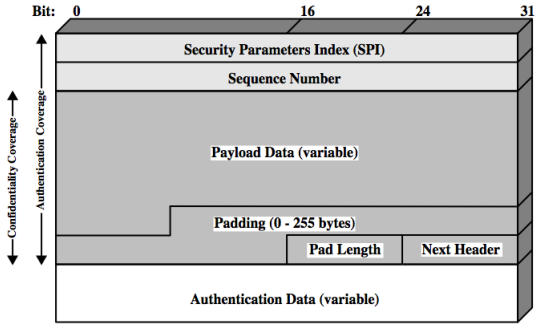
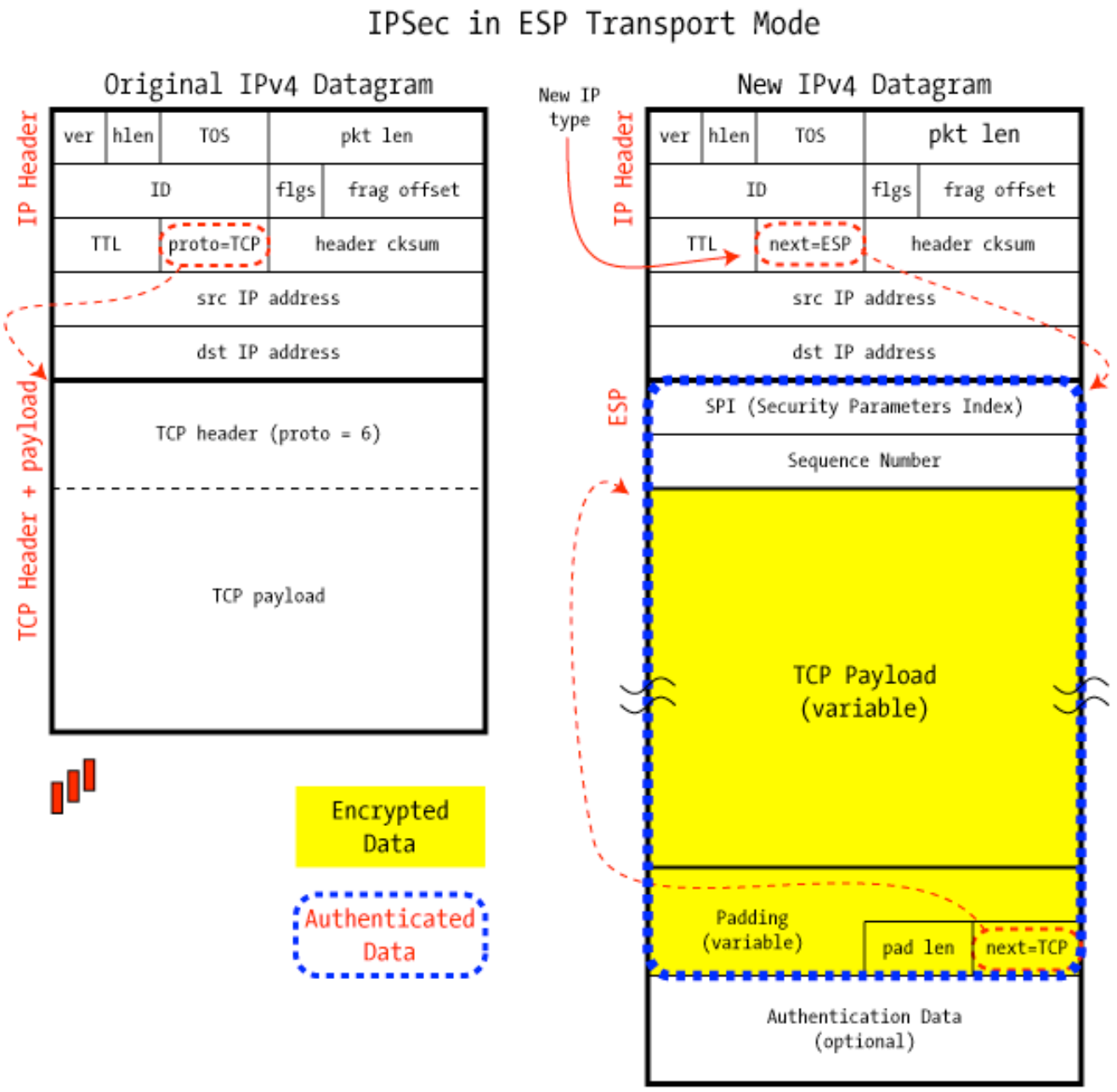
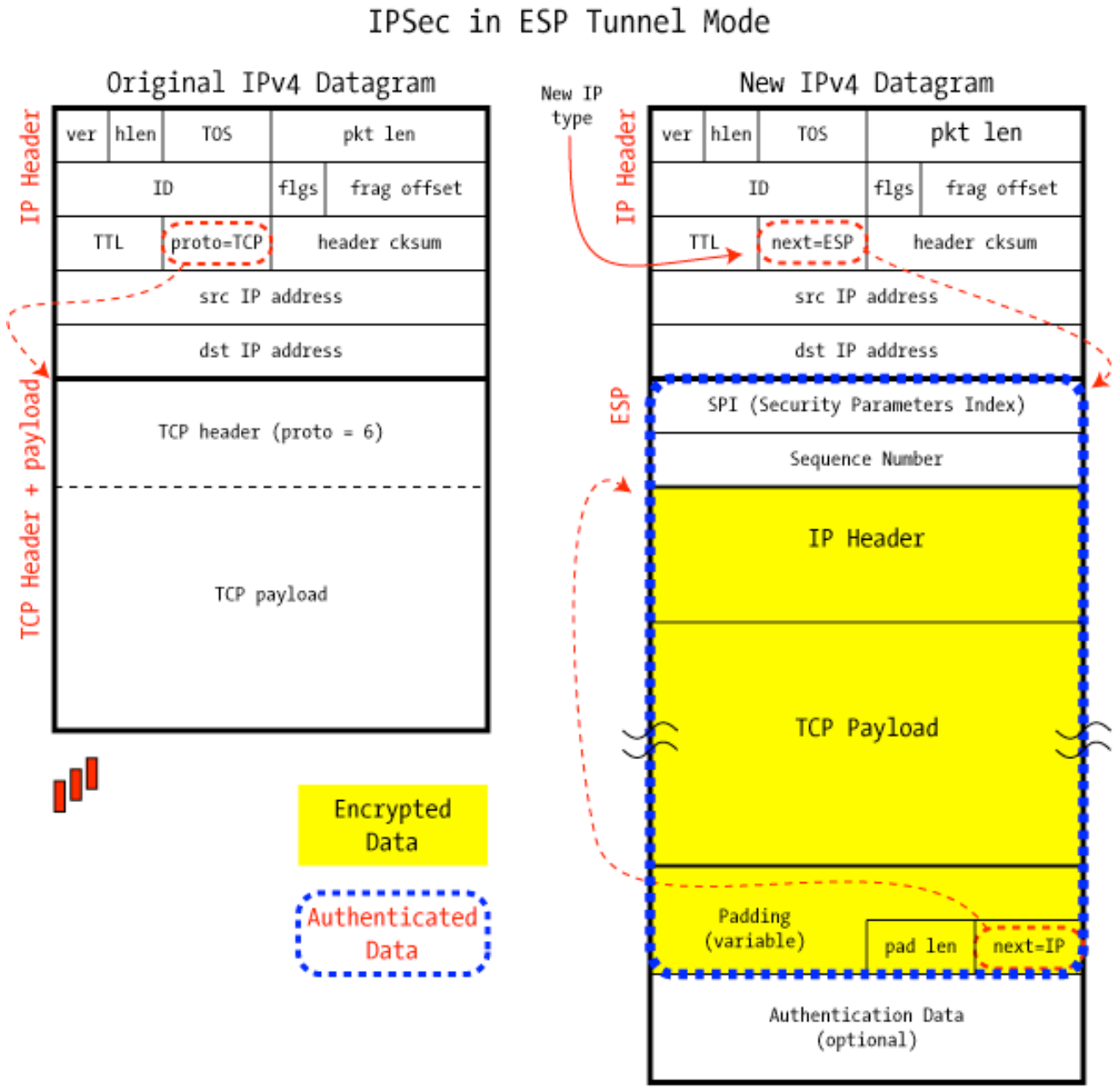


Figure 6.7 IPSec ESP Format



Source: http://www.unixwiz.net/techtips/iguide-ipsec.html



Source: http://www.unixwiz.net/techtips/iguide-ipsec.html

ESP and NATs

- ESP authentication and encryption do not include the IP header
- NATs can therefore modify the IP addresses

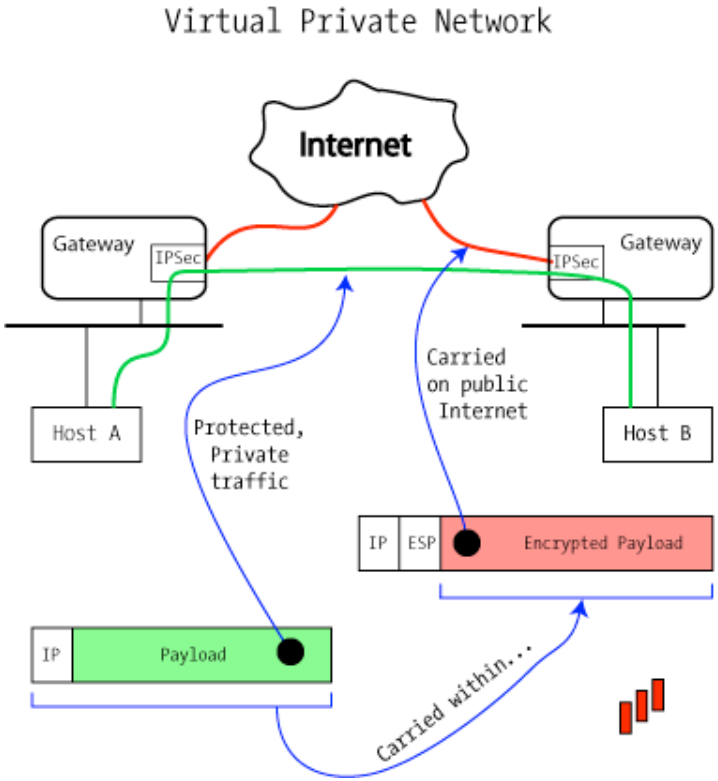
- NATs have to relate responses to requests, however
- Port numbers are usually used for that purpose
- ESP makes port numbers invisible, however
- SPI values can not be used instead, since they are different in both directions

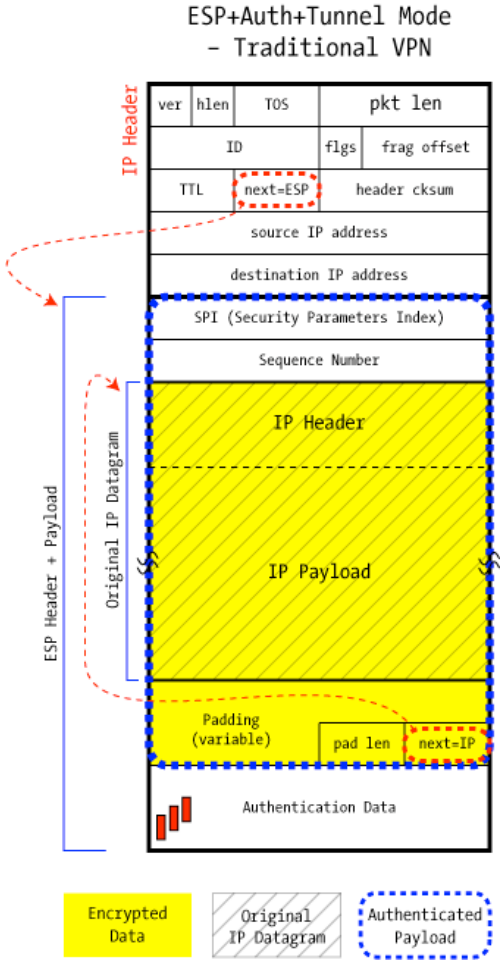
- See RFC 3715 : IPSec-NAT Compatibility Requirements

Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- **IPSec and VPNs**
- IPSec key management
- Summary

Virtual Private Network (VPN)





Source: http://www.unixwiz.net/techtips/iguide-ipsec.html

Different VPN solutions

- IPSec
- PPTP
  - Cisco, Microsoft
  - Informational RFC (RFC 2637)
  - Originally authentication only via passwords
  - Microsoft Challenge/Response Handshake Protocol (MSCHAPv2)
  - Encryption is optional
  - Outdated
- L2TP
- OpenVPN
  - SSL/TLS
- Hamachi

Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- **IPSec key management**
- Summary

IPSec key management

1. Manual

2. Automatic
   - Internet Key Exchange (IKE)
   - Combination and extension of:
     - Internet Security Association Key Management Protocol (ISAKMP)
     - Oakley: key exchange protocol
     - SKEME: another key exchange protocol
   - Two versions of IKE exist

IKE

- Two phases:
  1. Create an IKE SA (Security Association): a *secure and authenticated channel* between the two communicating entities
  2. Create and manage IPSEC SAs (child SAs)

IKE - Phase 1

- Two modes:
  - main mode
  - aggressive mode

- Four Authentication methods:
  - Pre-shared keys
  - Digital signatures
  - Public key encryption
  - Revised public key encryption

IKE - Phase 2

- One mode:
  - Quick mode
  - Involves exchange of 3 messages

- Again many options

IKE problems

- Interoperability:
  - Too many options
  - No safe default settings, dead-locks possible
  - Too much computation: vulnerable to DoS attacks
  - Too complex to understand
  - Description scattered over multiple RFCs
- IKEv2 should improve the situation
  - From the start addresses NATs

Contents

- IPSec overview
- IPSec in practice
- IPSec standardization
- IPSec modes: transport – tunnel
- IPSec AH
- IPSec ESP
- IPSec and VPNs
- IPSec key management
- **Summary**

Summary

- Two kind of protocols: AH and ESP
- Two different modes: transport and tunnel
- Separate key management protocol
- Usage is below expectation
- Various problems

IPSec problems

- Interoperability:
- (too?) many options
  Schreier & Ferguson: IPSec is too complex to be secure [1999]
- Network Address Translators (NATs)
- Some operators re-assign IP addresses periodically

- Performance:
- Fragmentation
- Time needed for key management
- Time needed for encryption / decryption

IPSec implementations

- Windows (2000, XP, Vista, W7)
  replacing PPTP
- Linux
- Mac OS X
- BSD
- All major network devices (routers)
- UMTS standards

References

- Stallings, chapter 6
- Wikipedia:
  http://en.wikipedia.org/wiki/IPSec
- An Illustrated Guide to IPSec
  http://www.unixwiz.net/techtips/iguide-ipsec.html
- IETF
  http://www.ietf/org/