ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

IPSec

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe
Freiburg

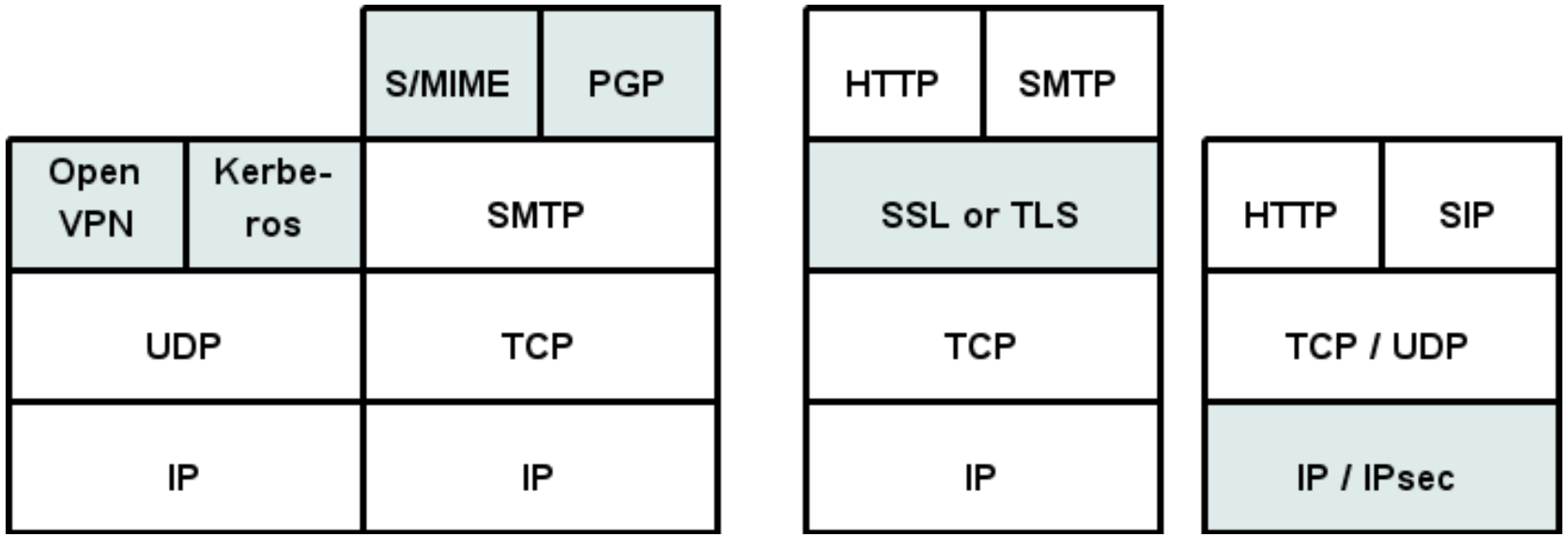
IIF
INSTITUT FÜR
INFORMATIK
FREIBURG

Organization

- I. Data and voice communication in IP networks
- **II. Security issues in networking**
- III. Digital telephony networks and voice over IP

Network Security on Different Layers

- Talked of transport Layer (SSL/TLS): easy, widely used, classical web security and application Layer (PGP, S/MIME) in last practical
- Today: Move down within the network stack to the network layer: IPsec as a general means to secure all higher level protocols between IP networked hosts



IP sec - Introduction

- IP level security -> IPsec
- IPSEC is Internet Protocol SECurity
- The level above the network layer is the place where IPsec was put - No alteration to the IP was needed, simply the transportation protocol was interchanged (or and additional security header introduced)
- Remember security requirements given in an earlier lecture
- It uses strong cryptography to provide both authentication and encryption services
  - Authentication ensures that packets are from the right sender and have not been altered in transit
  - Encryption prevents unauthorized reading of packet contents

IP sec - Introduction

- IPSEC tries to provide a framework for encrypting the whole IP traffic that might occur
- But in reality it mainly allows to build secure tunnels through untrusted networks
- Every packet passing through the untrusted net is encrypted by the IPSEC gateway machine and decrypted by the gateway at the other end
- The result is another implementation of a Virtual Private Network (VPN)
  - Seen OpenVPN in practical as another example

IP sec - Introduction

- IPSEC protocols were developed by the IETF, they are part of the IP version 6 (next generation Internet protocol, see earlier lecture)
- In theory a lot of networking software firms implement the IPSEC standard, but in real only a few products really operate
- With Linux there are several Free/Open/StrongSWAN implementations of IPSEC for the 2.6 kernel series available
- StrongSWAN implements IKE 2 and introduces a new user space daemon for key exchange
- For logging on the wireless campus LAN Cisco's IPsec implementation is used (operable with Cisco VPN concentrator (only))
  - Open source tool (vpnc) is available too (useful for PDAs and other embedded devices without official Cisco support, practical part)

IP sec - Introduction

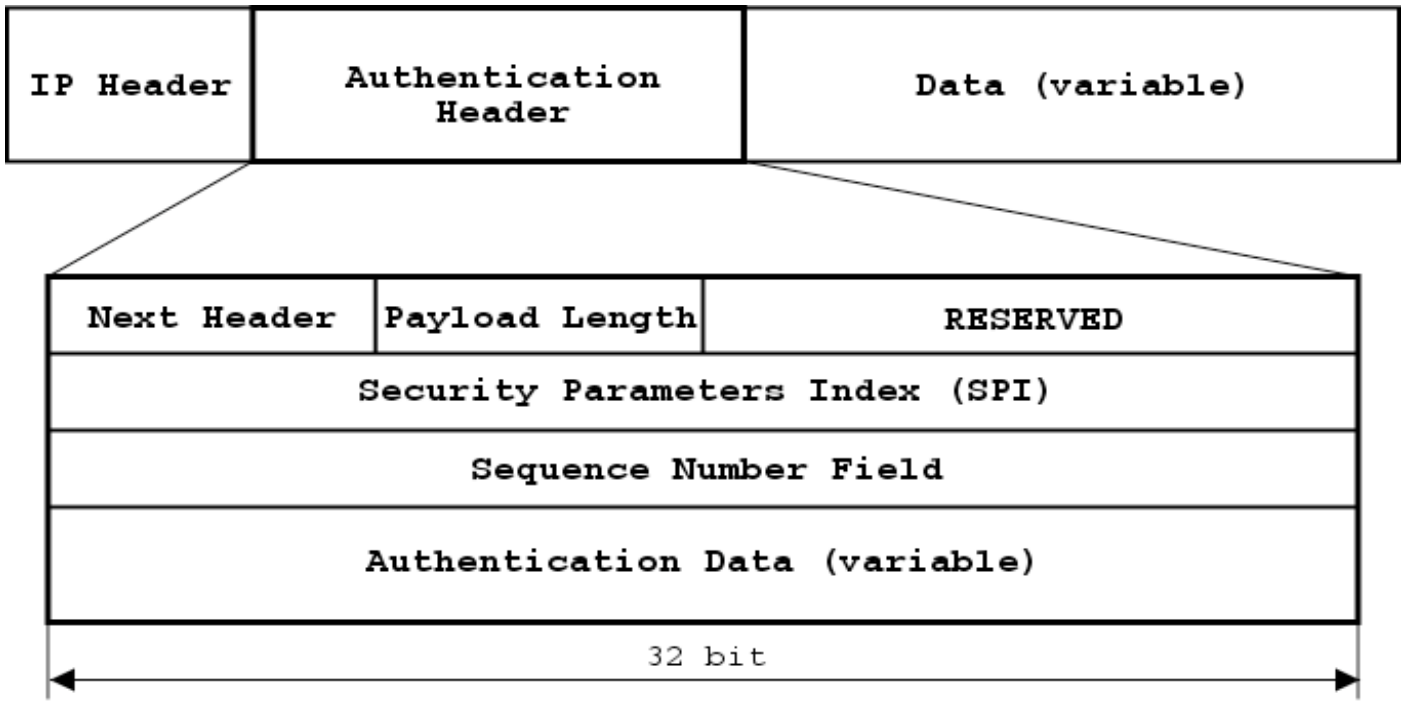
- IPsec can be used on any machine which does IP networking
- Dedicated IPsec gateway machines can be installed wherever required to protect traffic of LANs
- IPSEC can also run on routers, on firewall machines, on various application servers, and on end-user desktop or laptop machines
- Three protocols are introduced
  - AH (Authentication Header) provides a packet-level authentication service
  - ESP (Encapsulating Security Payload) provides encryption plus authentication
  - IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two

IP sec - Introduction

- IPsec Authentication Header (AH) is added after the IP header
- Authentication – ensures that a message originated from the expected sender and has not been altered on route
- For Authentication exchange of passwords or similar is needed – that means to establish a security association (SA)
- A common solution to this problem is a challenge-response system. It defeats simple eavesdropping and replay attacks

IP sec - Authentication Header

- AH's position in the IP packet (next header concept taken from the IPv6 standard, refer to earlier lecture)

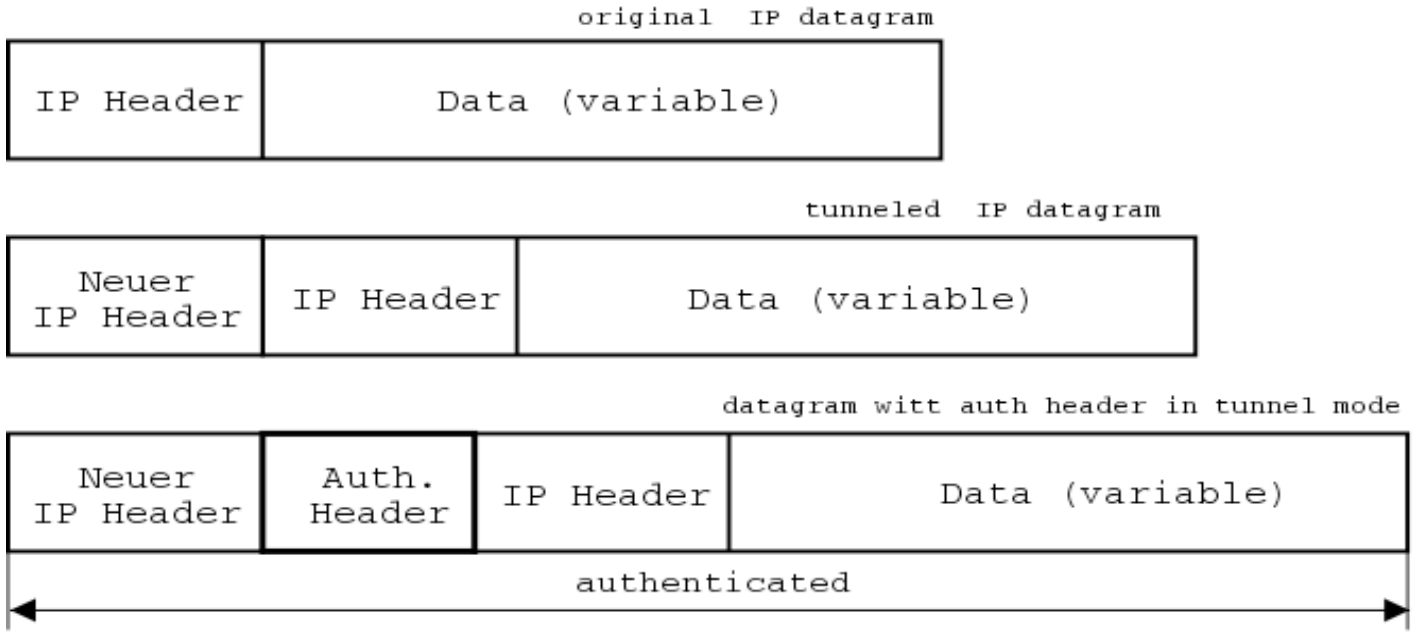


IP sec - Authentication and AH

- Header:
  - Contains a sequence number of four byte length
  - Maintains the length of the header itself (in unit of 32/64 bits)
  - Stores information on next header (IP: 4, TCP: 6, UDP: 17, ESP: 50, AH: 51 -> see /etc/protocols) -> depends on IPSEC mode
- IPSEC could be operated in two modes
  - Tunnel mode is used between firewalls or network host/end node and firewall
  - Transport mode is applied when IPSec is used end-to-end

IP sec - Authentication and AH

- In tunnel mode, the original IP packet will be kept intact (But: MTU size change – payload available to higher level protocols - results in shorter packets ...)
- AH used in tunnel mode:

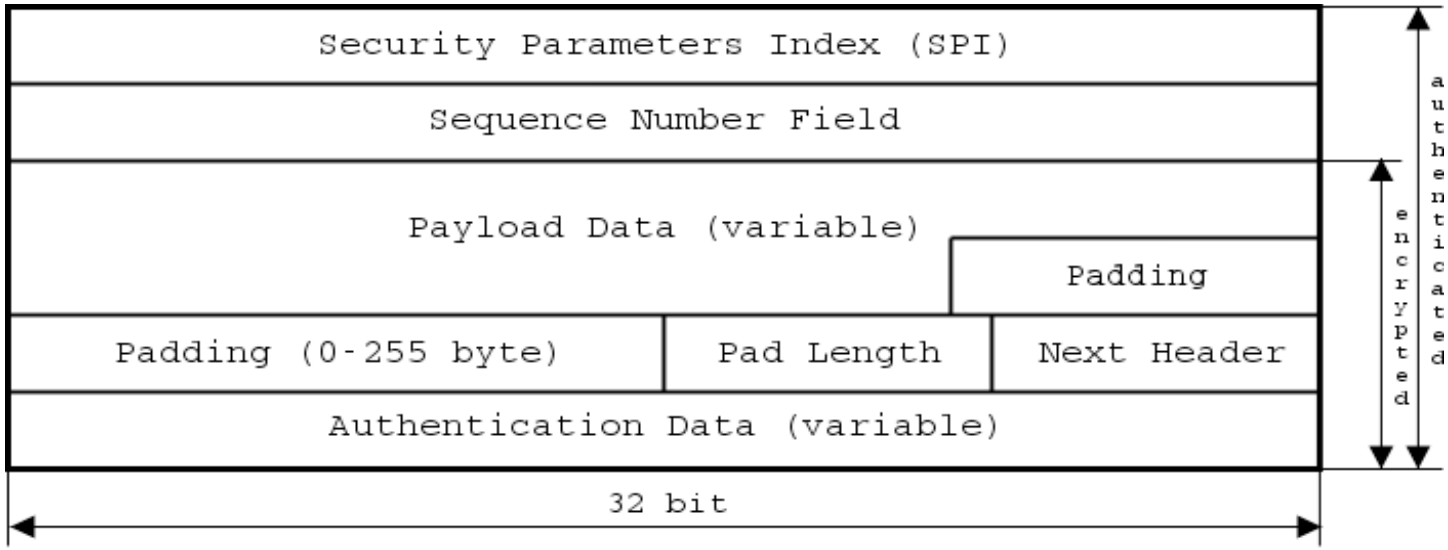


IP sec – Encapsulated Security Payload

- Encapsulated Security Payload is the IPsec protocol which provides encryption
- It can also provide authentication service and may be used with null encryption (which should be used for testing and analysis only)
- Its header contains
  - Next header/protocol type (one byte)
  - Padding length (in units of octets - one byte)
  - Padding (variable length)

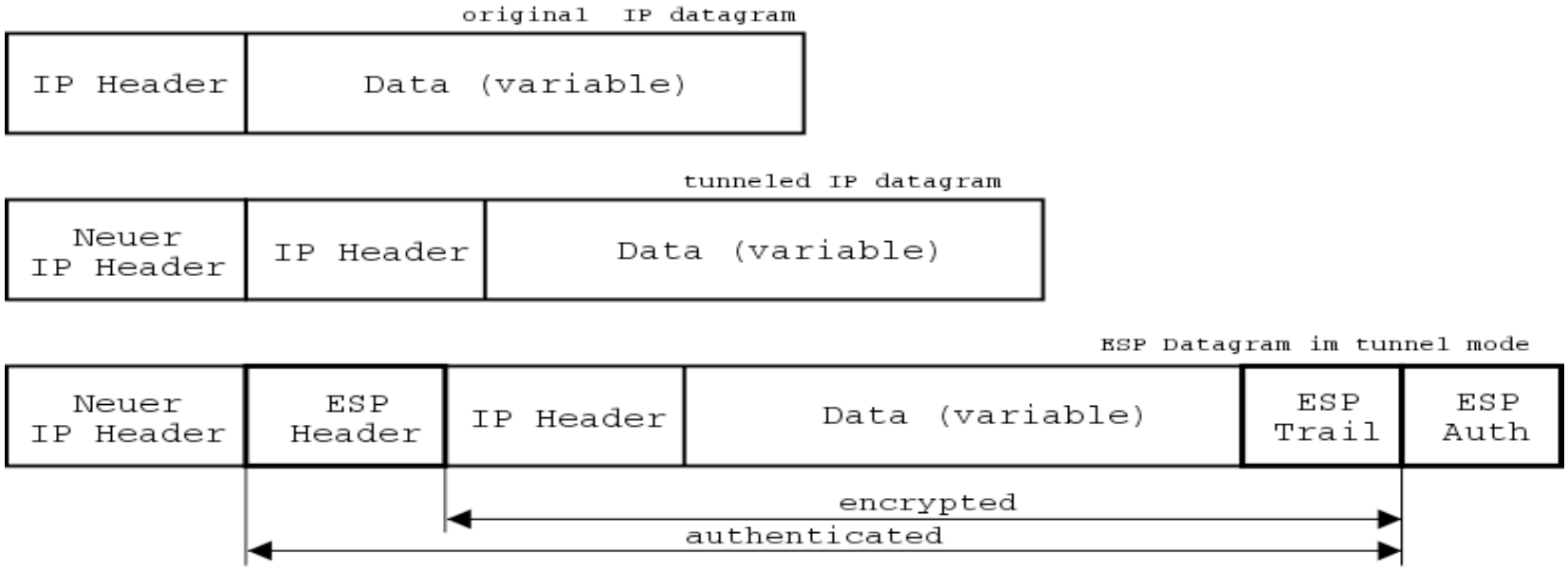
IP sec – Encapsulated Security Payload

- Encapsulated Security Payload Header
  - SPI (as known from AH - 4 bytes)
  - Sequence number (4 bytes)
  - Payload data (variable)



IP sec – Encapsulated Security Payload

- ESP in fact puts information both before and after the protected data
- Example of ESP packet in tunnel mode



IP sec – Encapsulated Security Payload

- For encryption, DATA, padding, padding length and next header are encrypted
- For authentication, all fields are included
- AH versus ESP
  - AH just does integrity
  - ESP does both encryption & integrity
  - If just integrity, use AH or ESP
  - If both integrity and encryption, then use both AH and ESP, or just use ESP

IP sec – Conclusion

- IP sec is rather “heavy stuff”
  - No simple plug-and-play implementation
  - Not suited to encrypt the whole Internet by now – only encryption of predefined connections by now
  - There are some suggestions to use “opportunistic encryption” - check if IP sec is available and use secure channel then
- Several vendors offer several solutions
  - Not all vendor solutions compatible with each other
  - High load on administration
- But IP sec in every day use to connect branches of firms / organizations via VPN (virtual private networks) over the insecure Internet

IP sec – Conclusion

- IP sec implementation of Ciscos concentrator series offer relatively easy adaptation of IP sec to end user devices
  - Used for the university WLAN – simple administration on both servers and clients side
  - But:
    - Xauth protocol to use username/password instead of certificates – shared secret (“community string/password”)
    - code is binary object only (nobody can tell if code is secure)
    - Unclean position in the Linux network stack
    - Prevention of local LAN access could be easily broken by recompilation of module wrapper
  - Free implementation is available for a while – proper Linux network device, support for unsupported (by Cisco) platforms

IP sec – Conclusion

- IP sec implementation of standard Linux kernels not without problems
  - No standard network interface is used (check in practical part to follow)
  - Difficult for firewall setup scenarios (on firewalls, package filters the upcoming lecture)
  - Different implementations available to improve usability and security (strongSWAN, developed at some Swiss University)

Literature

- General/RFC
  - S. Kent (BBN Corp) and R. Atkinson: “RFC 2406 IP Encapsulating Security Payload (ESP)”
  - Same Authors: “RFC 2402 IP Authentication Header”, Internet Engineering Task Force (IETF)
  - RFC 4306: IKE Version 2, Internet Engineering Task Force (IETF)
  - Lots of more RFCs on IPsec
- Linux IPsec implementations
  - Old implementation http://www.freeswan.org
  - 2.6 Kernel implementation
  - StrongSWAN/IKE 2 http://strongswan.org/

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer