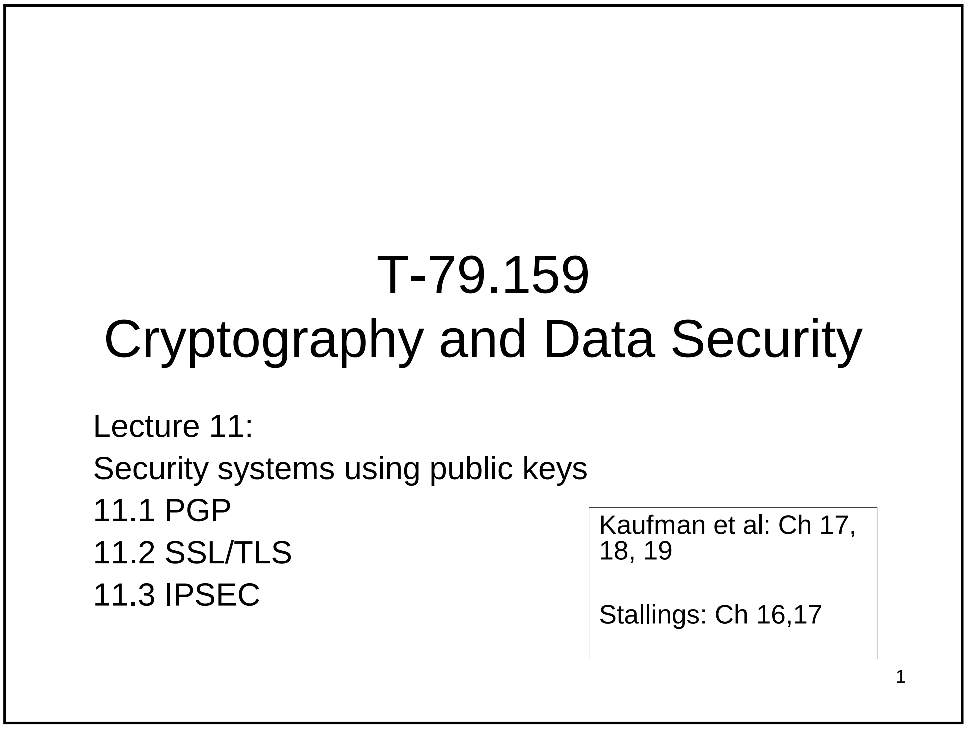


T-79.159
Cryptography and Data Security

Lecture 11:

Security systems using public keys

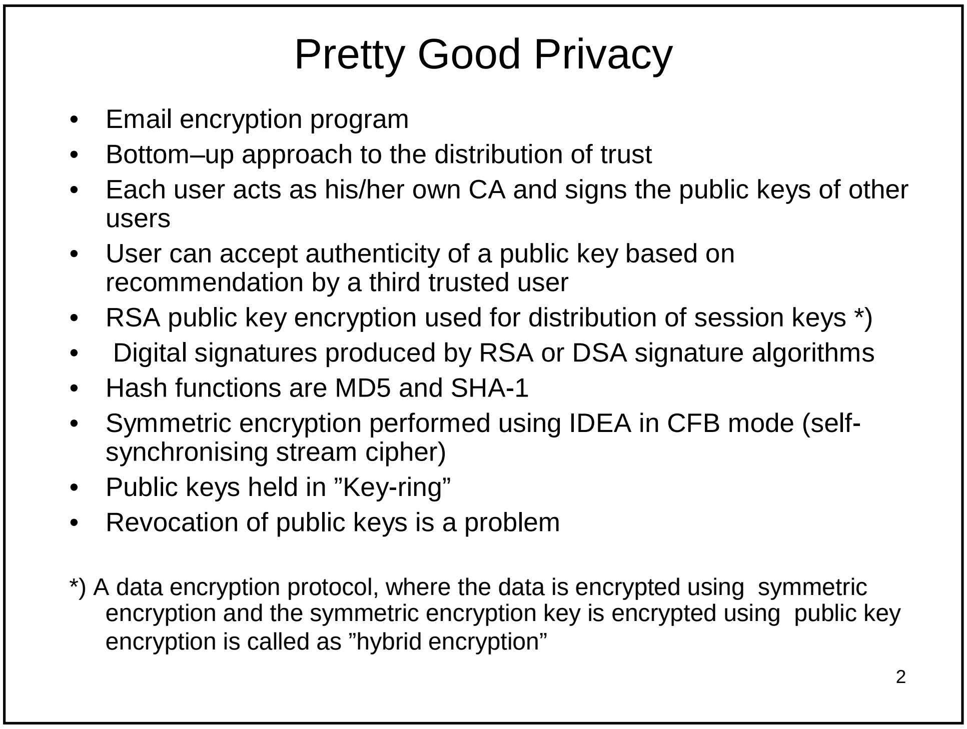
11.1 PGP

11.2 SSL/TLS

11.3 IPSEC

Kaufman et al: Ch 17, 18, 19

Stallings: Ch 16,17



Pretty Good Privacy

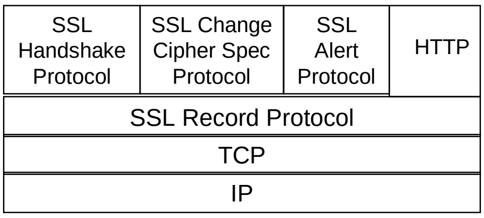
- Email encryption program
- Bottom–up approach to the distribution of trust
- Each user acts as his/her own CA and signs the public keys of other users
- User can accept authenticity of a public key based on recommendation by a third trusted user
- RSA public key encryption used for distribution of session keys *)
- Digital signatures produced by RSA or DSA signature algorithms
- Hash functions are MD5 and SHA-1
- Symmetric encryption performed using IDEA in CFB mode (self-synchronising stream cipher)
- Public keys held in ”Key-ring”
- Revocation of public keys is a problem

*) A data encryption protocol, where the data is encrypted using symmetric encryption and the symmetric encryption key is encrypted using public key encryption is called as ”hybrid encryption”

Secure Sockets Layer /Transport Layer Security

- SSL (by Netscape) adds security to the TCP level of the Internet Protocol stack
- Reliable end-to-end service.
- TLS developed by IETF is basically equivalent to SSL v 3.1

Structure:



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

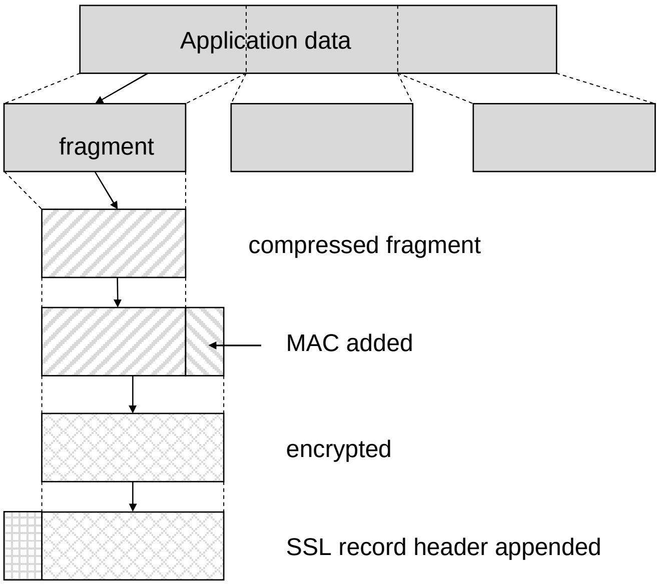
SSL Record Protocol

TCP

IP

- Hypertext Transfer Protocol (Web client/server interaction) an operate on top of SSL

SSL Record Protocol



compressed fragment

MAC added

encrypted

SSL record header appended

SSL Record Protocol Crypto

- The MAC is similar to HMAC (indeed, an early version of HMAC) with the difference that OPAD and IPAD fields are concatenated to the data (not xored as in HMAC) based on MD5 or SHA-1
- Block Cipher Algorithms available (key size in bits):
  - IDEA (128)
  - RC2-40 (40)
  - DES-40 (40)
  - DES (56)
  - 3DES (112-168)
  - Fortezza (Skipjack) (80)
- Stream Cipher Algorithms available (key size)
  - RC4-40 (40)
  - RC4-128 (128)

FORTEZZA

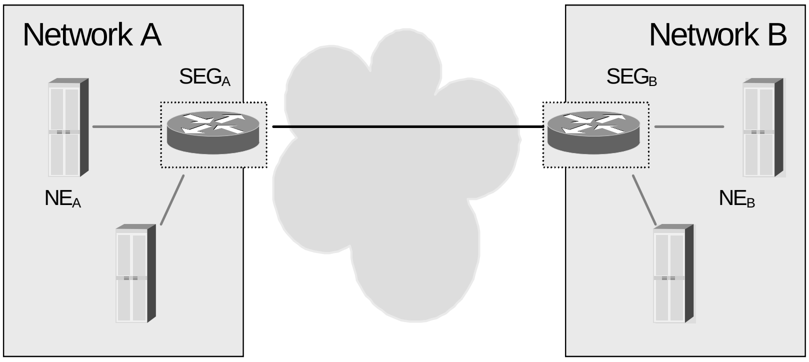
- FORTEZZA is a registered trademark of the U.S. National Security Agency (NSA)
  - Defense Message System
  - Encrypted voice communications over secure telephones.
- FORTEZZA cards
  - cryptographic "co-processors"
  - provide authentication (DSA), data integrity (SHA-1), and confidentiality (KEA and Skipjack).
- FORTEZZA-enabled devices
  - PCMCIA-based crypto cards
  - serial port devices, Ethernet cards, and modems.
  - Cellular telephones, pagers, PDAs, and other mobile devices.
- Microsoft supports FORTEZZA in its products.

SSL Handshake Protocol

- Phase 1: Establishing Security Capabilities
  - Nonces
  - Session ID
  - Cipher Suite
    1. Key Exchange method: RSA, Fixed, ephemeral, or anonymous Diffie-Hellman, Fortezza
    2. Cipher Algorithm: Any of the ones mentined above; Cipher type: Stream or Block; Exportability: Yes or No;
    3. Hash algorithm: MD5 or SHA-1; Hash size: 0, 16 (MD5), or 20 (SHA-1)
    4. Key Material (session key data) and IV size (for CBC mode)
  - Compression method
- Phase 2: Server Authentication and Key Exchange
- Phase 3: Client Authentication and Key Exchange
- Phase 4: Finish
  - Explicit verification that the authentication and key exchange was successful

IPSec

- The toolbox for building Virtual Private Networks (VPN)
  - Secure branch office connectivity over Internet
  - Secure Remote Access over Internet
  - Extranet and Intranet connectivity with partners
  - Enhanced electronic commerce security
- Efficient protection if IPSec implemented in firewall
- IPSec is below transport layer and so is transparent to applications
- IPSec is typically transparent to end users
- IPSec can be used to provide secure remote login for individual users.



IP Security Architecture

Specifications:

RFC 2401 Architecture

RFC 2402 Packet Authentication extension

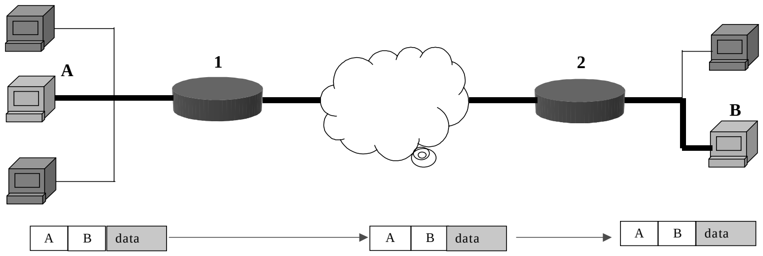
RFC 2406 Packet Encryption Extension

RFC 2408 Key Management Capabilities

Other documents in the following areas:

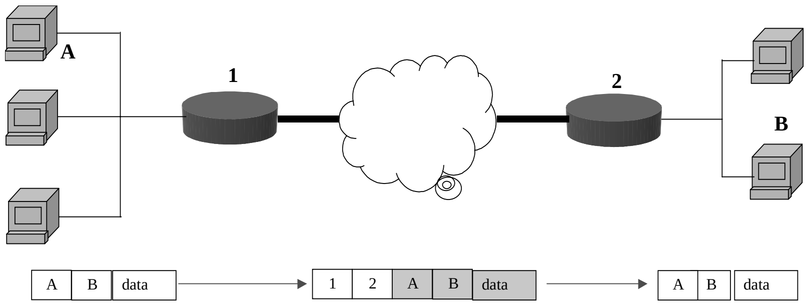
1. Architecture: general concepts, security requirements, definitions and mechanisms
2. Encapsulating Security Payload (ESP)
3. Authentication Header (AH)
4. Encryption Algorithms
5. Authentication Algorithms
6. Key Management Scemes
7. Domain of Interpretation (DoI)

End-to-End Security (Transport Mode)

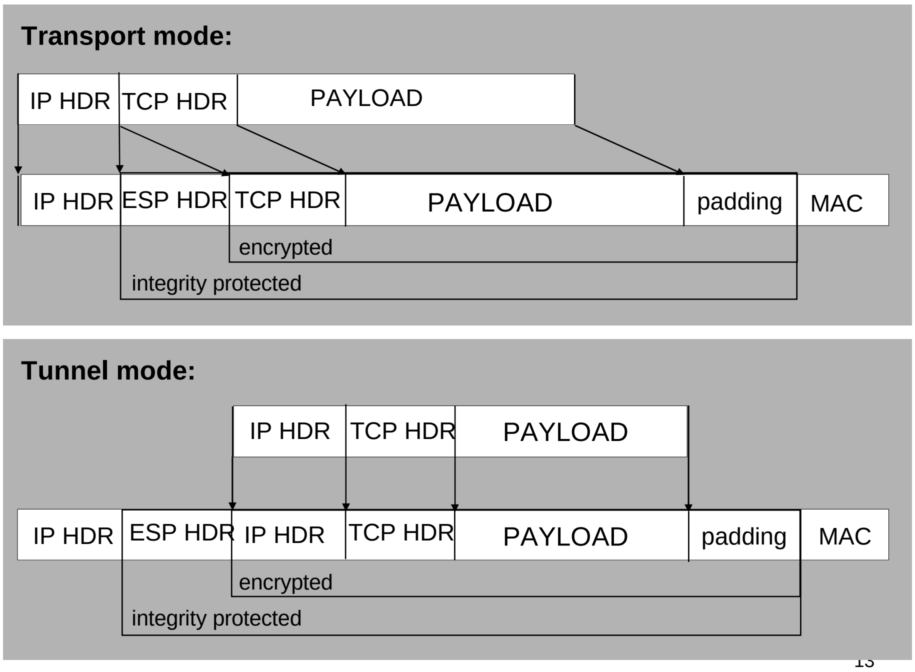


11

VPN Security (Tunnel Mode)



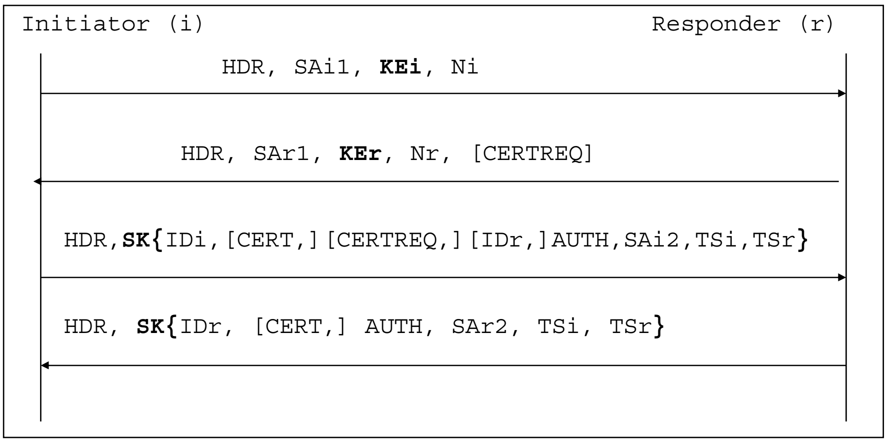
12



13

IKEv2

Based on Diffie-Hellman Key Exchange **KEi=g**^{a}**, KEr=g**^{b} → **SK=g**^{ab}



HDR, SAi1, **KEi**, Ni

HDR, SAr1, **KEr**, Nr, [CERTREQ]

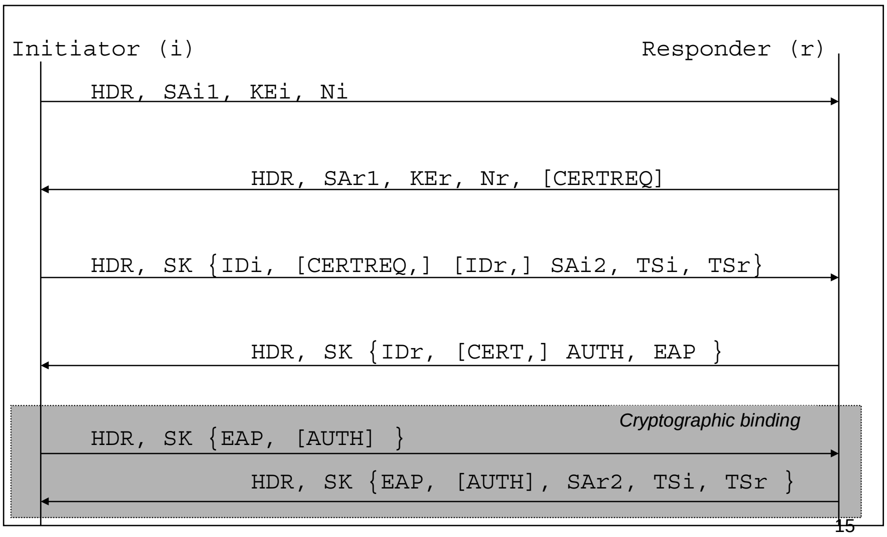
HDR,**SK**{IDi,[CERT,][CERTREQ,][IDr,]AUTH,SAi2,TSi,TSr}

HDR, **SK**{IDr, [CERT,] AUTH, SAr2, TSi, TSr}

14

IKEv2

Secure Legacy Authentication (SLA)



Initiator (i)

Responder (r)

HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTH, EAP }

Cryptographic binding

HDR, SK {EAP, [AUTH] }

HDR, SK {EAP, [AUTH], SAr2, TSi, TSr }

Legacy Protocols - EAP

- IETF PPPEXT working group:
  RFC 2284 Extensible Authentication Protocol (EAP)
- EAP is not an authentication protocol in itself, but a standard way of encapsulating an authentication protocol.
- Composed of message pairs: EAP_Request - EAP_Response; final pair: EAP_Success/EAP_Failure
- EAP types have been standardised (”legacy” protocols):
  RFC2716: PPP EAP TLS Authentication Protocol
  – Internet Drafts:
  EAP SIM Authentication
  EAP AKA Authentication
  Protected EAP Protocol (PEAP)
  EAP-SKE authentication and key exchange protocol
  Microsoft EAP CHAP Extensions
  The EAP GPRS Protocol (EAP-GPRS)