Telematics
Homework #12

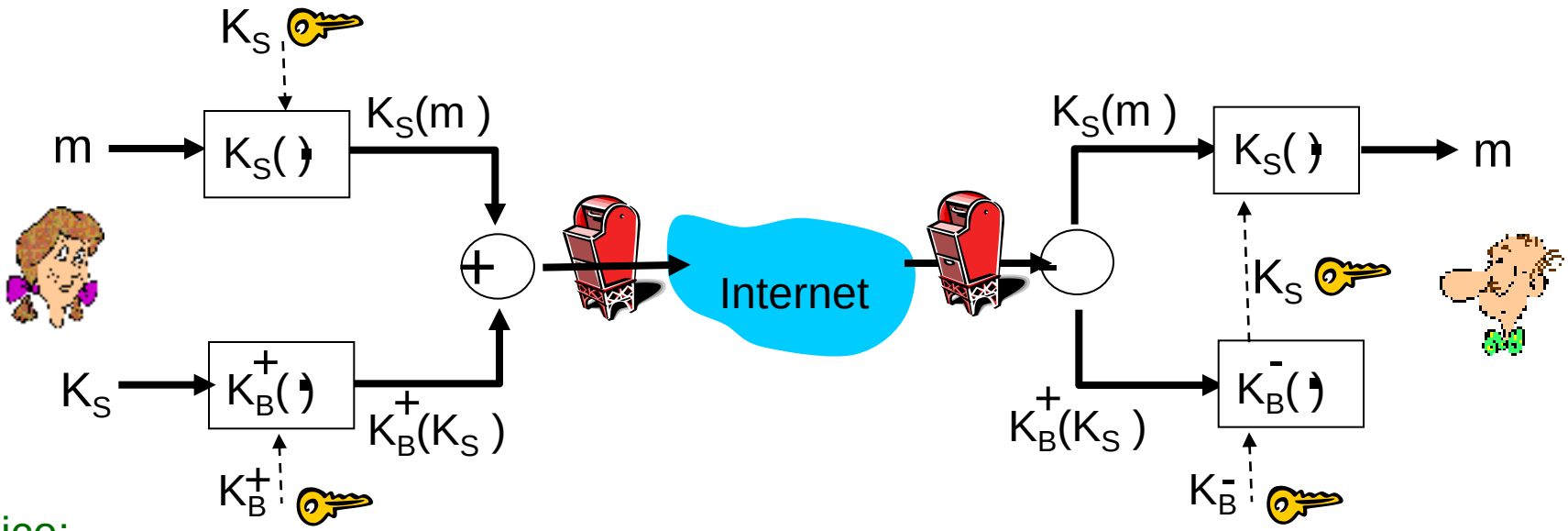
Florian Tegeler

28th of January 2010

Announcements

- Final exam: Thursday 04.02.2010
  - 10:00 -12:00 : GZG - MN08
- Language: English + German, answers possible in both languages
- No additional resources (calculator etc.) allowed. Just bring pens ;).

Secure E-Mail



Alice:

- generates random *symmetric* private key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Bob: uses his private key to decrypt and recover K_S

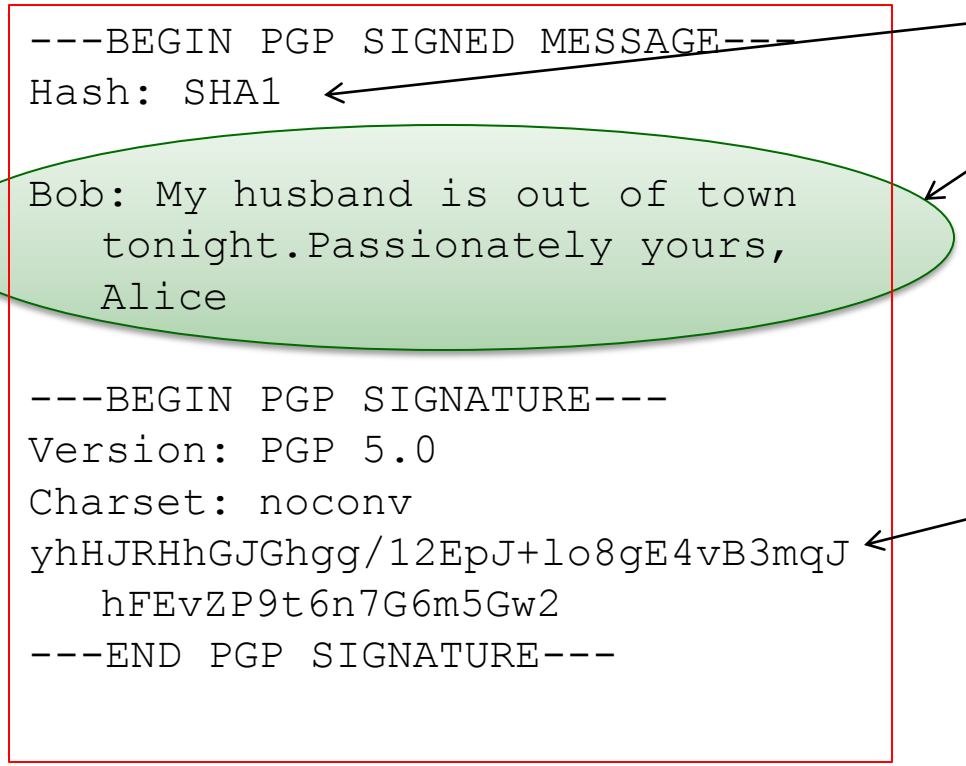
- uses K_S to decrypt $K_S(m)$ to recover m

Why symmetric keys?

- Why is a symmetric key used in most protocols to encrypt a data payload (the message etc.), even if a public/private key infrastructure exists?

- Public/Private keying more costly
- Minimal use of public/private key minimizes the key exposure
  - Symmetric key can be generated each time on the fly and is therefore always fresh
  - Public/Private key is always the same. Encrypting large amounts of data could compromise the key... (although no efficient algorithm is known yet)

PGP E-Mail signature



Used crypto hash

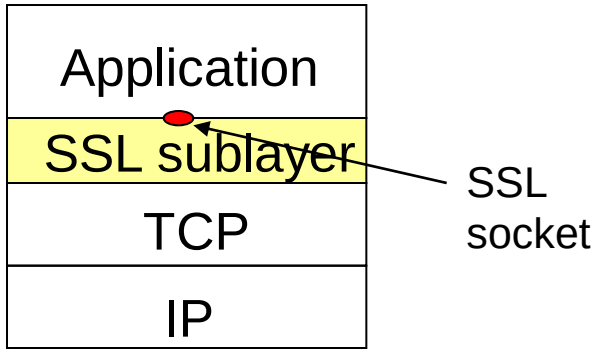
Message m that is hashed with SHA1

Real signature: This is the hash of the message (H(m)) encrypted with Alice's private key.

Verification: Bob decrypts the PGP signature and obtains H(m). Additionally he computes H(m) for the message himself and computes it with the H(m) Alice computed.

SSL

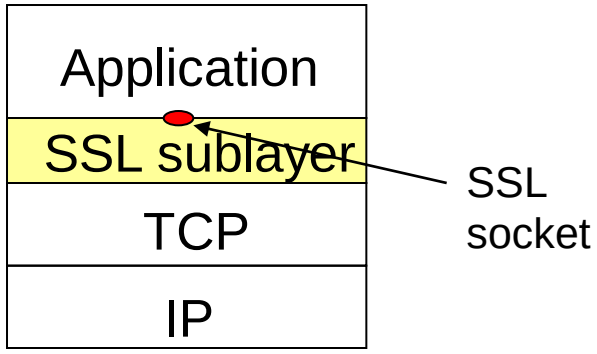
- What are the three main phases of SSL?
  - 1. Handshake (TCP connection, authentication + master secret generation)
  - 2. Key derivation
  - 3. Data transfer
- On what layer does SSL reside and why is that advantageous?
  - provides transport layer security to any TCP-based application using SSL services.



TCP enhanced with SSL

SSL

- What are the three main phases of SSL?
  - 1. Handshake (TCP connection, authentication + master secret generation)
  - 2. Key derivation
  - 3. Data transfer
- On what layer does SSL reside and why is that advantageous?
  - provides transport layer security to any TCP-based application using SSL services.



TCP enhanced with SSL

IPsec

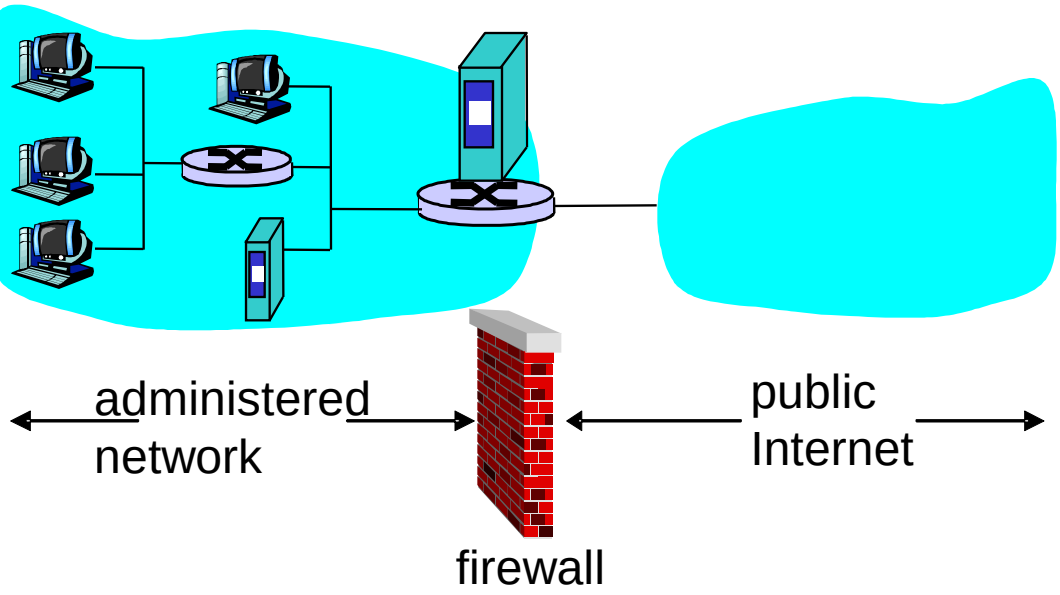
- Please sketch one typical scenario, where IPsec is used today.
  - VPN gateway at company or university. E.g. 134.76.22.1 is the VPN Gateway for the GWDG
- What are the two main protocols used in IPsec and what is their primary difference with respect to security properties?
  - Authentication Header (AH): Ensures authentication and data integrity. No encryption!
  - Encapsulated Security Payload (ESP): Ensures authentication, data integrity and encryption.

802.11i

- Should ensure better protection than WEP
  - WPA is a subset of 802.11i
- Who is handling the authentication information in an 802.11i scenario?
  - Using TLS-EAP (Extensible Authentication Protocol over Transport Layer Security) to contact an AAA (Authentication, Authorization, Accounting) Server

Firewalls

- What is the purpose of a firewall and what are filter rules?
  - Isolation of own network from internet!



Filter rules

- The firewall can be configured to only let certain packets pass. An administrator could be interested in setting up rules like:
  - No telnet connections to hosts behind the FW
  - Prevent outside machines to connect to inside machines, but still inside machines can connect to outsiders
  - Prevent web radios
  - Many more…

Thank you

Any questions?