Internet Security Protocols

Panko Chapter 9 p349 – 354, Chapter 3 p129-133 also these slides (adapted from 2015 slides) and the standards

Panko and Panko
Business Data Networks and Security, 10th Edition, Global Edition

Overview

- Why Internet security
- Layered view of network security
  - Application Layer: Electronic mail security (PGP, S/MIME), Web Payments, HTTPS
  - Transport Layer: SSL (Secure Socket Layer) and TLS (Transport Layer Security)
  - Internet Layer: IPSec and VPNs
- Data link and physical layer security not here
  - Provided by telephony/ Ethernet/ wifi standards

2

Why Internet Security

- More and more business activities are conducted over the Internet.
- More and more computers are connected to the Internet.
- More hackers (easy access to the Internet with lower cost).

3

Application Layer Security

- Electronic mail security – PGP (pretty good privacy)
  - Initially developed by Philip R. Zimmermann in 1991.
  - Uses a public key cipher to encrypt a session key.
  - Uses a secret key cipher with the session for data encryption.
  - Uses a public key ring and a private key ring for key management.
  - Users can choose to have confidentiality only, authentication only, or both.

5

PGP Cryptographic Functions

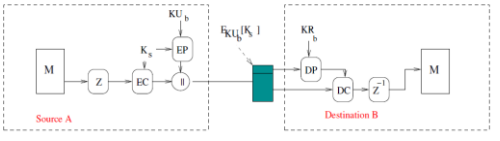
Explanation of symbols used in the next three figures

- M plain message
- K_s session key used in conventional (symmetric key) encryption
- KR_a private key of user A
- KU_a public key of user A
- EP public-key encryption
- DP public-key decryption
- EC conventional (symmetric) encryption
- DC conventional (symmetric) decryption
- H hash function
- || concatenation
- Z compression using ZIP algorithm

Data	Processes

6

PGP for Confidentiality only

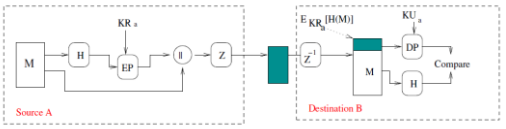


M plain message
Ks session key used in conventional (symmetric key) encryption
KRa private key of user A
KUa public key of user A

EP public-key encryption
DP public-key decryption
EC conventional (symmetric) encryption
DC conventional (symmetric) decryption
H hash function
|| concatenation
Z compression using ZIP algorithm

7

PGP for Authentication (+non-repudiation) only

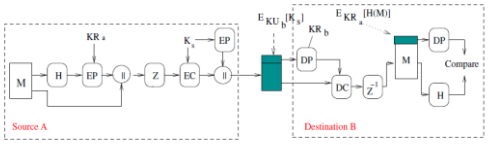


M plain message
Ks session key used in conventional (symmetric key) encryption
KRa private key of user A
KUa public key of user A

EP public-key encryption
DP public-key decryption
EC conventional (symmetric) encryption
DC conventional (symmetric) decryption
H hash function
|| concatenation
Z compression using ZIP algorithm

8

PGP for Confidentiality and Authentication



M plain message
Ks session key used in conventional (symmetric key) encryption
KRa private key of user A
KUa public key of user A

EP public-key encryption
DP public-key decryption
EC conventional (symmetric) encryption
DC conventional (symmetric) decryption
H hash function
|| concatenation
Z compression using ZIP algorithm

9

Application Layer Security

- Electronic mail security – S/MIME (Secure Multi-Purpose Internet Mail Extensions) v3.2 RFC5751 2010
  - Security enhanced version of MIME Internet email content type standard.
  - Targeting an industry standard; built in to most email clients.
  - Compared with PGP, format more fixed (less flexibility).
  - Utilizes X.509 protocol for key management.
- S/MIME versus PGP
  - PGP is a protocol on top of normal email applications (SMTP), while S/MIME is security enhanced version of normal MIME.
  - PGP is designed to be more flexible, while S/MIME tends to be more standard.
  - PGP uses its own PKI while S/MIME uses X.509 as its PKI.

10

Application Layer Security: HTTPS

- HTTPS is essentially HTTP over the Transport Layer security protocol called SSL/TLS
- Appears as a *scheme* in a URL
- Uses port 443, not 8
- One-way: authentication of server + two-way confidentiality
- HTTP is being phased out to be replaced by HTTPS

13

Strict-Transport-Security

HSTS: HTTP Strict Transport Security RFC 6797

- The "SSL stripping attack" works by a man-in-the-middle transparently converting a secure HTTPS connection into a plain HTTP connection.
- The host declares "Strict-Transport-Security" in HTTP header response.

```
2.  HTTP Strict Transport Security Policy Effects

The effects of the HSTS Policy, as applied by a conformant UA in
interactions with a web resource host wielding such policy (known as
an HSTS Host), are summarized as follows:

1.  UAs transform insecure URI references to an HSTS Host into secure
    URI references before dereferencing them.

2.  The UA terminates any secure transport connection attempts upon
    any and all secure transport errors or warnings.
```

https://tools.ietf.org/html/rfc6797

14

Migration: Update Insecure Requests

- W3C Candidate Rec October 2015
- HSTS is too strong for an upgrade path
- Aims to encourage move to HTTPS without needing to rewrite all the site's URLs
- Unlike HSTS, serves secure resources to clients that support upgrades, while insecure resources work for clients that don't.
- Defines response header field
  - Content-Security-Policy: upgrade-insecure-requests
- Like HSTS, Browser is supposed to rewrite http URLs in response page to https URLs.

15

Application Layer: W3C Web Payments

- Want the payment process to be managed in the browser so the client chooses the payment provider (e.g. their own bank) rather than the server
- Published first working drafts last week
  - Payment Request API
  - Payment Method Identifiers
  - Basic Card Payment
  - No security yet….

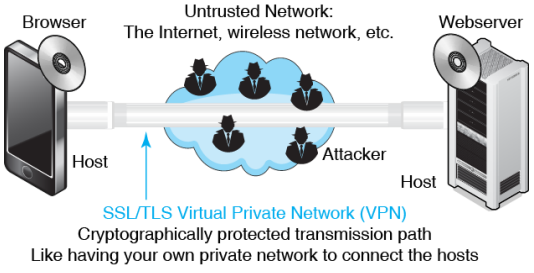
16

Transport Layer Security-- TLS

- TLS 1.2 RFC 5246 2008
  - Netscape specified Secure Socket Layer (SSL) protocol; broadly adopted.
  - Modified by Internet Engineering Task Force (IETF) as an Internet Standard, called **Transport Layer Security** (TLS). Commonly called "SSL"
- TSL services
  - Data encryption
  - message integrity
  - server authentication
  - client authentication

18

3.14 SSL/TLS Host-to-Host VPN



TLS Sub-protocols

- Essentially two sub-protocols, used in every session:
  - TLS Record Protocol, provides security services for various higher layer protocols.
  - TLS Handshake Protocol, making connections to remote machine.
- Other associated sub-protocols, invoked during SSL connection, and may not be used in every session:
  - TLS Alert Protocol, notifying errors.
  - TLS Change Cipher Spec Protocol, changing session key.

20

TLS Handshake

- The client sends the server its TSL version no, cipher settings and other data.
- The server sends the client similar info and its certificate.
- The client uses the server certificate to authenticate the server. If it can't, the problem is made known to the user.
- The client generates a random symmetric key and encrypts using the server's public key. Sends to server. Sends client authentication info, if required.
- The server may try to authenticate the client (if required). Client and server independently use the pre-master secret to generate a master secret. Client sends a 'change cipher spec' message to the server. Sends a 'finished' message encrypted with the new cipher.
- The server responds with a 'change cipher spec' and 'finished' message as well.
- The TSL Handshake is complete.

21

Heartbleed Security Attack, April 2014

- Security bug in OpenSSL cryptography library, a widely used implementation of the Transport Layer Security (TLS) protocol.
- Arose from improper input validation (due to a missing bounds check or buffer overrun)

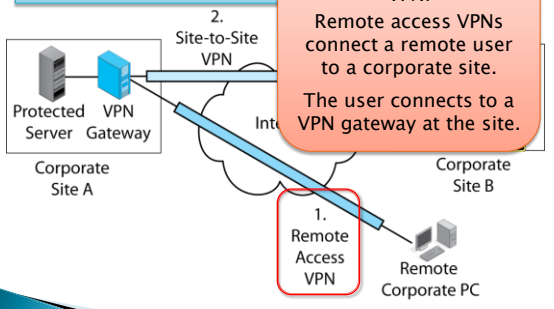
22

IP Layer Security

- IPSec RFC 2401 2005 dominates IP layer security protocols.
- Provides general purpose security services.
- Both encryption and authentication can be provided.
- Important use in VPNs

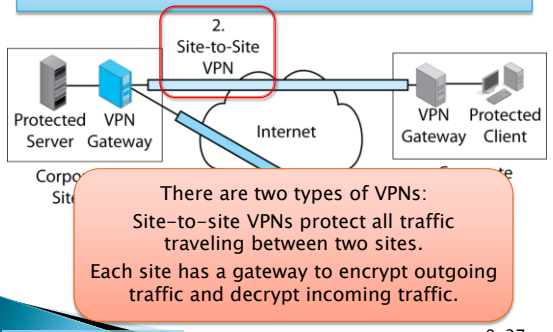
23

9.8: VPNs



9-26

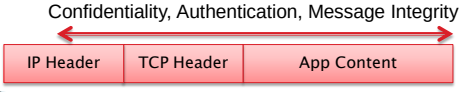
9.8: VPNs



9-27

IPsec VPNs

- Governed by the IPsec protocols
  - Operate at the internet layer
  - Protect transport header, application content, and at least some IP header content.
  - Protection is transparent. Upper-level content does not even know that it is being protected



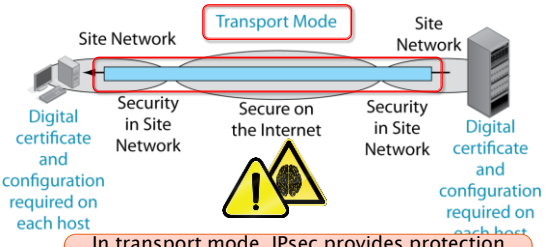
9-28

9.9: IPsec in Transport and Tunnel Modes

- IPsec has two modes (ways) of operating:
  - Transport mode
  - Tunnel mode
- Both are IPsec
- Each mode has strengths and weaknesses

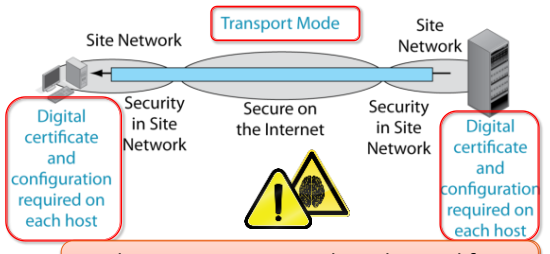
9-29

9.9: IPsec Transport and Tunnel Modes



9-30

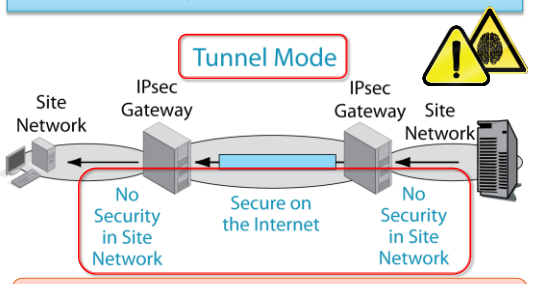
9.9: IPsec Transport and Tunnel Modes



The IPsec Transport mode is also used for remote client-to-site VPN

9-31

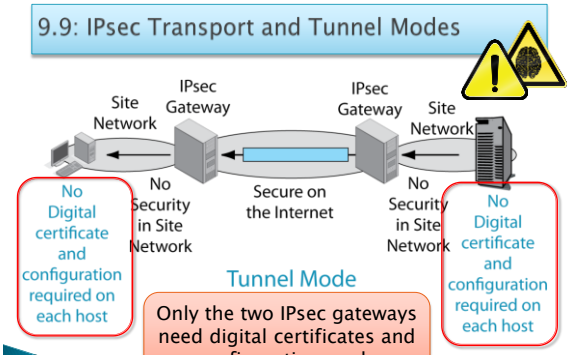
9.9: IPsec Transport and Tunnel Modes



In tunnel mode, IPsec only provides protection over the Dangerous Internet—not within site networks.

9-32

9.9: IPsec Transport and Tunnel Modes



Only the two IPsec gateways need digital certificates and configuration work.

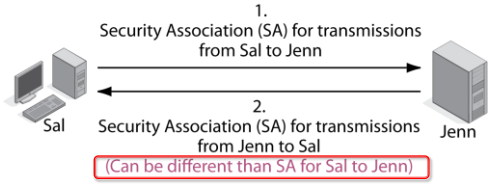
9-33

9.9: IPsec Transport and Tunnel Modes

Criterion	Transport Mode	Tunnel Mode
Security	Better because it provides host-to-host protection. But firewalls cannot read encrypted traffic.	Not as good because it only provides security over the Internet or another trusted network (a wireless network, etc.).
Cost	Higher because of configuration work on each host.	Lower because IPsec operates only on the IPsec gateway .

9-34

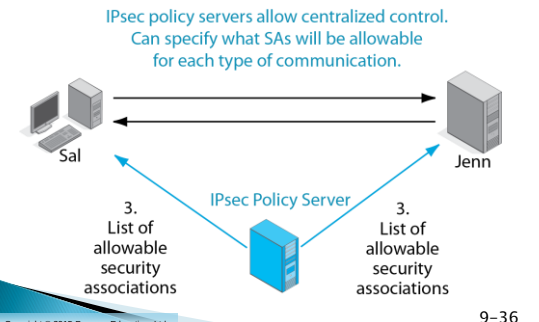
9.10: IPsec Security Associations and Policy Servers



An IPsec security association (SA) is an agreement about what security methods and options the two hosts or two IPsec gateways will use during their communication.

9-35

9.10: IPsec Security Associations and Policy Servers



9-36

9.11 IPsec vs. SSL/TLS VPNs

Characteristics of	IPsec	SSL/TLS
Standards Organization	IETF	IETF (created by Netscape as SSL, renamed TLS by the IETF)
Layer	Layer 3	Layer 4
Built into Browsers, Webservers, and Mail Servers, So Protects These Applications at Little or No Cost	No	Yes

9-37

9.11 IPsec vs. SSL/TLS VPNs

Characteristic	IPsec	SSL/TLS
Can protect any application	Yes (also protects transport-layer header and some of the IP header)	No (Only SSL/TLS-aware applications such as web and e-mail)
Type of VPNs Supported in the Standard	Host-to-Host Remote Site Access Site-to-Site	Host-to-Host

9-38

9.11 IPsec vs. SSL/TLS VPNs

Characteristic	IPsec	SSL/TLS
Strength of Security	Excellent	Good
Security can be Managed Centrally	Yes	No

9-39

Why IPsec is Not Enough

New. Not in the book.

- IPsec provides security to application content transparently
- Makes protection automatic
- However, this means that the application cannot tell if it is being protected
- So the application designer often requires SSL/TLS in order to be sure

9-40

Next Week

- Wireless Networks Ch 6 and Ch7
- TCP/IP revisited Ch 8 & Ch 9
- Following week
  - Ethernet Ch 5
  - Guest Lectures and Review

41