Cryptography on the Internet

Cryptography in TCPIP  
Key Concepts  
-MAC  
-Cas  
Transport Layer Cryptography (TLS)  
Network Layer Crytpography (IPSec)

Application Layer Security – PGP  
Transport Layer – SSL  
Network Layer – IPSec  
Network Access Layer – Switch Port, WEP

Roles of Cryptography  
-Transactions must be authenticated and confidential – Address information, details must be kept confidential  
Normally done at transport layer with Transport Layer Security (TLS)

-Two geographically separated networks.  
-Create dedicated WAN link (very expensive)  
OR  
-Public internet with VPN – Messages travelling via VPN encrypted for authentication and confidentiality. Either application layer VPNs or SSL VPNs, or IP layer with IPSec

VPNs –  
Virtual Encrypted Connections - Transmit private data across a public network while maintaining confidentiality and authenticity  
Encrypt TCPIP Packets  
Packet encrypted before IP header added  
Table of encryption algorithms and keys  
IPSec in transport mode (CISCO easy VPN)  
Tunnelling (IPSec in tunnel mode)  
-Greater chance of fragmentation & increased size, hence slower speeds

Key Concepts:  
- Symmetric Cryptosystems -  
-- One key for encryption and decryption (DES,AES,Red Pike)  
-- Fast & energy efficient  
-- Problem of secure key distribution  
- Public Key Cryptosystem -  
-- One key for encryption, one for decryption (RSA, ECC)  
-- No need for secure key exchange  
--Slower, requires more computation, less energy efficient  
-Combined Approach -   
-- (A) sends RSA public key to (B) over internet  
-- (B) chooses AES key  
-- (B) RSA encrypts key using (A) public key  
-- Sends encrypted key  
-- (A) uses own private key to decrypt AES key  
-- (B) AES-encrypts document  
-- Sends encrypted document to (A)  
-- (A) receives encrypted document and AES-decrypts it  
----  
-- Used in email security, PGP, TLS, IPSec, Diffie-Helman Algorithm

Hashing as an Integrity Check  
-Sender sending data. Sender wants to validate information. Puts data through hash function to create message digest. Digest goes into insecure channel and transmitted. Receiver hashes the data and compares his message digest to received message digest.

Message Authenticatin Code  
- A MAC is a “keyed hash”  
Data catenated with a MAC key and then hashed

Common MAC Algorithms  
HMAC (with SHA-1), CMAC(3DES)

Confidentiality and Authentication  
Encryption with public key provides confidentiality   
Encryption with private key provides authentication and non-repudiation  
- Proves origin (digital signature)  
- Fool’s Paradise problem

Certification Authority  
-Signs public keys using its own private key (Digital Certification)

TLS  
- Authenticated and encrypted communication between client and server  
Originally SSL  
IETF standard TLS  
Between Application Layer and Transport TCP Layer

TCP Socket (part of an API, represents a TCP connection(IP address and PORT)  
TCP Socket communicates not with application layer but a TLS sub-layer that has a TLS socket that communicates with the application layer – programmer now uses TLS API

TLS Architecture   
Application Data stream enters TLS session “pipe”, runs inside a TCP session “pipe”

SYN, SYN-ACK, ACK TCP Connection Handshake  
Hello + Algorithm List + Client Nonce, Algorithm Selected + Digital Certificate + Server Nonce, Encrypted Pre-Master Secret TLS Connection Handshake

Each side computes the master secret  
PMS + Server Nonce + Client Nonce = Master Secret  
Each side splits MS ito four different keys  
2 “E-keys” = used for encryption for confidentiality  
2 “M-keys” = used for authentication

Application Data Stream divided into “records”  
TLS Header (TLSH) added to each record. Start/end handshake or data transfer, Version, Length  
Record+M-key into MAC Function, stuck at the end as a MAC.  
Record+MAC+E-Key into Symmetric cipher to be encrypted  
TLSH+Encrypted Record goes into TCP Layer and encapsulated into segment with TCP Header  
TCPH|TLSH|Record|+M-key|+E-key|  
  
Order is reversed to be decrypted

Network Layer Cryptography  
IPSec Network Layer confidentiality and authentication encryption  
Inserts additional IPSec header between regular IPHeader and Segment  
Payload field encrypted/decrypted at IP layer (3)  
Invisible to transport layer   
Optional in IPv4, Standard in IPv6

IPSec mechanisms  
Authentication Header(AH) - Authentication  
Encapsulated Security Payload(ESP) – Authentication and Confidentiality  
Transport Mode (between end-hosts), Tunnel mode (between routers)