8 Security

8.1 Introduction to Cryptography

Symmetric Cryptography

Tool used	Same key for encryption and decryption
Advanced Encryption Standard (AES)	• Uses AES • Provides confidentiality • Does not provide integrity (message can be changed by decrypting)
Disadvantages	• Key distribution ⇒ Key must be shared secretly through a secured channel • Scalability ⇒ Requires $\binom{n}{2}$ for n users
Conclusion	✓ Confidential ✗ Integrity

Public Key Cryptography (or Asymmetric)

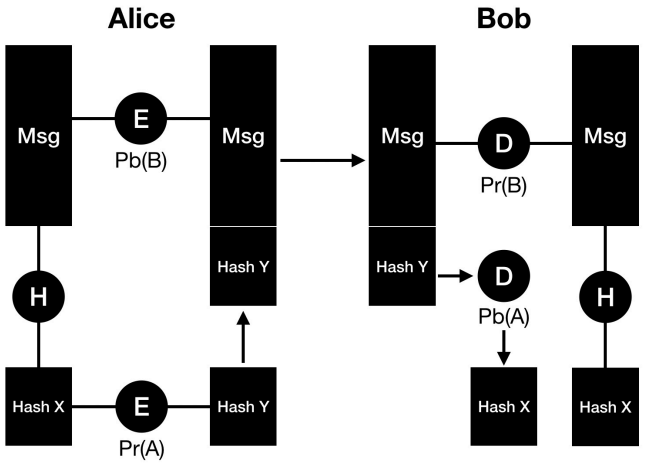
Tool used	A pair of keys – public key and private key
Process	• X encrypts message with Y's public key • Y decrypts X's message with Y's private key • Message encrypted with public key can be decrypted with private key (and vice versa)
Problem	Key sizes are huge (inefficient) • Need to generate lots of keys
Solution	Hybrid scheme • Uses key derivation function to generate a shared secret using two key pairs
Conclusion	⇧ Confidentiality ✗ Integrity

Cryptographic Hash Functions

Tool used	Mapping variable length to fixed length of message
Properties	• One-way property ⇒ Can move from actual message to hash but not has to actual message • Collision resistance ⇒ Two messages can't use same hash
Hash Functions	• MD5 (Integrity) • SHA-256 • SHA-384 • SHA-512
Conclusion	✓ Authentication

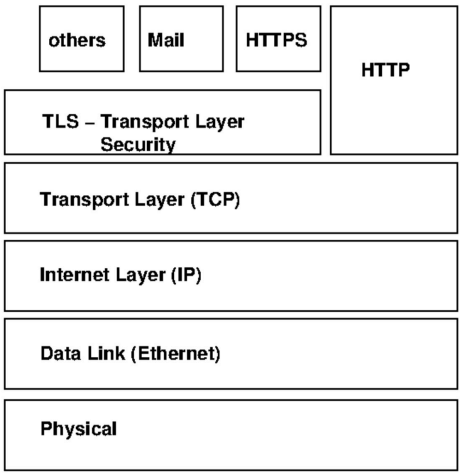
Complete Security Encryption

	Alice	**Bob**
Confidentiality	Encrypted with Pb(B)	Decrypted with Pr(B)
Integrity	Pass through Hash Function to get Hash X	
Authentication	Encrypt Hash X with Pr(A) to get Hash Y	Decrypt Hash Y with Pb(A) to get Hash X
	Both Hash X are the same	



8.2 Security Protocols and Firewall

Transport Layer Security (TLS)



Function	To establish a shared key to exchange messages (Confidentiality, Integrity, Authentication)
TLS Protocols	
TLS Handshake	Authenticate server and client. Result: • A shared key • Session ID / ticket
TLS Record	After the exchange of ChangeCipherSpec messages, all traffic is encrypted
TLS Alert	Immediately closes a session

Certificates

Properties	• Provide additional info for public key (authenticity) • Signed by known certificate authority
Problems	• Certificates revocation • Users accept certificates with errors • New policies are stricter

Virtual Private Network (VPN)

- Logically connects a client to a network via encrypted channel
- Tunnels created by TLS, IPSec
- Security at the tunnel endpoints (client & gateway)

IPSec

Function	Authenticate and encrypt each IP packet
Transport Mode	IP packets are encrypted, integrity protected.
Tunneling Mode	Complete IP packets are encrypted and contained in a new IP packet with new header [filter old header] (putting envelope in envelope)

Firewall and Packet Filter Firewall

	Firewall	**Packet Filter Firewall**
Description	Barrier between networks	Operates on network layer & filters packets
Method Used	Traffic filtering	Static filtering
Based On	Security rules (what can & can't enter)	Address, protocols, ports, & connection stage

Optimized Firewall Location

User: Method	**Details**
Home: Router	• Router acts as firewall
Enterprise: Demilitarized Zone (DMZ)	• Proper placing in a company network is complicated • DMZ is zone between two firewalls • Less secure than internal network (high security) • Prevents users from direct access to internal network • Allow access to DMZ
	Filtering outgoing traffic: • Prevent malicious software to send out data • Block IP spoofing • Logging of denied outbound traffic can detect infections

Firewall Proxies and NAT

Feature	Function
Network and Port Address Translation (NAT)	Hide internal network IP address from outsiders
Proxies (like HTTP)	Hide IP of individual devices in internal network to communicate with devices out of proxies

IDS (Detection) & IPS (Prevention)

IDS	IPS
• Monitors network or system activities • Alerts when potentially malicious activity found • Logs information about activity	
-	Block or stop malicious activity

Security Properties

Property	Description
1. Authenticity	Data comes from the person that we expect
2. Integrity	Data must not be changed
3. Confidentiality	Data only known to specific people
4. Privacy	Protect personal information
5. Availability	Service can be used at a particular time
6. Safety	Service must be safe at all times

Security Attacks

Attacks	Description
Phishing	• Create a fake website • Attacks take info entered by user (login details)
Ransomware	• Install malware that encrypts all data • Ask for money to remove malware
Botnets	• Malware combines all devices to a central point • Remotely control to gather information (camera, keystrokes, access info) • Can run Denial of Service Attacks (DDoS)

Malware Types

Type	Description
Virus	• Injected to a program • Spread out when program is used
Worn	• Standalone malware • Uses weakness in the system to spread itself
Trojan	• Hidden malware • Allowing attackers to access different aspects

Weakness Exploitation

Weakness	Description
Buffer Overflow	Program that causes the memory boundary to exceed (corrupts memory address)
Command Injection	Execute arbitrary shell commands
Cross-site Scripting (XSS)	Inject malicious code to a webpage remotely
SQL Injection	Attacking SQL databases