Computer Security and Cryptography

CS381

来学嘉

计算机科学与工程系 电院3-423室

34205440 1356 4100825 laix@sjtu.edu.cn

2016-05

Organization

- Week 1 to week 16 (2016-02-24 to 2016-06-08)
- 东上院502
- Monday 3-4节; week 9-16
- Wednesday 3-4节; week 1-16
- lecture 10 + exercise 40 + random tests 40 + other 10
- Ask questions **in** class – counted as points
- Turn ON your mobile phone (after lecture)
- Slides and papers:
  - http://202.120.38.185/CS381
    - **computer-security**
  - http://202.120.38.185/references
- TA: '薛伟佳' xue_wei_jia@163.com, '黄格仕' <huang.ge.shi@foxmail.com>
- Send homework to: laix@sjtu.edu.cn and to TAs

Rule: do not disturb others!

2

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions/MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- DDos
- Intrusion

Examples
- Bitcoin
- Hardware
- Wireless

contents

- IPSec
- VPN
- WLAN
- Quantum Crypto

TCP/IP Summary

- IP: network layer protocol
  - unreliable datagram delivery between hosts.
- UDP: transport layer protocol
  - unreliable datagram delivery between processes.
- TCP: transport layer protocol
  - reliable, byte-stream delivery between processes.

7 layers

OSI model
7. Application layer
NNTP ·SIP ·SSI ·DNS ·FTP ·Gopher ·HTTP ·NFS ·NTP ·SMPP ·SMTP ·SNMP ·Telnet ·DHCP ·Netconf ·RTP ·SPDY ·(more)
6. Presentation layer
MIME ·XDR ·**TLS** ·**SSL**
5. Session layer
Named pipe ·NetBIOS ·SAP ·PPTP ·SOCKS
4. Transport layer
TCP ·UDP ·SCTP ·DCCP ·SPX
3. Network layer
IP (IPv4, IPv6) ·ICMP **·IPsec** ·IGMP ·IPX ·AppleTalk
2. Data link layer
ATM ·SDLC ·HDLC ·ARP ·CSLIP ·SLIP ·GFP ·PLIP ·IEEE 802.2 ·LLC ·L2TP ·IEEE 802.3 ·Frame Relay ·ITU-T G.hn DLL ·PPP ·X.25 ·Network switch
1. Physical layer
EIA/TIA-232 ·EIA/TIA-449 ·ITU-T V-Series ·I.430 ·I.431 ·POTS ·PDH ·SONET/SDH ·PON ·OTN ·DSL ·IEEE 802.3 ·IEEE 802.11 ·IEEE 802.15 ·IEEE 802.16 ·IEEE 1394 ·ITU-T G.hn PHY ·USB ·Bluetooth ·Hubs

Security - OSI Layer

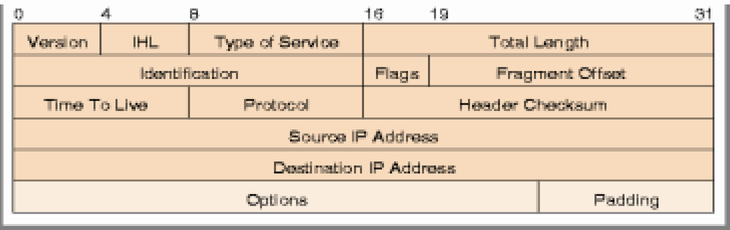
Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, https
Transport layer (TCP)	SSL, TLS, WTLS
Network layer (IP)	IPsec
Data Link layer	CHAP, PPTP, L2TP, WEP (WLAN), A5 (GSM), Bluetooth
Physical layer	Scrambling, Hopping, Quantum Communications

IPsec

- IPsec is a framework of open standards for ensuring private communications over public networks.
- It provides network layer security control,
- typically used to create a virtual private network (VPN).

IP Datagram

IPSec protects IP datagram



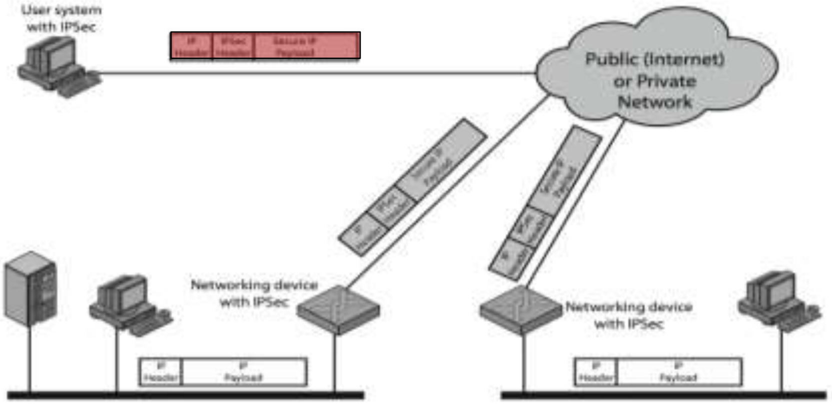
0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

Header

```
101010111010101010100101010101001010101001
110100101010100101011111110100000111011111
101000010111010101001101010111101000000101
001000000000101010000110100001111110101011
......... 10110110010101000110010010101 10
```

Data

☆ IPSec Uses



IPSec protects IP-datagram between user/LAN

Benefits of IPSec

- firewall/router provides security to all traffic crossing the perimeter
- firewall/router is resistant to bypass
- below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

☆ IP Security Architecture

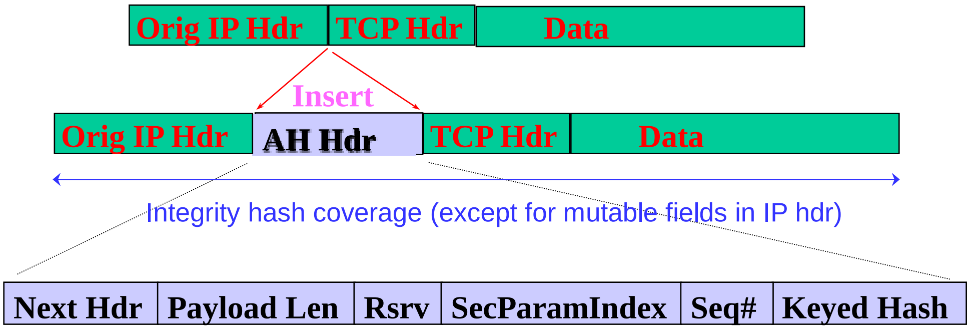
- specification defined in numerous RFC’s
  - incl. RFC 2401/2402/2406/2408, and many others
- mandatory in IPv6, optional in IPv4
- 2 security communication protocols with header extensions:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Key exchange protocol IKE（Oakley / ISAKMP)
- 2 database: security police SPD, security association SAD

Authentication Header (AH)

- provides data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

AH transport mode

- **insert AH after the original IP header and before the IP payload,**
- **typically used for end-to-end communication between two hosts.**



Orig IP Hdr | TCP Hdr | Data

Insert

Orig IP Hdr | AH Hdr | TCP Hdr | Data

Integrity hash coverage (except for mutable fields in IP hdr)

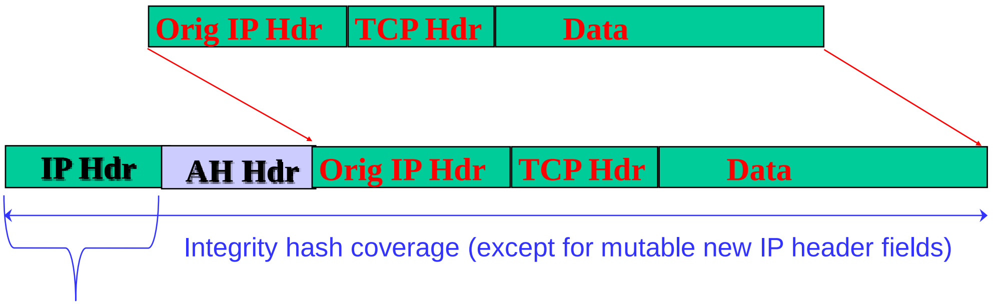
Next Hdr | Payload Len | Rsrv | SecParamIndex | Seq# | Keyed Hash

AH is IP protocol 51

24 bytes total

AH tunnel mode

- Tunnel mode provides protection to the entire IP,
- the entire IP packet is treated as the payload of new “outer” IP packet with a new outer IP header.
- Tunnel mode is used when one or both ends are a security gateway, such as a firewall or router.



Orig IP Hdr | TCP Hdr | Data

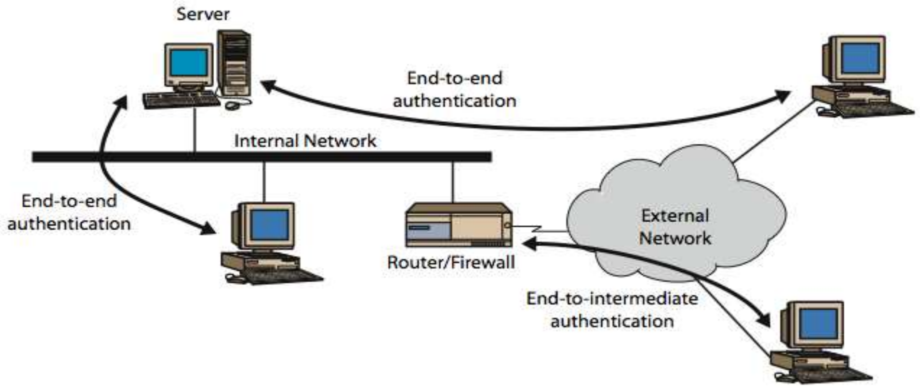
IP Hdr | AH Hdr | Orig IP Hdr | TCP Hdr | Data

Integrity hash coverage (except for mutable new IP header fields)

New IP header with source & destination IP address

Transport & Tunnel Modes

Transport mode: end-to-end

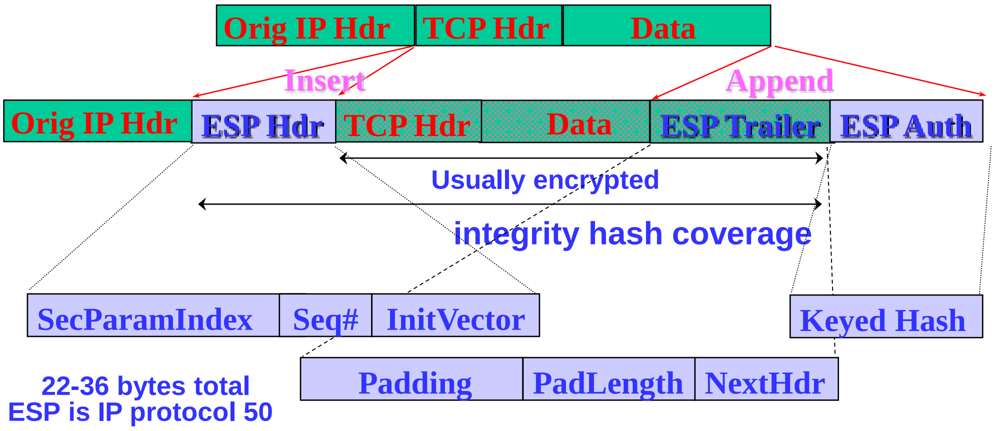

Server
End-to-end authentication
Internal Network
End-to-end authentication
Router/Firewall
External Network
End-to-intermediate authentication

tunnel mode: end-to-intermediate

Encapsulating Security Payload (ESP)

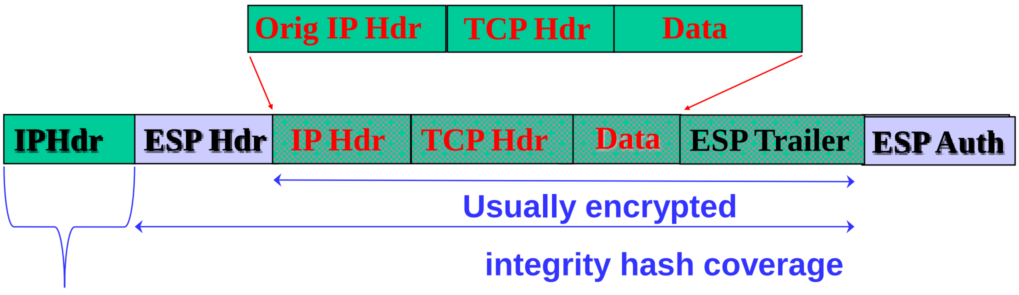
- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC & other modes
  - padding needed to fill blocksize, fields, for traffic flow

ESP transport mode



22-36 bytes total
ESP is IP protocol 50

ESP tunnel mode

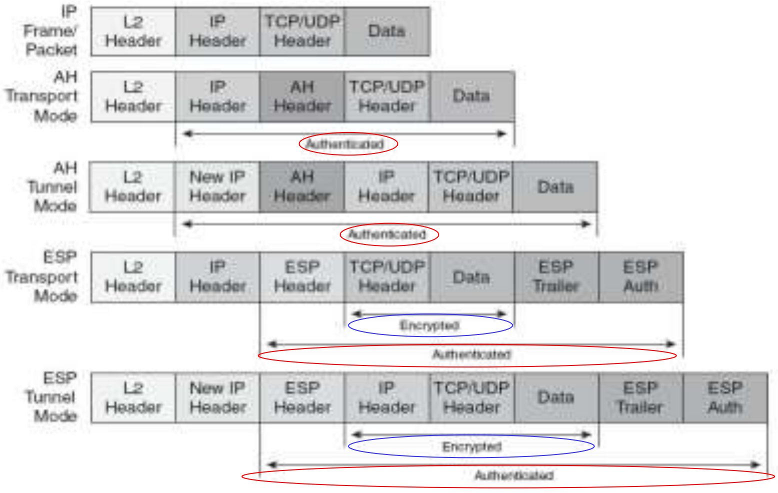


New IP header with source & destination IP address

Transport vs Tunnel Mode ESP

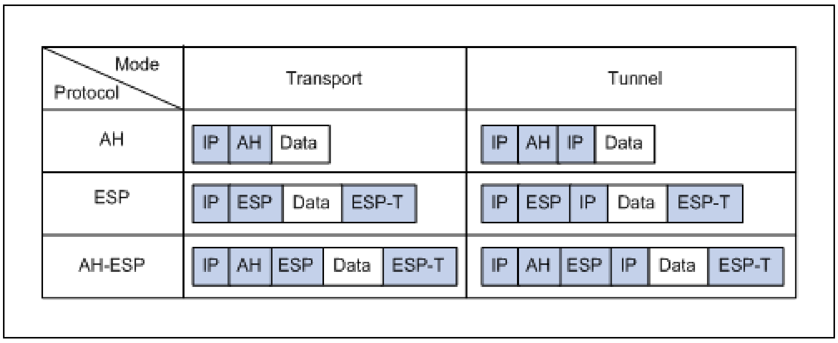
- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

☆ Security with AH/ESP



IP Frame/ Packet	L2 Header	IP Header	TCP/UDP Header	Data				
AH Transport Mode	L2 Header	IP Header	AH Header	TCP/UDP Header	Data			
AH Tunnel Mode	L2 Header	New IP Header	AH Header	IP Header	TCP/UDP Header	Data		
ESP Transport Mode	L2 Header	IP Header	ESP Header	TCP/UDP Header	Data	ESP Trailer	ESP Auth	
ESP Tunnel Mode	L2 Header	New IP Header	ESP Header	IP Header	TCP/UDP Header	Data	ESP Trailer	ESP Auth

Combined AH/ESP



Mode / Protocol	Transport	Tunnel
AH	IP | AH | Data	IP | AH | IP | Data
ESP	IP | ESP | Data | ESP-T	IP | ESP | IP | Data | ESP-T
AH-ESP	IP | AH | ESP | Data | ESP-T	IP | AH | ESP | IP | Data | ESP-T

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA’s in large systems
  - has Oakley & ISAKMP elements

Key Management

- Oakley
  - a key exchange protocol
  - based on Diffie-Hellman key exchange
  - adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
  - can use arithmetic in prime fields or elliptic curve fields
- ISAKMP
  - Internet Security Association and Key Management Protocol
  - provides framework for key management
  - defines procedures and packet formats to establish, negotiate, modify, & delete SAs
  - independent of key exchange protocol, encryption alg, & authentication method

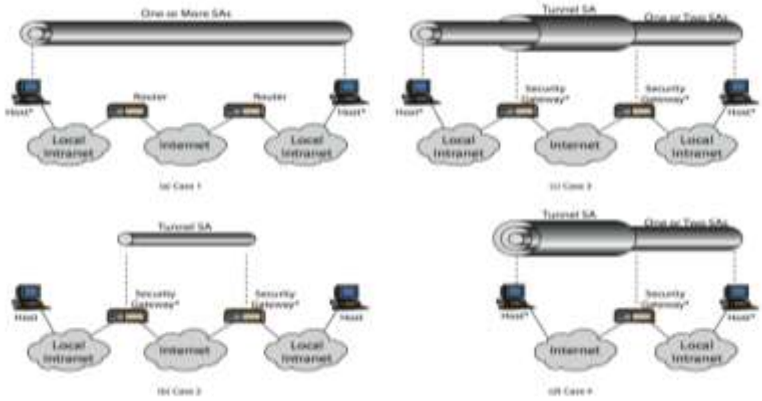
Internet Key Exchange (IKE)

- Security Association (SA)
  - A Security Association is a one-way relation established between two IPsec endpoints (hosts or security gateways).
  - Automatic negotiation of parameters to be used for the IPsec connection.
  - Separate IPsec SA required for each subnet or single host.
  - Separate IPsec SA required for inbound and outbound connection.
  - IPsec SAs are assigned a unique Security Parameters Index (SPI) and are maintained in a database.
- Negotiated Parameters
  - Authentication Mechanism (secret or public key, certificates)
  - Encryption Algorithm (mode, key length, initialization vector)
  - Hash Algorithm
  - Key values and key lifetimes
  - SA renewal period

Combining Security Associations

1. between end systems

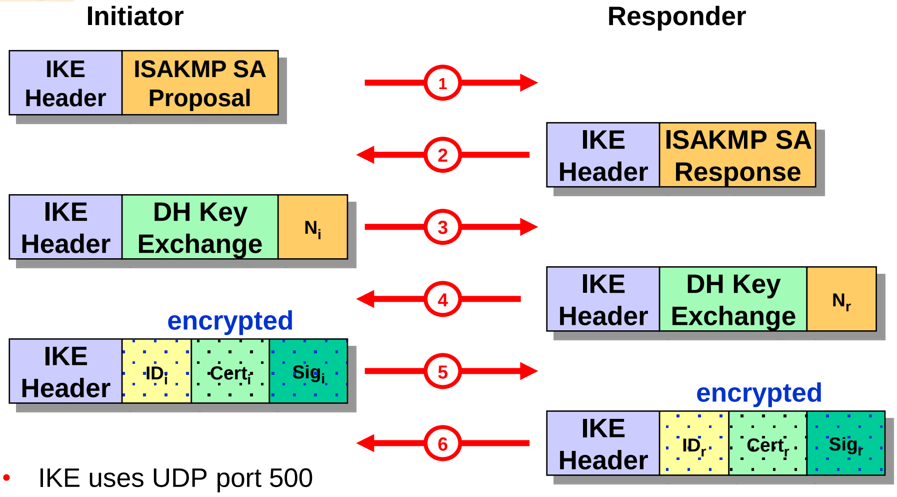
2. between gateways + **end-to-end security**



3. between gateways (router, firewall)

4. remote host uses the Internet to reach an organization’ s firewall and then to gain access to some server or workstation

Internet Key Exchange (IKE) – Main Mode



Initiator

Responder

1 IKE Header | ISAKMP SA Proposal →

2 ← IKE Header | ISAKMP SA Response

3 IKE Header | DH Key Exchange | N_i →

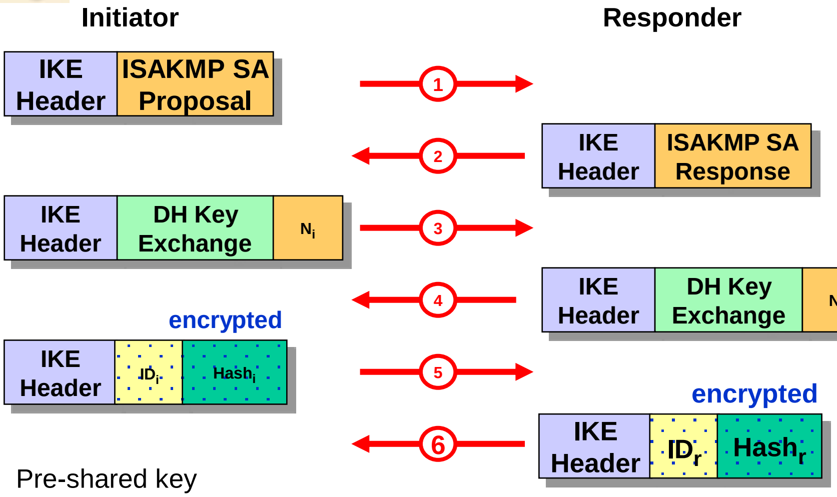
4 ← IKE Header | DH Key Exchange | N_r

5 encrypted: IKE Header | ID_i | $Cert_i$ | Sig_i →

6 ← encrypted: IKE Header | ID_r | $Cert_r$ | Sig_r

- IKE uses UDP port 500
- **IKE Quick Mode – 3 messages**

IKE Main Mode using Pre-Shared Keys



Initiator

Responder

1 IKE Header | ISAKMP SA Proposal →

2 ← IKE Header | ISAKMP SA Response

3 IKE Header | DH Key Exchange | N_i →

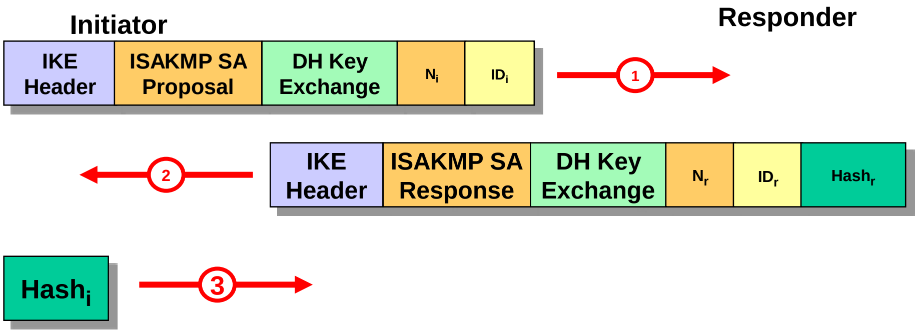
4 ← IKE Header | DH Key Exchange | N_r

5 encrypted: IKE Header | ID_i | $Hash_i$ →

6 ← encrypted: IKE Header | ID_r | $Hash_r$

- Pre-shared key
  - is worked into Hash
  - is part of the IKE session key

IKE Aggressive Mode using PreShared Keys



- Unencrypted IKE Aggressive Mode messages carrying cleartext IDs an be easily sniffed by a passive attacker.
- Pre-Shared Key is worked into $Hash_r$, together with other known parameters, so that an off-line cracking attack becomes possible.

VPN (virtual private network)

VPN extends a private network

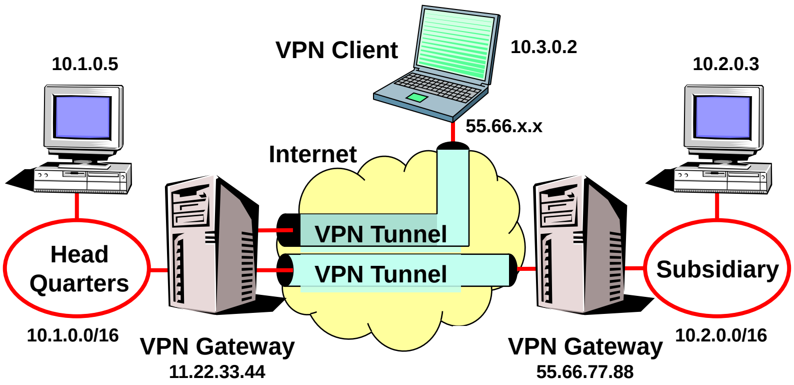
- – across public networks like the Internet.
- – It enables a host computer to send and receive data across shared or public networks
- – as if they were an integral part of the private network with all the functionality, security and policies of the private network.

•This is done by establishing a virtual point-to-point connection (IPSEC,SSL) through the use of dedicated connections.

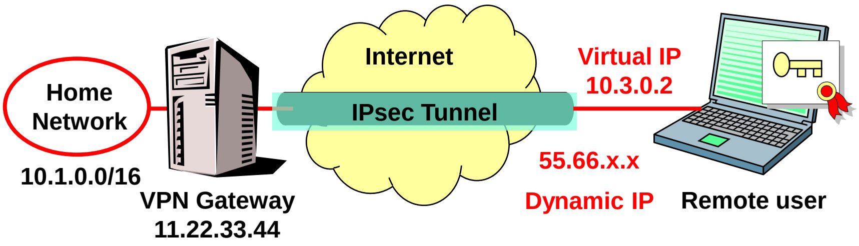
3 models for VPN

- **Gateway-to-gateway:** protects communications between two specific networks,
- **Host-to-gateway.** protects communications between a host and a specific network, typically used to allow hosts on unsecured networks, such as traveling user, to gain access to internal organizational services.
- **Host-to-host.** protects communication between two specific computers, often used when a user need to use or administer a remote system.

VPN (virtual private network)



Remote access via VPN



- Remote sign on to home network via IKE with varying IP addresses assigned dynamically by the local ISP.
- Authentication is usually based on RSA public keys and X.509 certificates issued by the home network.
- Virtual IP assigned statically or dynamically by the home network.

Host-to-host VPN

- **Host-to-host.** between two specific computers,
- a user need to use or administer a remote system.

SSL VPN

- An SSL VPN can be used with a standard Web browser.
  - In contrast to the traditional IPsec VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer.
  - It's used to give remote users with access to Web applications, client/server applications and internal network connections
- An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL/TLS
- NIST SP 800-113, Guide to SSL VPNs

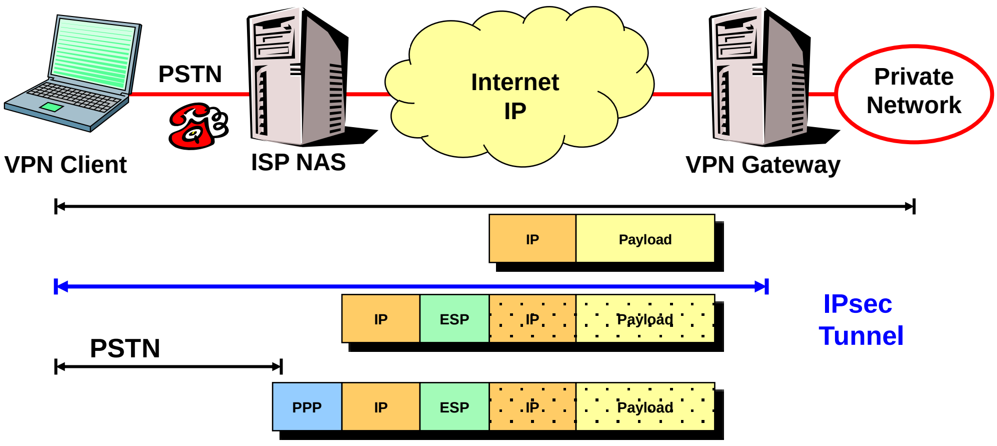
Two types of SSL VPNs

- SSL Portal VPN:
  - a single SSL connection to a Web site so the end user can securely access multiple network services.
  - The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any Web browser, authenticates to gateway and is then presented with a Web page that acts as the portal to the other services.
- SSL Tunnel VPN:
  - allows a Web browser to securely access multiple network services, including applications and protocols that are not Web-based, through a tunnel that is running under SSL.
  - SSL tunnel VPNs require that the Web browser be able to handle active content, provide functionality that is not accessible to SSL portal VPNs. Examples of active content include Java, JavaScript, Active X, or Flash applications or plug-ins.

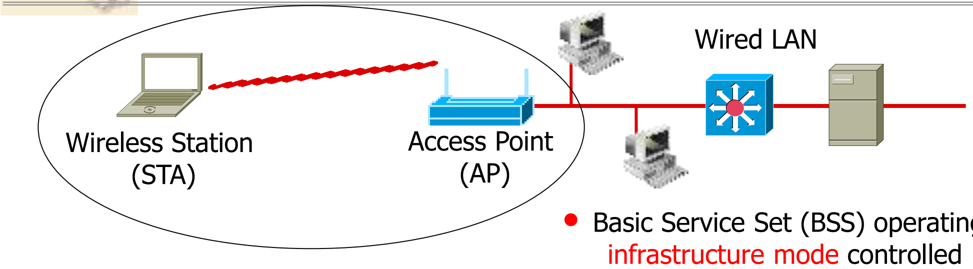
Layer -- VPN

Application layer	ssh, S/MIME, PGP, http digest
Transport layer	SSL, TLS, WTLS
Network layer	IPsec
Data Link layer	PPTP, L2TP, PPP, MPLS
Physical layer	Scrambling, Hopping, Quantum Communications

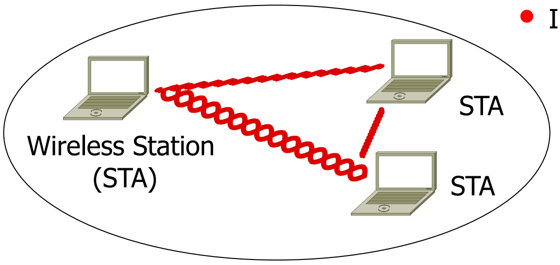
Layer 3 Tunnel based on IPSec



IEEE 802.11 WLAN Architecture



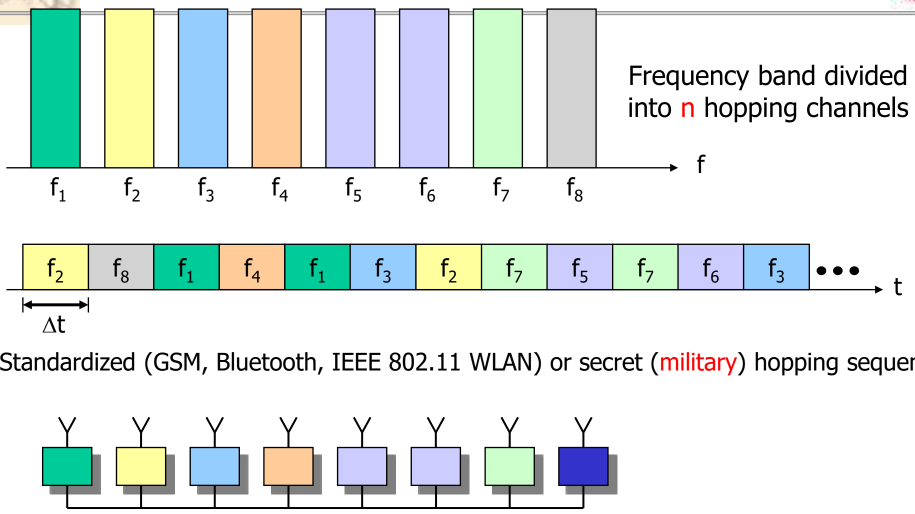
- Basic Service Set (BSS) operating in infrastructure mode controlled by access point
- Independent Basic Service Set (IBSS) operating in ad hoc mode forms a peer–to–peer network



Layer 1 Security

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, http digest
Transport layer	SSL, TLS, WTLS
Network layer	IPsec
Data Link layer	CHAP, PPTP, L2TP, WEP (WLAN), A5 (GSM), Bluetooth
Physical layer	Frequency Hopping, Quantum Cryptography

Layer 1 Security – Frequency Hopping


f_1
f_2
f_3
f_4
f_5
f_6
f_7
f_8
f
f_2 f_8 f_1 f_4 f_1 f_3 f_2 f_7 f_5 f_7 f_6 f_3 •••
t
Δt

Frequency band divided into n hopping channels

Standardized (GSM, Bluetooth, IEEE 802.11 WLAN) or secret (military) hopping sequence

Counter measures: e.g. n parallel receivers

Quantum Cryptography

- **Quantum key distribution**
- using quantum communication to establish a shared key between two parties
- Use one-time-pad to achieve unconditional security,
- Based on the properties of Quantum Physics
- Requires an additional authencated channal

Fundamental Laws of Quantum Physics

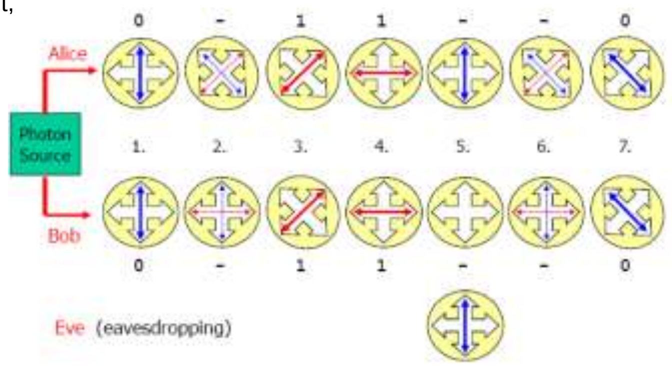
- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and in the diagonal basis.
- One cannot draw pictures of individual quantum processes.
- One cannot duplicate an unknown quantum state.

Quantum Key Exchange using Entangled Photons

For each photon measurement, choose filters (vertical-horizontal or diagonal) randomly and independently.

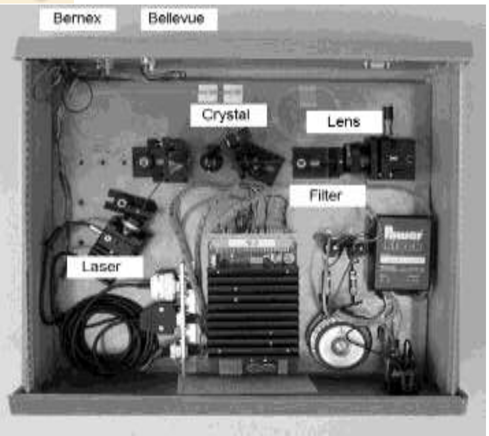
Alice and Bob exchange filter settings (not the measure result)

same settings: keep the bits as a secret key
Different settings: discard



If Eve listens (measure) on Bob's channel, then Bob will either not receive a photon or a duplicated photon, and the eavesdropping will be discovered.

Quantum Cryptography



- University of Geneva: Quantum correlation over
  more than 10 km (1990)
- 中科大：40 km (2008)

Summary

- IPSec
  - AH
  - ESP
  - IKE-key management
- Link layer and below
  - PPP
  - WLAN
  - Quantum
- Next part: computer security

Exercise 15

1. Draw the figures of IP-frame in transport mode:
   a) first ESP then AH
   b) first AH then ESP

2. Describe the different VPNs and their usage

- Deadline: before next lecture