CpE654 / NIS654
Design and Analysis of Network Systems

Security and Privacy Architecture

Reading Assignment!

McCabe's Book. - Chapter 9

Please **read the book** along with this presentation. **Chapter 4 onwards are important chapters that cover the core of the topic for this class**

Network Security and Privacy

- **Operational Security:** is the protection of network as a whole and their services from
  - unauthorized access,
  - modification,
  - destruction,
  - disclosure.
- **Network Privacy (Cryptograhy):** is a subset of network security, focusing on protection of networks and their services from unauthorized access or disclosure.
- **Message Security**: The network should protect the integrity of traffic:
  - Message Confidentiality (only sender and receiver able to understand the content)
  - Message Integrity: Content has not been altered in transit.
  - Message Authentication: Both sender and receiver can confirm the identity of the other
  - Message Nonrepudiation: Sender can't deny sending the message.

The Classic Security Considerations

- **Protecting Integrity:** to ensure
  - ➢ Modifications are not made to data by unauthorized personnel or process.
  - ➢ Unauthorized modification are not made to data by authorized personnel or process.
  - ➢ The data is internally and externally consistent. The internal information is consistent among all internal components and that the internal information is consistent with the real-world, external information.
- **Protecting Confidentiality:** to prevent the unauthorized disclosure of message contents.
- **Protecting Availability:** to ensure the reliable and timely access to data, computer, and network resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when needed.

Developing a Security and Privacy Plan

- There are different network security techniques and technologies.
- In order to develop a security and privacy plan, information from the threat analysis is needed to help us decide how much security we should have in our network.
- In general, we should avoid implementing securities mechanisms just because they are interesting or new.

Developing a Security and Privacy Plan

In developing the security architecture, you should determine what problems your customer is trying to solve. This information can be:

- Clearly stated in the problem definition
- Developed as part of threat analysis
- Or you need to probe further

Common issues that are addressed by the security architecture are:

- What resources need to be protected
- What problems (threats) are we protecting against
- The likelihood of each problem (threat)

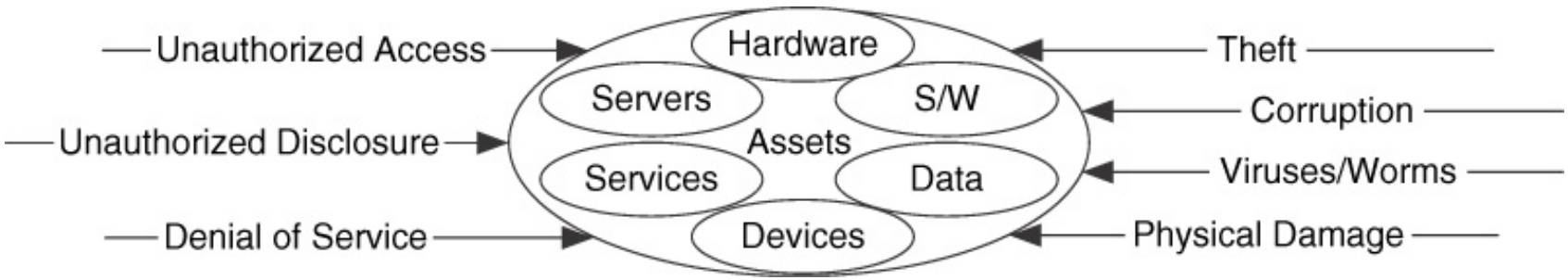
Threat Analysis

- A threat analysis is to determine:
  - which components of the system to protected
  - the types of security risk (threats) to protect them from.
- Threat Analysis determines locations in the network for implementation of security mechanisms

Threat Analysis
Assets to Consider for Protection

- User hardware (workstation/PCs)
- Servers
- Specialized devices
- Network devices (hubs, switches, routers)
- Software (operating system, utilities, and client programs)
- Services (applications, IP services)

•Data (local/remote, stored, archived, databases, and data in transit)



Type of Threats

- Unauthorized access to data, services, software, and/or hardware
- Unauthorized disclosure of information
- Denial of service
- Theft of data, services, software, and/or hardware
- Corruption of data, services, software, and/or hardware
- Viruses, worms, Trojan horses
- Physical damage.

Effect/ Likelihood	User Hardware	Servers	Network Devices	Software	Services	Data
Unauthorized Access	B/A	B/B	C/B	A/B	B/C	A/B
Unauthorized Disclosure	B/C	B/B	C/C	A/B	B/C	A/B
Denial of Service	B/B	B/B	B/B	B/B	B/B	D/D
Theft	A/D	B/D	B/D	A/B	C/C	A/B
Corruption	A/C	B/C	C/C	A/B	D/D	A/B
Viruses	B/B	B/B	B/B	B/B	B/C	D/D
Physical Damage	A/D	B/C	C/C	D/D	D/D	D/D

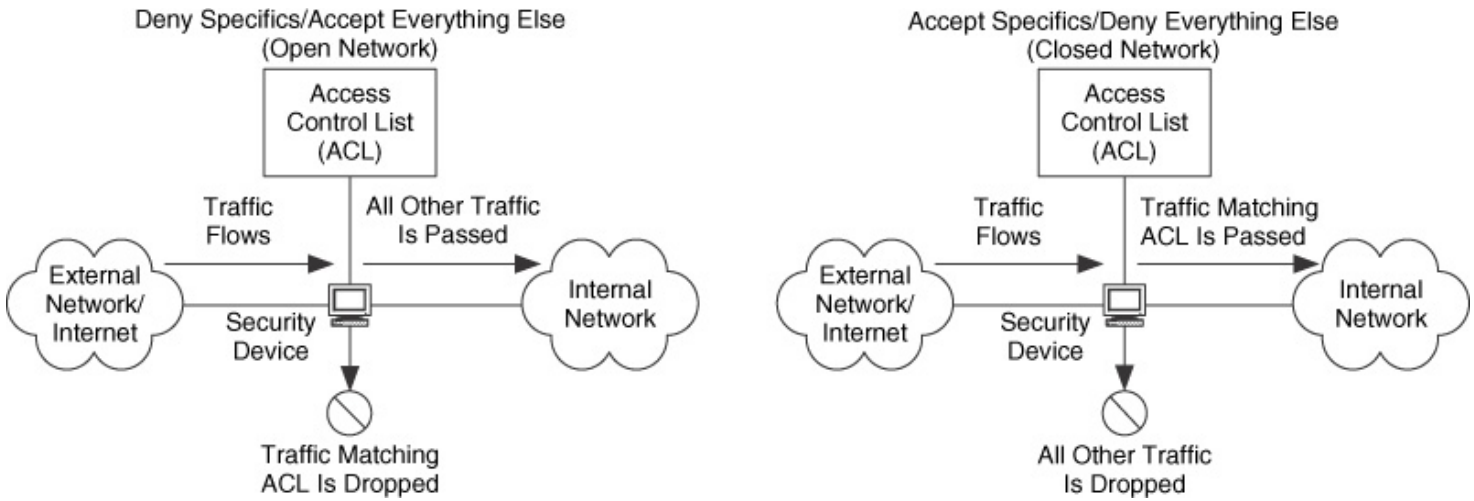
Effect:
A: Destructive B: Disabling
C: Disruptive D: No Impact

Likelihood:
A: Certain B: Likely
C: Unlikely D: Impossible

A list of threats and their impacts can be gathered in a worksheet for an environment which can help identifying the security needs for the environment.

Policies and Procedures

- These are formal statements on rules for access and use of the system, network and information.
- They represent organizations overall security policy
  - Open network philosophy; deny specifics, accept all else
  - Closed network philosophy: accept specifics, deny the rest. Requires deeper understanding of organizations security needs
- Access Control List (ACL)



Security and Privacy Mechanisms

- Several types of security mechanisms are available; however, not all mechanisms are appropriate for every environment.
- Mechanisms should be evaluated for the network, based on:
  - The degree of protection they provide
  - Their impact on users' ability to do work
  - The amount of expertise required for installation and configuration
  - The cost of purchasing, implementing, and operating them
  - The amounts of administration and maintenance required.

Network Security and Privacy

- Physical Security and Awareness
- Protocol and Application Security*
- Encryption/Decryption and Hash functions*
- Network Perimeter Security
- Remote Access Security*

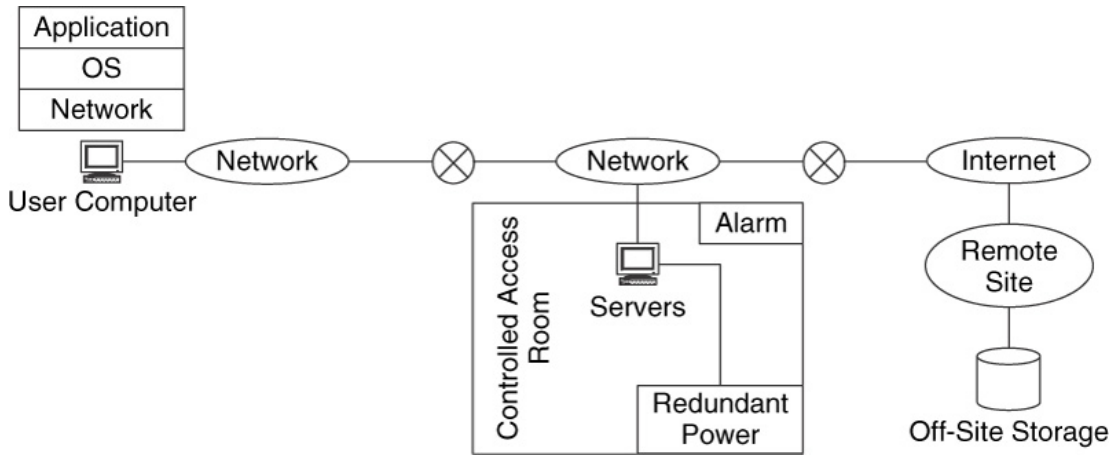
* Are complex areas and we only touch on them. Refer to a good book on network security (e.g., Cryptography and network Security by William Stallings)

Physical Security

Physical security is the protection of devices from physical access, damage, and theft.

Ways to implement physical security include:

- Access-control rooms for servers and network devices
- Backup power sources and power conditioning
- Off-site storage and archival
- Alarm systems for fire and illegal entry alarms



Security Awareness

Security awareness is getting users educated and involved with the day-to-day aspects of security in their network and helping them understand the potential risks of violating security policies and procedure.

Protocol and Application Security

Some common protocol and security mechanisms:

- IPSec at Network Layer
- SSL at Transport Layer
- PGP at Application Layer
- SNMP at Management Layer
- Packet Filtering

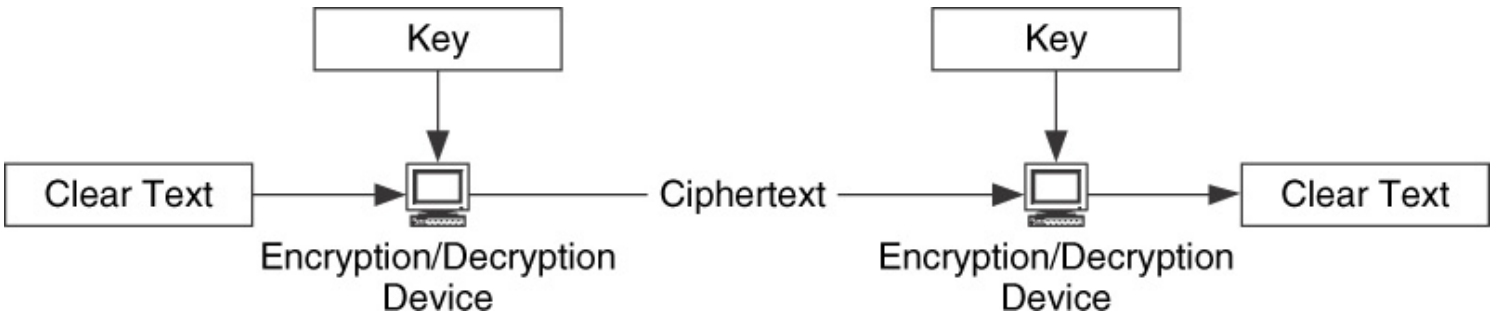
To better understand these mechanism, we enourage you to refer to a good source on network security

Encryption / Decryption

Encryption/decryption is a security mechanism in which cipher algorithm are applied together with a secret key to encrypt data to make it unreadable if intercepted.

There are different types of encryption/decryption mechanisms

However, the network performance (capacity and delay) is degraded from 15% to 85% in encryption/decryption due to overhead



Common Encryption/Decryption Methods

Symmetric Key: Between two parties. Examples are DES, Triple-DES, AES, and CBC (Cypher Block Chaining)

Public/Private Key: Example are Diffie-Hellman Key Exchange and RSA public key encryption.

- The public key is published and made available to receive encrypted data.
- Private key can be used to encrypt, authenticate and for digital signatures
- Public private key (Diffie-Hellman) can be used to establish symmetric key, e.g., DES for symmetric key exchange.

Private Key: Private Keys are only known to specific key users in the enterprise for encryption/decryption.

Public Key Infrastructure (PKI) is a security infrastructure that uses one or more trusted Certification Authorities (CA) for managing, distributing, publishing the keys and authenticating the key holders.

Diffie-Hellman Algorithm

- Used to set up a shared session secret, from which cryptographic keys are derived
- Used to set up a security association (SA) in the IPsec protocol suite
- Algorithm

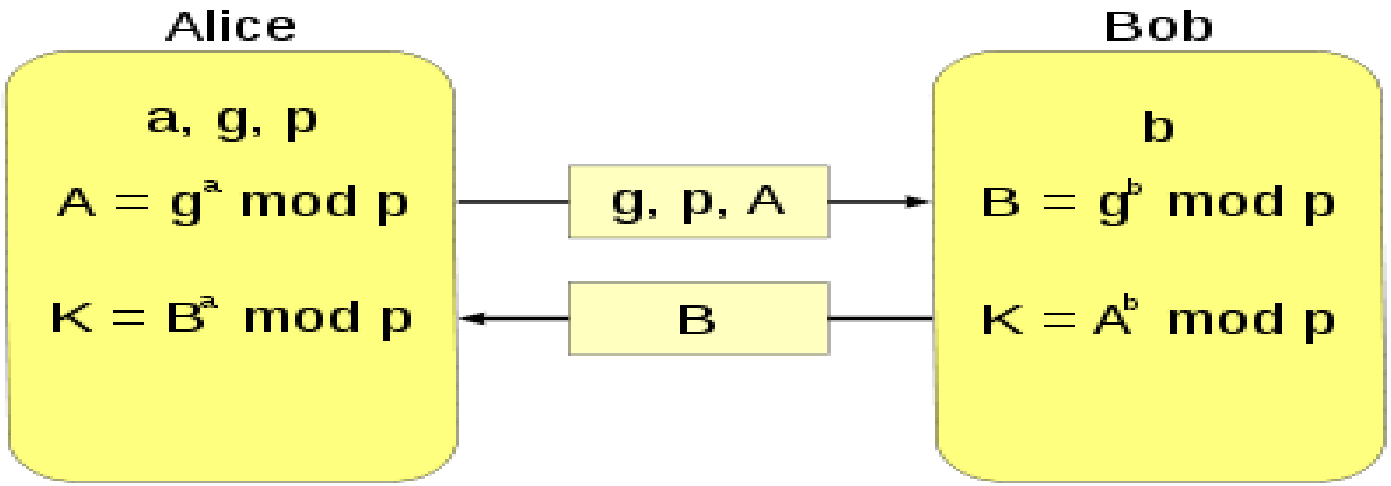
  Alice picks **a, g**, and a large **prime p; g** need not be large, in practice it is usually either 2 or 5.

  Alice derives **A** as in the figure. Keeping **"a"** private, Alice sends **g, p, A** to Bob.

  Bob picks a **"b"** which is private to Bob and computes **B** and **K** as in the figure using **g, b, p** and **A**. Bob then sends **B** to Alice.

  Alice computes **K** using **B** it received, and **a** and **p**.

  K.is then the shared key they use for encrypting and decrypting.



Diffie-Hellman Example

Alice and Bob agree to use a prime number p=23 and base g=5.

Alice chooses a secret integer ***a*=6**, then sends Bob A = g^a mod p

A = 5^{6} mod 23 = 8.

Bob chooses a secret integer ***b*=15**, then sends Alice B = g^b mod p

B = 5^{15} mod 23 = 19.

Alice computes **s** = B^a mod p

19^{6} mod 23 = **2**.

Bob computes **s** = A^b mod p

8^{15} mod 23 = **2**.

2 is used by both Alice and Bob as encryption key

Red denotes secret numbers.

RSA – Public and Private Key

1. Choose two distinct prime numbers p and q (preferably at random and of similar bit-length)
2. Compute n = p * q
3. Compute φ = (p – 1) * (q – 1)
4. Choose an integer "e" such that 1 < e < φ and gcd(e, φ) = 1, i.e., e and φ are relative prime. Then (n,e) is the Public Key released.
5. Find d = e^{-1} *mod*(φ); i.e., d is multiplicative inverse of e, i.e., e*d *mod*(φ) = 1. Then (n,d) is the Private Key

Alice sends public **key (n, e)** to Bob and keeps **d** secret

Bob want to send a message to Alice; Bob converts the message into an integer m where 0< m<n

using "padding" for extra security

Encryption: Bob computes c = m^e *mod*(n) and transmits **c** to Alice

Decryption: Alice computes m = c^d *mod*(n) from which she get the original message m.

Example:

Assume p = 61and q = 53. Then p*q = n = 3233 and φ = (p-1)*q-1) = 60*52 = 3120.

Alice chooses **e** = 17 (note 1< 17<3120 and 17 and 3120 are relative prime. Alices public key is (3233,17). Alice also computes **d** such that ed mod(φ) = 1, or d = 2753 Then (3233, 2733) is Alice's private key.

Now say Bob wants to send the message after padding = "01000001", i.e., **65.** Bob then sends c = 65^{17} *mod* (3233) = 2790 to Alice. Alice converts the received 2790 thru her private key by calculating 2790^{2753} *mod* (3233) = **65**

Cryptographic Hash Functions (Examples: SHA-1 and MD5) MAC and HMAC

Cryptographic Hash Function:

It is a digest of the original message.

It is computationally infeasible to find two different messages which would have the same hash.

One-wayness: From this hash, the original message cannot be created.

Algorithms: They all essentially follow the same concept: They create a digest of length N from a multi-block message (message is split into blocks). An Initial value (random) is used to mangle the first block. The result is mangles with the second block. In the end one has a N block message digest.

SHA-1: Here the blocks are 512 bits. Padding a used in a block if needed. The message digest is a 160 bit long (5 words of 32 bits each).

MAC (Message Authentication Code): MAC is obtained by concatenating the message with a authentication key and then creating an hash of it. These is no encryption.

HMAC (Hashed MAC): HMAC runs the message and the authentication key twice.

IPSec – Network Layer Protocol

IPSec is a protocol for providing authentication and encryption/decryption between devices at the network layer.

IPSec mechanisms consist of:

- authentication header (AH)
- encapsulating security payload (ESP).

Two operation modes of IPSec:

- Transport: IP payload is encrypted using ESP and clear IP header.
- Tunneling: used to encapsulate packets between two virtual private network (VPN) gateways. Both IP header and IP payload are encrypted and encapsulated in another IP packet.

Reference on IPSec: http://unixwiz.net/techtips/iguide-ipsec.html

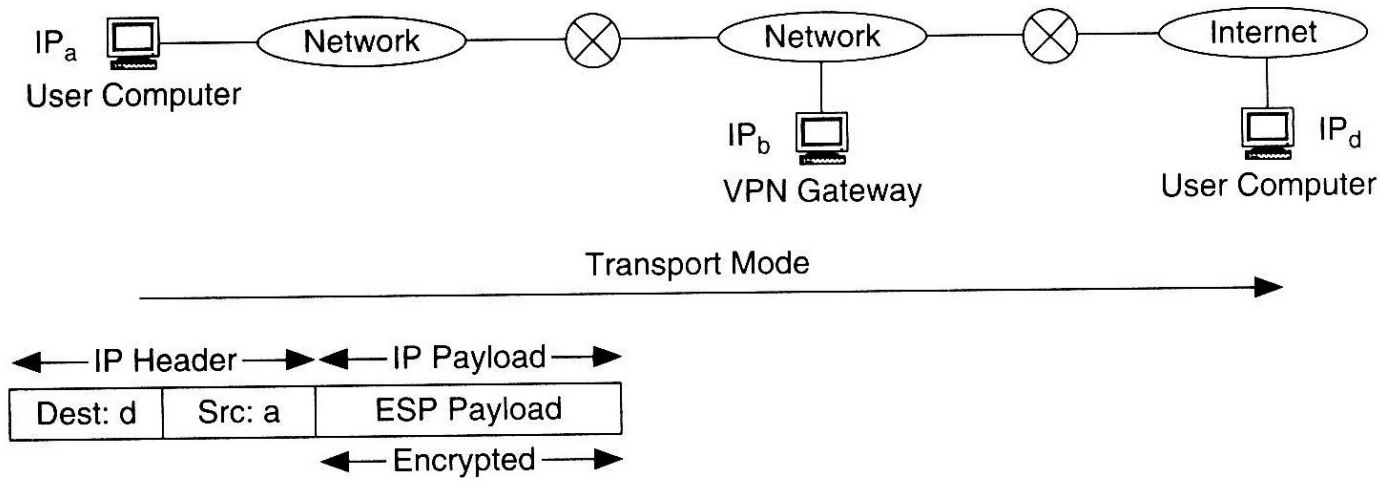
Four combinations are possible!

Transport mode with AH	Transport mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

most common and most important (creates Virtual Private Networks)

IPSec Modes - The Transport Mode

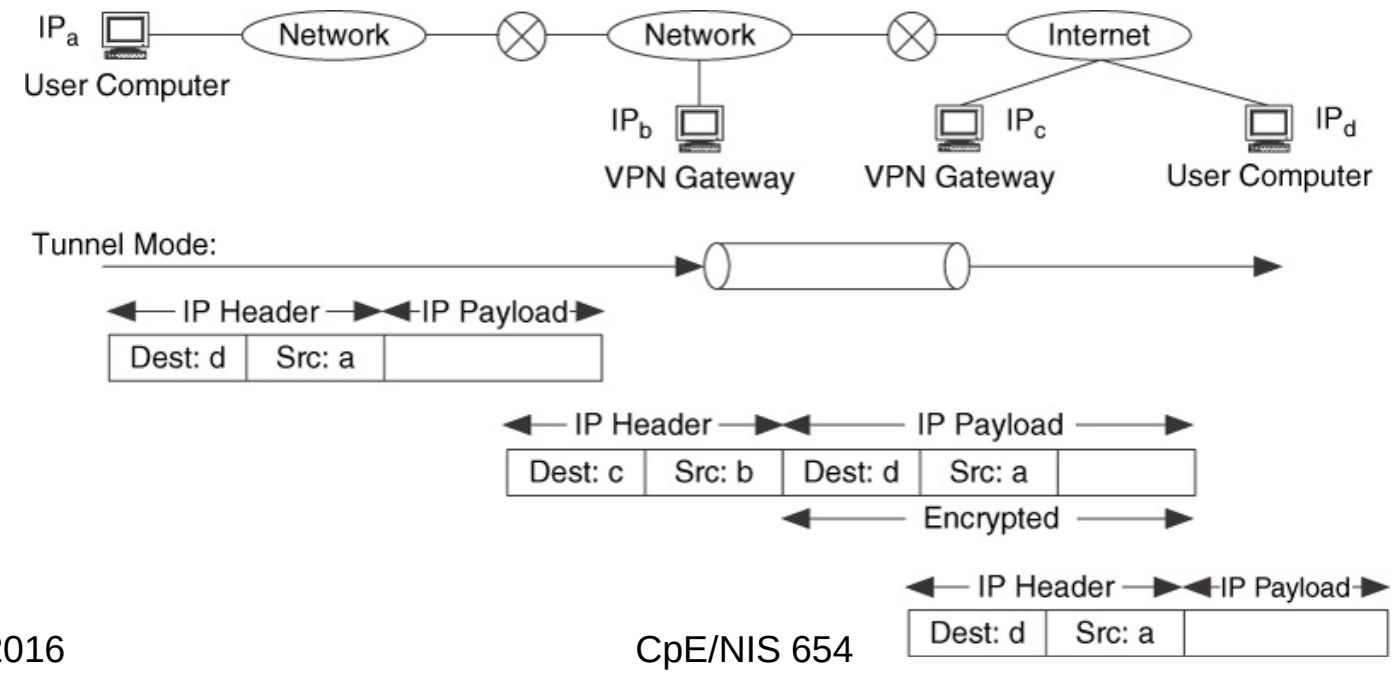
In the the Transport Mode of IPSec, IP payload is encrypted using ESP and IP header is left in the clear.

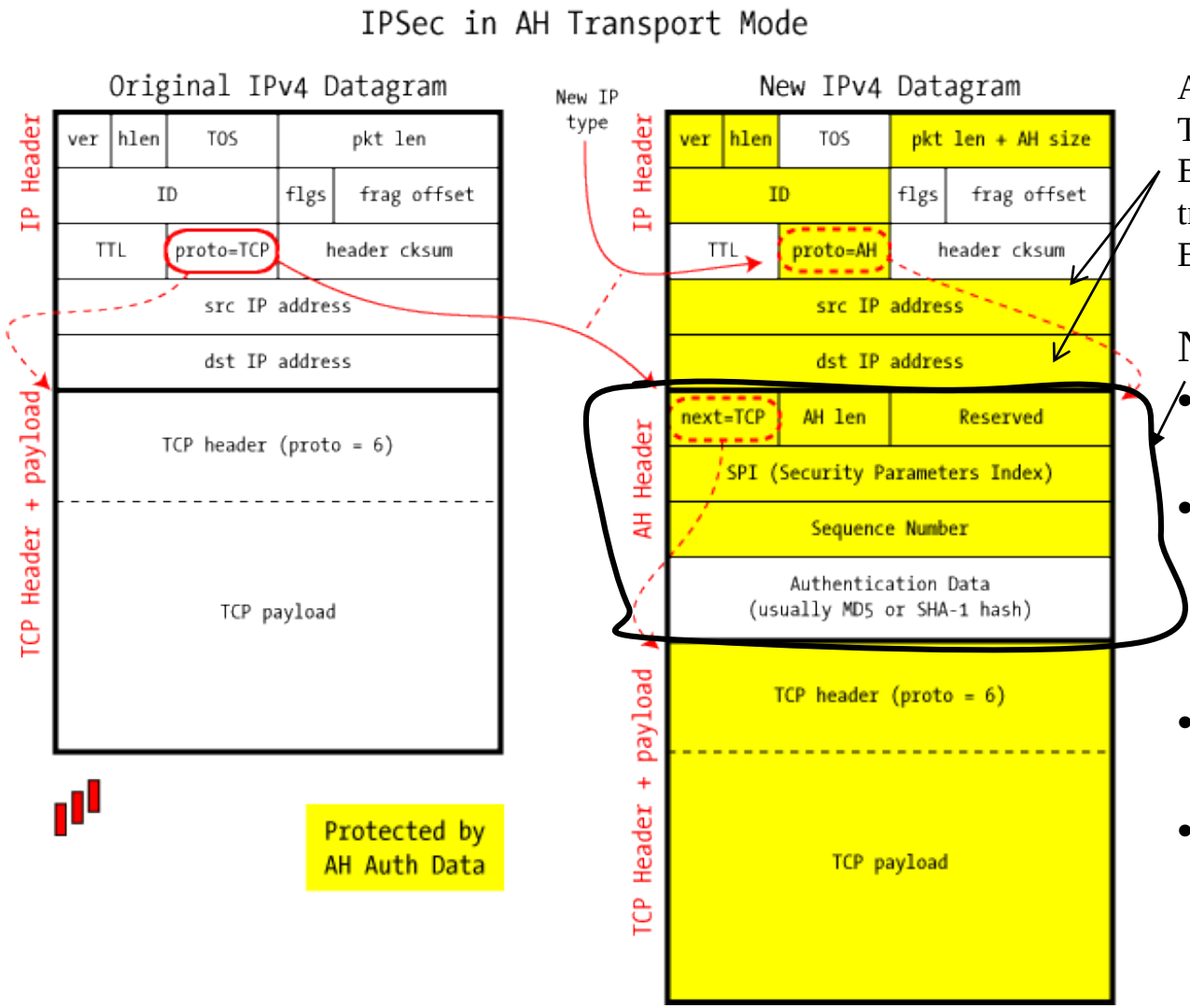


IPSec Modes -The Tunnel Mode

In tunnel mode, the IPSec can be used to encapsulate packets between two virtual private network gateways, as shown:

- IPSec tunnels are created between IPb and IPc in figure
- IP packets are encrypted using ESP
- These packets are then encapsulated within another IP packet and addressed with the ends of the IPSec Tunnel
- At the end of the tunnel, i.e., the gateway serving IPd, the original packet is un-encapsulated and decrypted and sent to its destination IPd



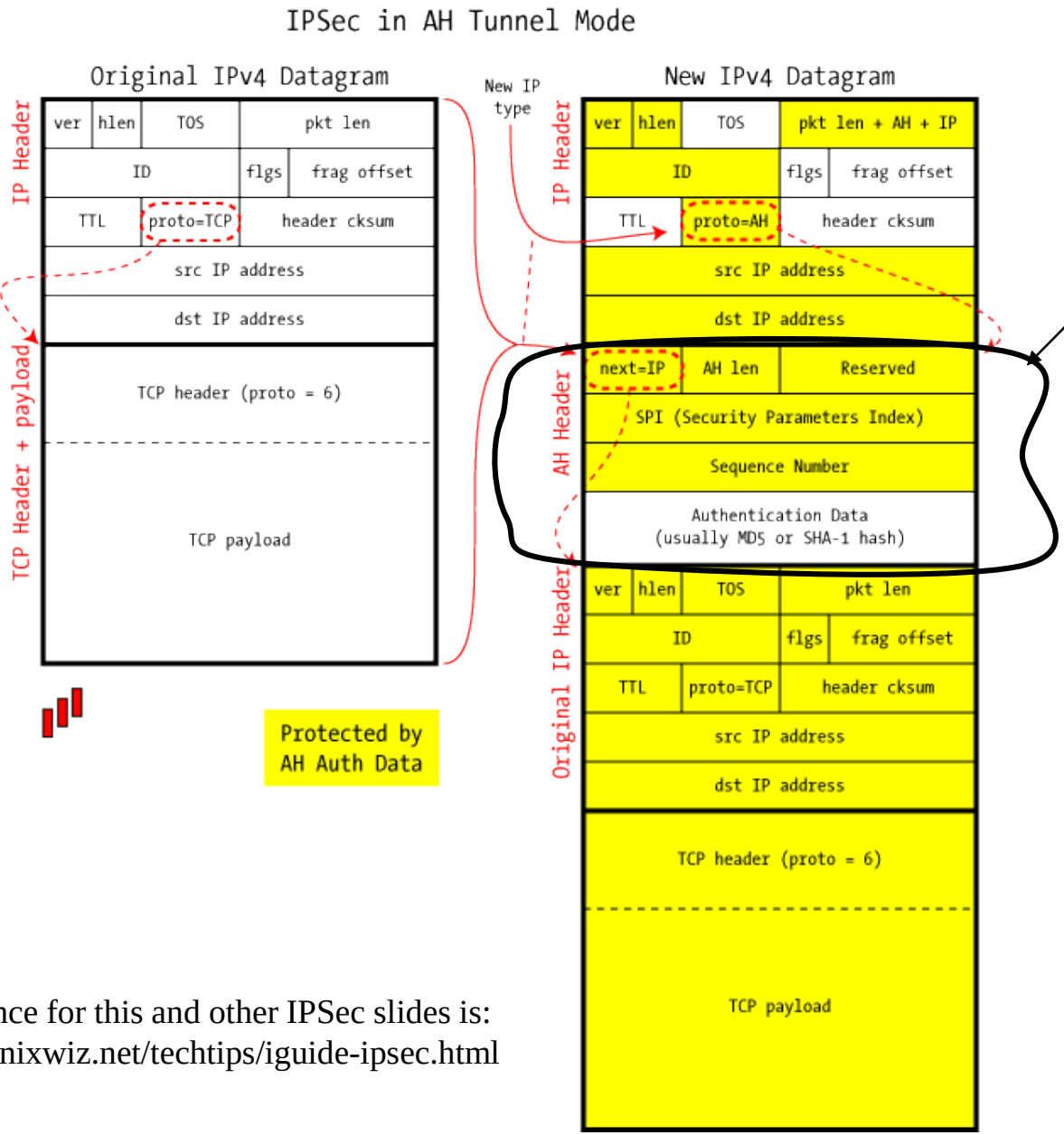


AH Incompatible with NAT: Therefore, SRC and DST must Be reachable without Net translation
ESP does not suffer from this

Note:

- AH header is inserted as shown
- Fields that are looked by intermediate nodes are not protected by AH.
- Proto field is changed to AH
- Src. and dest. Address are not changed.

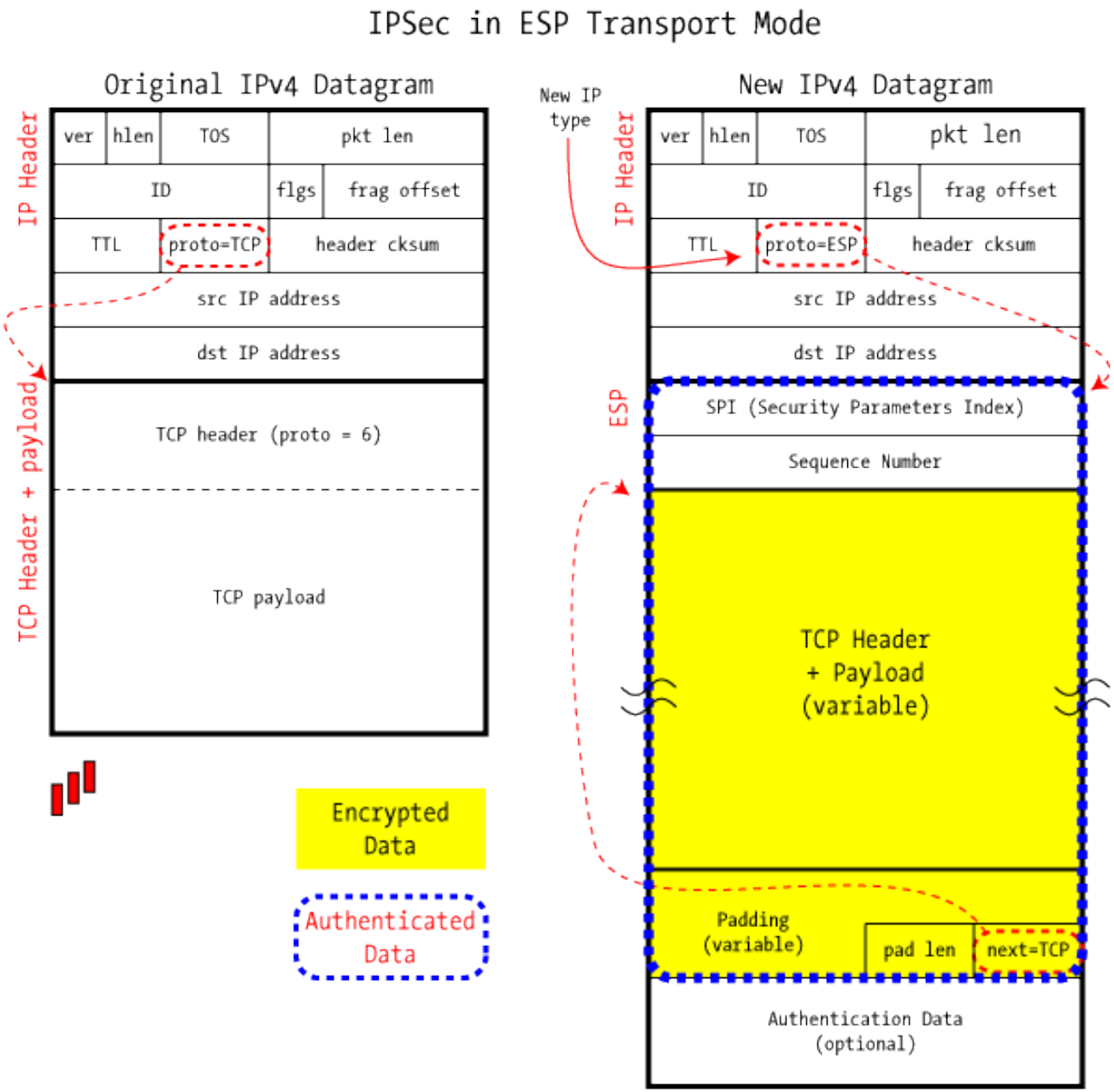
Reference for this and other IPSec slides is: http://unixwiz.net/techtips/iguide-ipsec.html



Note:

- AH is inserted.
- In tunnel mode the src. And dest. Addresses are different.
- The whole IP packet is protected by AH.
- For tunneling, ESP is the choice.

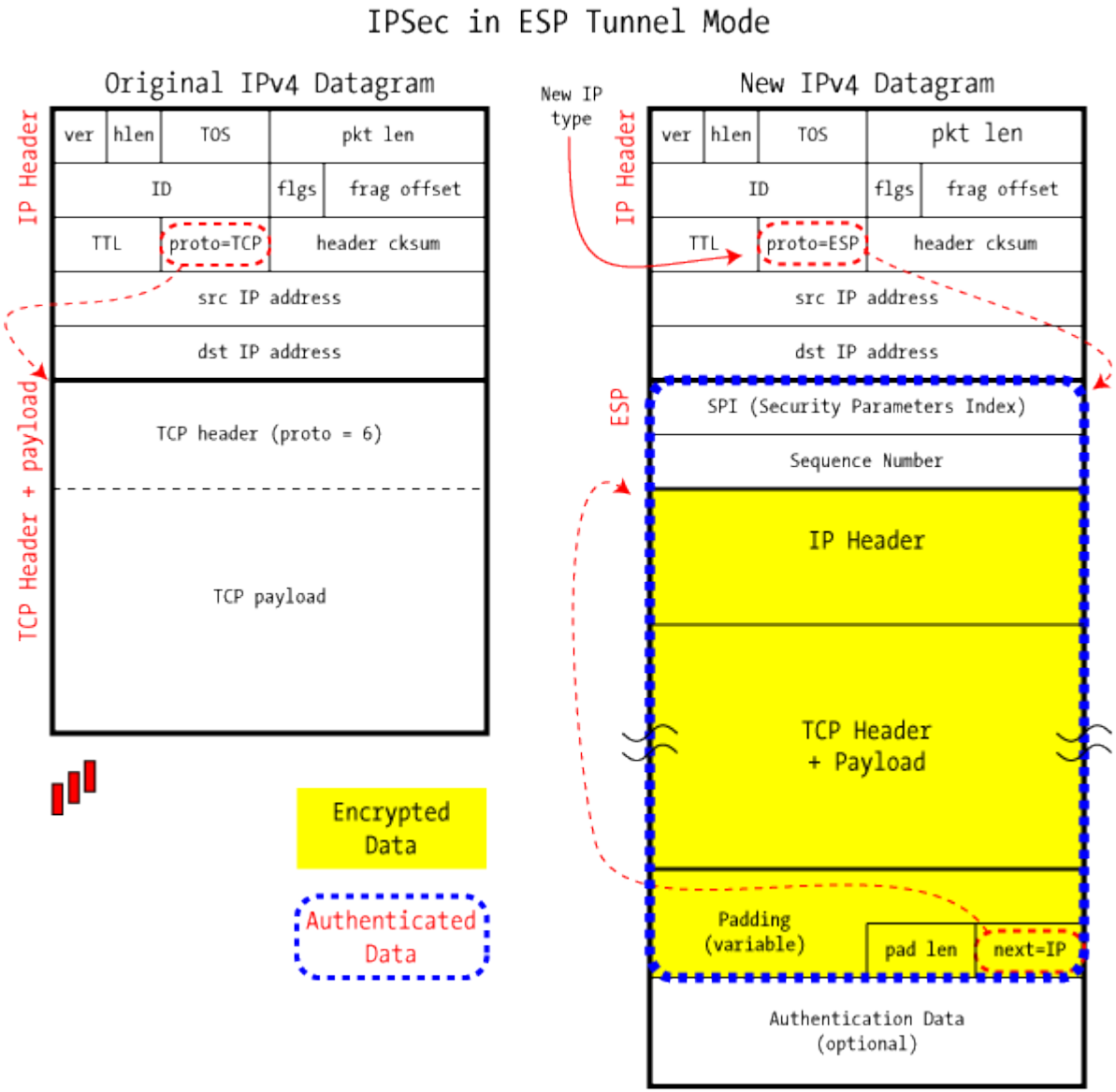
Reference for this and other IPSec slides is:
http://unixwiz.net/techtips/iguide-ipsec.html



Note:

- The payload is only encrypted
- Proto fieled is changed.
- Padding is required since encryption is done in blocks
- Sequence Number to guard agaist playback.
- SPI crypto related info.
- Original source and destination are in clear.

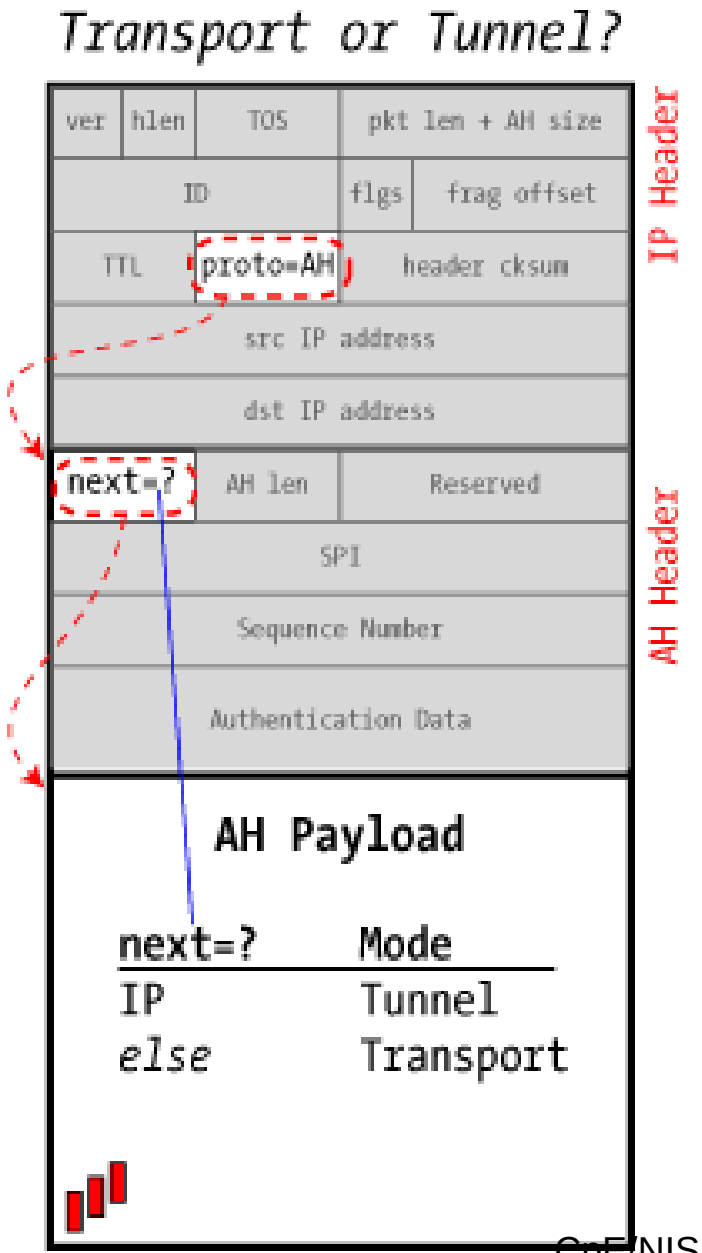
Reference for this and other IPSec slides is: http://unixwiz.net/techtips/iguide-ipsec.html



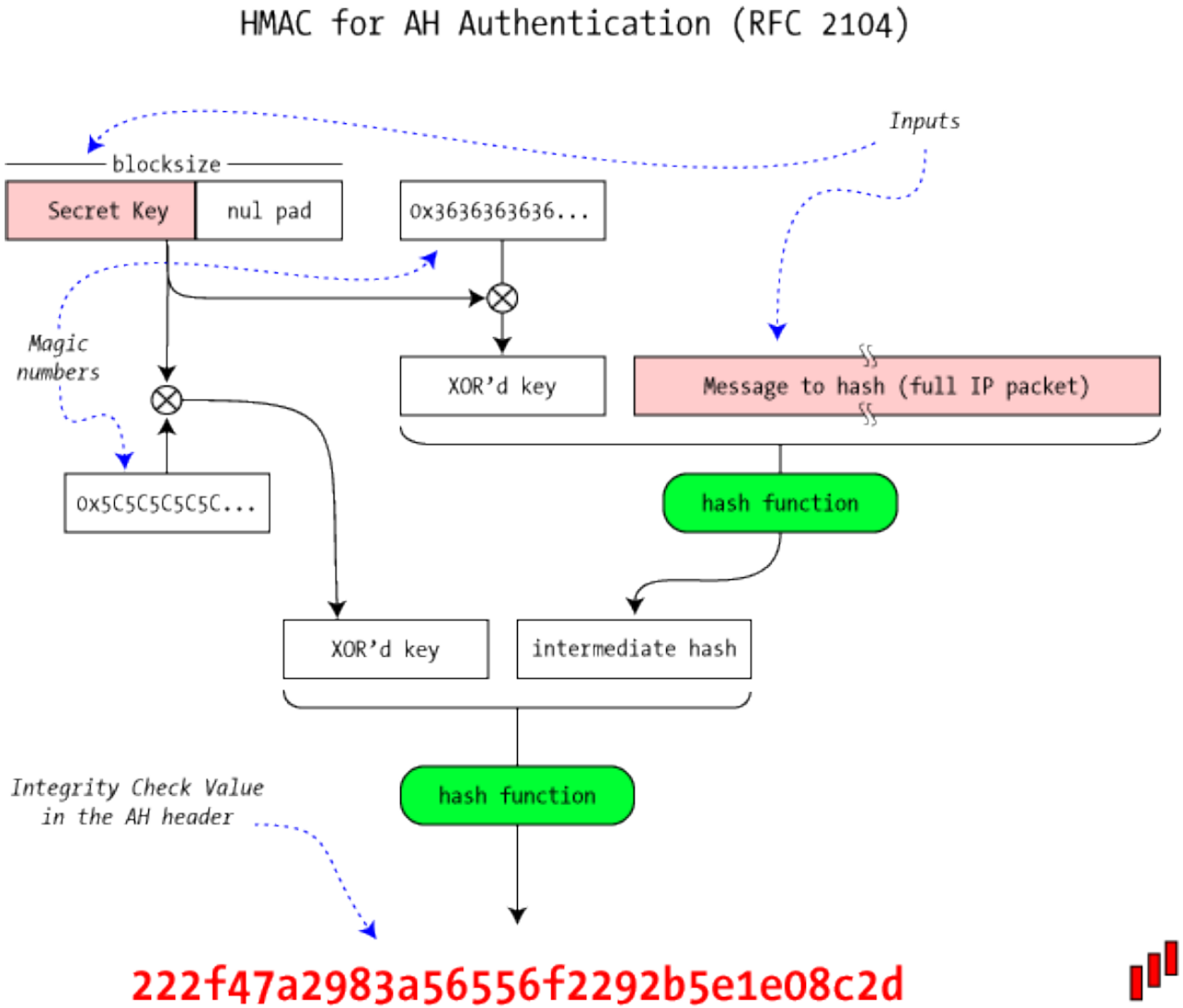
Note:

- In tunnel mode, the whole packet is encrypted and protected.
- Is used for setting up VPN connections

Reference for this and other IPSec slides is: http://unixwiz.net/techtips/iguide-ipsec.html



In ESP mode you cannot tell by examining the NEXT_HDR field if the Transport or Tunnel mode is used, because it is encrypted Note the next field. If IP then tunnel, otherwise transport



Reference for this and other IPSec slides is: http://unixwiz.net/techtips/iguide-ipsec.html

IPSec – Need More for it to Work

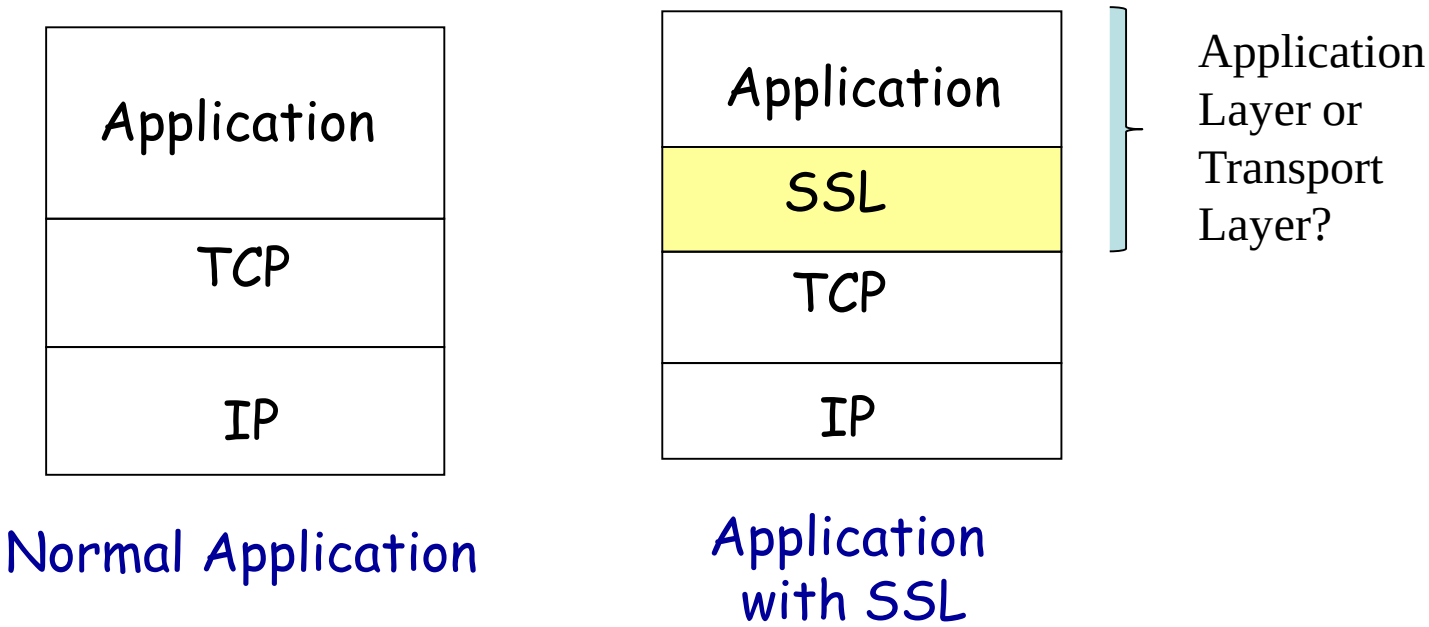
As we have noted, IPSec to work, we need keys, associations between the two communicating entities, key exchange protocols, etc. Here are other key functions needed for IPSec:

- **Security Association (SA)** and **Security Association database (SADB).** The SA specifies which key, algorithm and policies to use with the entity it is communicating with (i.e., it is pairwise between two entieis). This information resides is SADB.
- SADB has all the information it needs to process information (in terms of algorithms (AH, ESP), Keys, routing restrictions, etc.) between each pair
- When a datagram arrives, the three pieces of data in the datagram is used to locate correct SA inside the SADB:
  - Partner's IP address.
  - IPSec Protocol (AH or ESP)
  - Security Parameter Index (SPI).
- Security Associations are one way, one is needed for each AH and ESP. (four associations).
- **Key Management**. Obviously IPSec to work, keys needs to be managed between entities.
  - Manual, but scaling and other problems with manual operation.
  - IKE (internet Key exchange) protocol: Multiple key exchange protocols, (e.g. Oakley)

SSL-Transport Level Security

- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP, such as HTTP
- Internet version (IETF standardized) is called TLS (Transport layer Service)
- SSL/TLS provided confidentiality using symmetric inscription and message integrity using a MAC(message Authentication Code)
- SSL/TLS includes protocol mechanisms to enable two TCP users to determine security services they will use (Handshake)
- HTTPS (HTTP over SSL) combines HTTP and SSL to provide secure communication between a browser and web server.
- SSH (Secure Shell) provides secure remote login and other secure client/server communication.

Transport Level Security (Contd.)



Secure Socket Layer (SSL) provides application programming interface (API) to applications

SSL - Key Concepts

- *handshake:* Alice and Bob use their certificates, private keys to authenticate each other and exchange shared secret
- *key derivation:* Alice and Bob use shared secret to derive set of keys
- *data transfer:* data to be transferred is broken up into series of records
- *connection closure:* special messages to securely close connection

For details, refer to a good source such as Computer Networking by Kurose and Ross text

Security for the Network Management Functions

- A comprehensive set of security messages (management traffic):
- SNMP message verification: data integrity, user identity verification (data origination authentication), data confidentiality
- Message timeliness and limited replay (e.g., via snmpEngineID), etc.)
- Encryption
- Many other mechanisms for security

SNMPv3

SNMPv3 primarily added security and remote configuration enhancements to SNMP.

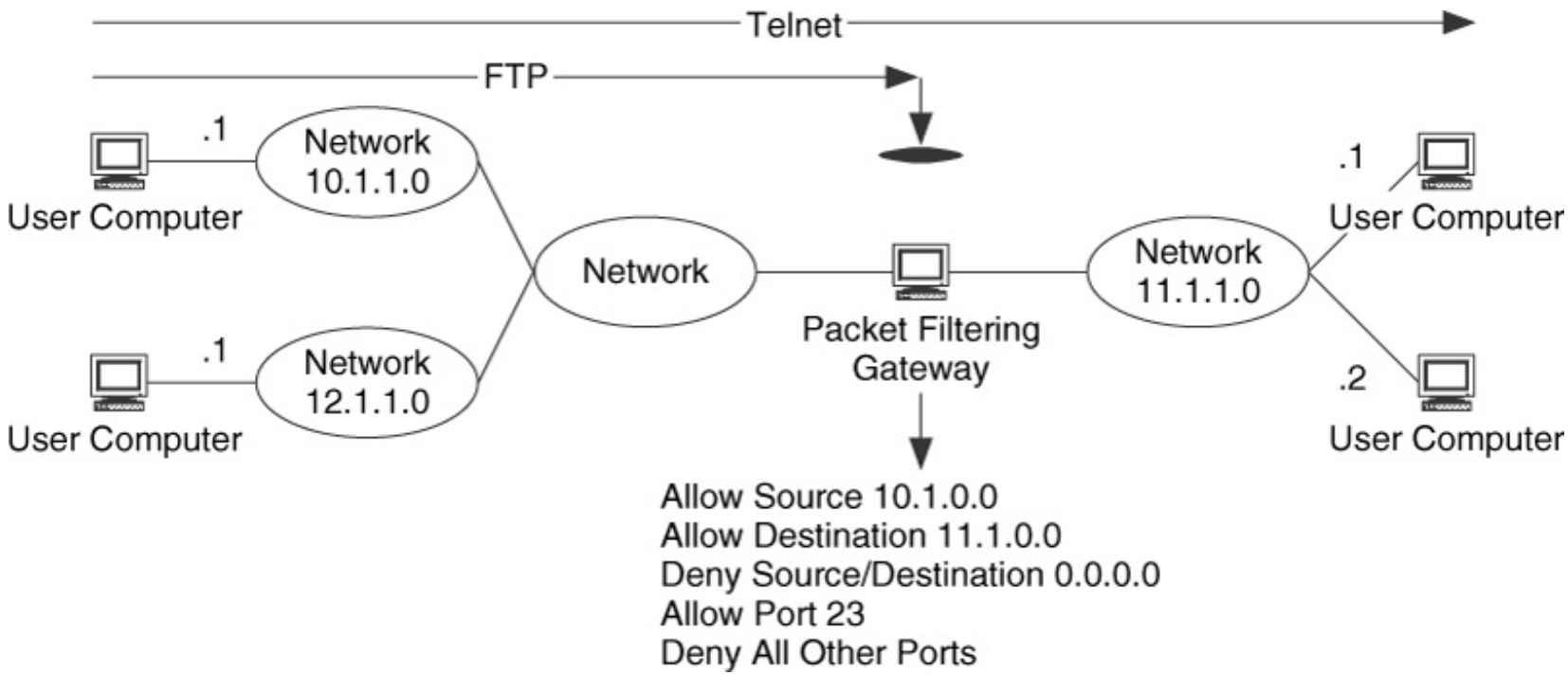
SNMPv3 makes no substantial changes to the protocol aside from the addition of cryptographic security

SNMPv3 provided important security features:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered with in transit.
- Authentication – to verify that the message is from a valid source.

Packet Filtering

It is a mechanism to explicitly deny or allow packets to pass at strategic points



Network Perimeter Security

To protect the external interfaces between a local network and external networks.

Hide the local IP addresses by using Network address translation (NAT).

NAT creates the bindings between public and private IP addresses. Many packet parameters available, such as addresses, ports, etc.

•as one-to-one binding (static NAT),

•one-to-many (dynamic NAT), and

•address and port bindings (Network Address Port Translation or NAPT)

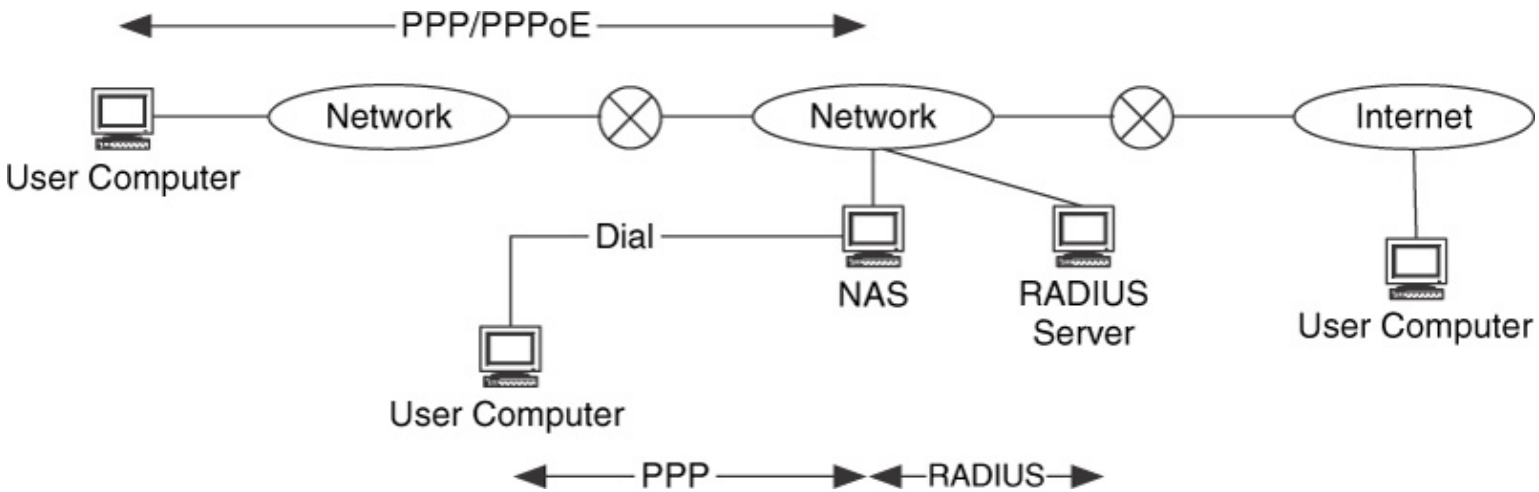
Remote Access Considerations

Security for remote access includes what is commonly called AAAA:

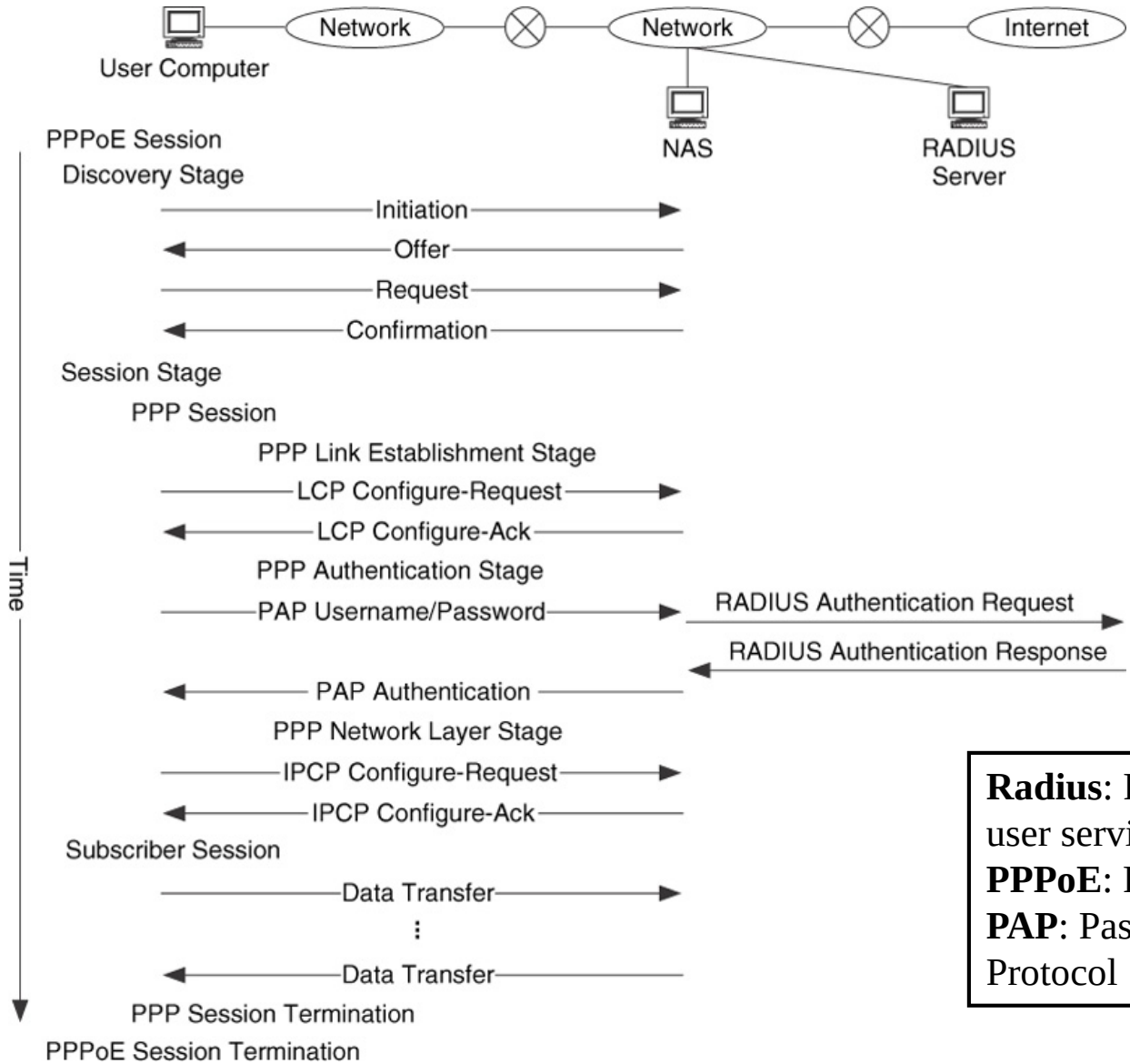
- Authentication of users
- Authorization of resources for authenticated users
- Accounting or resources and service delivery
- Allocation of configuration information (default routes, etc.)

A combination of protocols to accomplish:

- PPP, PPPoE, RADIUS, etc (e.g. PPP in link establishment authentication)
- NAT: hide addresses
- VPN: policies for its provosioning
- Routing protocols: BGP and MPLS for routing control
- Network Access System (NAS); Subscriber Management System (SMS) Interfaces



PPPoE Session



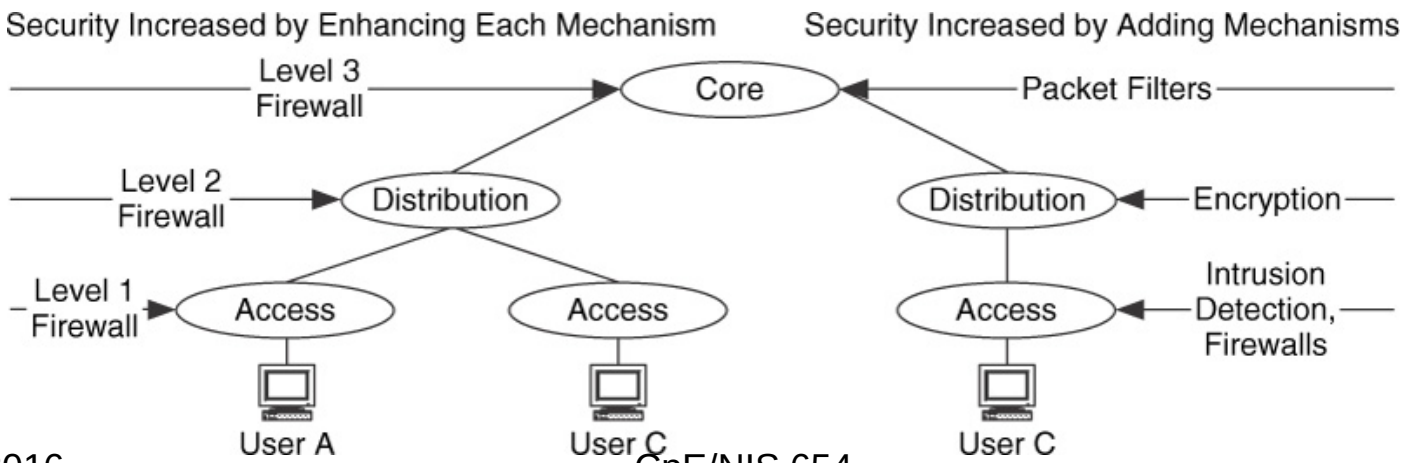
Radius: Remote access dial-in user service
PPPoE: PPP over Ethernet
PAP: Password Authentication Protocol

Evaluation of Security Mechanisms

The set of security mechanisms that are used, depends on:

- The result of the requirement analysis.
- The security and privacy plan.

Question: Where should we apply security mechanisms?
The access/distribution/core architectural model, which segments a network based on functions, can be used as a starting point for applying security mechanisms. Using this model, we can increase security at each level, from access network to distribution networks to core networks, by either adding security mechanisms or enhancing the amount of security provided by each mechanism.



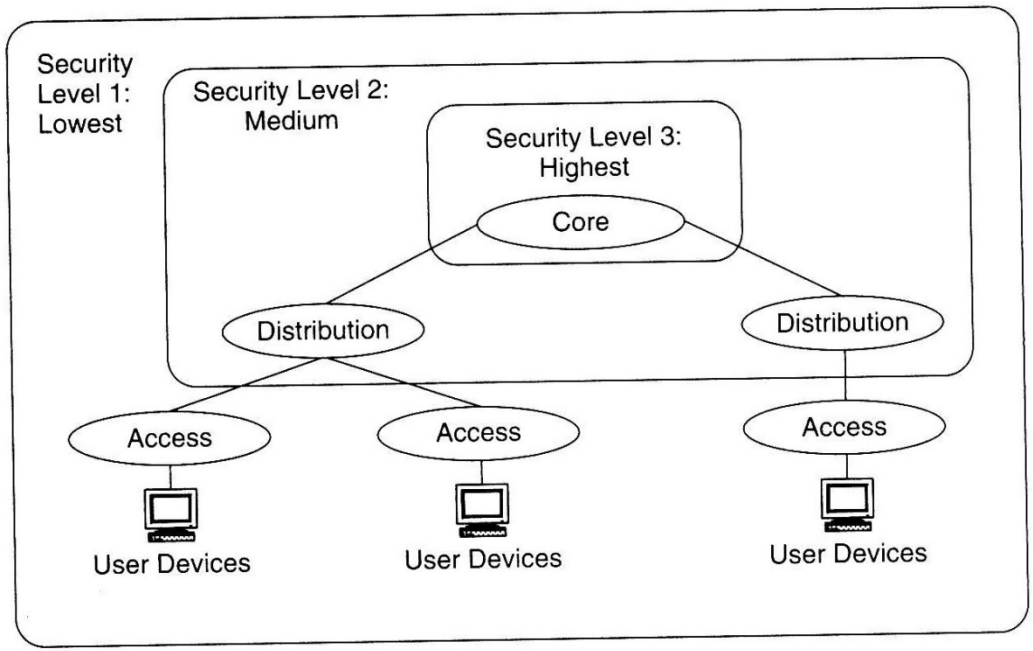
Different Levels of Security Requirements

In case there are multiple different levels of security requirements, security zones can be established.

There are two methods of developing security zones:

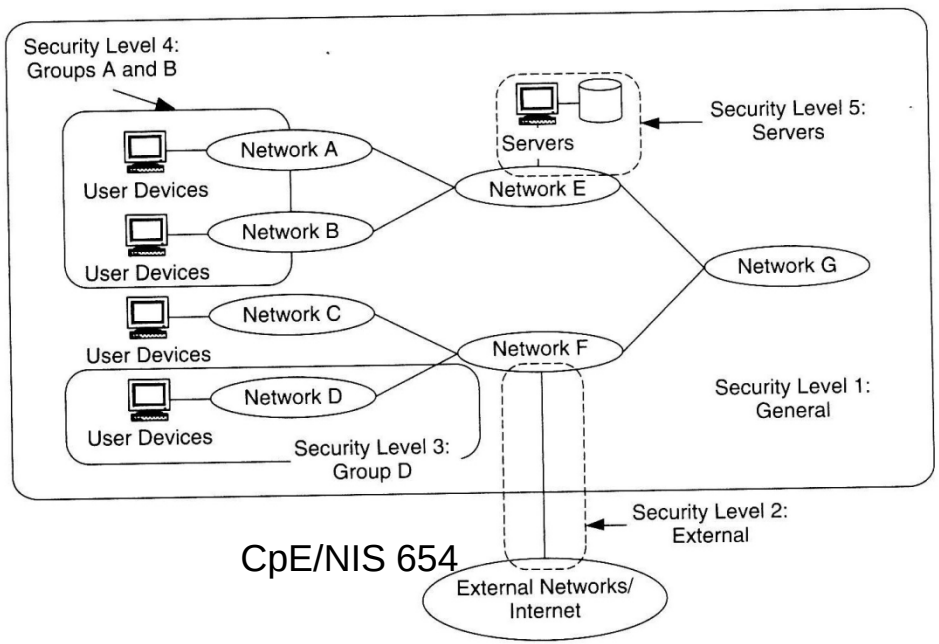
- Increased security as you moved deeper to the core of the network.
- Developing zones wherever they are needed in the network, regardless of topology.

Security Zoning – Two methods



Security Zones Embedded Within Each Other

Security Zones Throughout the Network



Internal Relationships

- Some security mechanisms require the ability to look at or change various fields within the packet; however, if encryption is used then these security mechanisms will be impacted.
- Example: Between NAT and Encryption
- using NAT for security (and preserving IP addresses and for internal routing) could interfere with encryption since NAT needs to translate IP addresses between public and private. Encrypted packets will disable NAT.
- Recall NAT is incompatible with AH in IPSec

External Relationships

External relationships are trade-offs, dependencies, and constraints between security architecture and other architecture.

Examples:

- **Interactions Between Security and Network Management:** security depends on network management to configure, monitor, manage, and verify security throughout any networks.
- **Interactions Between Security and Performance:** Using security will reduce end-to-end bandwidth and increase end-to-end transfer time.