Overview of Network Security

Davydenko Pavel

Presentation Content

- What is Internet?
- What do we need to protect?
- Threat Motivation
- Attack Types
- Security Objectives
- Security mechanisms
- References

What is Internet?

- The Internet is a worldwide IP network, that links collection of different networks from various sources, governmental, educational and commercial.

What do we need to protect

- Data
- Resources
- Reputation

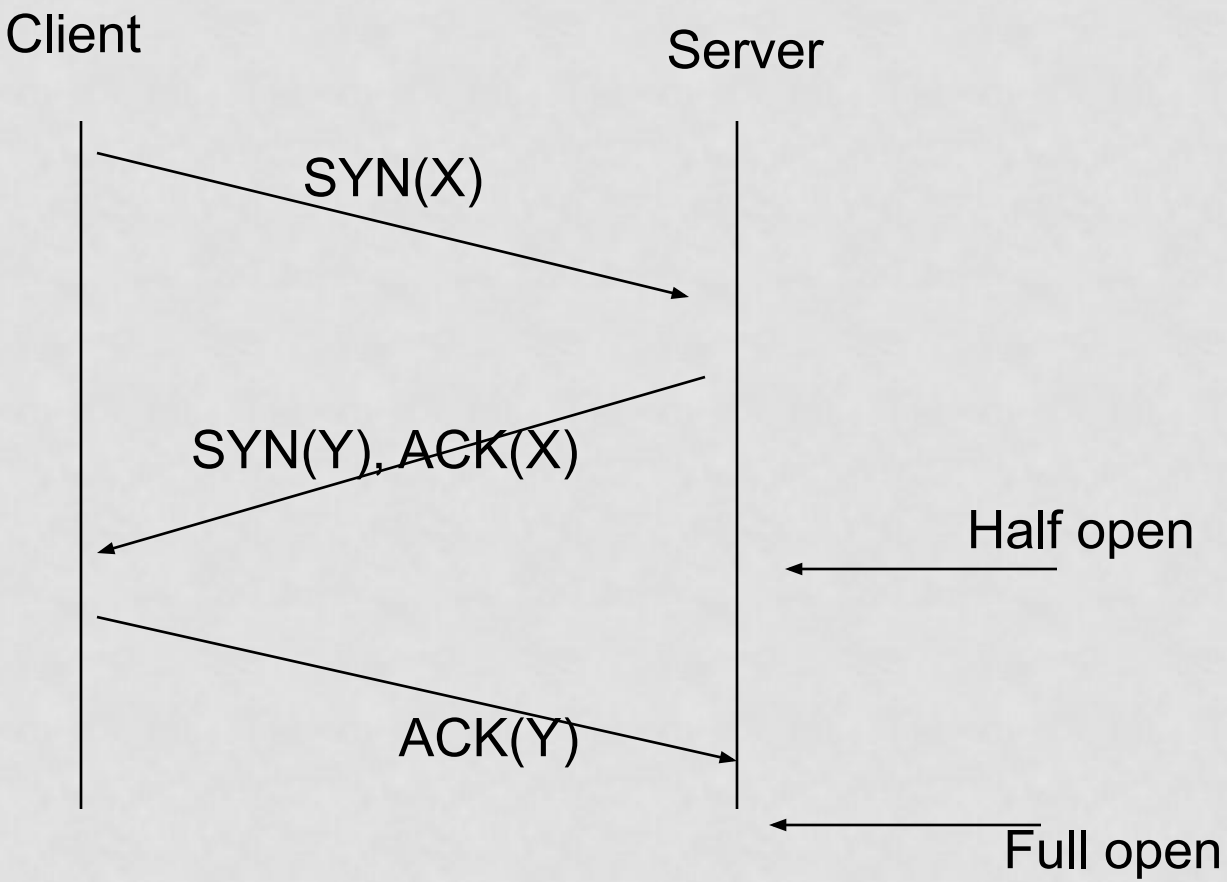
Threat Motivation

- Spy
- Joyride
- Ignorance
- Score Keeper
- Revenge
- Greed
- Terrorist

Types of Attacks

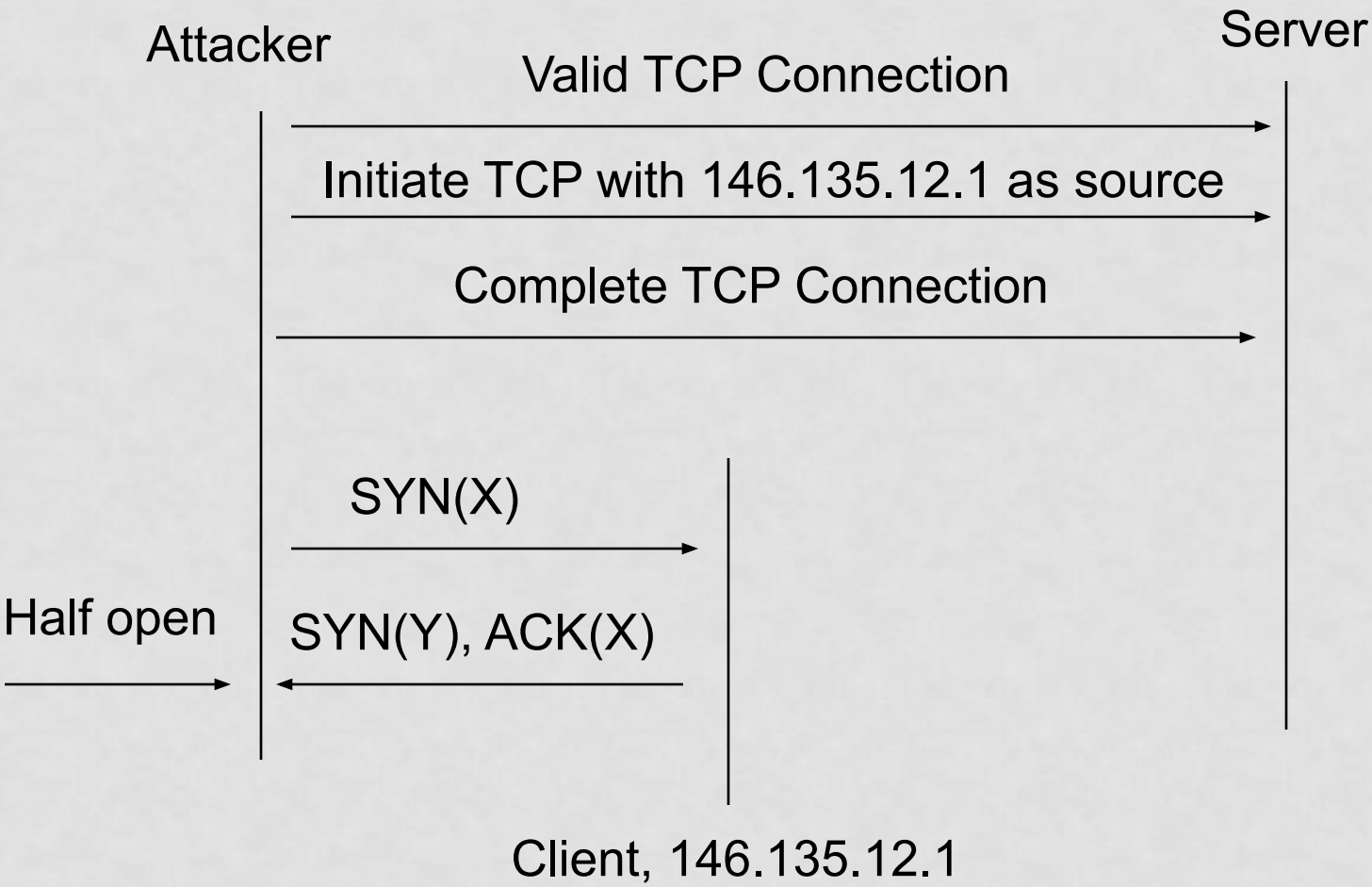
- Passive
- Active
  - Denial of Services
  - Social Engineering

TCP 3 way handshake



X, Y are sequence numbers

TCP Session Hijack



Security Objectives

- Identification
- Authentication
- Authorization
- Access Control
- Data Integrity
- Confidentiality
- Non-repudiation

Identification

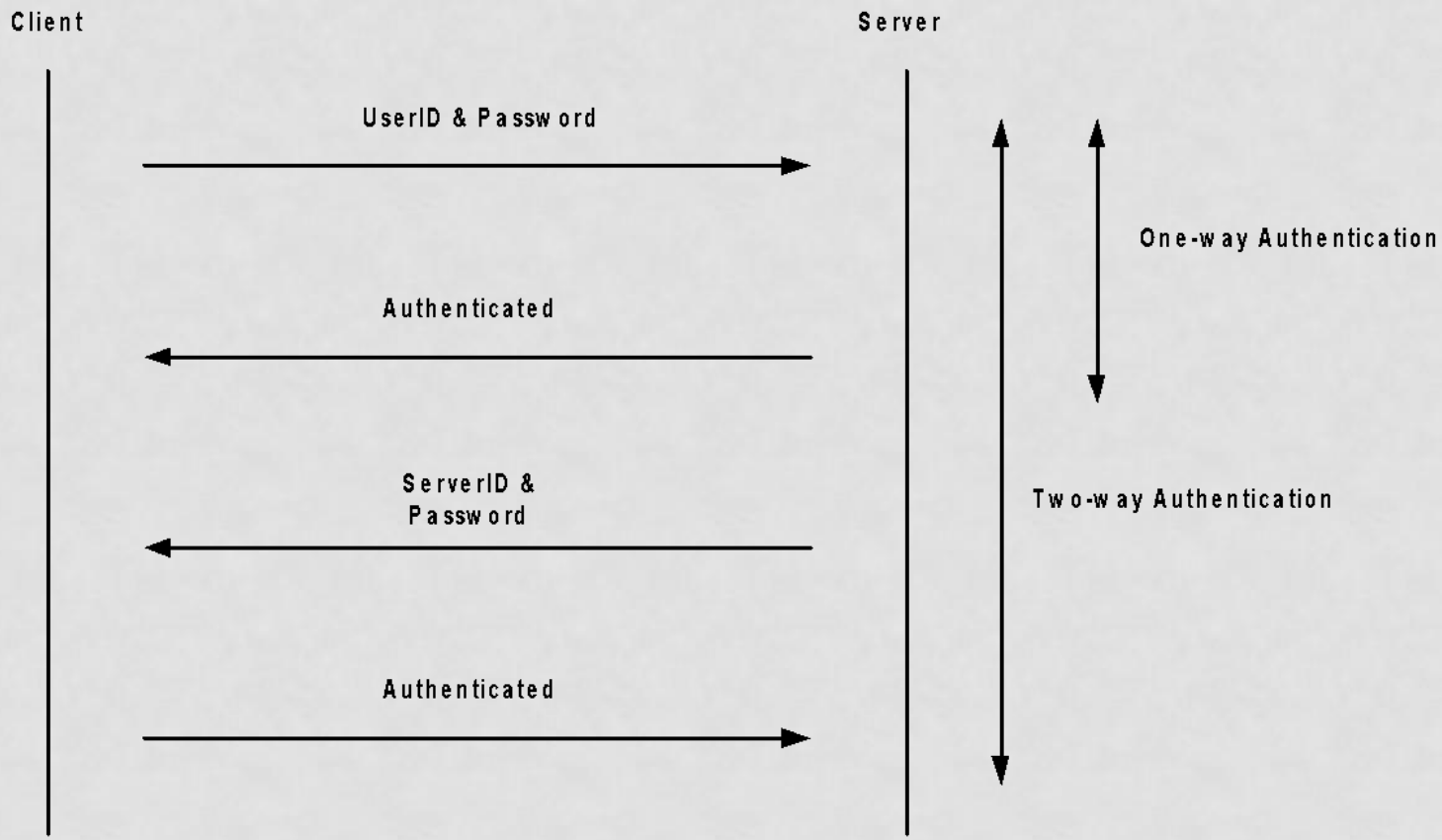
- Something which uniquely identifies a user and is called UserID.
- Sometime users can select their ID as long as it is given too another user.
- UserID can be one or combination of the following:
  - User Name
  - User Student Number
  - User SSN

Authentication

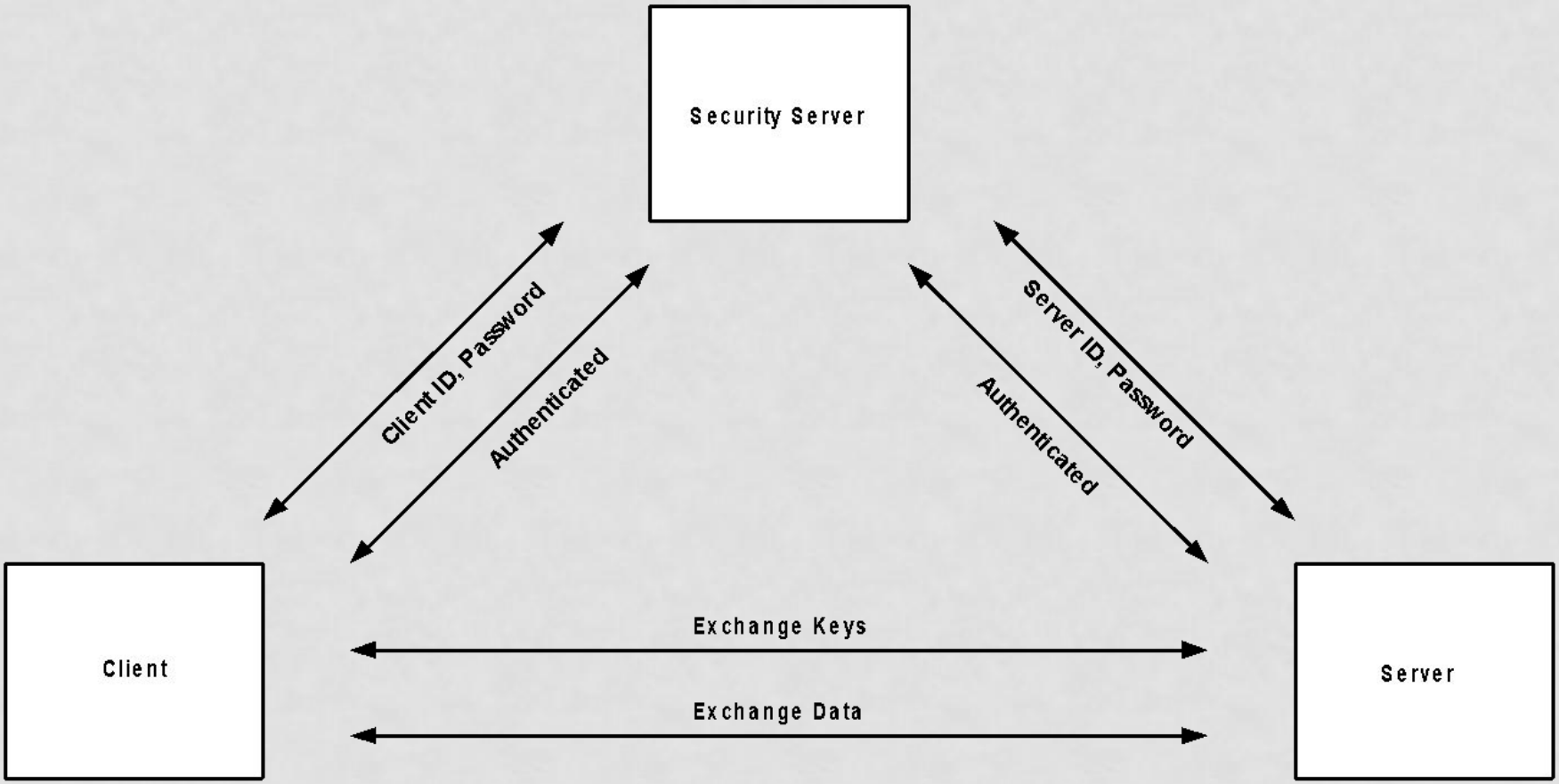
- The process of verifying the identity of a user
- Typically based on
  - Something user knows
    - Password
  - Something user have
    - Key, smart card, disk, or other device
  - Something user is
    - fingerprint, voice, or retinal scans

Authentication Cont.

- Authentication procedure
  - Two-Party Authentication
    - One-Way Authentication
    - Two-Way Authentication
  - Third-Party Authentication
    - Kerberos
    - X.509
  - Single Sign ON
    - User can access several network resources by logging on once to a security system.



Two-Party Authentications



Third-Party Authentications

Authorization

- The process of assigning access right to user

Access Control

- The process of enforcing access right
- and is based on following three entities
  - Subject
    - is entity that can access an object
  - Object
    - is entity to which access can be controlled
  - Access Right
    - defines the ways in which a subject can access an object.

Access Control Cont.

- Access Control is divided into two
  - Discretionary Access Control (DAC)
    - The owner of the object is responsible for setting the access right.
  - Mandatory Access Control (MAC)
    - The system defines access right based on how the subject and object are classified.

Data Integrity.

- Assurance that the data that arrives is the same as when it was sent.

Confidentiality

- Assurance that sensitive information is not visible to an eavesdropper. This is usually achieved using encryption.

Non-repudiation

- Assurance that any transaction that takes place can subsequently be proved to have taken place. Both the sender and the receiver agree that the exchange took place.

Security Mechanisms

- Web Security
- Cryptographic techniques
- Internet Firewalls

Web Security

- Basic Authentication
- Secure Socket Layer (SSL)

Basic Authentication

A simple user ID and password-based authentication scheme, and provides the following:

- To identify which user is accessing the server
- To limit users to accessing specific pages (identified as Universal Resource Locators, URLs

SECURE SOCKET LAYER (SSL)

- Netscape Inc. originally created the SSL protocol, but now it is implemented in World Wide Web browsers and servers from many vendors. SSL provides the following
  - Confidentiality through an encrypted connection based on symmetric keys
  - Authentication using public key identification and verification
  - Connection reliability through integrity checking
- There are two parts to SSL standard, as follows:
  - The SSL Handshake is a protocol for initial authentication and transfer of encryption keys.
  - The SSL Record protocol is a protocol for transferring encrypted data

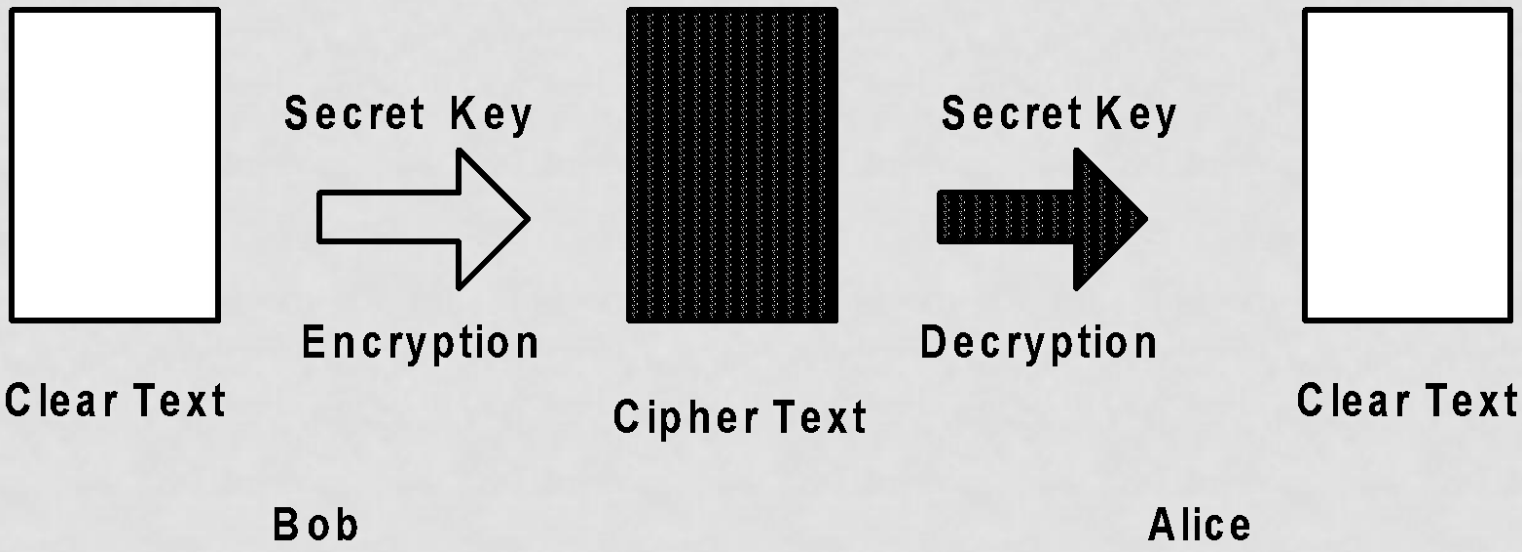
Secure Socket Layer Cont..

- The client sends a "hello" message to the Web server, and the server responds with a copy of its digital certificate.
- The client decrypts the server's public key using the well-known public key of the Certificate Authority such as VeriSign.
- The client generates two random numbers that will be used for symmetric key encryption, one number for the receiving channel and one for the sending channel. These keys are encrypted using the server's public key and then transmitted to the server.
- The client issues a challenge (some text encrypted with the send key) to the server using the send symmetric key and waits for a response from the server that is using the receive symmetric key.
- Optional, server authenticates client
- Data is exchanged across the secure channel.

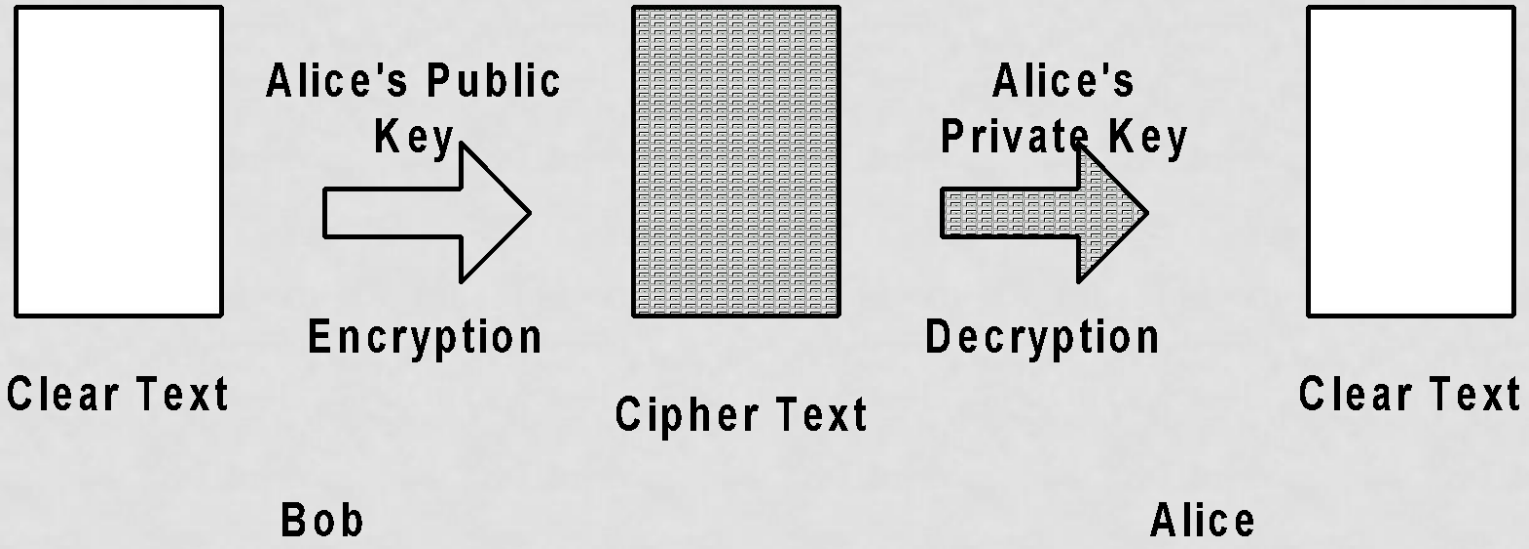
Cryptographic Techniques

- Secret Key Algorithm
- Public Key Algorithm
- Secure Hash Function
- Digital Signature
- Certificate Authority

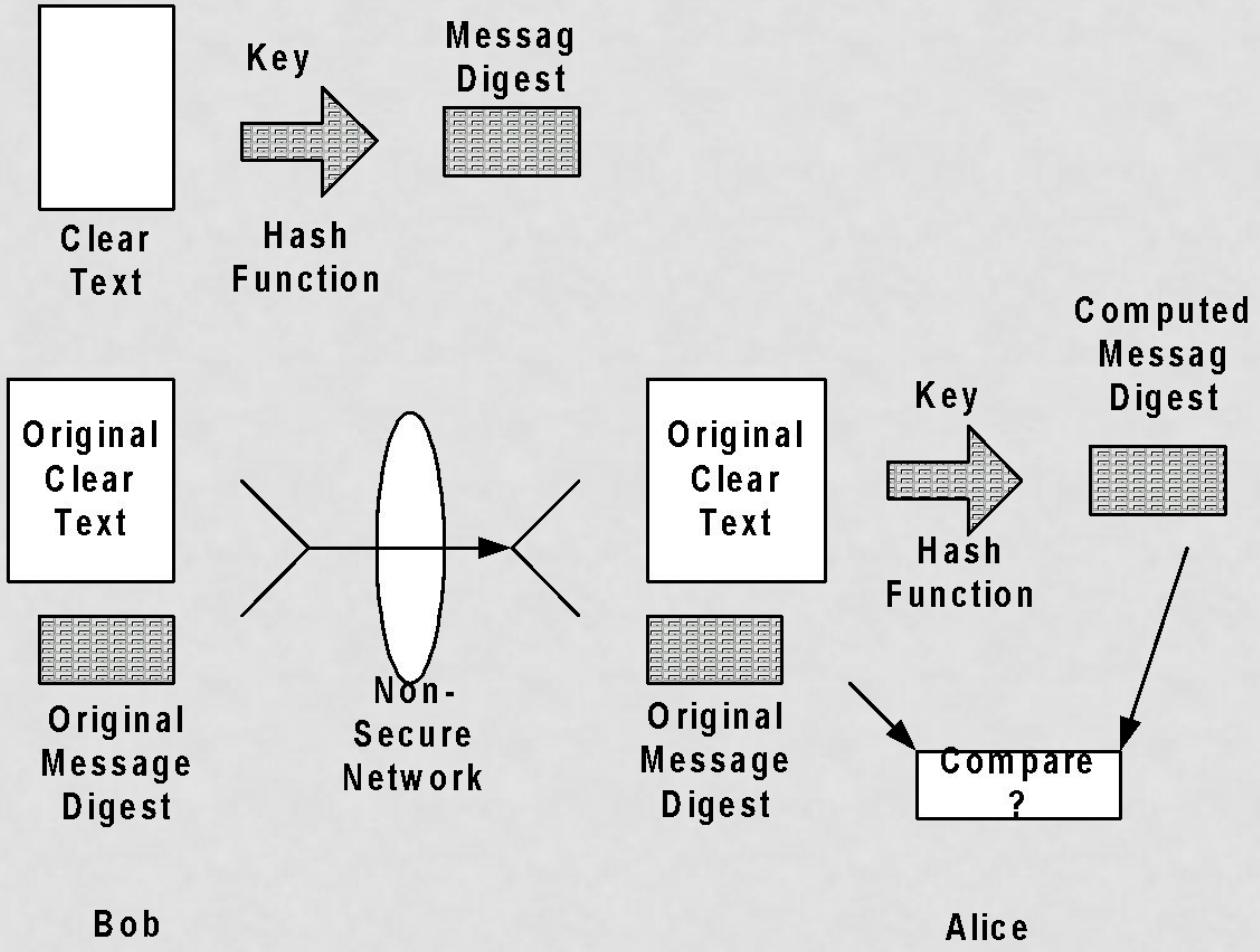
Secret Key Algorithm



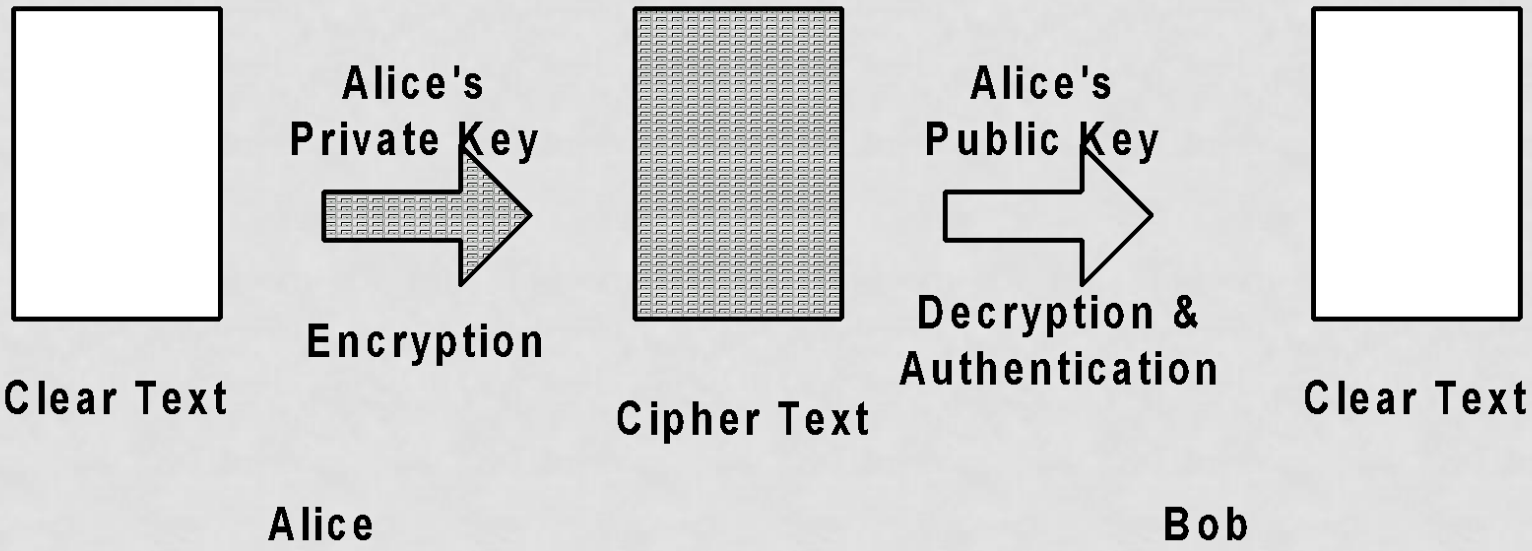
Public Key Algorithm



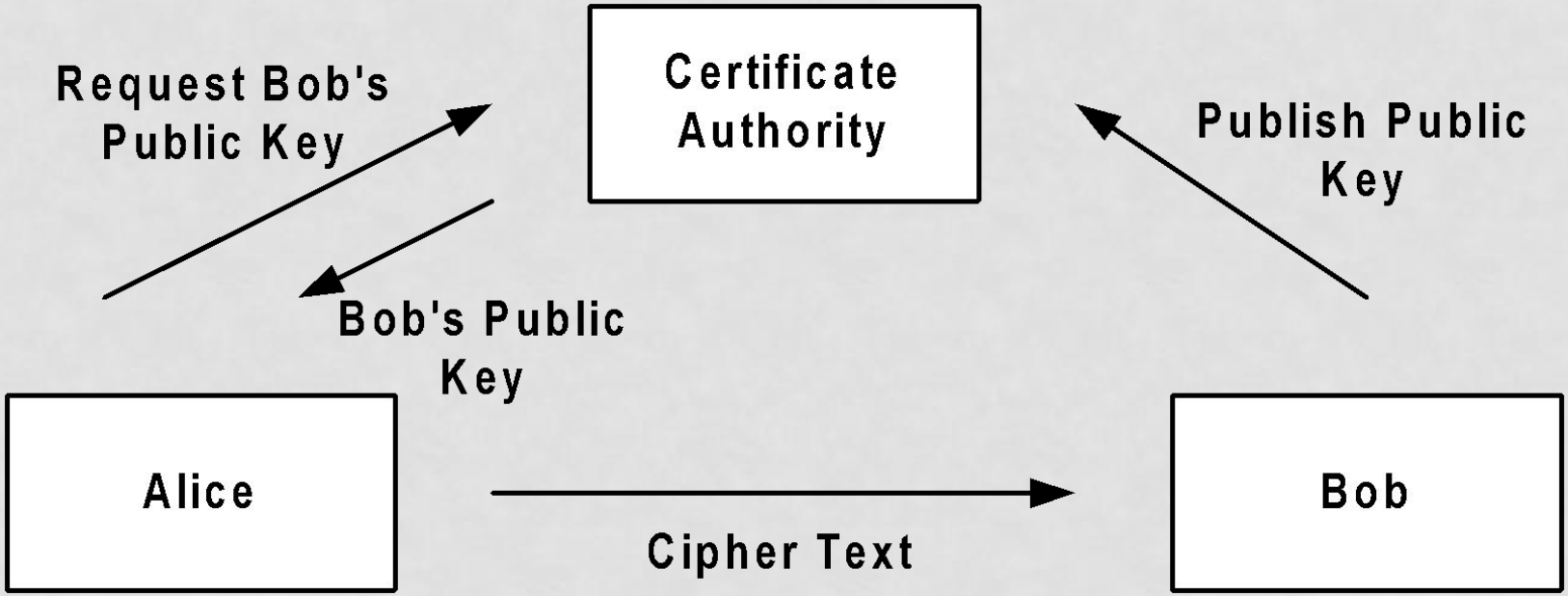
Secure Hash Function



Digital Signature



Certificate Authority



X.509 Certificate

- Is a ITU-T Recommendation.
- Specifies the authentication service for X.500 directories
- X.500 specifies the directory services.
- Version 1 was published in 1988.
- Version 2 was published in 1993.
- Version 3 was proposed in 1994 and approved in 1997.
- Binds the subject (user's) name and the user's public key.

X.509 Certificate (cont..)

- X09 certificate consists of the following fields:
  - Version
  - Serial Number
  - Algorithm Identifier
  - Issuer name
  - Validity period
  - Subject name
  - Subject public key information
  - Issuer unique identifier (Version 2 & 3 only)
  - Subject unique identifier (Version 2 & 3 only)
  - Extensions (Version 3 only)
  - Signature

X.509 Certificate (Cont..)

- Version 1
  - Basic
- Version 2
  - Adds unique identifier to prevent reuse of X.500
- Version 3
  - Adds extension to carry additional information and some of them are
    - Distinguish different certificates
    - Alternative to X.500 name
    - Limit on further certification by subject
    - Policy and Usage

X.509 Certificate Revocation List (CRL)

- Is to prevent fraud and misuse.
- A certificate may be revoked for one the following reason:
  - The user's private is compromised
  - The user is no longer certified by this CA
  - The CA's private key a compromised
- Version 1 was published in 1988.
- Version 2 was published in 1997.

X.509 CRL (cont..)

- X09 CRL consists of the following fields:
  - Version
  - Serial Number
  - Revocation Date
  - Algorithm Identifier
  - Issuer name
  - Last update
  - Next update
  - Extensions (Version 2 only)
  - Signature

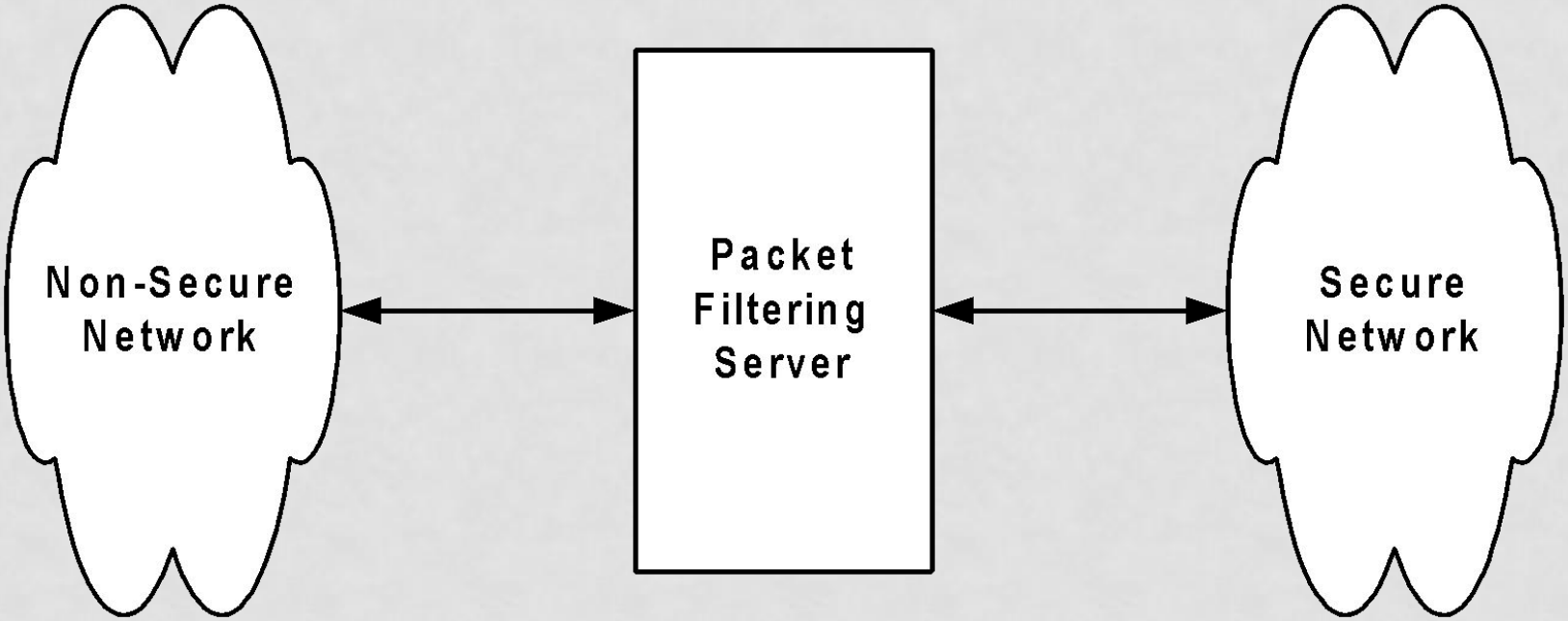
Internet Firewall

- A firewall is to control traffic flow between networks.
- Firewall uses the following techniques:
  - Packet Filters
  - Application Proxy
  - Socks servers
  - Secure Tunnel
  - Screened Subnet Architecture

Packet Filtering

- Most commonly used firewall technique
- Operates at IP level
- Checks each IP packet against the filter rules before passing (or not passing) it on to its destination.
- Very fast than other firewall techniques
- Hard to configure

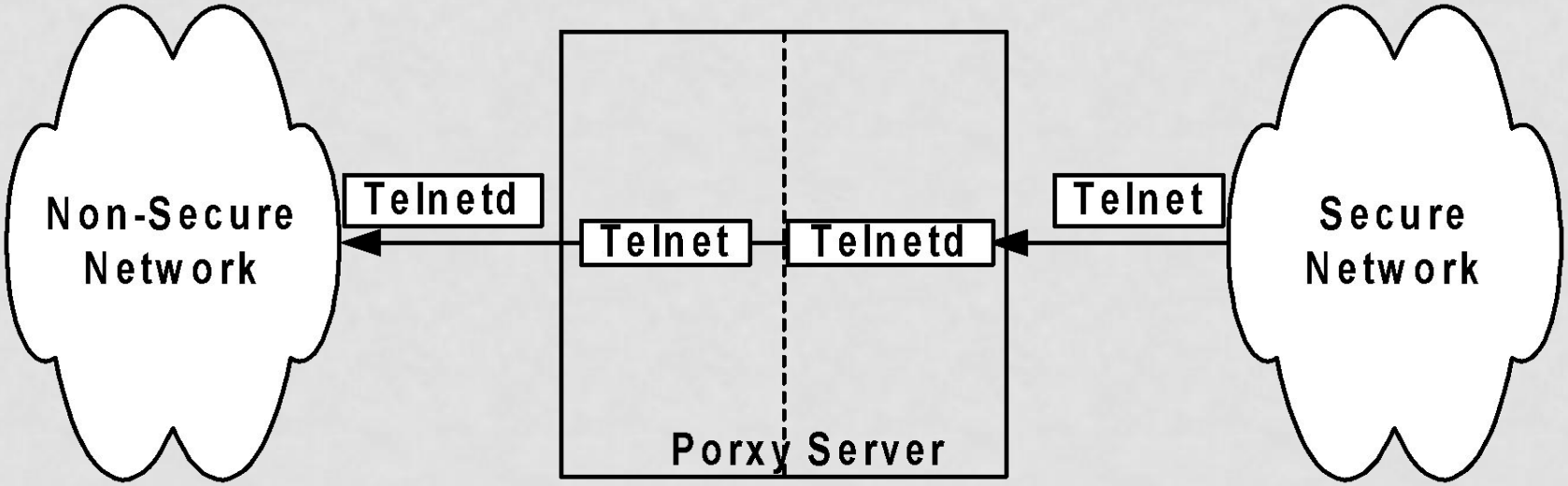
Packet Filter Cont..



Application Proxy

- Application Level Gateway
- The communication steps are as follows
  - User connects to proxy server
  - From proxy server, user connects to destination server
- Proxy server can provide
  - Content Screening
  - Logging
  - Authentication

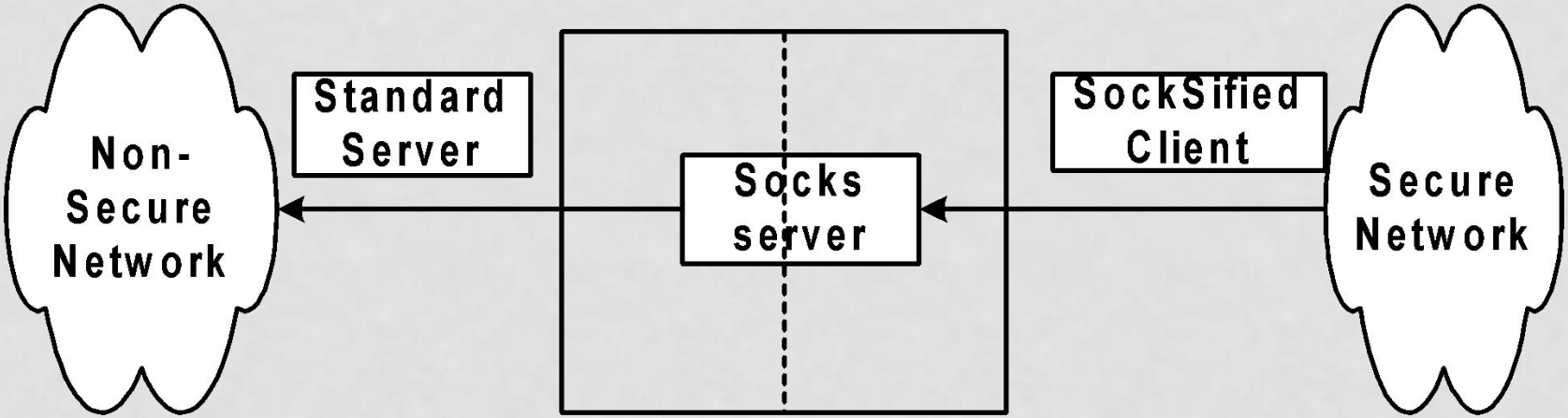
Application (telnet) Proxy Cont..



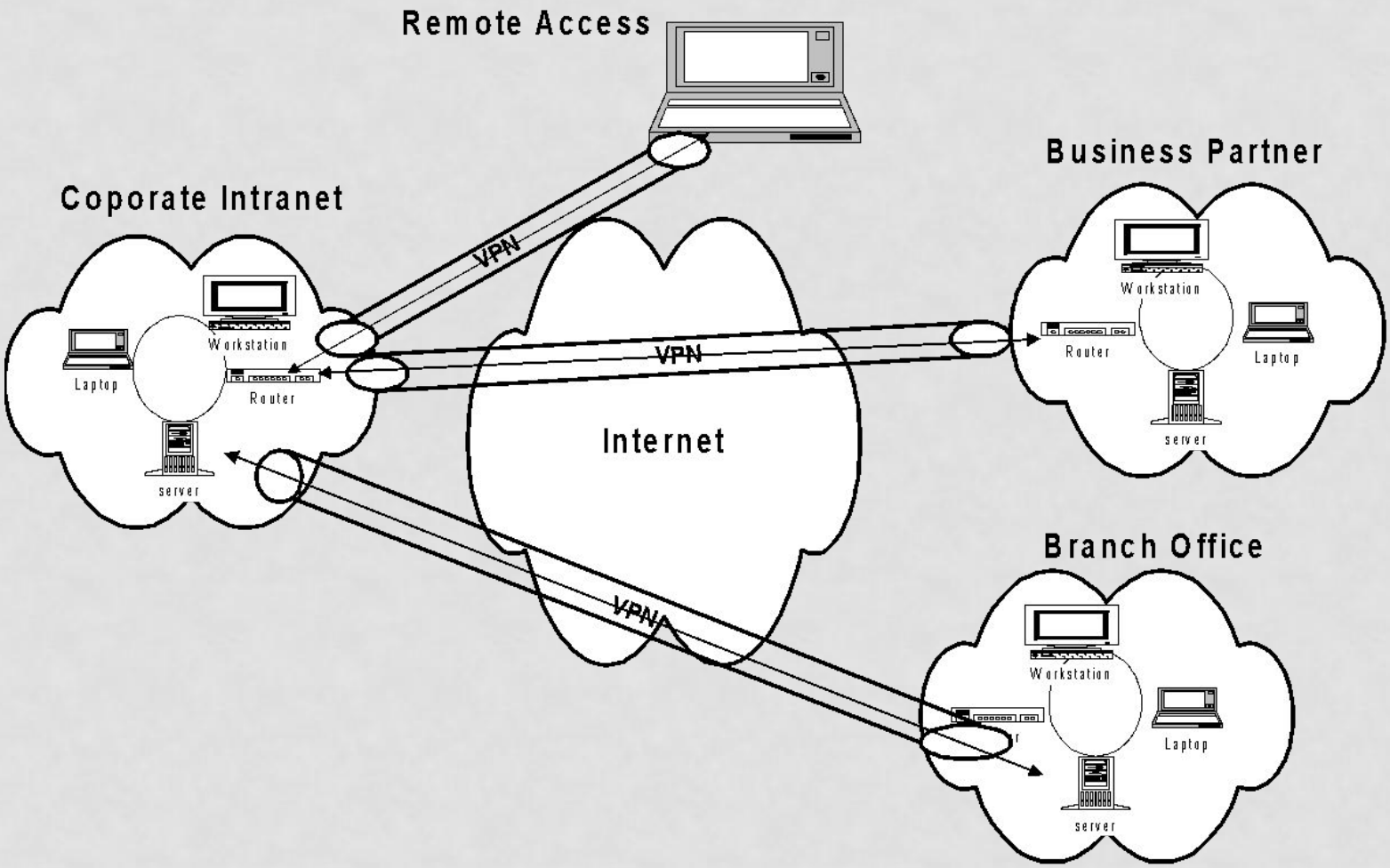
SOCKS Server

- Circuit-level gateways
- Generally for *outbound* TCP traffic from secure network
- Client code must be installed on the user's machine.
- The communication steps are as follows:
  - User starts application using destination server IP address
  - SOCKS server intercepts and authenticates the IP address and the userID
  - SOCKS creates a second session to non-secure system

Socks Servers Cont..



Secure Tunnel Cont..



Secure IP Tunnel

- A secure channel between the secure network and an external trusted server through a non-secure network (e.g., Internet)
- Encrypts the data between the Firewall and the external trusted host
- Also identifies of the session partners and the messages authenticity

VPN Solutions

- IP Security (IPSec)
- Layer 2 Tunnel Protocol (L2TP)
- Virtual Circuits
- Multi Protocol Label Switching (MPLS)

IPSec Solution

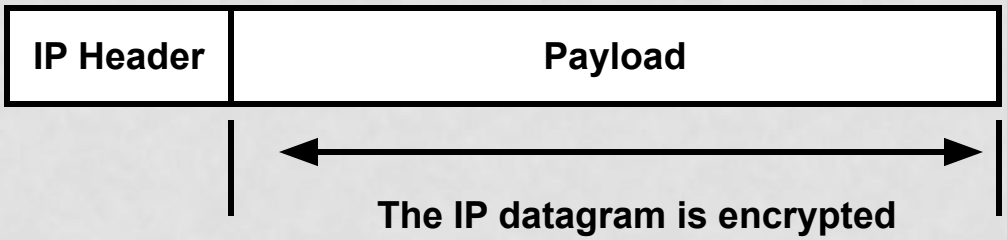
- IPSec is an Internet standard for ensuring secure private communication over IP networks, and it was developed by IPSec working group of IETF
- IPSec implements network layer security

Principle of IPSec protocols

- Authentication Header (AH)
  - Provides data origin authentication, data integrity and replay protection
- Encapsulating Security Payload (ESP)
  - Provides data confidentiality, data origin authentication, data integrity and replay protection
- Internet Security Association and Key Management Protocol (ISAKMP) or Internet Key Exchange (IKE)
  - Provides a method for automatically setting up security association and managing their cryptographic key.
- Security Association (SA)
  - Provides all the relevant information that communicating systems need to execute the IPSec protocols.

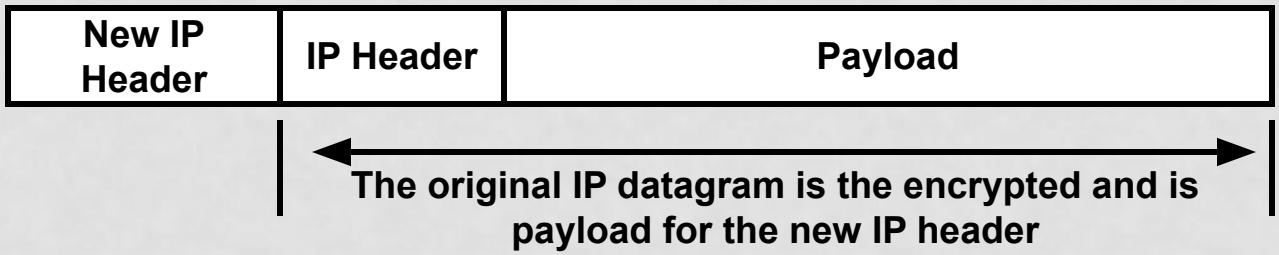
Operation Modes of IPSec

- Transport Mode
  - The IP payload is encrypted and the IP headers are left alone



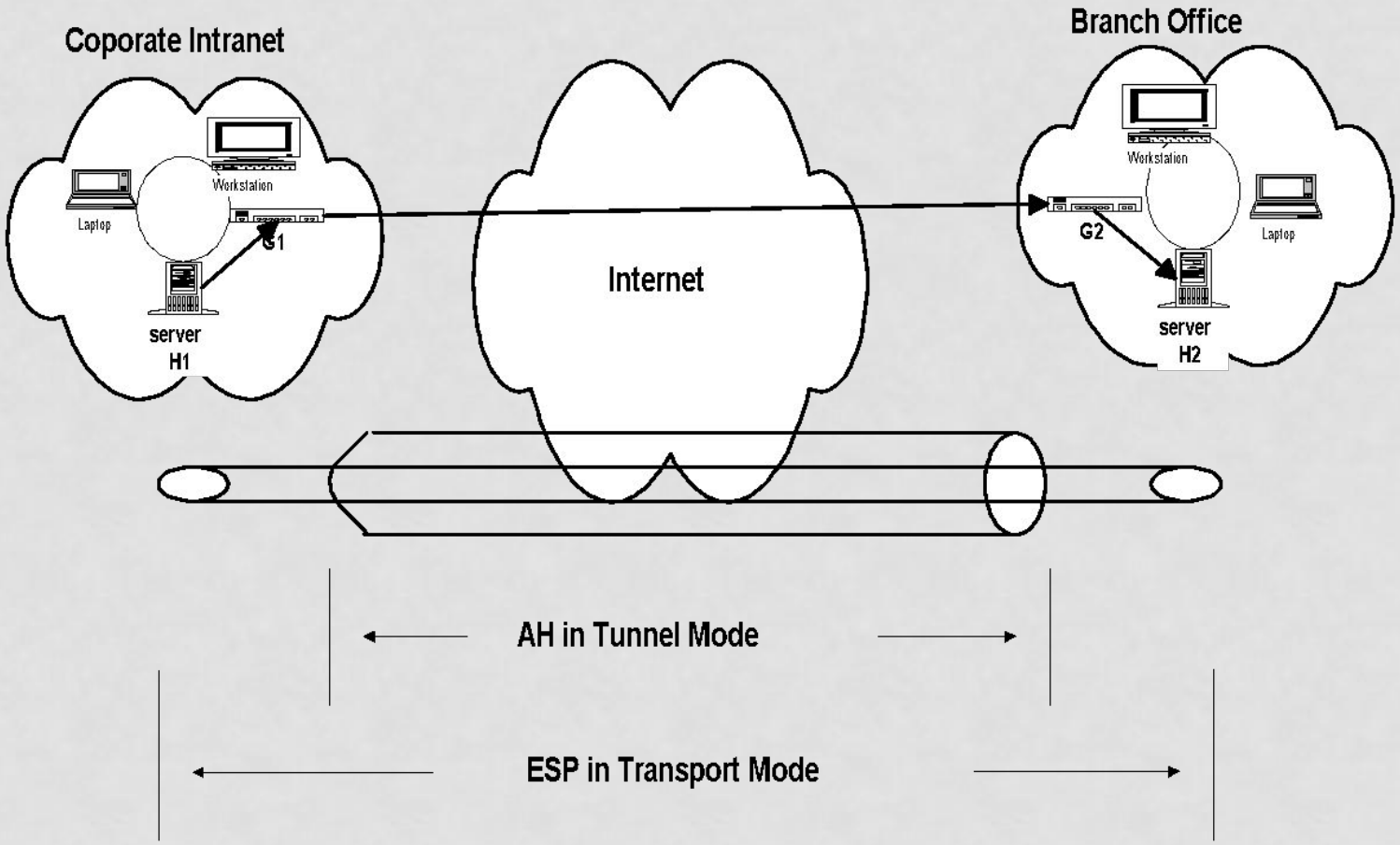
Operation Modes of IPSec Conti...

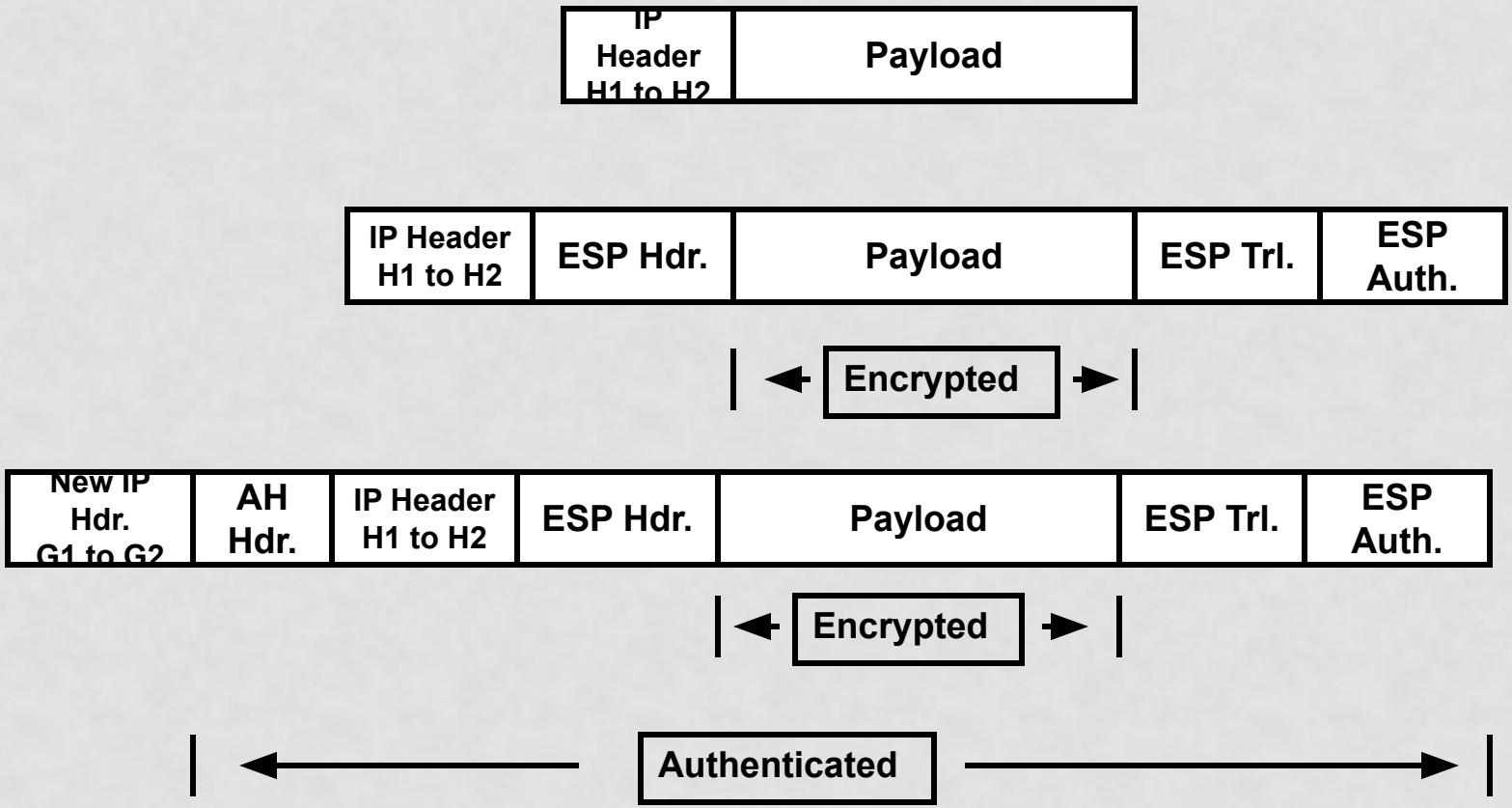
- Tunnel Mode
  - The entire original IP datagram is encrypted and it becomes the payload in the new IP

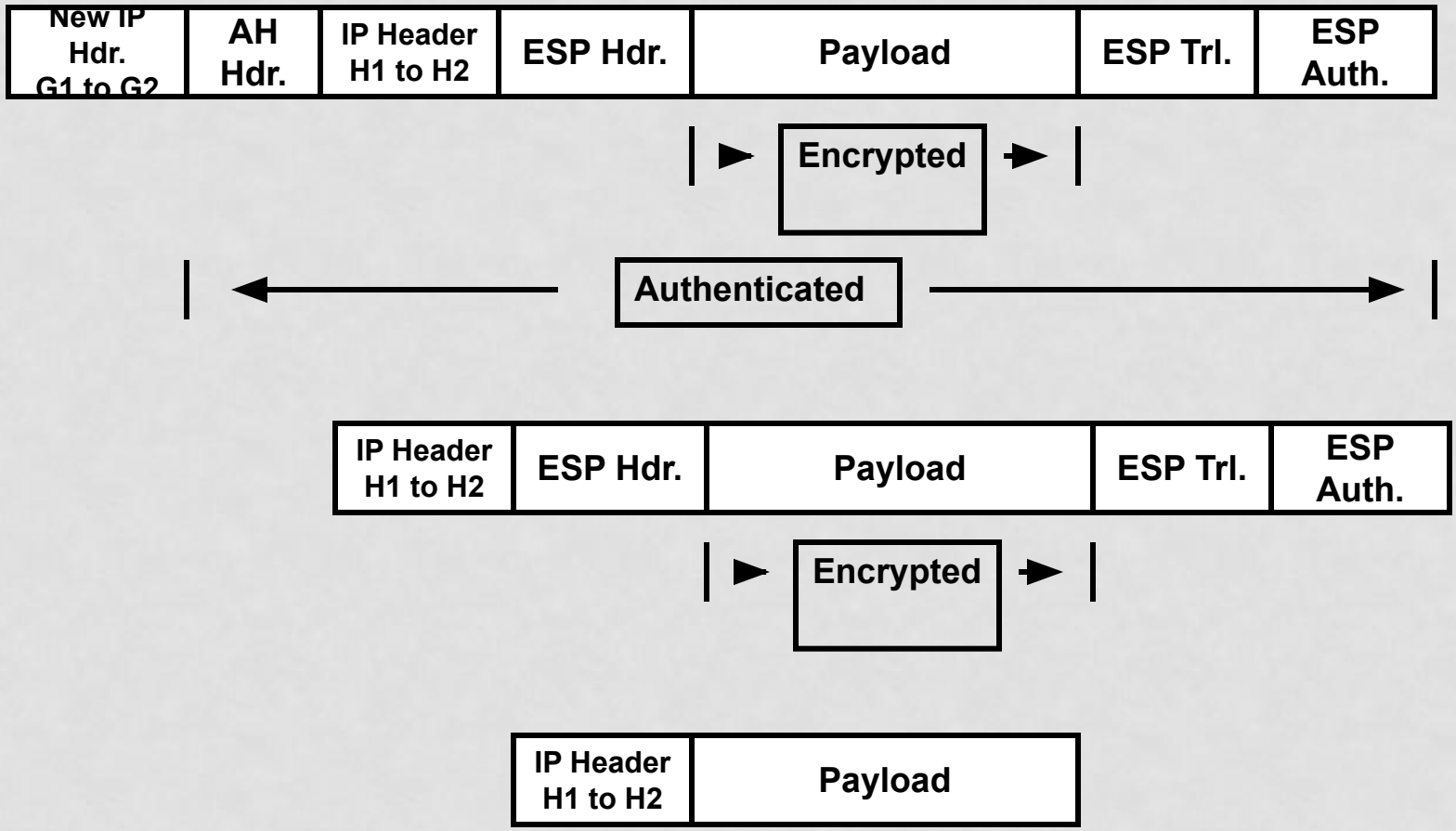


IPSec Example

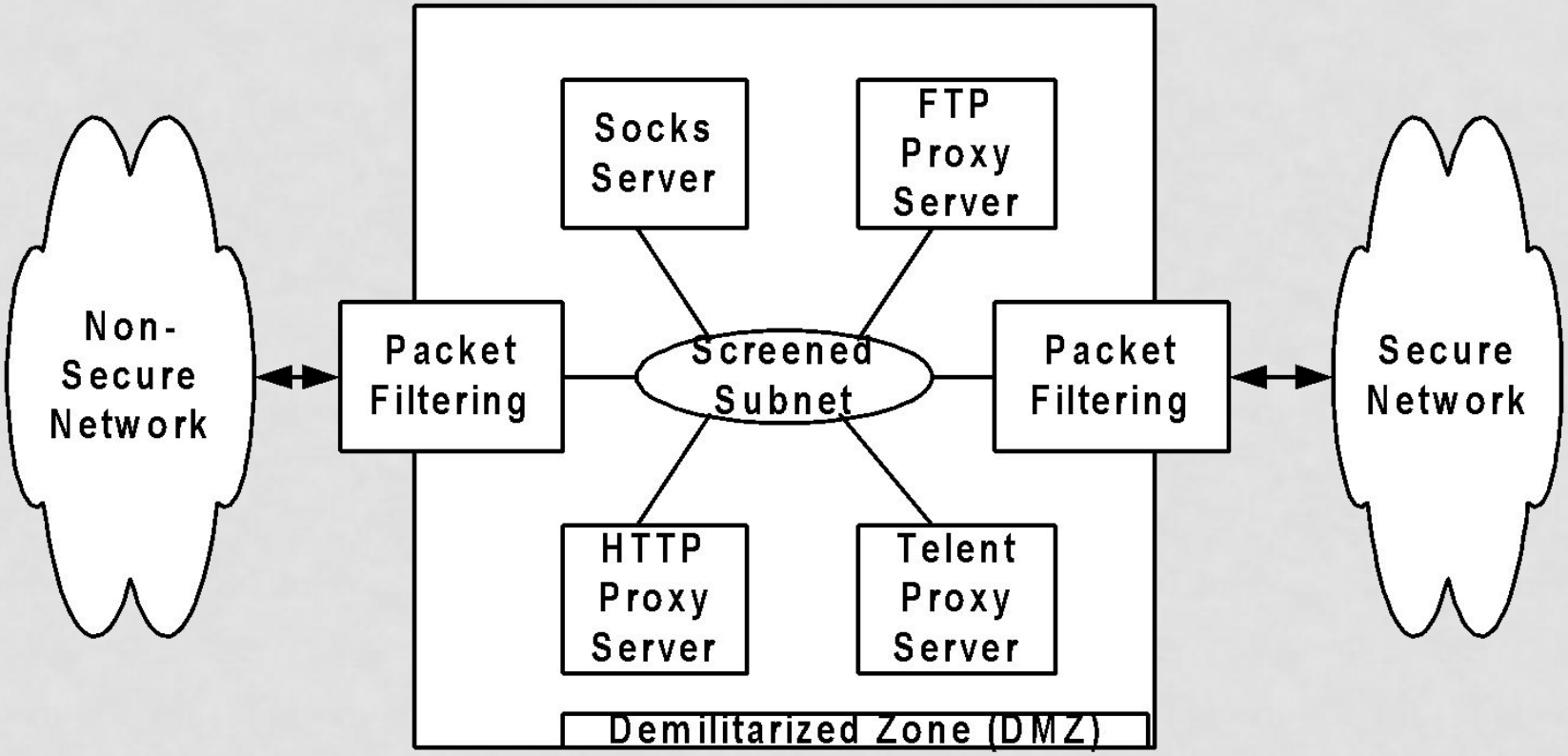
- This example combines IPSec protocols and is AH in tunnel mode protecting ESP traffic in transport mode. This example assume that the SA's for communicates points have set up.




IP Header H1 to H2
Payload
IP Header H1 to H2
ESP Hdr.
Payload
ESP Trl.
ESP Auth.
Encrypted
New IP Hdr. G1 to G2
AH Hdr.
IP Header H1 to H2
ESP Hdr.
Payload
ESP Trl.
ESP Auth.
Encrypted
Authenticated


New IP Hdr. G1 to G2
AH Hdr.
IP Header H1 to H2
ESP Hdr.
Payload
ESP Trl.
ESP Auth.
Encrypted
Authenticated
IP Header H1 to H2
ESP Hdr.
Payload
ESP Trl.
ESP Auth.
Encrypted
IP Header H1 to H2
Payload

Screened Subnet Architecture Cont..



Screened Subnet Architecture

- The DMZ (perimeter network) is set up between the secure and non-secure networks
- It is accessible from both networks and contains machines that act as gateways for specific applications

Firewall Conclusion

- Not the complete answer
  - The fox is inside the henhouse
  - Host security + User education
- Cannot control back door traffic
  - any dial-in access
  - Management problems
- Cannot fully protect against new viruses
  - Antivirus on each host Machine
- Needs to be correctly configured
- The security policy must be enforced