

# Cryptography Internet Security

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: cryptography\_internet\_security.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ Secure Protocols

### ➤ IPsec

- **Internet Protocol Security**
- **Work at Layer 3**
- **Ensures confidentiality and integrity to IP packets**
- **Uses either ESP or AH to secure the packets.**
- **They work only with IP they are NOT multi-protocol**
- **Authenticate and encrypt IP data**
- **Ensures confidentiality and integrity to IP packets**
- **Enable multiple and simultaneous tunnels**
- **Focus more on Network-To-Network connectivity**
- **Method of setting up a secure channel for protected data exchange between two devices**
- **IPsec - is more flexible and less expensive than application and Link-Layer encryption**
- **Widely accepted standard for secure network layer transport**
- **Have strong encryption and authentication methods**
- **IPsec - Use Public Key cryptography**
- **Useful for VPN and for remote user access through dial-up connection**
- **Is not a strict protocol that dictates the type of algorithm, keys, and authentication**
- **Is an open modular FRAMEWORK that provides a lot of flexibility**
- **Bi-directional communication requires two Security Associations**
- **A big advantage of IPsec does not require changes to individual user computers**
- **Provides**
  - Message integrity
  - Source authentication
  - Confidentiality
  - Authenticity
  - Encryption functionality
  - Access control
  - ONLY WORK WITH IP
- **Use Two Main Protocols**
  - Authentication Header (AH)
    - ◆ Is the authenticating protocol
    - ◆ Authenticate the sender of the packet by user or source IP address
    - ◆ When Added to IP datagram to ensure integrity and authenticity
    - ◆ Provides
      - Message integrity
      - Source authentication
  - Encapsulating Security Payload (ESP)

- ♦ Is an authentication Protocol + Encryption Protocol
  - ♦ When Added to IP datagram provides confidentiality, integrity and authenticity
  - ♦ Provides
    - Message integrity
    - Source authentication
    - Confidentiality
    - Encryption
  - AH and ESP can be used independently or together
- **Security Association (SA)**
  - At the heart of IPSec is the Security Association (SA)
  - Each device will have one Security Association (SA) for each session that it uses
  - SA is a record of the configuration the device needs to support an IPSec connection
  - A device keep track for all (SA) using a Security Parameter Index (SPI) 32 bit
  - SA is uniquely identified by using a random unique number Called (SPI)
  - SA is a method that IPSec uses to track IPSec communication sessions
  - SA is unidirectional
    - ♦ For each pair of communicating systems there are at least TWO security connections
    - ♦ One From A to B and one From B to A
  - Can contain
    - ♦ The authentication and encryption keys
    - ♦ The agreed upon algorithms
    - ♦ Key lifetime
    - ♦ Source IP address
- **IPSec - work in two modes**
  - Transport mode
    - ♦ Payload of the message is encrypted
  - Tunnel mode
    - ♦ Payload and the routing and header information is also encrypted
- **(S/MIME, SSL, SET, PEM, SHTTP)**
  - **Application Layer Security Protocols (S/MIME, SSL, SET, PEM)**
  - **S/MIME**
    - Secure Multi-Purpose Internet Mail Extensions
    - A secure method of sending email that uses RSA encryption system
    - S/MIME is included in the latest versions of the Web browsers
    - An alternative to S/MIME is PGP/MIME
    - Describes how encryption information and a digital certificate can be part of the msg
    - S/MIME follows the syntax provided in the Public-Key Cryptography Standard format #7
  - **SSH-2**
    - SSH is a program and a set of protocols that work together to provide a secure tunnel between two computers
    - SSH functions as a type of tunneling mechanism that provides terminal like access to remote computers
    - Provides authentication and secure transmission over vulnerable channels like that internet
    - A strong method of performing client authentication.
    - It supports authentication, compression, confidentiality, and integrity.
    - Uses RSA for certificate exchange
    - Uses triple DES for session encryption
    - Comprised of:
      - ♦ Transport Layer protocol

- ♦ User Authentication protocol
  - ♦ Connection Protocol
- **SSL**
  - Secure Sockets Layer SSL
  - Developed by Netscape in 1994
  - Protect communication channel instead of individual messages
  - An encryption technology that provide secure transactions
  - SSL is a layered approach to providing a secure channel
  - SSL secure the channel by providing End-To-End Encryption
  - SSL uses two Public Key (Asymmetric) and Private Key (Symmetric)
  - Uses symmetric key for private connections
  - Uses ASYymmetric key for peer authentication
  - Supports RSA public Key Algorithms, IDEA, DES, and 3DES, MD5 Hashing
  - SSL - lies beneath the Application layer (7) and above the Transport layer (4)
  - Can be used by telnet, FTP, HTTP and e-mail protocols.
  - Uses message authentication code for message integrity checking.
  - Protocol for managing the security of a message transmission on the Internet
  - Two-layered protocol
    - ♦ Contains the SSL record protocol
    - ♦ Contain the SSL handshake protocol
  - SSL is session based
    - ♦ The path stay open until one of the parties request to close it
    - ♦ Usually the client click on a different URL
  - Provides
    - ♦ Server authentication
    - ♦ Client authentication
    - ♦ Secure Communication
    - ♦ Data Encryption
    - ♦ Message integrity
  - TLS and SSL are an integral part of most Web browsers (clients) and Web servers
  - Transport Layer Security (TLS) is replacing SSL
  - TLS and SSL are not interoperable.
    - ♦ Msg TLS -> SSL = OK
    - ♦ Msg SSL -> = NOT OK
  - TLS is based on SSL
- **SET**
  - Secure Electronic Transaction
  - Developed in 1997 by VISA and mastercard as a means of preventing fraud.
  - It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others
  - It supports the authentication of both the sender and the receiver
  - Created to support Internet transactions and authentication.
  - It ensures content privacy using digital certificates and signatures.
  - Uses DES symmetric key system for encryption of the payment info
  - Uses RSA for the symmetric key exchange and digital signature.
  - SET uses some but not all aspects of a public key infrastructure
  - SET requires 2 pairs of asymmetric keys and 2 digital certificates!
  - Operate at the application (7) layer
  - Is being overtaken by SSL
  - SET is comprised of three main parts
    - ♦ The Electronic Wallet

- ♦ The software running on the merchant's server at its web site
- ♦ The payment server that is located at the merchant's bank
- How SET works
  - ♦ 1. The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.
  - ♦ 2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been digitally signed by the bank to ensure its validity.
  - ♦ 3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
  - ♦ 4. The customer places an order over a Web page, by phone, or some other means.
  - ♦ 5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
  - ♦ 6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.
  - ♦ 7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
  - ♦ 8. The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
  - ♦ 9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
  - ♦ 10. The bank digitally signs and sends authorization to the merchant, who can then fill the order
- **SHTTP**
  - Secure Hypertext Transport Protocol
  - Early standard for encrypting HTTP documents.
  - Created to support Internet transactions and authentication.
  - The HTTP server caches and secures stored S/HTTP documents.
  - Operate at the application (7) layer
  - Encrypts messages with session keys that are calculated
  - Can support multiple encryption modes and types
  - SHTTP - is not a stateless protocol like HTTP
  - SHTTP - is a technology that protects each message sent between two PCs
  - Used when an individual message needs to be encrypted
  - Can use public key technology and symmetric encryption
  - Used when an individual message needs to be encrypted
  - SHTTP - compute a hash value of the message and the value can then be digitally signed
  - Can be used to secure individual WWW Documents
  - Can use public key technology and symmetric encryption and PEM
  - Developed to provide secure communication.
  - Encrypts messages with session keys that are calculated.
  - Provides integrity and sender authentication capabilities.
  - Is not a stateless protocol
  - Can support multiple encryption modes and types.
  - Is being overtaken by SSL
  - Provides
    - ♦ Authentication
    - ♦ Data Integrity
    - ♦ Security policies

- ♦ Key management
- **HTTPS**
  - Developed to provide secure communication
  - Protects the communication channel between two computers
  - Uses SSL and HTTP to provide a protected circuit between a client and server
  - Used when all information that passes between two computers needs to be encrypted.
- **SKIP**
  - (Simple Key Management for Internet Protocols).
  - Provides high availability in encrypted sessions (e.g, crashed gateways).
  - Requires no prior communication in order to exchange keys
- **PEM**
  - Created by the IETF to act for email in a similar fashion as IPSEC does to IP.
  - The standard was finalized in 1993
  - PEM is an application-layer security protocol developed by the IETF
  - Add confidentiality and authentication services to electronic messages on the Internet
  - Could be implemented on any host
  - Compatible with existing mail systems
  - Support standard key management schemes
  - Protect both individually addressed and list-addressed mail
  - Not interfere with non secure mail delivery
  - Can be MIC-CLEAR and provide integrity and authentication only
  - Can be ENCRYPTED and provide integrity, authentication, and confidentiality
- **(SKIP, SWIPE)**
- **Secure Telnet**
- **(CHAP) (PAP)**
- **PAP**
  - Password Authentication Protocol
  - Username and password are sent in clear
  - Is the most basic form of authentication
  - User's name and password are compared to a table of name-password pairs
  - Typically, the passwords stored in the table are encrypted
  - The Basic Authentication feature built into the HTTP protocol uses PAP
  - Shouldn't even be considered as an appropriate method of authentication
  - Use static replayable password for authentication
  - Does not encrypt the user ID or password
  - Both the username and password are transmitted "in the clear"
- **CHAP**
  - Challenge Handshake Authentication Protocol
  - Password Authentication Protocol
  - Authenticates using a challenge response mechanism
  - Server will send the client a key to encrypt the username and password
  - Send logon credentials encrypted.
  - Only thing sent across the line is a hashed (MD5) value
  - Unidirectional, so a server can challenge a client for a password
  - Commonly used by xDSL, ISDN and cable modems
  - CHAP provides more security than PAP
- **MS-CHAPv2**
  - MicroSoft's CHAP version 2

- Increasing the initial size of the encryption keys
- Requires a challenge in both directions
- **(PPP) (SLIP) (PPTP) (L2TP)**
  - **PPP**
    - Point-to-Point Protocol
    - A protocol for communicating between two computers using serial interfaces
    - PPP uses the Internet protocol (IP)
    - It uses IP to transfer the traffic but operates at layer 2
    - PPP is a full-duplex protocol that can be used on various physical media
    - It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation
    - Can handle synchronous as well as asynchronous communication
    - PPP can share a line with other users
    - It has error detection that SLIP lacks
    - PPP is usually preferred over the earlier de facto standard (SLIP)
  - **SLIP**
    - Serial Line Internet Protocol
    - Allow two machines to communicate that have been previously configured
    - A better service is provided by the Point-to-Point Protocol (PPP)
  - **PPTP**
    - Point To Point Tunneling Protocol
    - Work at the Data Link Layer (2)
    - Enable ONLY one single point-to-point connection per session
    - Use PPP authentication and encryption services
    - Use PAP or CHAP
    - It is asynchronous
  - **L2TP**
    - Combination of PPTP and earlier Layer 2 forwarding Protocol
    - Dial-up VPN use this standard
    - Designed for Single Point-To-Point client to server Like PPTP
    - Multiple protocol can be encapsulated within L2TP tunnel
    - Work at the Data Link Layer (2)

## ❖ Un-Secure Protocols

- **BootP**
- **NFS**
- **LPD**
- **SNMP**
- **SMTP**
- **TFTP**
- **FTP**
- **Telnet**
- **Xwin**

## ❖ Email Security Issues

- **PEM**
  - **Privacy-Enhanced Mail**
  - **Developed by consortium of Microsoft, Sun, and Novell**

- **PEM - use DES for encryption**
- **PEM - use RSA for sender authentication and key management**
- **Compliant with Public Key Cryptography Standards (PKCS)**
- **Provides**
  - Authentication
  - Message integrity
  - Nonrepudiation
  - Encryption
  - Digital Signature
  - Key management
- **Components used in PEM**
  - Authentication is provided by MD2 and MD5 Message Digest
  - Messages encrypted with DES in CBC mode
  - Public key management provided using RSA
  - X.509 standard used for certification structure and format

#### ➤ **MSP**

- **Message Security Protocol is the military's PEM**
- **Was developed by NSA**
- **MSP - used to secure e-mail messages**
- **MSP - is an X.400 compatible application level protocol**
- **Provides**
  - Digital Signature
  - Encryption
  - Authentication
  - Message integrity (hashing functions)

#### ➤ **PGP**

- **Designed by Phil Zimmerman**
- **First widespread public key encryption program**
- **Use IDEA (symmetric) cipher for bulk encryption of data**
- **Uses RSA (Asymmetric) public key encryption for key management**
- **PGP uses passphrases, to encrypt the user's private key**
- **Four (4) types of PGP certificates**
  - Make up yourself
  - Provided commercially
  - Vouching on business relationship
  - Authenticated individual activity
- **RSA is used for signatures and key distribution**
- **PGP - does not use CA but it uses "web of trust"**
  - Users can certify each other
- **PGP - use Key ring**
  - Each user keeps a collection of signed public keys
- **Provides**
  - Confidentiality
    - ◆ Through the IDEA encryption algorithm
  - Authentication
    - ◆ Through the public key certificates
  - Message integrity

- ♦ Through MD5 hashing algorithm
- Nonrepudiation
  - ♦ Through cryptographically signed messages
- Encryption
- Digital Signature
- Key management
  - ♦ Through a "web of trust"
- **Most common are PGP and S/MIME**

### ➤ **MOSS**

- **MIME Object Security Services (MOSS)**
- **Provides flexibility by supporting different trust models**
- **Uses MD5, RSA Public Key and DES**
- **Permits identification outside of the X.509 Standard**
- **MOSS - Provides**
  - Authenticity
  - Integrity
  - Confidentiality
  - Non repudiation

### ➤ **MIME**

- **Multi-Purpose Internet Mail Extensions**
- **Specification indicating how multimedia data and email attachments are to be transferred**
- **MIME spells out how an electronic message will be organized**
- **Servers insert the MIME header at the beginning of any Web transmission**
- **Clients use this header to select a "player" for the type of data the header indicates**

### ➤ **S/MIME**

- **Secure Multi-Purpose Internet Mail Extensions**
- **A secure method of sending e-mail that uses the Rivest-Shamir-Adleman encryption system**
- **Describes how encryption and a digital certificate can be included in the message body**
- **Adds secure services to messages in MIME format**
- **Provides authentication through digital signatures**
- **Follows Public Key Cryptography Standards (PKCS)**
- **Uses X.509 Signatures**
- **Included in most browsers Microsoft and Netscape**
- **Most common are PGP and S/MIME**

## ❖ **ISAKMP**

- **Internet Security Association and Key Management Protocol**
- **ISAKMP is an authentication and key exchange architecture**
- **Key management can be handled by (ISAKMP)**

## ❖ **IKMP**

- **Internet Key Management Protocol**
- **IKMP is used to negotiate security Association (SA)**

## ❖ **IKE**

- **Internet Key Exchange**
- **The standard method of configuring security association for IPSec**
- **IKE creates an authenticated secure tunnel between two entities**
- **Provide flexible framework for authentication that support multiple authentication methods**
- **Both parties must have a shared session key in order to encrypt the IKE tunnel**
- **Mechanisms implemented**
  - **Pre-shared Keys**
    - The same Key is pre-installed on each host
  - **Public Key Cryptography**
    - Each party generates a pseudo-random
  - **Digital Signature**
    - Each device digitally signs a set of data and sends it to the other party

## ❖ **Kerberos**

- **" Kerberos (MIT project Athena)**
- **A trusted, third party authentication protocol that was developed at MIT.**
- **Widely used to authenticate users and uses encryption to secure authentication data**
- **Using symmetric key cryptography, it authenticates clients to other entities on a network of which a client requires services**
- **Kerberos secret-key authentication system involves a central database that keeps copies of the secret keys of all users**
- **Use Transmission by ticket**
- **Kerberos issues and use tickets**
- **Tickets**
  - Both based on private key encryption
  - Securely pass identity of person Between authentication server and end server
- **Ticket use**
  - Single server and single client
  - Contains: server and client's names, client Internet address, timestamp, Lifetime, random session key
  - Encrypted in key of server
- **A distributed Kerberos implementation is generally not sufficient for Nonrepudiation service**
- **This is because with Kerberos, two parties have to possession of the same symmetric key which can be forged or altered.**
- **An attack on the database would allow widespread forgery**

## ❖ **MONDEX**

- **Smart cash card application**
- **Proprietary encryption algorithm**
- **Card is same as cash**

## ❖ **Wireless Application Protocol WAP**

- **WML Wireless Markup Language**
- **WAE Wireless Application Environment**
- **WSP Wireless Session Protocol**
- **WTP Wireless Transport Protocol**
- **WTLS Wireless Transport Layer Security**
- **WDP Wireless Datagram Protocol**
- **The IEEE 802.11 Wireless Standard**
  - **802.11 Layers**
- **For security WAP uses Wireless Transport Security Protocol (WTLS)**
  - **Class 1 - Anonymous Authentication**
  - **Class 2- Sever Authentication**
  - **Class 3 - Two way client and server authentication**

## ❖ **Secure wireless traffic**

- **Radio waves cannot be directly observed without equipment.**
- **Data sent by this means a difficult risk to manage.**
- **WAP**
  - **Protocol in low-bandwidth, high-latency wireless devices**
  - **WAP is a wired access point, which is the “wireless hub”**
  - **Data is sent in compressed binary packets.**
  - **HTML replaced with Wireless Markup Language (WML)**
  - **WAP UDP**
  - **Overcomes the limitations of being UDP by the WAP Gateway**
- **802.1x**
  - **Provide authentication mechanism over physical media**
  - **Used to improve the privacy of wireless LAN**
  - **To get authentication functionality**
    - **You must choose a particular flavor of EAP**
    - **Install it on your authentication server.**
    - **Transport Layer Security (EAP-TLS)**
    - **RADIUS (FRC 2138,2139)**
    - **LEAP84, by Cisco**
  - **IEEE - 802.11 Standards**
    - **Interface between clients and base station**
    - **The physical layer can use:**
      - ◆ **DSSS - Direct Sequence Spread Spectrum**
      - ◆ **FH - Frequency Hoping Spread Spectrum**
      - ◆ **IR - Infrared pulse modulation**
    - **MAC Layer - Medium Access Control**
    - **Specifies CSMA/CA Carrier Sense Multiple Access Collision Avoidance**
    - **Provides:**
      - ◆ **Data Transfer**
      - ◆ **Association**
      - ◆ **Re-association**
      - ◆ **Authentication - WEP**

- ♦ Privacy - WEP
- ♦ Power Management
- 802.11b works at 2.4 GHz and provides data rates up to 11 Mbps
- 802.11b standard uses the Wireless Application Protocol (WAP)

### ➤ **Wireless Requires**

- **To connect to an 802.11b LAN, you must know**
- **SSID (Service Set Identifier)**
- **WEP (Wired Equivalent Privacy) key**

### ➤ **Security method**

- **WEP**
  - WEP (Wired Equivalent Privacy)
  - WEP works by using a RC4 encryption scheme,
  - With a key that can be 40, 64 or 128 bits
  - WEP Uses a shared key
  - Key must be the same among all the devices
  - Key reuse breaks a cardinal rule in RC4 design. (GOOD PART)
  - WEP on is better than no WEP.
  - It is possible to “break” this WEP encryption
- **WTLS**
  - Wireless Transport Layer Security
  - WTLS is the WAP security protocol
  - Provides privacy, data integrity and authentication for WAP
  - Suited for the low-bandwidth, high-latency, less robust
- **802.11x**
  - Be careful not to confuse this with 802.1X,
  - Wireless Requires
  - In the future, 802.11i will include support for TKIP
  - (Temporal Key Integrity Protocol)

### ➤ **Vulnerabilities**

- **Data stored in plaintext**
- **A larger rock will make stronger waves than a smaller rock.**
- **Shielding issues**
- **Wireless Configuration**
- **Shared Frequencies**
- **Unauthorized access**
- **Viruses**
- **Buffer overflows**
- **2.6.4.1. Site Surveys**
  - Perform a Technical Surveillance Counter Measures (TSCM)
  - Consider installing in place monitoring devices
  - Searches for light based Infra-Red (IR) or cellular phone based
  - Netstumbler is useful for finding the rogue access point
  - Kismet add support for GPSDrive
- **802.11a**
  - It operates in a different frequency, reducing hardware attacks against you.
  - 802.11a has a much shorter range.
  - Bandwidth of 54Mbps up to 75Mbps

- Encryption in some products goes up to 156bit

### ➤ Harden

- **Change the password on access points.**
- **Turn off DHCP and assign static addresses,**
- **Make sure hardware has upgradeable firmware.**
- **Consider configurations that are “closed”**
- **Use an access point that does not broadcast an SSID.**
- **Enable MAC filtering on your wireless routers**
- **Enable data encryption with WEP, WTLS, or 802.1x**
- **Limit administrative access to your wireless routers**

## ❖ Key Management

### ➤ Key Management Issues

- **The principle of key management**
  - Must be fully automated
  - No key in clear outside of crypto device
  - The key is what brings secrecy to encryption
  - The keys can be captured, modified, corrupted or disclosed
  - Key management is the most challenging part of cryptography
  - More key is used, more likely a successful attack and greater the consequences
  - A longer key will provide better protection than a shorter key
- **Rules**
  - The key length should be long enough to provide a good protect
  - Keys should be stored and transmitted by secure means
  - Keys should be extremely random and use the full spectrum of the keyspace
  - Key's lifetime should correspond with the sensitivity of the data it is protecting
  - The more the key is used, the shorter its lifetime should be
  - Keys should be properly destroyed when their lifetimes come to end
  - Keys should be backed up or escrowed in case of emergencies
- **Types of key management**
  - Two communication levels
    - ♦ Link encryption
    - ♦ End-To-End
  - Link encryption
    - ♦ Link layer encryption happens at LOWER layers (Physical) of the OSI
    - ♦ Hardware encryption devices interface with the physical layer it encrypt all data that pass
    - ♦ No part of data is available to attacker this is called TRAFFIC-LOW security
    - ♦ It encrypt the following
      - Encrypts all the data along a specific communication path
        - Satellite link, or
        - T3 line
        - Telephone circuit
      - User information
      - Header
      - Traillers
      - Addresses and routing data
    - ♦ Advantages
      - All data is encrypted, including headers, addresses, and routing information
      - Users do not need to do anything to initiate it, it work at a lower layer in the OSI model

- Provides protection against packet sniffers and eavesdroppers
- ◆ Disadvantages
  - Key distribution is more complex because each HOP computer must receive a key
  - Messages are decrypted at each HOP, thus, there are more points of vulnerabilities
- End-To-End encryption
  - ◆ Is usually initiated at the application layer
  - ◆ Only information is encrypted
  - ◆ Stays encrypted from one end of its journey to the other
  - ◆ It Does not encrypt the following
    - Header
    - Trailers
    - Addresses
    - Routing Data
  - ◆ Advantages
    - It protects information from start to finish throughout the network
    - It provides more flexibility to the user in choosing what gets encrypted and how
    - Granularity of encryption because each application or user can use a different key
    - Each hop computer on the network does not need to have a key to decrypt each packet
  - ◆ Disadvantages
    - Headers, addresses, and routing information are not encrypted
    - The destination system needs to have the same encryption mechanisms as source

- **Key Management Issues**

- -key control measures
- -key recovery
- -key storage
- -key retirement/destruction
- -key change
- -key generation
- -key theft
- -Frequency of key use
- -NOT KEY EXCHANGE!!!!

- **Key recovery and key recovery systems**

- **Kerberos**

- **Use key distribution center (KDC) To:**
  - Store Key
  - Distribute keys
  - Maintain keys

- **Diffie-Hellman**

- **Uses a key exchange algorithm (KEA)**

## ❖ **Secure client Internet access**

- **Browsers are applications and vulnerable to same attacks**

- **Vulnerabilities**

- **ActiveX**

- ActiveX is a Microsoft technology for downloading miniature executable
- The ActiveX controls execute on the client machines
- Attackers can create malicious ActiveX scripts
- That can be downloaded and executed on users' systems
- ActiveX controls must be specifically compiled for the processor and os
- ActiveX can be embed in a Web page

- ActiveX uses digital code signing in the form of a digital certificate
- To identify the origin of the control.
- Signed scripts and applets help reducing this threat
- Does not guarantee that the functionality of the control is not malicious.
- **CGI scripts**
  - Way of executing an external program or “script” on the server
  - CGI scripts can provide system information
  - Can be used to execute commands
  - Very difficult to get them right.
- **Cookies**
  - Piece of information sent from a web server to a web browser
  - Stored on the user’s PC for future use.
  - Cookies can provide attackers with private user data
  - Can be stolen and replayed at later time (“cookie snarfing”)
  - Contain information that was provided by the user to the web server
- **Java Script**
  - Java Script is human-readable program code
  - Can be included on a web page.
  - Java Script code runs within the user’s browser
  - Java Script can also run on the server side of a web connection,
  - Java Script is also found in many HTML emails
  - Run malicious code
- **Signed Applets**
  - Enables its authenticity and data integrity to be guaranteed by its author
  - Trusted third party called a certificate authority verify the identify
  - Signing an applet does not protect against malicious code
  - Just gives you an idea of who to blame
- **Spyware**
  - Used to relay private information to attackers
- **Buffer Overflows**
  - Program tries to copy too much data into too small an area of the memory
  - Causing the data to fill up that area and overwrite other areas
  - This may crash the computer
  - Or enable an attacker to execute program code
- **Logging and Privacy**
  - Logging that occurs on a web server can compromise user privacy
  - By providing a history of the user’s visits to a site.
  - Damaging to individual privacy are browser history, “favorites” or “bookmark”
  - Assisting with this logging can be “web bugs”

➤ **Harden**

- **Configure Internet zone security in your browser**
- **Configure content ratings**
- **Prevent the download of unsecure cookies.**
- **Prevent the browser from saving user passwords**
- **You can automate this process by using Kit (IEAK)**

❖ **Secure the remote access channel**

- **Remote access servers and connections are vulnerable to many attack**

➤ **Remote Access Protocol Port Numbers**

- 500 ISAKMP
- 1293 TCP/UDP IPSec
- 1701 L2TP
- 1723 PPTP

➤ **Vulnerabilities**

- **Wardialers**
  - Used to dial every available phone # to find modems
  - Wardialers include ToneLoc and PhoneSweep.
  - A wardialer can detect the type of PBX
- **Improperly configured**
  - Could lead to brute force attacks against a dial-in server
- **PBX systems**
  - PBX systems ship with default user names / Pass

➤ **Harden**

- **Disable PPTP on your remote access server.**
- **Limit administrative access to the remote access server.**
- **Configure input and output filters to only allow valid traffic**
- **Set up a static pool of addresses to give out to remote clients**
- **Place the remote access server behind firewalls**
- **Enabling auditing or logging**
- **Keep current with security patches**