Wireless Network Security

Wireless Information warfare

- The information warfare (IW) model helps us to define the relationships relative to the security of a wireless communications system.
- It is necessary to integrate these concepts with specific measures such as cryptographic, anti-jamming (A/J), and low probability of detection (LPD) and apply them to commercial and military operations.

The Objective of the Countermeasures for the each security property

- Availability of information services (processes) or information may be attacked to achieve disruption or *denial of services* (DoS).
- Integrity of information services or content may be attacked to achieve

corruption objectives: deception, manipulation of data, selective enhancement, or disinformation.

- Confidentiality or privacy of services or information may be attacked to achieve exploitation objectives.

Protecting Privacy

- Privacy always has been a concern for modern society.
- Why is our awareness of privacy heightened?
- *Carnivore* is a computer automated snooping tool developed by the FBI that is capable of intercepting and sorting out millions of text messages from many sources such as telephone conversations, Internet, e-mail, radio's and satellite downlinks to reduce to *intelligence take*.
- Our virtual world of banking online, paying bills online, doing anything we want online comes at a price: we have to share our vital information with virtual persons.

A Taxonomy Based on Mobility Only

- Consider the general problem of providing connectivity to mobile users through a supporting infrastructure of base stations.
- One could use a single base station capable of covering the entire area, or a number of base stations, each covering a smaller area.
- The transfer of a user connection from one base station to another is called a *handover.* Base stations must track the locations of mobile users even when they are not connected so that connections can be established to them at any time.

A Model for Cost-Effective Risk Management

- A fundamental problem of risk management and then is to link the choice of design characteristics and of counter measures to threat and impact, in order to create a cost-effective balance that achieves an acceptable level of risk.
- This uncertainty is a contributing cause of our tendency to rely on risk avoidance.
- By assuming the threat to be capable, intense, and competent, by valuing our potential targets highly, and by conservatively estimating uncertainties.

1. The impact of loss of or damage to the potential target.
2. **Specify the level of risk of damage or destruction that is acceptable**. This may well be the most difficult part of the process.
3. **Identify and characterize the threat**. The leaders of our country, diplomats, military commanders, and intelligence and counterintelligence officers who constantly seek to understand the capabilities, intentions, and activities of our enemies perform this function. The damage that can be caused by accident, disease, or such natural forces as earthquakes, hurricanes, tornadoes, fires, or floods and Criminal behavior can be described and predicted.

4. **Analyze vulnerabilities** for individuals, dietary and exercise regimens can reduce vulnerability to some health threats. Fire and intrusion alarms can detect problems and alert response teams. Computer systems and networks can be designed to be less vulnerable to hacker attacks.
5. **Specify counter measures**, where vulnerabilities are inherent or cost too much to eliminate during the design and development of facilities or systems, countermeasures must be selected to reduce risk to an acceptable level. Access to facilities can be controlled.
6. No countermeasure is completely effective, and, short of complete destruction, the impact of damage to an asset is problematic. Risk management requires the realistic assessment of uncertainties, erring on neither conservative nor optimistic sides.

Cryptographic Attacks

- The most devastating attacks on a wireless system are those that involve the cryptographic security of the system or network.The analysis and breaking of encryption is performed to penetrate cryptographic information security to:

1. Gain one-time access to information that has been encrypted. This information may represent knowledge, electronic funds, certification, or many other information representations.
2. Commit one-time security forgery (for example, to create a secure authentication).
3. Spoof a user by presenting a valid authentication intercepted and copied from a valid user.
4. Fully understand an encryption and keying process to permit repeated and full access to traffic on the targeted system.

Cryptanalysis attacks seek to locate access vulnerabilities of the general cryptographic system

Securing WLANS

- A WLAN operates in the same manner as a wired LAN except that data is transported through a wireless medium—usually radio waves—rather than cables.
- Accordingly, a WLAN harbors many of the same vulnerabilities as a wired LAN, plus some that are specific to it. This section discusses common threats facing WLANs, some of the countermeasures that have been designed to address those threats, and the strengths and limitations of those countermeasures.

Classical cryptanalysis

- Classical cryptography had a weakness that was security-fatal—linguistic patterns or repetitions.
- Linguistic patterns hold true for every language and follow through from plaintext to cipher text.
- Unique attributes of letter and word usage in languages have helped cryptanalysts decrypt secret messages for more than 3,000 years.
- An attempted cryptanalysis is called an attack.
- Cryptologists always assume that enemies know the encipherment and decipherment algorithms, so security resides entirely in the key or keys used by the cipher.
- By knowing the frequencies with which English letters in occur, it is possible to determine almost immediately if a cipher is a transposition or a substitution.

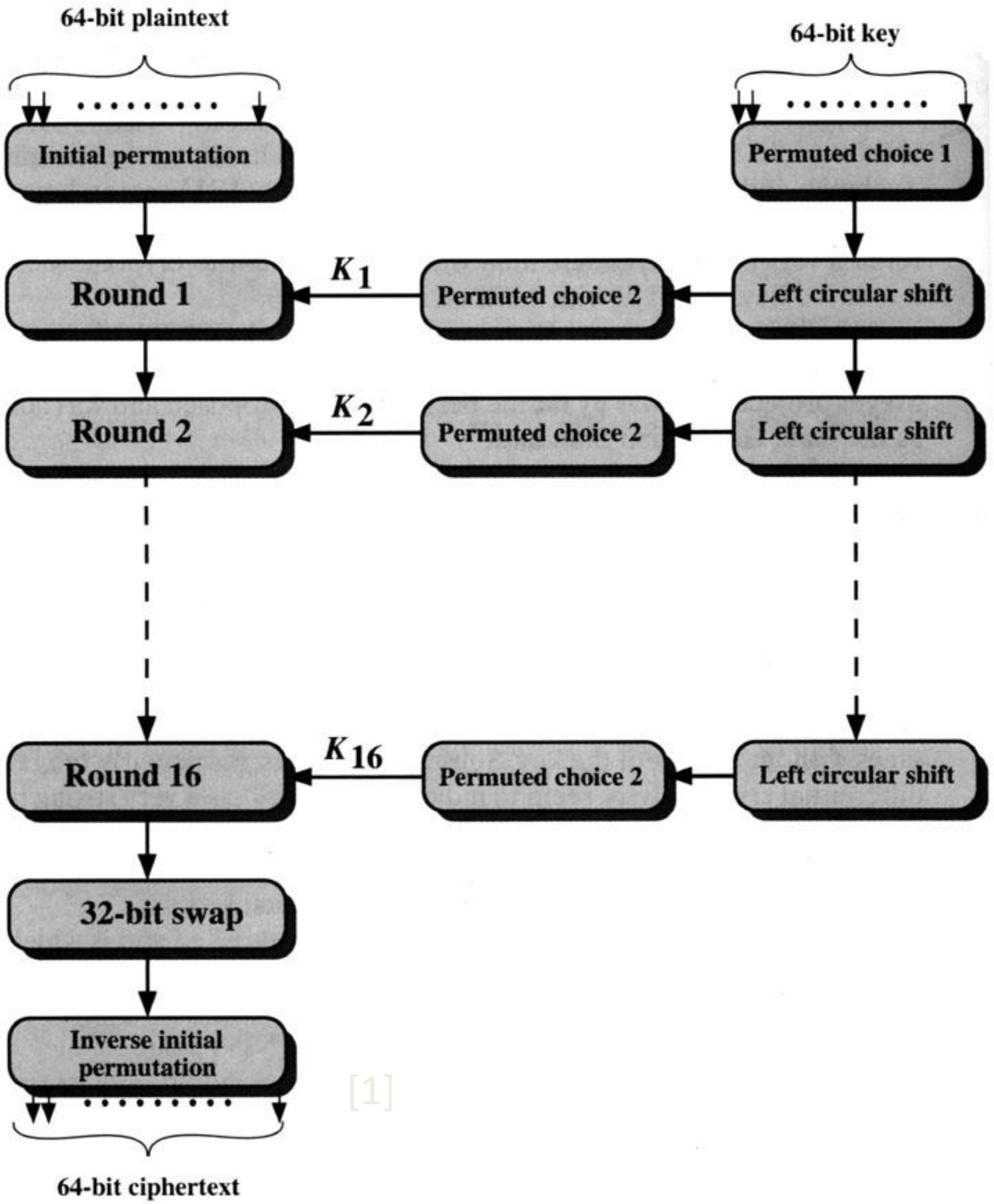
Digital cryptography

- Modern cryptography is almost exclusively concerned with protecting information that is in digital form, a set or sequence of 1’s and 0’s.
- To create the key bitstream, we can use any sufficiently robust pseudo-random number generator.
- Pseudo-random number generators are mathematical functions that produce a sequence of numbers that are apparently random numbers even though they are deterministically produced

A Simplified DES-Type Algorithm

- Suppose that a message has 12 bits and is written as L_0R_0 , where L_0 consists of the first 6 bits and R_0 consists of the last 6 bits.
- The key K has 9 bits. The *i*th round of the algorithm transforms an input $L_{i-1}R_{i-1}$ to the output L_iR_i using an 8-bit key K_i derived from K.
- The main part of the encryption process is a function $f(R_{i-1},K_i)$ that takes a 6-bit input

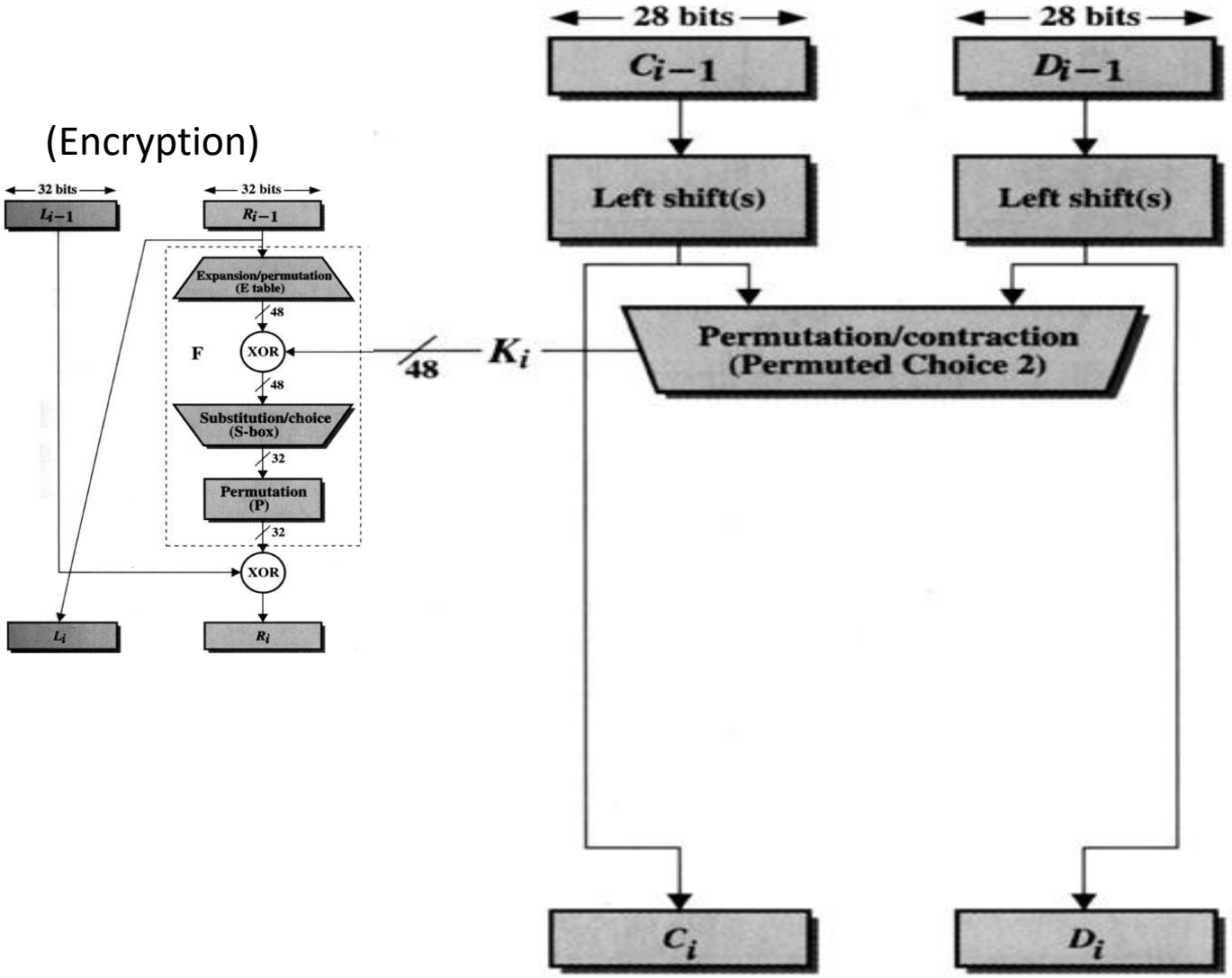
Encryption



[1]

Key Generation

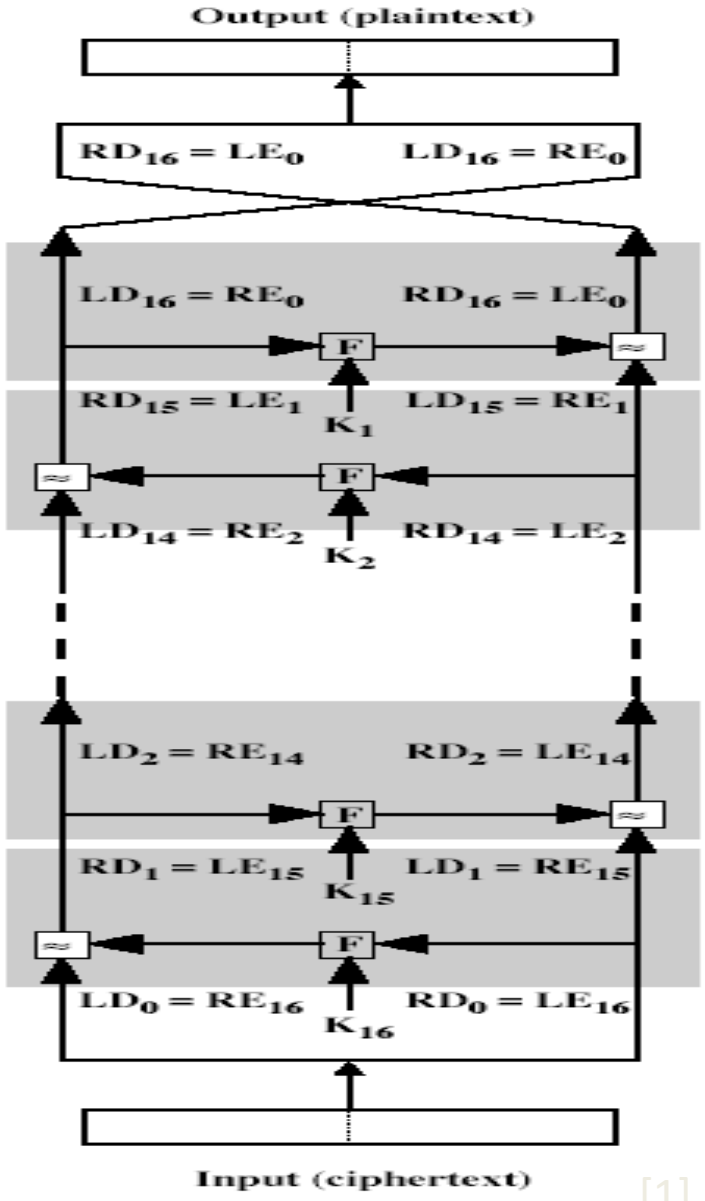
(Encryption)



[1]

Decrypt

- The same algorithm as encryption.
- Reversed the order of key (Key_{16}, Key_{15}, … Key_1).
- For example:
  - IP undoes IP^{-1} step of encryption.
  - 1st round with SK16 undoes 16th encrypt round.



[1]

Elliptic curve cryptography

- A major issue with the use of Public-Key Cryptography, is the size of numbers used, and hence keys being stored.
- Recently, an alternate approach has emerged, elliptic curve cryptography (ECC), which performs the computations using elliptic curve arithmetic instead of integer or polynomial arithmetic.
- Already, ECC is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography.
- The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- Although the theory of ECC has been around for some time, it is only recently that products have begun to appear and that there has been sustained cryptanalytic interest in probing for weaknesses.
- Accordingly, the confidence level in ECC is not yet as high as that in RSA.

Real Elliptic Curves

- An elliptic curve is defined by an equation in two variables, with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field, which results in the definition of a finite abelian group.
- Before looking at this, we first look at elliptic curves in which the variables and coefficients are real numbers.
- Elliptic curves are not ellipses. They are so named because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse.
- For our purpose, we can consider cubic equations for elliptic curves of the form shown here. Also included in the definition of an elliptic curve is a single element denoted *O* and called the *point at infinity* or the *zero point.*
- Now, consider the set of points E(*a, b*) consisting of all of the points *(x, y*) that satisfy this equation together with the element *O.* Using a different value of the pair *(a, b)* results in a different set *E(a, b).*

Network Security Model

- A successful network security program demands a great deal more than the parts and pieces that help enforce it.
- The process of a successful security program include
  - End user awareness training
  - staff education
  - policy and planning
  - least privilege principle
- The security cycle includes the following practices
-
  - Awareness
  - planning
  - management
  - assessment
  - detection
  - response

Process of security

- Security is everyone's business.
- It is important to understand in this process the value of what is being protected.

1. **User awareness and education**

- One of the best tools in information protection program.
- A bi-annual security awareness workshop can be a helpful way to re-emphasis the importance of security.
- Workshop often helps to explain the reasons why security is important and helps reduce complaints about long passwords, frequent password changes, and website filtering
- User awareness training is also one of the most critical elements of a security program.

2. Principle of least privilege:

- Least privilege is one of the most fundamental principles of security
- An example of how to violate the principle of least privilege is that all those users had access to sensitive materials that the majority of them had no reason to access.
- Anther example of violation of least privilege is the daily use of administrators account.
- The classic scenario in which the least privilege principle is useful is in managing user access in file system.

3. Technical training:

- The lack of technical training related to security is a big problem, particularly in small and medium sized enterprises that may not have personnel dedicated to security.
- An responsible person to coordinate security should be

  - Trained in basic security fundamentals
  - Able to report on internal security risks and vulnerabilities
  - Knowledgeable enough to engage a competent security consultant if required

4. Vulnerability awareness:

- System administrators and engineers need to be aware of potential problems with their equipment that may place the organization at risk for compromise or disaster.

- Ways of managing awareness of the security vulnerabilities in system are,

  * Ascertain current security status
  * Keep aware of vendor advisories
  *Seek out non-vendor vulnerability notifications
  *Manage vulnerability alerts.

Security Cycle

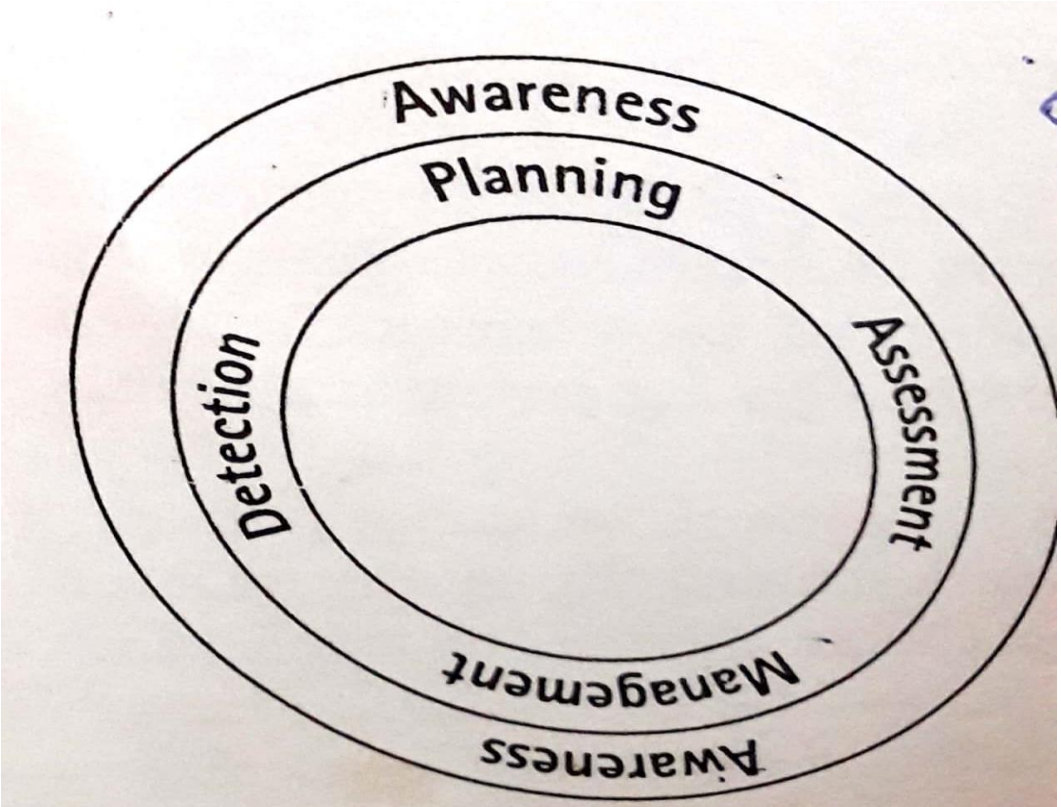


Figure 4-1: The security cycle

Network Intrusion protection

- **Security Architectures:**

  - A standard security architecture might consist of an internal network, a demilitarized zone(DMZ) and the internet.
- This architecture is an example of single-line access to the internet.
- Single line is the most common form of access, but it may not be appropriate for large organizations because this configuration represents a single point-of-failure connection.
- Alternative architecture:

  - Alternatively, we can configure multiple lines to a single ISP.

  - Using Virtual Private Network (VPN) technology, an organization can even replace its wide area network (WAN) backbone by tunneling traffic from one node to another over the internet.

  - The application level firewall requires more overhead than the packet filter. It cannot block an attack or does not recognize a certain connection as an attack.

Firewall configuration

- The first rule in any firewall configuration should be to deny all inbound traffic.
- Depending on the network configuration, inbound SMTP may be allowed if the mail server is located behind the firewall.
- Port-25 traffic should be restricted to the mail server only; there is no reason to allow inbound SMTP traffic to any other host.

Denial of Service Attacks and Availability

- Firewalls are designed by default to fail closed i.e., to deny all traffic if they crash.
- Firewalls can help protect against denial of service attacks by filtering suspicious connections.
- Firewall should not allow any outbound connections where the source address is not the same as the internal network.
- Outbound services are often unlimited users can connect outbound on any port.

Secure Authentication

- Authentication is the process of positive identification. Though many methods to perform authentication exist, the most common that users are familiar with is password authentication.
- Applying password authentication
- Exploring two-factor authentication
- Choosing wireless authentication options

THE EVOLUTION OF PASSWORDS

- Password authentication has evolved quite a lot since the concepts was first introduced in computing.
- Earlier implementations, passwords were stored simply as plain, readable text, which wasn’t such a big concern when the internet was more about sharing information than safeguarding.
- later the password was stored as hash, a mathematical one-way function that is not possible to reverse.

PASSWORD VULNERABILITIES

- Hashes cannot be reversed to reveal the plain text password, an attacker can still use a couple of techniques try to reavel what plain text made the hash.

DICTONARY ATTACK

- If an attacker has the password file.He or she can use the same algorithm to hash an entire dictionary of words and compare the hashes to the password file.

BRUTE-FORCE ATTEMPT

- The second form is a brute-force attempt that generates hashes for every possible combination of letters,numbers,and characters and compare that to password file.

HYBRID PASSWORD ATTACK.

These two techniques can be combined to form a hybrid password attack.

- The online attack basically fires off the dictionary or brute force at the authentication serever,which either locks the account after several failed attempts or lets the attcaker in after the correct password is generated.A malicious person may even attempt to purposely lock accounts to create a rudimentary,yet effective denial of service attack.
- The offline attack requires access to the password file,which is world-readable in some operating systems.

TWO FACTOR AUTHENTICATION

- The most obvious limitation of passwords is their inherent susceptibility to theft and compromise.

TOKENS AND SMART CARDS

- The use of RSA's secure ID key fob tokens for authentication. The key fob displays a different 6-digit number every minute.
- The user basically has their password with them, it also reduces lost password calls.

BIOMETRIC AUTHENTICATION

- The biometric authentication devices include fingerprint scanners, retina scanners, and face recognition.

✓ Fingerprint scanners are currently the most prevalent form of biometric authentication for computing.

✓ Retina scanners are regarded as the most accurate form of biometric authentication in use today.

✓ Face recognition has not really been deployed as a computer authentication mechanism.

ONE TIME PASSWORDS

- One of the earliest forms of two-factor authentication is a one time password system.
- LIMITATIONS

✓ The primary limitations of most authentication mechanism is user error.

✓ Some biometric systems are prone to false rejection

✓ Some systems have an administrative overhead that is higher than the operator may have expected.

Network Intrusion Detection system-INTRODUCTION

- NIDS- Network Intrusion Detection system
- NIDS monitor real time traffic to discover any attacker is attempting to penetrate the network.
- It is a basic component of network security architecture
- Cyber analogy to a burglar alarm.
- To gather additional intelligence about the attacker.
- IDs runs on a separate server
- It can continue to collect data even the server or host is compromised.

PACKET SNIFFERS

- The simplest form of detection machine network captures traffic (packet sniffing).
- capture could consist of entire packets or may simply log the header information.
- Specialized tools pattern.

Advantages:

- Machines that they capture everything.

Limitations:

- Volume of data capture is extremely large analyzing it is cumbersome.
- “Network grep” systems –to automate the process of analysis.

SIGNATURE DETECTORS

- Optimized to detect common attacks
- First developed in an attempt to automate and standardize the process of examining raw packet captures for specific attack signatures.
- Similar to antivirus software- tools to examine the network traffic and compare it against database of known attack patterns.

Drawbacks:

- They can detect only attacks whose signatures exit in their data base.
- They tend to have a high false negative rate: miss actual attacks - signature file is not up to date (ignore certain types of attacks).

ANOMALY DETECTORS

- To develop a pattern of what is considered statistically normal traffic.
- Traffic that deviates from this baseline can be logged and administrators are alerted.
- They can offset the problem of unknown or new attack detection.
- **Limitations:**

✓ Developing a good baseline is key. If the network traffic varies widely and if there is no good normal pattern, the system may not be able to distinguish what is normal.

✓ These systems have a high false positive rate i.e.,thay may give an alarm on what is actually legitimate traffic if it somehow differs from the norm.

Host based security in wireless networks

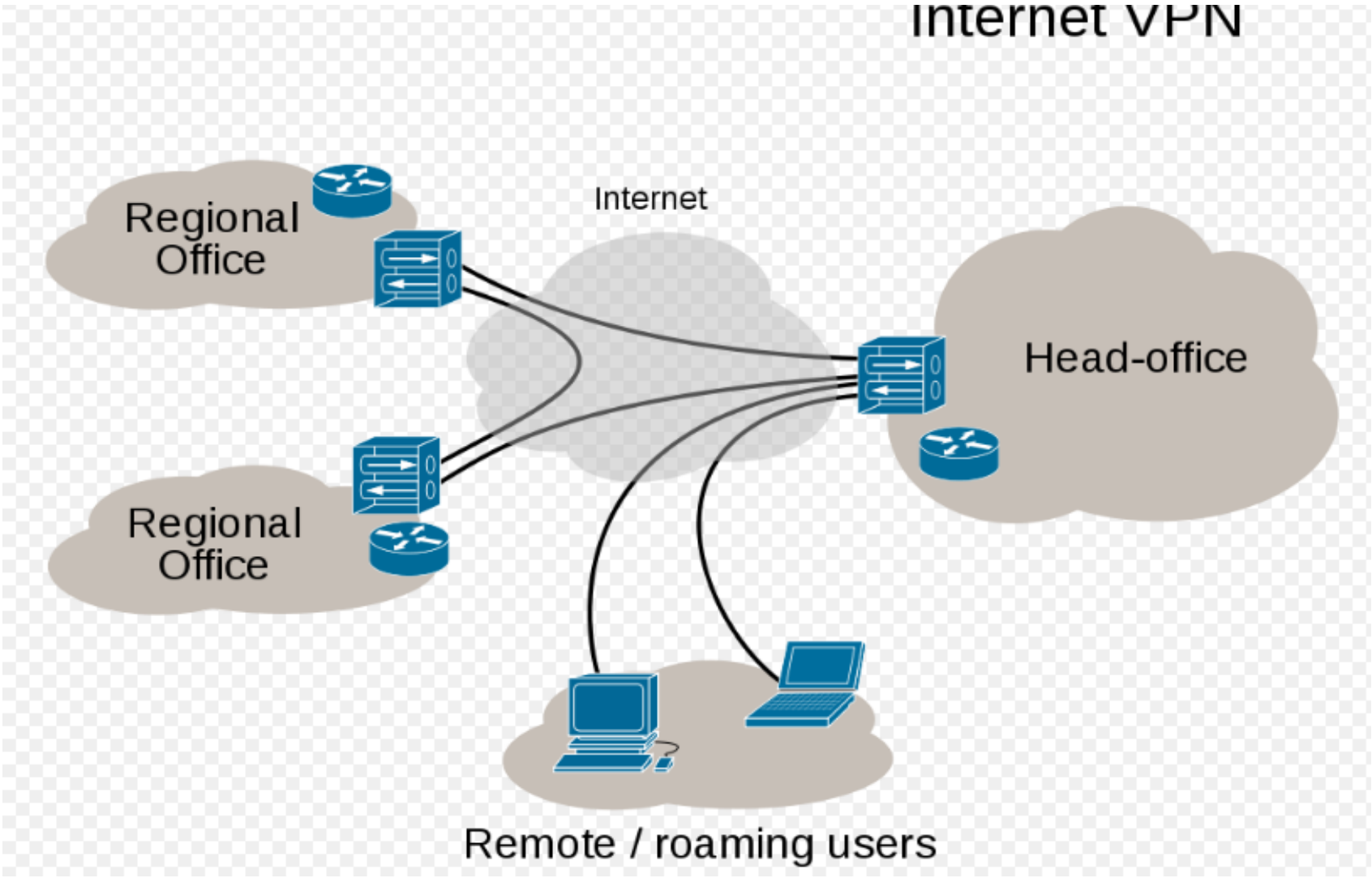
- Securing hosts to prevent network based attacks
- Using host based intrusion detection to detect both local and network based attacks
- Checking file integrity in order to detect modification to host operating systems

Host based attack prevention

- IEEE 802.11b networks operate at the bottom two layers of OSI network model
- All the layers are responsible for host operating system
- Essential Basic of securing a host :
  - Require authentication
  - Strong password
  - Disable unnecessary services
  - Install updates and patches
  - Log critical events

VPN

- A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet.
- It enables users to send and receive data across shared or public networks.
- Applications running across the VPN the functionality, security, and management of the private network.


Internet VPN
Regional Office
Internet
Head-office
Regional Office
Remote / roaming users

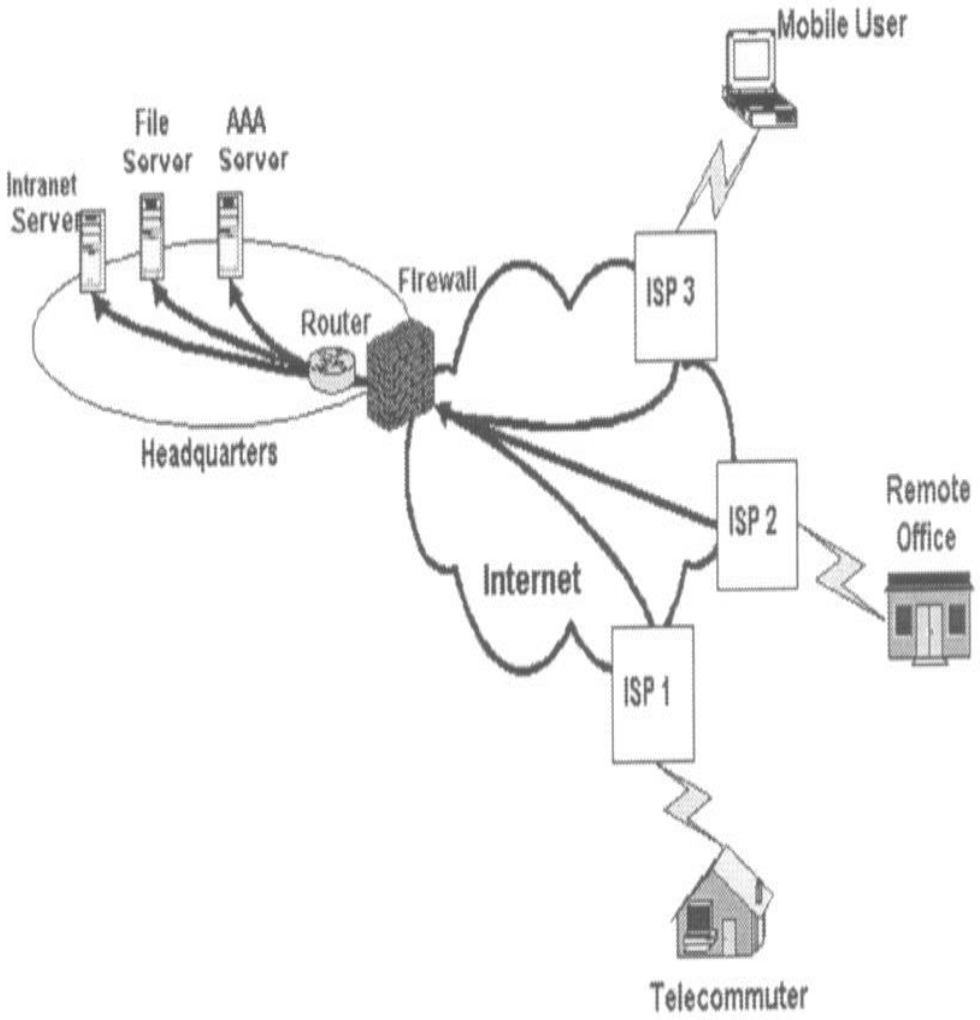
PRIVATE NETWORK VS VPN

- VPNs based on IP and IP/Multi-protocol Label Switching (MPLS) Networks.
- cost-reductions and increased bandwidth.
- new technologies such as Digital Subscriber Line (DSL)and fiber-optic networks.
- Employees can access the network (Intranet) from remote locations.

- Secured networks.

- The Internet is used as the backbone for VPNs

VPN


Mobile User
File Server
AAA Server
Intranet Server
Firewall
Router
ISP 3
Headquarters
ISP 2
Remote Office
Internet
ISP 1
Telecommuter

HOW IT WORKS?...

- ✓ Two connections – one is made to the Internet and the second is made to the VPN.
- ✓ Datagrams – contains data, destination and source information.
- ✓ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✓ Protocols – protocols create the VPN tunnels.

SECURE CONFIGURATION AUTHENTICATION AND ENCRYPTION

SECURE CONFIGURATION

- Broadcasting Station Set Identifiers
- Using MAC address filtering
- Working with Wired Equivalent Privacy

ENCRYPTION

- WEP uses a secret key which is shared between the wireless station and the access point.
- The data sent and received is encrypted using this key.
- One key is shared among all the stations and the access points in a given system.
- Two process are used.

AUTHENTICATION:

- WEP provides two types of authentication
  - A default open system where all users are permitted to access a WLAN.
  - A shared key authentication which controls WLAN and prevents unauthorized network access.
- The shared key authentication process is the secure method.

WIRELESS DEVICE PLACEMENT

Placement consideration

- Coverage is the most important goal in most wireless network deployment
- Low powered wireless equipment such as WLAN access point won’t extend beyond the walls of their building.
- Many people perceive their wireless network in only 2 dimensions. They did not concern about above and below.

Physical security

- Wireless networking equipment is usually arranged in a way that promotes good coverage throughout the facility.
- This arrangement sometimes leads operators of wireless equipment to place access points, bridges, or antennas in areas where unauthorized personnel may physically access them.
- Issues of physical security are particularly relevant in wireless point-to-point connection here the equipment is often placed outside.

Perimeter coverage

- Popular method for covering a large area is to place the network's access points around the interior perimeter walls.
- This design extend to range where the people did not able to use wireless connectivity.
- To minimize the risk of wireless leakage place AP in the center of area.
- Drawback- this is difficult to extend the range into corner of the area.
- Placement is away from public access roads, parking lots and side walks.

Limiting power output

- If design goal is offer a wireless networking in many different section of building. You must limiting the power output of your access point.
- This reduce the area of unintended coverage.
- If you cover area with 100mW, try to cover with 50mW.

Directional antenna

Directional antennas are very effective way limiting span of coverage in point-to-point wireless connection.

Performance improved

This is used to transmit and receive in very specific direction.

Terrain masking

- This is the technique used by military to reduce the range of transmission expect in the direction it was intended.
- It requires knowing the direction that the intended receiver is in so the unmasked side of the antenna is be able to transmit unimpeded.

Logging wireless events

- **Why logs are important?**

  -Logs are used to identify an attacker attempting to or has successfully compromised with network

  - Log files are the first check item for many system administrators who are working on a problem.
- **Working with syslog:**

  - Syslog provides a method for journaling messages for a particular system or group of systems.

  - Typical uses include UNIX system logs, router events and firewall events.
- **Logging with syslog:**

  - syslog messages are generally sent using UDP to port 514.

  - UDP is a connectionless protocol, which means it provides no facility .

  - syslog messages are sent in plain text and could be intercepted by anyone with a packet analyzer on our shared media.

Commercial tools for syslog

- Winsyslog
- SL4NT

Working with Simple network management protocol

- Simple network management Protocol (SNMP) is a management tool for monitoring and managing device on IP devices.
- It works using a management application or manager that communicates with all the SNMP-capable devices called agents.
- Agents are run on many different types of devices such as servers, routers, printers and in some wireless access points.

Commercial tools for SNMP

- HP OPenView
- IBM Tivoli Netview
- Cisco Works 2000
- Castlerock SNMPc

Policy issues

- **Amending the network security policy:**

  - The basic purpose of information security policies is to transfer liability and responsibility from the organization to the user.

  - Policies are standard rules of behavior providing a framework for enforcement of policies.

  -Policies serve a purpose only if users know of their existence and understand their content.

  -Two types of users that cause security incidents:

    * First type causes problems when they simply don't know any better.

    * Second type user intends to cause problems and commits violations on purpose

Assessing wireless network security

- Wireless Security assessments:
  - One must decide upon the goal of the assessment
- Network security Auditing:
  - It is the process of verifying compliance with a pre-established set of criteria.
  - The audit is a mostly automated process conducted internally on a scheduled basis
  - The first step in auditing is to create a standard for each device or process to be evaluated against.
- Vulnerability testing:
  - Involves scanning information systems for problems that may lead to the lack of availability of resource.
  - Result of a vulnerability tests is usually a report that details the vulnerabilities discovered on each of the hosts scanned.

- The type of test can be externally or internally.
- The internal scan is run from a machine connected to internal LAN and can be connected within or without login privileges.
- The external tests for vulnerabilities are conducted in the perimeter of your network.
- **Penetration testing:**
- It is the process of having a tester who has no prior knowledge of a network's security posture or architecture attempt to hack into the network.
- Penetration test primarily measure risk.
- **Preparing for a Wireless Security Survey**
- Establish a security baseline for all equipment
- Create a network diagram and list of all equipment
- Check each piece of equipment for compliance with the baseline

- Gather specific firmware versions for each piece of equipment
- Determine if security problems exist in any of the firmware versions
- Discover any unauthorized access points
- Determine the maximum distance that wireless traffic can be received from each access point.
- Verify that unencrypted traffic is not traversing the wireless network.
- Verify that weak forms of WEP re not in use
- Document deficiencies and begin to plan corrections.
- **Drafting a security standard:**
- Wireless small office or home
- Wireless enterprise with 802.1 X
- Wireless enterprise with IPSEC
- Wireless public access

WIRELESS SECURITY MODEL USING CISCO IMPLEMENTATION WITH LEAP

INTRODUCTION

- LEAP is an enhancement to the EAP protocol, the EAP protocol was created in an effort to provide a scalable method for a PPP-based server to authenticate its clients.

- Packet exchange for authentication between client and PPP server-PPP server rely on centralized authentication-there comes RADIUS server

- RADIUS SERVER-protocol-transfers EAP packet between the authentication server and PPP server

- RADIUS SERVER tell the PPP server about authentication(fail/pass)-establish secure connection between client and network

Contd..

- When 802.11 specifications were standardized-encryption of data traffic between APs and clients - WEP encryption key.
- When it was first implemented-the AP would have a single key, and this key had to be configured on each client. All traffic would be encrypted using this single key.
- LIMITATION: secret key can be broken easily-overcome by LEAP

LEAP

- The server will then pass certain information to the AP so that the client and AP can derive encryption keys that are unique for this client-AP pair. This is called Cisco LEAP authentication.

- LEAP authentication works through three phases: the *start phase, the authenticate phase, and the finish phase*.

START PHASE FOR LEAP AUTHENTICATION:

- In the start phase, information (in packet form) is transferred between the client and APs:
- The EAPoW-Start (this is also called EAPOL-Start in 802.1x for wired networks) starts the authentication process.This packed is sent from the client to the AP.

- The EAP-Request/Identity is sent from the AP to the client with request for the clients Identity.

- The EAP-Response/Identity is sent from the client to the AP with the required information.

AUTHENTICATION PHASE FOR LEAP AUTHENTICATION:

- Mutual authentication between server and AP-if select TLS- for the transfer of certificates-PKI deployment, EAP-TLS messages will be used, but because we are talking about LEAP, it would go more like this:

- 1. The client sends an EAP-Response/Identity message to the RADIUS server through the AP as a RADIUS-Access-Request with EAP extensions.

- 2. The RADIUS server then returns access-request with a RADIUSchallenge, to which the client must respond.

FINISH PHASE FOR LEAP AUTHENTICATION:

- If the client- invalid-the RADIUS server- send -RADIUS deny packet with an EAP fail packet embedded within it.

- the client- valid- the server will send a RADIUS request packet with an EAP success attribute.

- The RADIUS-Access-Accept packet contains the MS-MPPE-Send-Key attribute to the AP, where it obtains the session key that will be used by client-unique at each session.

CONFIGURATION AND DEPLOYMENT OF LEAP

- LEAP solution that consists of a client, an AP and a RADIUS server for key distribution in your network.

- CLIENT SUPPORT FOR LEAP:
- You can configure your client to use LEAP mode in one of two modes

- **Network Logon Mode:** In Network Logon Mode: an integrated network logon -single-sign on for both the wireless network-Microsoft Networking.- provide users with a transparent security experience- probably the most common method of authenticating into the wireless network (or the wired network).

- **Device Mode:** In Device Mode, the wireless LAN stores the username/:password identification, non-interactive authentication into the wireless LAN.

ACCESS POINT SUPPORT

- You need to configure the AP to use 40/64- or 104/128-bit WEP mode.
- You must give the LEAP RADIUS server address and configure the shared secret key that the AP and RADIUS server use, so that they can communicate securely.

- To configure the RADIUS server for authentication and key distribution users, you will need to do the following:
- You need to create the user databases.
- You need to configure the APs as Network Access Servers (NASs).This will enable users that are configured with Cisco-Aironet RADIUS extensions on the NAS to use RADIUS. RADIUS requests from the AP with EAP extensions are passed as described earlier

SECURE WIRELESS POINT-TO-POINT CONNECTIVITY

SECURE WIRELESS POINT-TO-POINT CONNECTIVITY

- Using IPSEC to augment your point to point connection
- considering placement of your equipment
- using directional antennas to enhance performance and security.
- Exploring sample configurations for Cisco PLX firewalls and Cisco routers.

Selecting wireless point to point

- Cost
- Bandwidth
- Flexibility
- Security
- consistent service
- learning curve for employees or IT folks
- Equipment placement

Encryptor Structures in Wireless

Scrambling

- Scramblers are one of the first methods of providing rudimentary voice security for wireless devices.
- It occurs at the analog processing stage of voice input or just after the voice digitization stage.
- It uses relatively simple techniques of rearranging formants and in some case spectrally relocating specific parts of the transmitted information.

Interception and Vulnerability of Wireless Systems

- Wireless transmissions have been subjected to attacks of many types.
- The functional interest is to explain the vulnerabilities of these systems and how EW support measures and ECM systems function to exploit them.
- EW is organized into three categories: *Electronic Support Measures* (ESM), *Electronic Countermeasures (ECM), and Electromagnetic Counter Counter-measures (ECCM).*
- *In ESM the objective is to intercept, identify, analyze,* and localize an enemy's transmission sources.

Communications ESM and Interception Receiver

Types of DSM and COMINT

- CVR-Crystal Video Receiver
- IFM-Instantaneous Frequency Measurement Receiver
- YIG tuned narrowband superheterodyne
- Wideband superheterodyne
- Spectral analyser ESM receiver
- Channelized receiver
- Compressive receiver
- Acoustic-optical Bragg cell receiver