Network Security: Introduction

1. Network security models

2. Vulnerabilities, threats and attacks

3. Basic types of attacks

4. Managing network security

1. Network security models

Security

- **Security** has one purpose: „***to protect assets***“

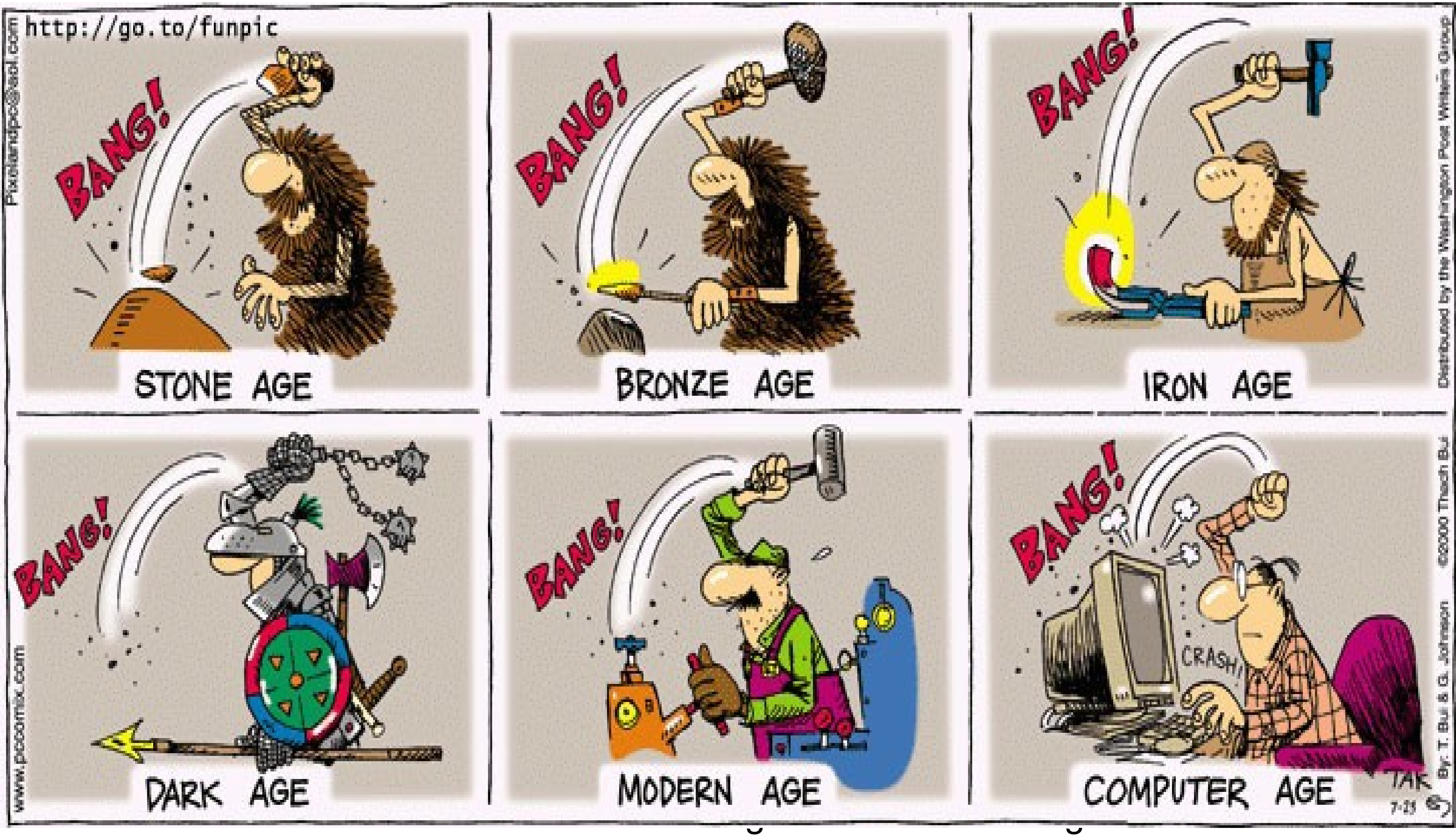
- In terms of computer networks the assets can be:
  - Information – files, data streams …
  - Servers
  - Configurations
  - User accounts
  - Passwords
  - Devices
  - …

History of Security Measures

- For most of time periods in the past, security meant :

  - building big strong walls to
  - stop the bad guys, and
  - establishing small, well-guarded doors
    to provide secure access for the good guys.

Advance in Technology

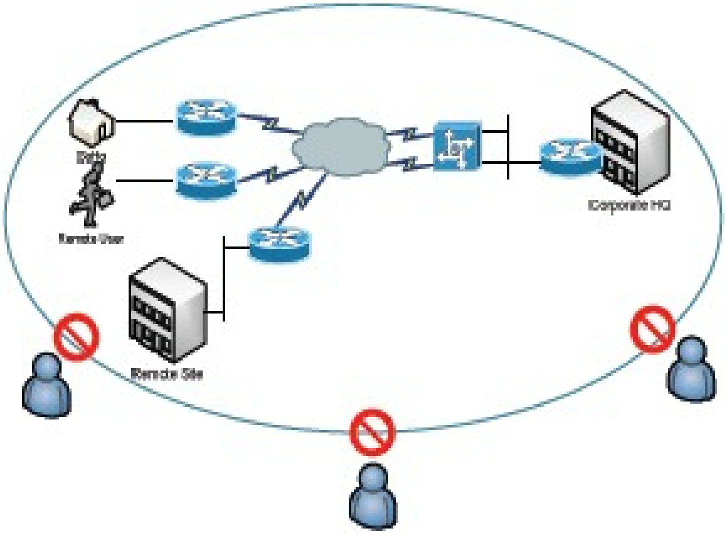


Network Models

According to the IT security terms there are two network models:

1. Closed network model
2. Open network model

Closed Network Model



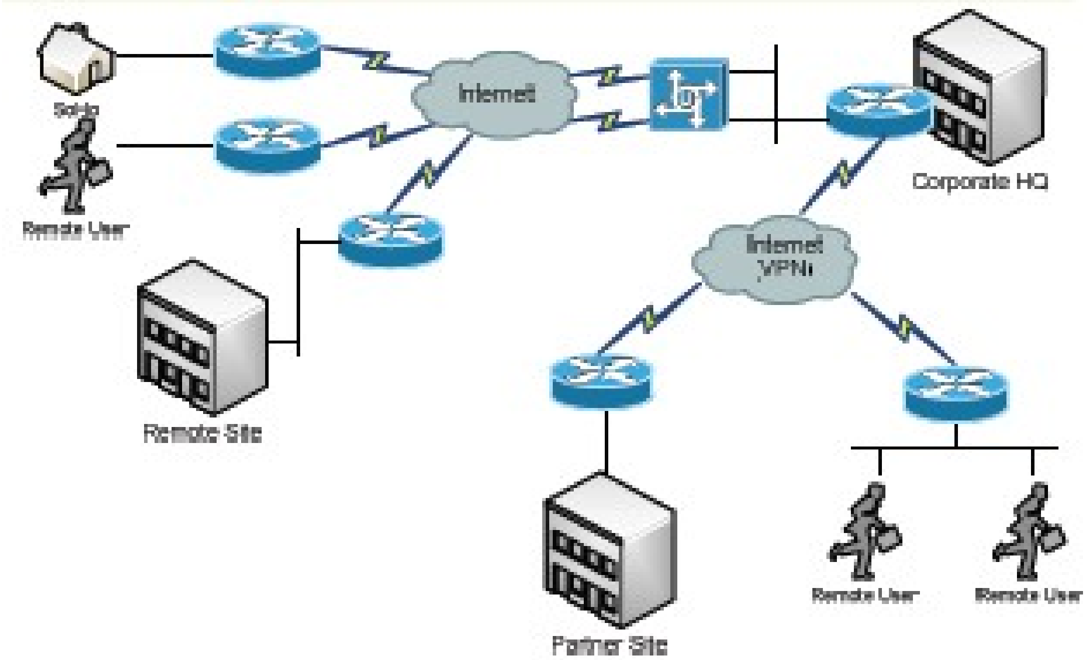
Advantages:

- Strong security
- Strict security policy
- Typically implemented in corporate environments
- Easy support and monitoring

Disadvantages:

- Low flexibility (typically no WLANs, no external connections)
- No external access for business partner
- No connection from public networks

Open Network Model



Advantages:

- External access
- Business advantages
- Flexible for users
- Internet access

Disadvantages:

- This is the required model for modern enterprises
- Hard to support, secure and monitor
- Many potential threats
- Requires very strict security policy and disaster recovery plan

Needed Balance

- E-business, mobile commerce, need for wireless communication and Internet applications continue to grow

- Finding the balance between being isolated and being open will be critical, along with the ability to distinguish the good guys from the bad guys.

Security Devices and Technologies

- Special security devices and technologies must be implemented to achieve the required network up-time of 99.999% as for instance:
  - Firewalls
  - Intrusion Detection and Prevention Systems (IDS)
  - Virtual Private Networks (VPN)
  - Tunneling
  - Network Access Control (NAC)
  - Security Scanners
  - Protocol Analyzers
  - Authorization, authentication and accounting (AAA)

Firewall

- Most used security device is the firewall.

- Firewalls types:

  1. Hardware Firewalls
  2. Server Firewalls
  3. Personal Firewalls

- Modern firewalls includes

  - intrusion detection,
  - authentication,
  - authorization, and
  - vulnerability assessment systems.

What is Expected from Network Security (CIA Model)

1. ***Confidentiality***: Ensure that the secrecy is enforced and the information is not read by unauthorized users. Cryptography and encryption may ensure the confidentiality of the transferred data.

2. ***Integrity:*** modification of data is not permitted to unauthorized users; it provides assurance of the accuracy of information and systems. Users can obtain only authorized information.

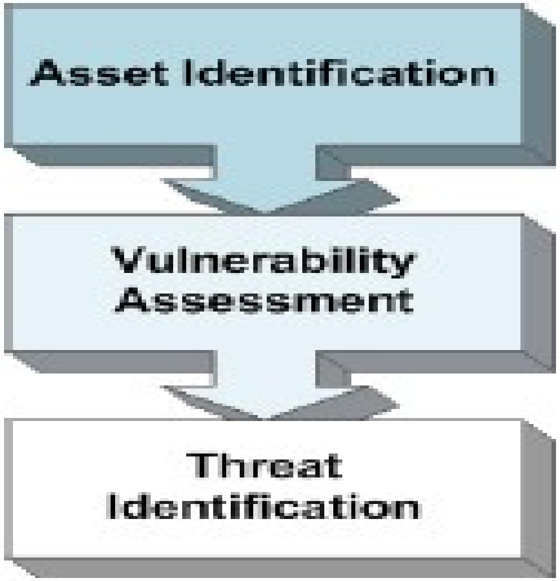
3. ***Availability:*** prevention of loss of access to resources and information. Information requested has to be available to the authorized users at all times. when is needed

Security Models

- ***Security model***: integrates the security policy that should be enforced in the system; it a symbolic form of a security policy
- ***Security policy:*** a set of abstract goals and high-level requirements ; security model is the do‘s and dont‘s to make security policy happen.
- ***Baseline:*** minimum level of security requirement in a system; provide users to achieve a minimum security that is consistent across all system in the organization (ex. all systems of the company have to have the latest MS-Service Pack)

Identifying Potential Risks for Network Security

- A risk analysis should identify the risks to the network, global and shared resources, and data



- The intent of a risk analysis is to identify the components of the network, evaluate the importance of each component, and then apply an appropriate level of security.

Asset Identification

- Before the network can be secured, the individual components that make up the network must be identified (asset inventory must be created).

- All of the network devices and endpoints, such as routers, switches, hosts and servers, should be included in the asset inventory.

Vulnerability Assessment

- Once the network components have been identified, they can be assessed for vulnerabilities.

- These vulnerabilities could be:
  - Technology weaknesses
  - Configuration weaknesses
  - Security policy weaknesses

- Any vulnerability that is discovered will need to be addressed to mitigate any threat that could take advantage of the vulnerability.

Threat Identification

- A threat is an event that can take advantage of vulnerability and cause a negative impact on the network.
- Potential threats to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the threat.

Open and Closed Security Model

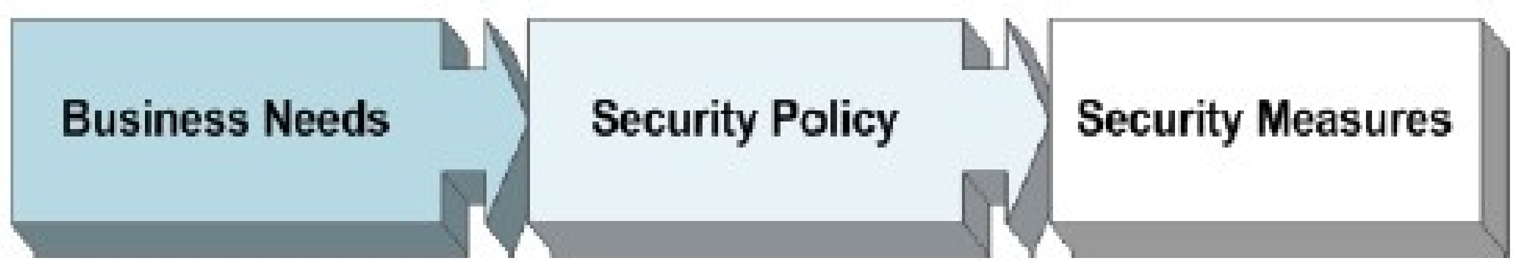
- With all security designs, there is some trade-off between user productivity and security measures.

- The goal of any security design is to provide maximum security with minimum impact on user access and productivity.

User Productivity and Security Measures

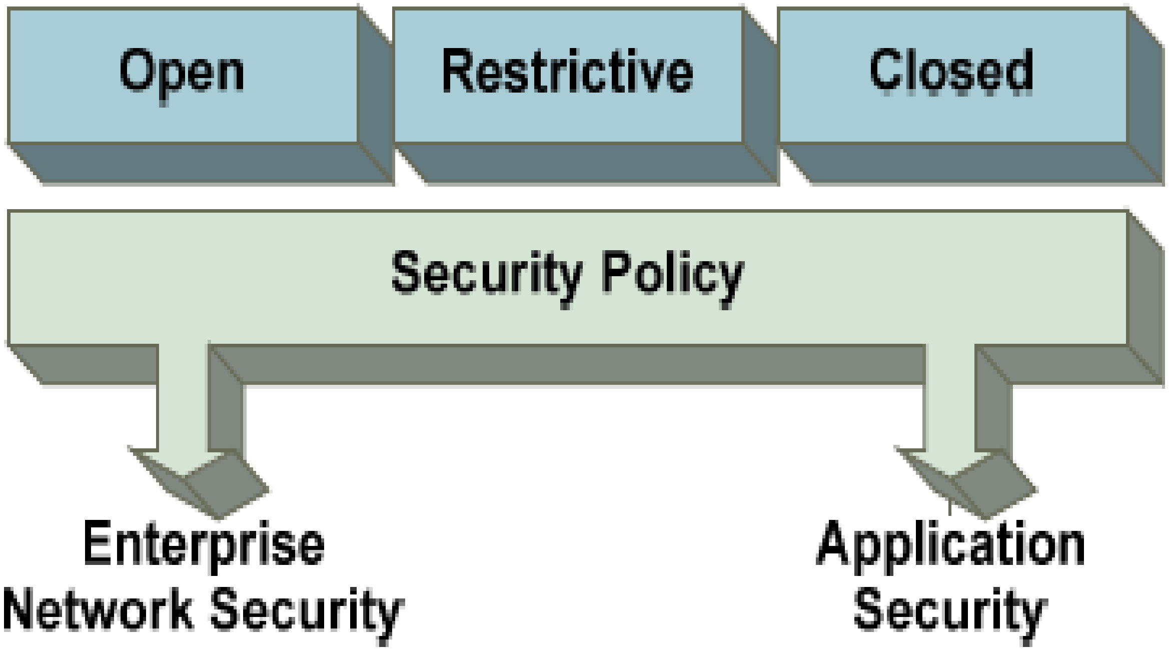
- Some security measures, such as network data encryption, do not restrict access and productivity.
- On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and prevent access to critical network resources.

Business needs should dictate the security policy.
A security policy should not determine how a business operates.



General Types of Security Models

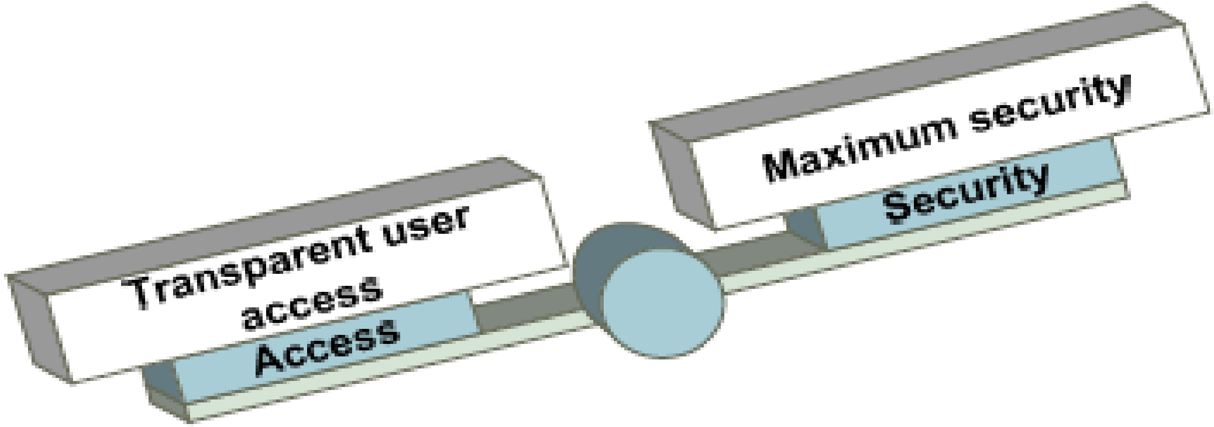
1. Open
2. Restrictive
3. Closed



Open Access

- Easy to configure
- Easy to administer
- Easy for network users
- Security cost: Least expensive

PERMIT EVERYTHING THAT IS NOT EXPLICITY DENIED



Open Access

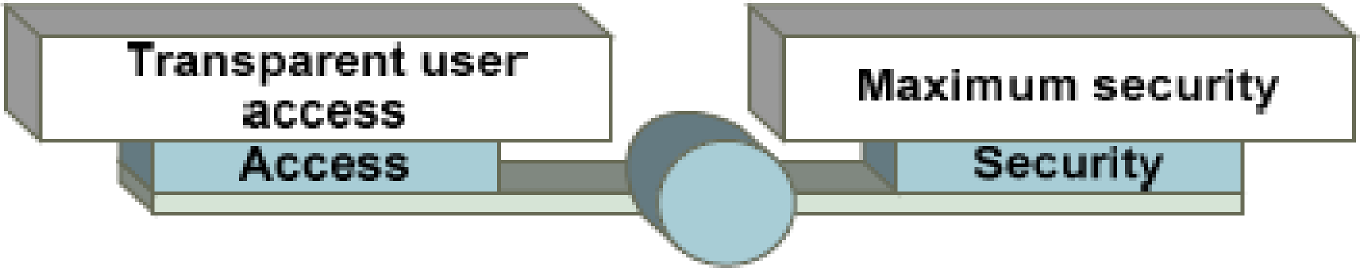
- This model assumes that:
  - the protected assets are minimal,
  - users are trusted and
  - threats are minimal

- Network administrators are usually not held responsible for:
  - network breaches or
  - network abuse

Restrictive Access

- More difficult to configure and administer
- More difficult for network users
- Security cost: More expensive

COMPILATION OF SPECIFIC PERMISIONS AND RESTRICTIONS



Restrictive Access

- This model assumes that the protected assets are substantial

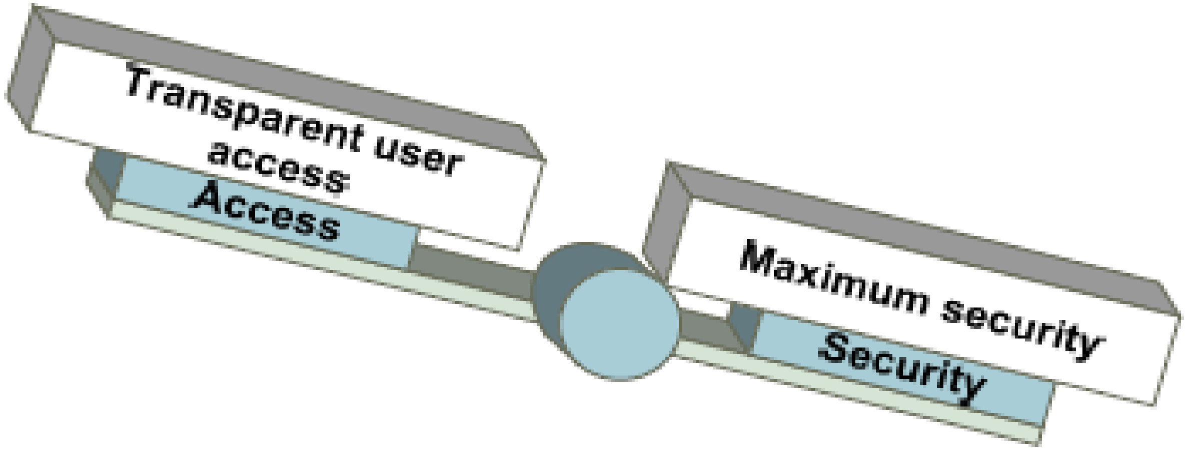
- Some users are not trustworthy, and that threats are likely.

- Ease of use for users is diminished as security is tightened.

Closed Access

- Most difficult to configure and administer
- Most difficult for network users
- Security cost: Most expensive

EVERYTHING WHICH IS NOT EXPLICITY PERMITED IS DENIED



Closed Access

- This model assumes that the protected assets are premium, all users are not trustworthy, and that threats are frequent.

- User access is very difficult and cumbersome.

- In many corporations and organizations, these administrators are likely to be very unpopular while implementing and maintaining security.

Legal Issues and Privacy Concerns

- For many businesses today, one of the biggest reasons to create and follow a security policy is compliance with the law.
- If a business is running a publicly held e-business and a catastrophic attack seriously impairs the business, a lawsuit is possible.

Wireless Access and Wireless LANs

- WiFi connections do not respect firewalls the way wired connections do.
- Implementation of Wireless LANs or other wireless technologies bring additional security threats.

IT staffing shortage

- The IT staffing shortage is especially evident in the security field.

- To solve this problem, many enterprises are increasingly outsourcing day-to-day security management tasks.

- Clearly, there is a demand for ***skilled network security professionals.***

Information Security Organizations

- CERT/CC
- US-CERT
- SANS Institute
- (ISC)2
- Common Criteria
- FIPS
- ICSA Labs

2. Vulnerabilities, threats and attacks

Terminology

Vulnerability is a weakness which is inherent in every network and device.

This includes routers, switches, desktops, servers, and even security devices themselves.

Threats are the people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Treats use a variety of tools, scripts, and programs to launch **attacks** against networks and network devices.

Typically, the network devices under attack are the endpoints such as servers and desktops.

Types of Vulnerabilities (weaknesses)

1) Technological Weaknesses:

- Computer and network technologies have intrinsic security weaknesses.
- These include protocol weaknesses, operating system weaknesses, and network equipment weaknesses.
- Common examples of technological weaknesses are:
    - HTTP, FTP, ICMP and other protocols are inherently insecure
    - OS security holes and problems. (Visit Computer Emergency Response Team – CERT at www.cert.org for details)
    - Network equipment weaknesses:
        - password protection,
        - lack of authentication,
        - different security holes, etc.

Types of Vulnerabilities (weaknesses)

2) Configuration Weaknesses:

- Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

- Examples of configuration weaknesses are:
  - Unsecured user accounts
  - Easily guessed passwords
  - Misconfigured services
  - Default settings used in running configurations
  - Misconfigured network equipment

Types of Vulnerabilities (weaknesses)

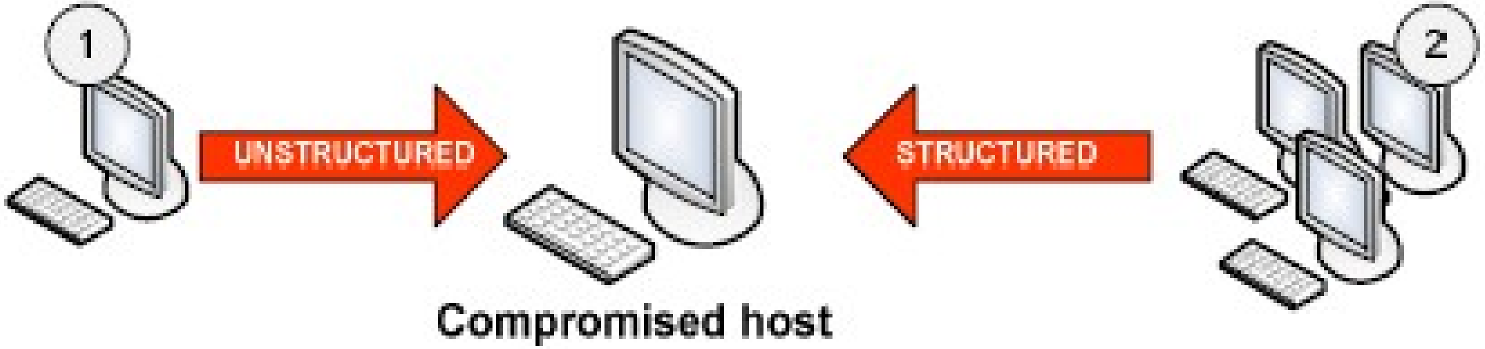
3) Security Policy Weaknesses:

- Security policy weaknesses can create unforeseen security threats.
- The network may pose security risks to the network if users do not follow the security policy.
- Examples of security weaknesses are:
  - Lack of written security policy
  - Politics
  - Lack of continuity
  - Software and hardware installations or installation changes do not follow the policy
  - Nonexistent disaster recovery plan

Threats

1. ***Unstructured threats*** - Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.

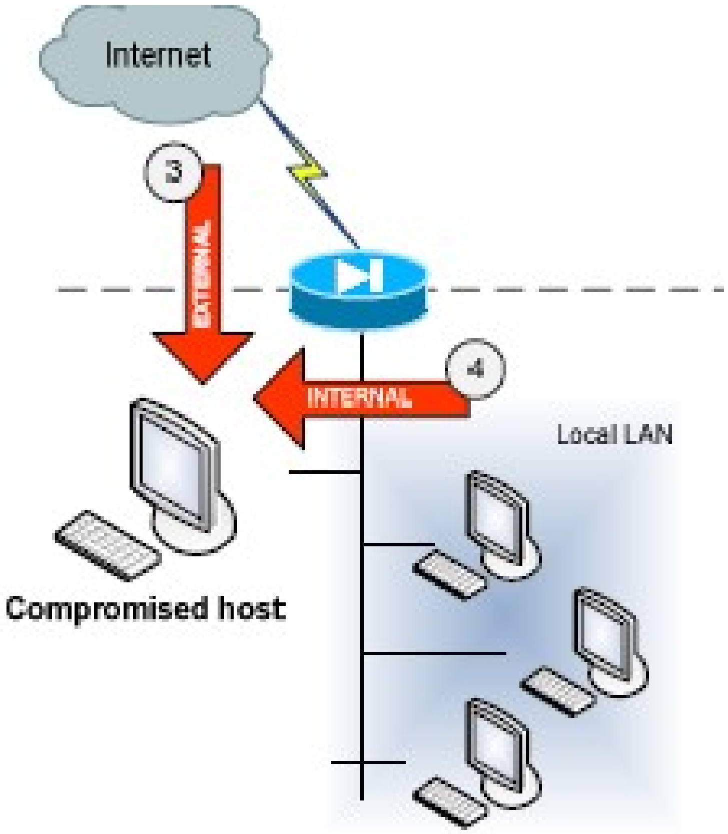
2. ***Structured threats*** - Structured threats come from hackers that are more highly motivated and technically competent. These people know system vulnerabilities, and can understand and develop exploit-code and scripts.



Threats

3. ***External threats*** - External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network.

4. ***Internal threats*** - Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.



Attacks

There are 4 primary classes of attacks:

1. Reconnaissance
2. Access
3. Denial of Service
4. Worms, Viruses and Trojan horses

Reconnaissance

- Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities.

- It is also known as *information gathering* and, in most cases, it precedes an actual attempt for not authorized access or Denial of Service (DoS) attack.

Access

- System access is the ability for
  an unauthorized intruder to gain access
  to a device for which the intruder does not have an account or a password.

- Entering or accessing systems to which one does not have access usually
  involves running a hack, script, or tool
  that exploits a known vulnerability
  of the system or application being attacked.

Denial of Service (DoS)

- Denial of service (DoS) implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.
- DoS attacks involve either crashing the system or slowing it down to the point that it is unusable.
- The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, *DoS attacks are the most feared*.

DoS Consequences

OUR COMPUTERS ARE DOWN, SO WE HAVE TO DO EVERYTHING MANUALLY...
http://go.to/funpic/

Worms, Viruses and Trojan Horses

Malicious software packages are inserted onto a host in order to:

- damage a system,
- corrupt a system,
- replicate itself,
- deny services or
- access to networks, systems, or services

3. Basic types of attacks

Reconnaissance Attack

- Reconnaissance attacks can use various tools and techniques for example:
  - Packet sniffers
  - Port scans
  - Ping sweeps
  - Internet information queries

Packet Sniffing (*Eavesdropping*)

Typically eavesdropping is used for:

a) ***Information gathering*** – Network intruders can identify usernames, passwords, or information carried in the packet such as credit card numbers or sensitive personal information.

b) ***Information theft*** – Network eavesdropping can lead to information theft. The theft can occur as data is transmitted over the internal or external network. The network intruder can also steal data from networked computers by gaining unauthorized access.

Counteract Eavesdropping

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping
- Using encryption that meets the data security needs of the organization without imposing an excessive load on the system resources or the users
- Using switched networks

Access Attacks

- Access attacks basically exploit known vulnerabilities in: authentication services, FTP services, and Web services to gain entry to Web accounts, confidential databases, and other sensitive information.

- Ways to generate access attacks:
  - Password Attacks
  - Trust exploitation
  - Port redirection
  - Man-in-the middle
  - Social engineering
  - Phishing

Password Attacks

- Password attacks can be implemented using several methods:
    - brute-force attacks,
    - dictionary or modified dictionary attacks,
    - Trojan horse programs,
    - IP spoofing, and
    - packet sniffers.

Password Attacks

Methods for computing passwords:

Dictionary cracking – The password hashes for all of the words in a dictionary file are computed and compared against all of the password hashes for the users.
This method is extremely fast and finds very simple passwords.

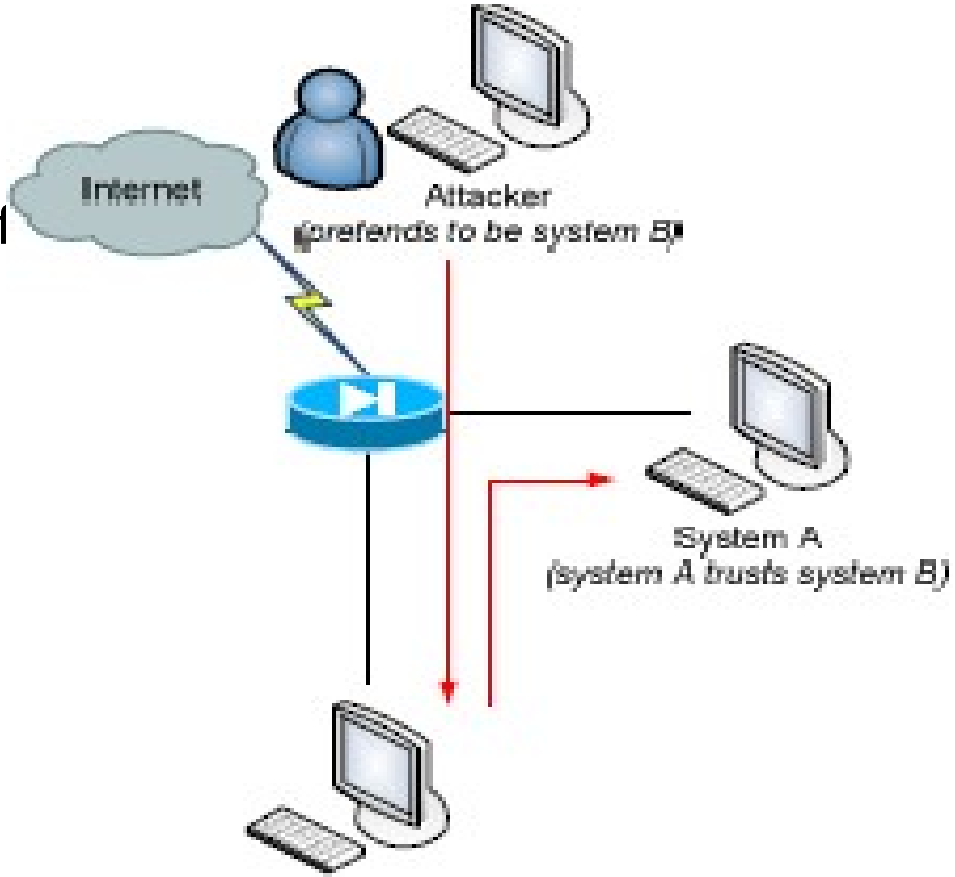
Brute-force computation – This method uses a particular character set, such as A to Z, or A to Z plus 0 to 9, and computes the hash for every possible password made up of those characters.
It will always compute the password if that password is made up of the character set you have selected to test.
The downside is that time is required for completion of this type of attack.

Trust Exploitation

- ***Trust exploitation***

  refers to an attack in which a individual takes advantage of a trust relationship within a network.

  It is more of a technique than a hack itself



Port Redirection

- ***Port redirection***
  attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.

  They can be mitigated primarily through the use of proper trust models, which are network specific (as mentioned earlier) and implementing Intrusion Detection and Prevention Systems (IDS/IPS).

Man-in-the-middle

- ***A man-in-the-middle attack***
  requires that the hacker have access to network packets that come across a network.

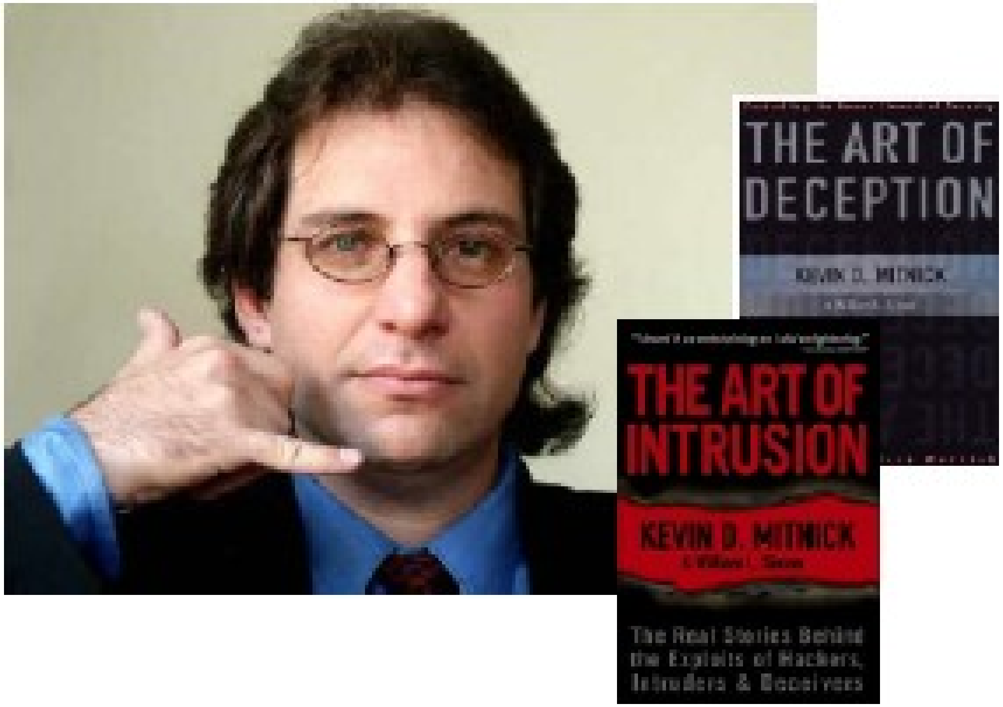
- An example could be someone who is working for an Internet service provider (ISP) and has access to all network packets transferred between the ISP network and any other network.

- Such attacks are often implemented using network packet sniffers and transport protocols.

- ***Man-in-the-middle attack mitigation***
  is achieved by encrypting traffic in an IPSec tunnel, which would allow the hacker to see only cipher text.

Social Engineering

- The easiest hack involves no computer skill at all.
- If an intruder can convince a member of an organization into giving over valuable information, such as: locations of files, servers, passwords.
- The process of hacking is made immeasurably easier.



Soceanu

Phishing

- ***Phishing is a type of social engineering attack*** that involves using email or other types of messages in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords.

- ***The phisher will masquerade as a trusted party*** that has a seemingly legitimate need for the sensitive information.

Denial of Service

- Certainly the most publicized form of attack, DoS attacks are also among the most difficult to completely eliminate.
- DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute.
- Because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

Distributed Denial of Service (DDoS)

- ***DDoS attacks*** are designed to saturate network links with spurious data. This data can overwhelm an Internet link, causing legitimate traffic to be dropped.

- DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale.

- Typically hundreds or thousands of attack points attempt to overwhelm a target..

- DDoS Example:
  - Smurf
  - Tribe Flood Network (TFN)
  - Stacheldraht

Masquerade/IP Spoof

- ***Masquerade attack:*** the network intruder can manipulate TCP/IP packets by IP spoofing, falsifying the source IP address, thereby appearing to be another user.

- The intruder assumes the identity of a valid user and gains that user's access privileges by IP spoofing.

- ***IP spoofing:*** intruders generate and transmit IP data packets with falsified IP source addresses.

Malicious Code

The primary vulnerabilities for end-user workstations are:

1. Worms
2. Viruses
3. Trojan Horses

4. Managing Network Security

Vulnerability Analysis

- ***Before adding new security solutions*** to an existing network, the current state of the network and organizational practices needs:
    - to be identified to verify their current compliance with the requirements,
    - identify possible improvements
    - consider potential need to redesign a part of the system, or to rebuild a part of the system from scratch

to satisfy the requirements.

Security Policy Identification

Initially, two basic areas of the policy should be examined:

1. *The policy should identify the assets that require protection.*

   This will help the designer provide the correct level of protection for sensitive computing resources, and identify the flow of sensitive data in the network.

2. *The policy should identify possible attackers*.
   This will give the designer insight into the level of trust assigned to internal and external users, ideally identified by more specific categories such as business partners,customers of an organization, outsourcing IT partners.

Manage Network Security

- ***Managing network security*** is a continous recoursive ongoing process build arround secirity policy

- Network security paradigm incorporates following steps:

  1) Develop a Security Policy

  2) Make the network secure (implement security solutions: authentication, encryption, firewalls, intrusion prevention, etc.)

  3) Monitor and Respond; detects violations to the security policy

  4) Test; validates the effectivness of the security policy, test the security safeguards

  5) Manage and Improve; use information from the steps 3) and 4) to improve the implementation of the security