Network Security

Information Assurance & Security

IS – 21218

V.Diluxshan EP-2037

Department of Computing & Information System,
Sabaragamuwa University of Sri Lanka.

12 July 2017

CONTENT

INTRODUCTION

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However , as more and more people become "wired" , an increasing number of people need to understand the basics of security in a networked world.

Network security starts with authenticatingcommonly with the username and password. Every networks need to conform their security for their client uses. Security management for networks is different for all situations.

Computer security has been a topic of great importance since the emergence of second generation main frame computers (early 1960's). Some of the earliest applications of these main frame machines involved financial calculations. Floating point arithmetic was often used to represent (inexactly) the values of a penny or dime. More than one dishonest programmer developed software which would accumulate the inaccuracy of each account transaction into a single account. The losses were not noticed on individual accounts, but were later noticed at the institutional level.

In the early 1960's, as the first time-sharing/multi-user systems were being developed, system designers realized that they had to give serious consideration to security designs because these systems allowed remote access to the computer which were not covered by the physical security measures protecting the computer.

It is important to separate the establishment of security policy from the mechanisms one might use to implement or enforce a particular security policy.

For an Example:-

> For example, one might decide that it will be the policy to not allow access to a certain building after 11 p.m. on weekdays. A mechanism for implementing this policy might involve the installation of door locks on all entry points and providing staff which will lock the doors promptly at 11 p.m. on weekdays.

Why you Need to Know.....?

Just we go through the Example -

When applied to a multiuser file system, might be that users have read-write access to their own files but no access to any other user's files. Such a policy may make file sharing cumbersome. An alternate policy might allow read, but not write, access to other user's files. This would go beyond *need to know* because a user may be able to see the contents of files he or she has no need to, even though the user is prohibited from changing such files.

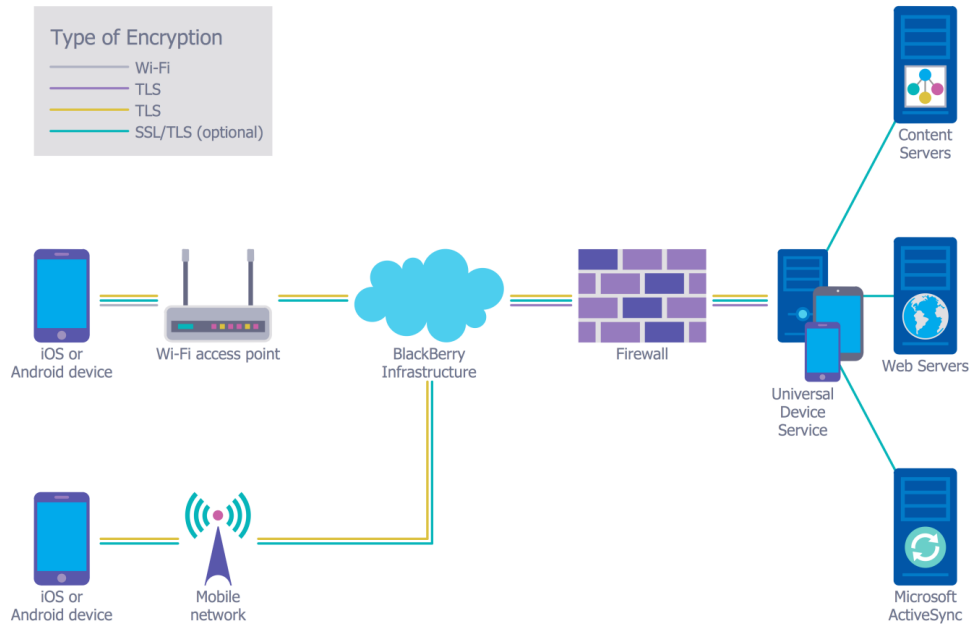
WHAT IS NETWORK SECURITY.....!

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources .Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Network Security is a branch of computer science that involves in securing a computer network and network infrastructure devices to prevent unauthorized access, data theft, network misuse, data modification. We are dependent on computers today for controlling large money transfers between banks, insurance, markets, telecommunication, electrical power distribution, health and medical fields, nuclear power plants, space research and satellites. We cannot negotiate security in these critical areas.

Security Management

As the complexity of the systems and the networks are increasing, vulnerabilities are also increasing and the task of securing the networks is becoming more complex. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer Trojan being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS). Help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine language with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.



Security objectives

- IDENTIFICATION

  Something which uniquely identifies a user and is called User ID.
  Sometimes users can select their ID as long as it is given too another user.
  User ID 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 Procedure

  Authentication procedure

  ✓ Two-Party Authentication
    - One-Way Authentication
    - Two-Way Authentication

  ✓ Third-Party Authentication
    - Kerberos

- X.509

✓ Single Sign ON

- ACCESS CONTROL

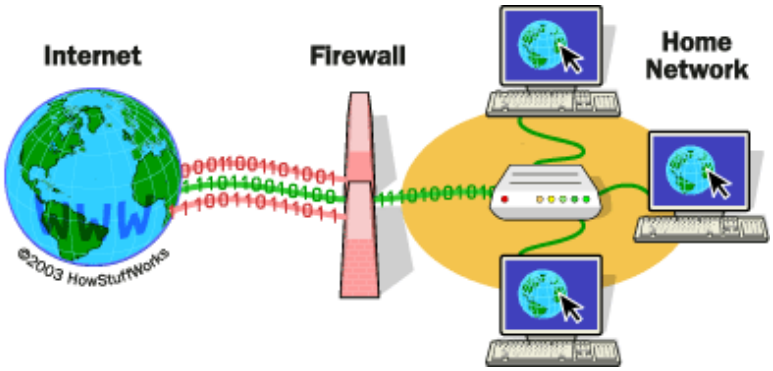
Refers to security features that control who can access resources in the operating system. Applications call access control functions to set who can access specific resources or control access to resources provided by the application.

TYPES OF ATTACKS

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

Types of attacks which is include

- Passive
  - Wiretapping
  - Port Scanner
  - Idle Scan
  - Encryption
  - Traffic Analysis
- Active
- Virus
- Eavesdropping
- Data Modification
  - DNS Spoofing
  - VLAN hopping
  - SQL injection



INTERNET SECURITY

Ultimately, computer system security may be reduced to the physical security of the components of the computing system. This introduction focuses on the security of systems which use Internet technology. Such systems themselves are often distributed over a geographic area and are accessed by users which are potentially at any geographic location.

Types of Network Security

Security is a very, very, very important thing for your network to have. The number of hackers are increasingly exponentially.

One of the most important types of security you should have is network security. This security will work to protect the usability and integrity of your network and data. Network security works by identifying and targeting a variety of threats, then stops them from entering your network. It's like your own personal, protection wall.

Network Access Control

This is when you control who can and can't access your network. You do this by identifying which devices and users are allowed into your network. From there, you can enforce various security policies such as blocking certain devices and controlling what someone can do within your network. You can also utilize behavioural analytic tools to identify what normal and abnormal behaviour is. Once you do that, you can set it up where you'll get notifications whenever something is acting abnormally.

Similarly, you can implement firewalls, which is when you put a barrier between your internal network and untrusted outside networks, such as the internet. This way, you can also control your staff's web use and block any threats or dangerous websites.

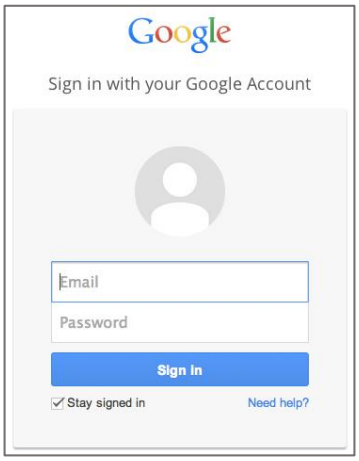
Application Security

Application security is exactly how it sounds – security that protects your applications. This type of security is important to have because no app is created perfectly… they can have a lot of holes or weaknesses where a hacker can enter. A lot of your business operations and devices may run on applications, so this type of security is a must-have.

Antivirus and Antimalware Software

This software is used to protect against malware, which includes anything from viruses, Trojans, ran-some ware, or spyware. Besides the obvious reasons, malware can be very dangerous because sometimes, it can will stay calm within your network for days and weeks, just sitting there ready to spring up and attack. Antivirus and antimalware software deal with this threat by scanning for malware entry and tracking files afterward to find any that may have slipped in and are laying low.

Email Security



Here's a big one. Your email is pretty important for your business, and considering that email gateways are the number one threat for a security breach, email security is an absolute vital one to have. Attackers can use your personal information to do all kinds of damage, such as blackmail or emailing on your behalf to deceive your clients and send them to sites full of malware. An email security application can help block these attacks and control what is sent out.

Wireless Security

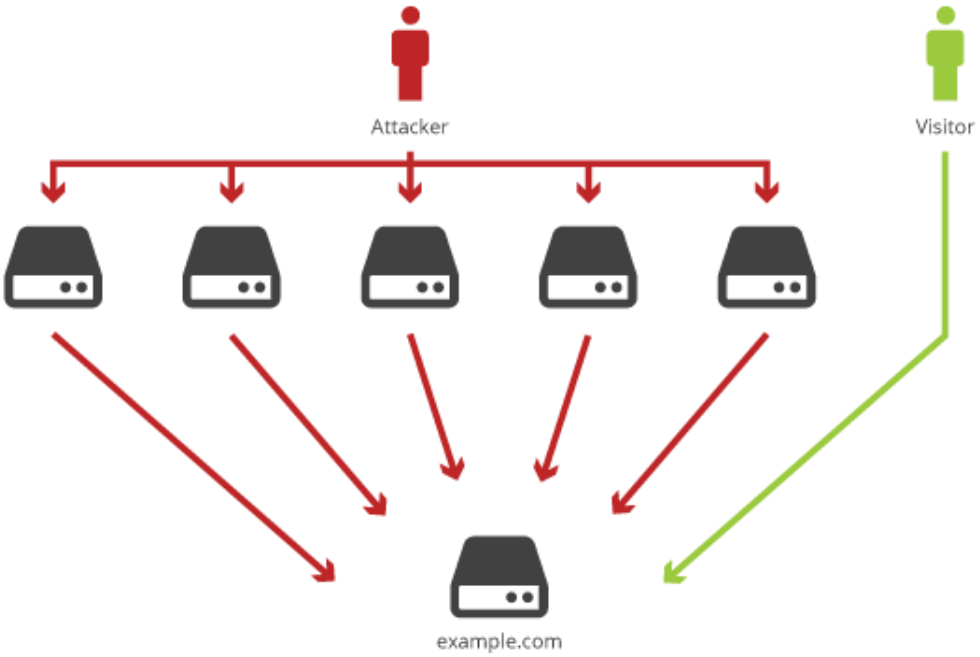
Here's another big one. The mobile office movement is gaining momentum, and with that comes wireless networks and access points. However, wireless networks are not as secure as wired ones, allowing more room for hacker entry, so the power of wireless security needs to be strong.
Since there are many parts to your infrastructure, there are many types of security out there to protect it. There are a lot more that we didn't mention in this blog, but we know all about them here at Alliance Technology Partners.

Authentication Methods

In this case we are going to focus four major types of Methods, and how those methods are taking part in the sub contents….

- ✓ Operating System
  - ✖ Authentication by the Operating System
- ✓ Networks and LDAP Directories
  - ✖ Authentication by the Network.
- ✓ Databases
  - ✖ Authentication by Oracle Database.

- ✓ Multitier Systems
  - ✖ Multitier Authentication and Authorization.



IDENTIFYING NETEORK STATIONS

In an internet, networks are numbered and, within each network, each network interface is numbered. Hence, it is possible to identify each network station (computer) with at least one number which consists of the network number followed by the interface number.

This number is known as the IP (Internet Protocol) number of the station. Stations which have more than one network interface will have more than one IP number and have the potential of forwarding packets of information from one network to another. Messages are sent from one station to another station using message formats consisting of a pair of items; (message-header, message-data).

IP numbers are used to identify internet hosts and must be entered by users when accessing internet services such as Telnet, FTP, WEB URL's, etc. Multi-digit numbers are difficult to enter into user interface programs and recall from memory.

Internet developers devised a *Domain Name System* (DNS) which consists of a distributed hierarchical database of names which may be used for most of the IP numbers on the Internet. Internet hosts are grouped together into domains within an organization and networks are grouped together by type, educational (EDU), commercial (COM), etc.

Finally, the previously mentioned types of networks are grouped together by country to form the top level of the DNS database hierarchy. The DNS system automatically converts host names, which are easier to remember, to actual IP numbers.

ADVANTAGES & DISADVANTAGES

Network security is basically securing your network. Networks can be private, like a network within a company, or public. Securing the network involves preventing any misuse or unauthorized access of the network or its resources. For this, every user is given a unique user ID and password to access data pertaining to them. Without this authentication, no user is permitted to access the network. The network administrator oversees the operations of the network. Let us see some of the advantages and disadvantages of network security.

ADVANTAGES

- Protect Data
  As discussed, network security keeps a check on unauthorized access. A network contains a lot of confidential data like the personal client data. Anybody who breaks into the network may hamper these sensitive data. So, network security should be there in place to protect them.

- Prevents Cyber Attack
  Most of the attack on the network comes from internet. There are hackers who are experts in this and then there are virus attacks. If careless, they can play with a lot of information available in the network.

- Levels of Access
  The security software gives different levels of access to different users. The authentication of the user is followed by the authorization technique where it is checked whether the user is authorized to access certain resource. You may have seen certain shared documents password protected for security. The software clearly knows which resources are accessible by whom.

- Centrally Controlled
  It is very important that the anti-virus software is timely updated. An old version may not offer you enough security against attackers. But it is not guaranteed that every user of the network follows it religiously. A network security system which is centralized offers this advantage of timely updates without even the knowledge of the individuals.

DISADVANTAGES

Network security is a real boon to the users to ensure the security of their data. While it has many advantages, it has lesser disadvantages. Let us discuss some of them.

- Costly set Up
  The setup of a network security system can be a bit expensive. Purchasing the software, installing it etc.Can become costly especially for smaller networks. Here we are not talking about a single computer, but a network of computers storing massive data. So, the security being of prime importance will definitely cost more. It cannot be ignored at any cost!

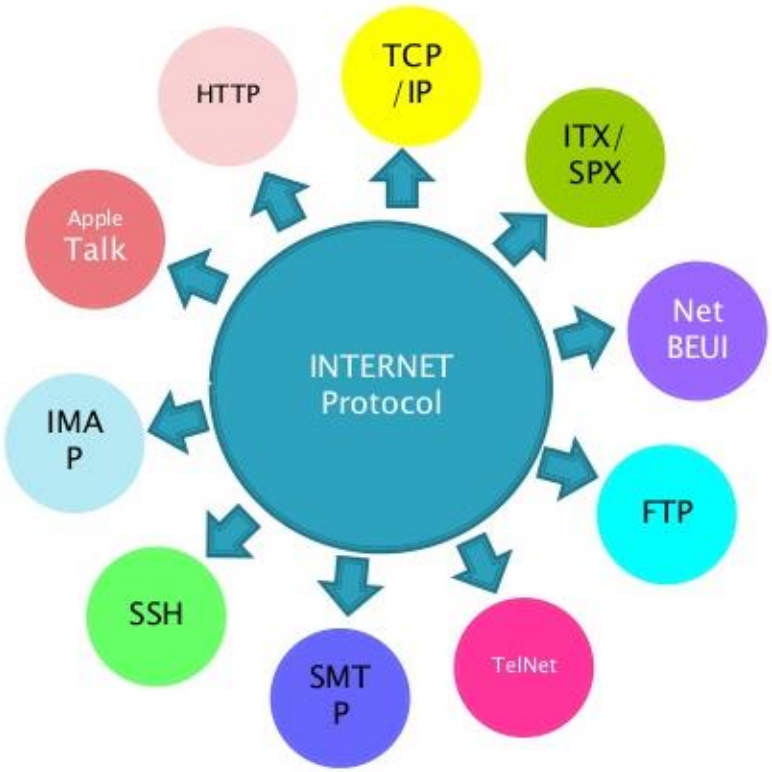
- Time Consuming
  The software installed on some networks is difficult to work with. It needs authentication using two passwords to ensure double security which has to be entered every time you edit a document. It also requires the passwords to be unique with numbers, special characters and alphabets. The user may have to type a number of sample passwords before one is finalized which takes a lot of time.

- Careless Admin
  When the best software is installed and everything required is done, it is natural for the admin to be careless at times. It is his job to check the logs regularly to keep a check on the malicious users. But sometimes, he just trusts the system and that is when the attack happens. So, it is very important that the admin remains vigilant always.

NETWORK PROTOCOLS

Network protocols are standardized communication conventions (implemented in computer software) to provide a variety of internet work services. Among these are protocols for transmission of files (FTP), transmission of WEB documents (HTTP), remote interactive terminal sessions on another computer (Telnet), etc.

Protocols exist to provide higher level services, such as reliable point to point connections (Streams) or secure transmission of information. These protocols may cause lost packets to be automatically retransmitted or may encrypt and decrypt data so that it is not easily readable at intermediate routing points during the transmission.



ISSUES & SOLUTIONS

☑ Weak Network Access Passwords

A complex password. In order to create a complex password, you need seven or more characters combined with at least three numbers and one special character (capital letters, @ or # signs, etc.).

Network security administrators should require the creation of complex passwords as well as implement a password expiration system to help remind users to change their passwords often. A restriction on how soon a password can be reused is also another handy precaution, that way someone isn't cycling between two different passwords every month or so.

☑ Outdated Server Application Software

Companies constantly release patches in order to ensure that your system is not vulnerable to new public threats. Hackers consistently release new threats and exploits which could allow harm to befall your network if these patches are not in place. A simple solution is to ensure your system administrator is regularly informed of new threats and is updating your applications on a monthly basis.

☑ Web Cookies

Although cookies do not carry viruses and cannot install malware on the host computer, the tracking of cookies and third-party tracking cookies are commonly used ways to compile records of individuals' browsing histories. Unencrypted cookies are a major network security issue because they can open your system to a XSS (Cross Site Scripting) vulnerability and that is a major privacy concern. With 'Open Cookies' anyone could have access to any login data cookies (saved password sessions) on the network,

which creates a major vulnerability on your network security system.

☑ Plain Hashes

Hashing is used to index and retrieve items in a database and Plain Hashes are also used in many encryption algorithms. A Salt (which is another type of encryption) is added to Hashes in order to make a lookup table assisted Directory Attack (or Brute-Force) impractical or extremely difficult, provided the Salt is large enough. Basically, an attacker wouldn't be able to use a pre-computed look up table to assist in exploiting your network, which adds a whole new level of complexity to your network security system. So even if an attacker gains access and compromises your database (table), it will still be very difficult for the attacker to retrieve the information.

The best way to ensure safety in regard to Hashes is for your network administrator to hide the Salt (or encryption key), because if the hacker is able to gain access to your Salt encryption they can access your network system. Salt all of your Hashes. No Salt means no security.

☑ Share Hosting

If you are running a legitimate business and have a website with access to your internal network, Shared Hosting is not the way to go! A shared web hosting service is where many websites reside on one web server connected to the Internet. Each site sits on its own partition, or section or space on the server, to keep it separate from other sites. This is generally the most economical option for hosting, because people share the overall cost of server maintenance. The best solution is to have dedicated Server Hosting and/or Secure Cloud Hosting.

ETHICAL HACKING

- *HACKER* A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers, who prefer to learn only the minimum amount necessary.

➢ Def :

Evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

This method has been in use from the early days of computers.

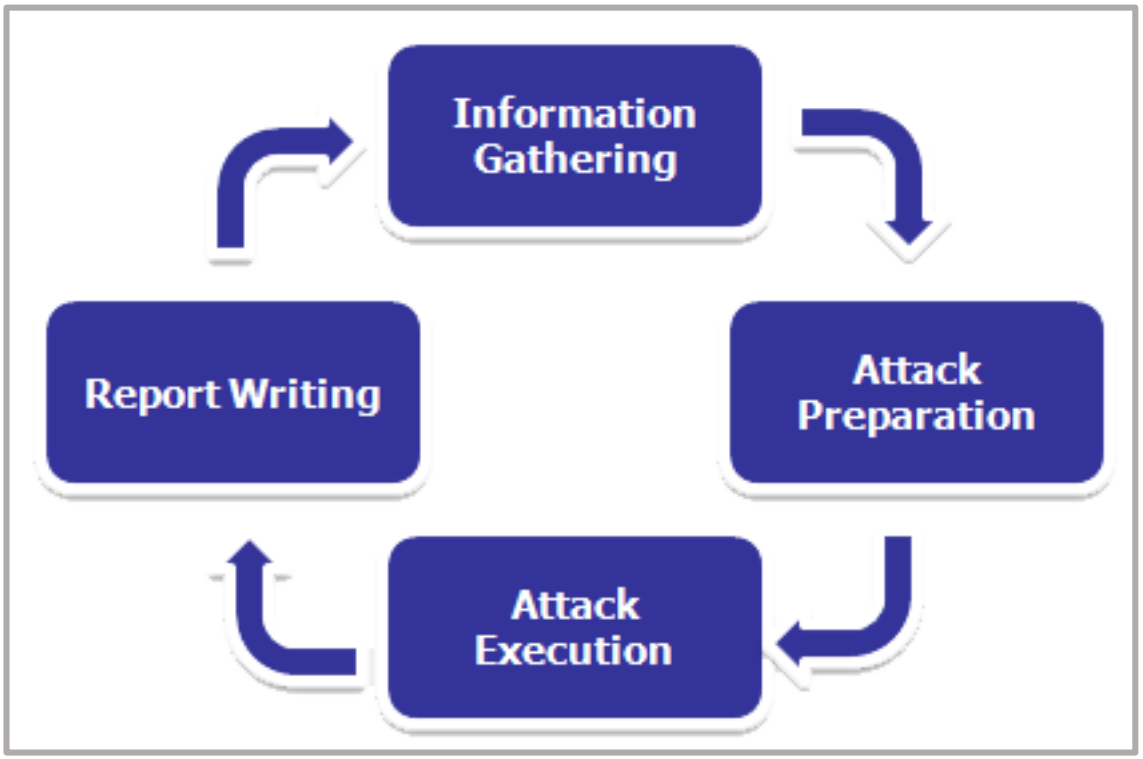
➢ Goals :

- Hack your systems in a non destructive fashion.
- Enumerate vulnerabilities and if, necessary, prove to upper management that vulnerabilities exists.
- Apply results to remove vulnerabilities & better secure your systems.

➢ What do ethical hackers do..?

- Stolen Laptop computer- the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers.
- Social Engineering- evaluates the target organization's staff as to whether it would leak information to someone.
- Physical Entry- acts out a physical penetration of the organization's building].
- The final report- collection of all of the ethical hacker's discoveries made during the evaluation.

Hacking Progress Model...!



REFERENCE

http://www.conceptdraw.com/How-To-Guide

http://www.webopedia.com/TERM

http://www.wikipedia.com

https://www.alliancetechpartners.com