Data security:

Data Security means protecting a database from destructive forces and the unwanted actions of unauthorized users. In simple terms, data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Data is the raw form of information stored as columns and rows in our databases, network servers and personal computers. This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form. There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down your data from software solutions to hardware mechanisms.

Encryption

Encryption has become a critical security feature for thriving networks and active home users alike. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only by decoded or decrypted by the party that possesses the associated key. (FDE) Full-disk encryption offers some of the best protection available. This technology enables you to encrypt every piece of data on a disk or hard disk drive. Full disk encryption is even more powerful when hardware solutions are used in conjunction with software components. This combination is often referred to as end-based or end-point full disk encryption.

Strong User Authentication

Authentication is another part of data security that we encounter with everyday computer usage. Just think about when you log into your email or blog account. That single sign-on process is a form authentication that allows you to log into applications, files, folders and even an entire computer system. Once logged in, you have various given privileges until logging out. Some systems will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter.

The single sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. This may include a password, a one-time password, a smart card or even a fingerprint.

Backup Solutions

Data security wouldn't be complete without a solution to backup your critical information. Though it may appear secure while confined away in a machine, there is always a chance that your data can be compromised. You could suddenly be hit with a malware infection where a virus destroys all of your files. Someone could enter your computer and thieve data by sliding through a security hole in the operating system. Perhaps it was an inside job that caused your business to lose those sensitive reports. If all else fails, a reliable backup solution will allow you to restore your data instead of starting completely from scratch.

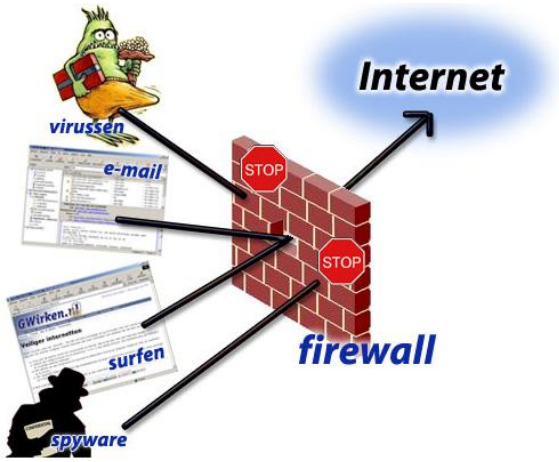
Firewall:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall, working closely with a router program, examines each network packetto determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.

A number of companies make firewall products. Features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall.



There are several types of firewall techniques:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and

transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
Circuit-level gateway: Applies security mechanisms when a TCP orUDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Intrusion prevention systems

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

Signature-Based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

Statistical anomaly-based detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Stateful Protocol Analysis Detection: This method identifies deviations of protocol states by comparing observed events with predetermined profiles of generally accepted definitions of benign activity.

Intrusion detection system (**IDS**):

An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

All Intrusion Detection Systems use one of two detection techniques:

Statistical anomaly-based IDS

A statistical anomaly-based IDS determines normal network activity like what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous(not normal).

Signature-based IDS

Signature based IDS monitors packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures. The issue is that there will be lag between the new threat discovered and Signature being applied in IDS for detecting the threat. During this lag time your IDS will be unable to identify the threat.

Virtual Private Network:

A **virtual private network** (**VPN**) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. VPNs can connect individual users to a remote network or connect multiple networks together. Through VPNs, users are able to access resources on remote networks, such as files, printers, databases, or internal websites. VPN remote users get the impression of being directly connected to the central network via a point-to-point link.

VPNs can be either remote-access (connecting an individual computer to a network) or site-to-site (connecting two networks together). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while traveling outside the office, and site-to-site VPNs allow employees in geographically separated offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

VPN systems can be classified by:

- the protocols used to tunnel the traffic
- the tunnel's termination point, i.e., customer edge or network-provider edge
- whether they offer site-to-site or remote-access connectivity
- the levels of security provided
- the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity

Virtual Private Server(VPS):

Virtual private server (**VPS**) is a term used by Internet hosting services to refer to a virtual machine. The term is used for emphasizing that the virtual machine, although running in software on the same physical computer as other customers' virtual machines, is in many respects functionally equivalent to a separate physical computer, is dedicated to the individual customer's needs, has the privacy of a separate physical computer, and can be configured to run server software.

The terms **virtual root server** (**VRS**) and **virtual dedicated server** (**VDS**) are also used as synonyms of VPS. However, the latter also occasionally indicates that the server does not use burst/shared RAM through multiple machines and may use individual CPU cores. The term **cloud server** is also used to describe the same concept, normally where such systems can be setup and re-configured on the fly.

The concept behind server virtualization is a specific example of the same concepts that led to the development of time-sharing and multiprogramming. Generally, client users tend to ask for computer resources in a "bursty" fashion, demanding fast-as-possible response to requests, but then entering long periods of no activity while they examine the results. During these idle periods, the computer's resources can be used to service requests from other clients. This model makes more efficient use of the computer's resources, reducing the time the system is idle, regardless of user patterns. It also allows the users to share resources, save files on a hard drive or take turns using a printer.

Virtualization extends this basic concept to the computer as a whole. In the traditional model, the operating system shares access to the resources, but there is still a single machine being shared. In the virtual server model, the virtualization software instead provides the illusion of more than one computer, hard drive, printer, etc. Although the resources are still shared, as under the time-sharing model, virtualization provides a higher

level of security as the individual virtual servers are isolated from each other. Each virtual server can run its own full-fledged operating system and can be independently rebooted. This is valuable as it allowed businesses to run their legacy applications on older versions of an operating system on the same server as newer applications.

Partitioning a single server so that it appears as multiple servers has long been common practice on mainframe computers and mid-range computers such as the IBM AS/400. It has become more prevalent with the development of virtualization software and technologies for microcomputers.

The physical server typically runs a hypervisor which is tasked with creating, releasing, and managing the resources of "guest" operating systems, or virtual machines. These guest operating systems are allocated a share of resources of the physical server, typically in a manner in which the guest is not aware of any other physical resources save for those allocated to it by the hypervisor.

The guest system may be fully virtualized, paravirtualized, or a hybrid of the two.

In a fully virtualized environment, the guest is presented with an emulated or virtualized set of hardware and is unaware that this hardware is not strictly physical. The hypervisor in this case must translate, map, and convert requests from the guest system into the appropriate resource requests on the host, resulting in significant overhead. Almost all systems can be virtualized using this method, as it requires no modification of the operating system, however a CPU supporting virtualization is required for most hypervisors that perform full virtualization.

Proxy Server:

A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

A proxy server receives a request for an Internet service (such as a Web page request) from a user. If it passes filtering requirements, the proxy server, assuming it is also acache server , looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

To the user, the proxy server is invisible; all Internet requests and returned responses appear to be directly with the addressed Internet server. (The proxy is not quite invisible; its IP address has to be specified as a configuration option to the browser or other protocol program.)

An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. In fact, there are special servers called cache servers. A proxy can also do logging.

The functions of proxy, firewall, and caching can be in separate server programs or combined in a single package. Different server programs can be in different computers. For example, a proxy server may in the same machine with a firewall server or it may be on a separate server and forward requests through the firewall.

Proxy servers have two main purposes:

Improve Performance: Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both userX and user Y access the World Wide Web through a proxy server. First user X requests a certain Web page, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such asAmerica Online, MSN and Yahoo, for example, employ an array of proxy servers.

 Filter Requests: Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.