9.1 The Challenges of Client / Server Security
9.2 Security for the Clients and Servers
- 9.2.1 Physical security
- 9.2.2 Software security
- 9.2.3 Network security

What Is Security?

In general, security is "the quality or state of being secure--to be free from danger." It means to be protected from adversaries--from those who would do harm, intentionally or otherwise.

- **Authentication** deals with user account validation, verifying the identity of a user. Is this a valid user? Is this user registered in our application? e.g.: Login
- **Authorization** deals with user access validation to certain feature, allowing an authenticated user to access. Does this user have the authorization/right to access this feature? e.g.: Claims, Roles

When configuring the security for a Sun Ray environment, you should evaluate the security requirements. You can choose one of the following security policies between the server and clients:

- Enable encryption for upstream traffic only (client to server)
- Enable encryption for downstream traffic only (server to client)
- Enable bidirectional encryption
- Enable server authentication
- Disable client authentication

Additionally, you must decide whether to enable hard security mode for encryption and client authentication.

9.1 The Challenges of Client / Server Security

Challenges of Client Server security are focusses mainly in three parts; -

1. Challenges on Physical Security – Processor speed, Storage, Memory, System Failure
2. Challenges on Software Security – Malware and threats attacking, Cracked software,
3. Challenges on Network Security – DoS Attack, Congestion, Network Speed, Throughput, Delay, Poor Network Design

CLIENT SECURITY THREATS

Client threats mostly arise from malicious/ bad data or code, malicious code refers to Viruses, Worms, Trojan Horses.

- **Viruses** : A computer virus is a program or piece of code that is loaded onto your computer without your knowledge & runs against your wishes. Virus can also replicate themselves.
- **Trojan horse** is a program that appears harmless, but is, in fact, malicious. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive (e.g. Crashing the computer or device, Modification or deletion of files, Data corruption, Block any anti-virus program, Block any installation process, Formatting disks, destroying all contents, Spreading malware across the network, Spying on user activities and access sensitive information.)

  Some Trojan Horses :
  - ✓ **Trojan-SMS :** These programs can cost you money – by sending text messages from your mobile device to premium rate phone numbers.
  - ✓ **Trojan-Spy** : Trojan-Spy programs can spy on how you're using your computer – for example, by tracking the data you enter via your keyboard, taking screen shots or getting a list of running applications.
  - ✓ **Trojan-Downloader** : Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and adware.
  - ✓ **Trojan-Banker :** Trojan-Banker programs are designed to steal your account data for online banking systems, e-payment systems and credit or debit cards.
- **Worms** : A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install backdoors on computers.

  Worms are often confused with computer viruses; the difference lies in how they spread. Computer worms self-replicate and spread across networks, exploiting vulnerabilities, automatically; that is, they don't need a cybercriminal's guidance, nor do they need to latch onto another computer program

SERVER SECURITY THREATS

- **Brute Force Attack :** In a brute force attack, the intruder, attacker attempts to gain access to a server by guessing a user password (usually the root administrator) through the SSH server, Mail server, or other service running on your system. The attacker will normally use software that will check every possible combination to find the one that works. Brute force detection software will alert you when multiple failed attempts to gain access are in progress and disable access from the offending IP address.

- **Open Relay**: A Mail Transfer Agent (MTA) normally uses an SMTP server to send email from your server's users to people around the world. With an open relay, anyone can use your SMTP server, including spammers. Not only is it bad to give access to people who send spam, it could very well get your server placed on a DNS blacklist that some ISPs will use to block mail from your IP. It is very easy to close an open relay. Just follow the documentation for your MTA.
- **Botnet**: e.g., to send spam messages. Attackers use botnets to automatically run and distribute malicious software on "agent" servers. They then use the agent machines to attack or infect others. Because all of this can be done automatically without user intervention, botnets can spread very quickly and be deadly for large networks. They are commonly used in DDoS attacks and spam campaigns.
- **DoS** : DoS stands for **Denial of Service,** and is a technique attackers will use to effectively shut off access to your site. They accomplish this by increasing traffic on your site so much that the victim's server becomes unresponsive. While some DoS attacks come from single attackers, others are coordinated and are called Distributed Denial of Service (DDoS) attacks.
  The 2 most common types of these attacks are: -
  - **Service overloading**: Servers are vulnerable to service overloading. DoS will occur due to overloading of the server.
  - **Message overloading**: Message overloading will occur when someone sends a very large file to the message box of server at every few seconds. The message box rapidly grows in size & begins to occupy all space on the disk & increase the number of receiving process on the recipient's machine & causing a disk crash.
- **Cross-site Scripting** : Cross-site scripting or XSS is a technique that makes use of vulnerabilities in web applications. According to UK dedicated hosting server specialists at 34SP.com, the vulnerability allows the attacker to inject code in a server-side script that they will use to execute malicious client-side scripts or gather sensitive data from the user. You can fix most XSS problems by using scanner software to detect vulnerabilities and then fix whatever you find.
- **SQL Injection** : Like XSS, SQL injection requires a vulnerability to be present in the database associated with a web application. The malicious code is inserted into strings that are later passed to the SQL server, parsed, and executed. As with other vulnerability-dependent attacks, you can prevent it by scanning for problem code and fixing it.
- **Malware** : Malware can take many forms, but as the name implies, it is malicious software. It can take the form of viruses, bots, spyware, worms, trojans, rootkits, and any other software intended to cause harm. In most cases, malware is installed without the user's direct consent. It may attack the user's computer and/or attack other computers through the user's own system. Having proper firewall and security software protection can usually prevent malware from spreading.
- **Unpatched Software** : Most threats to a server can be prevented simply by having up-to-date, properly-patched software. All server operating system vendors and distributions publish security updates. By installing them on your system in a timely manner, you prevent attackers from using your server's own vulnerabilities against it.
- **Careless Users** : The number one, most prevalent threat to a server's security is user carelessness. If you or your users have passwords that are easy to guess, poorly written code, unpatched software, or a lack of security measures like anti-virus software, you are just asking for trouble. By enforcing strong security practices and secure authentication, you can lessen or even eliminate most threats.

9.2 Security for the Clients and Servers

- Client-server environments are popular because they increase application processing efficiency while reducing costs and gaining the maximum benefit from all resources working together. These benefits are gained by splitting processing between the client machine/software and server machine/software. Each process works independently but in cooperation and compatibility with other machines and applications (or pieces of applications).
- All independent processing must be performed to complete the requested service. Cooperation of application processing produces another client-server advantage, it reduces network traffic. Since each node (client and/or server) performs part of the processing within itself, network communication can be kept to a minimum. For example, static processes, like menus or edits, usually take place on the client-side. The server, on the other hand, is responsible for processes like updating and reporting.
- There are three components to client-server environments: the client, the server (there may be multiple servers), and the network. The network bridges the physical and functional separation between the client and the server. The multiple connections possible between clients and multiple servers really provides the visual of a web or network. Networks provide a flexible environment where clients can mix and match hardware, software, and operating systems.
- However, the very characteristic that make client-servers popular are also what make it the most vulnerable to breaches in security. It is precisely the distribution of services between client and server that open them up to damage, fraud, and misuse. Security consideration must include the host systems, personal computers (PCs), local area networks (LANs), global wide area networks (WANs), and users. *Because security investments don't produce immediately visible returns and client-server buyers sometimes don't educate themselves about security, this area of development is often overlooked until a problem occurs.*

9.2.1 Physical security

Users should lock their workstations when they walk away, even for a minute. That is all it takes for a malicious co-worker to send out an email in the user's name, or surf a website that downloads a virus or some other software unknown to the perpetrator. At the end of the day, lock the room if possible, to protect the computer from intruders who gain access to the building. Physical security is the first line of

defense for client computers. Users who work from home should log off while they are going to be away from home for an extended period of time. A laptop should never be left on a car seat or hotel room.

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

Physical security has three important components: access control, surveillance and testing.

I. Access Control : hardening measures include fencing, locks, access control cards, biometric access control systems and fire suppression systems
II. Surveillance : physical locations should be monitored using surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors and smoke detectors
III. Testing : disaster recovery policies and procedures, Backups should be tested on a regular basis to ensure safety and to reduce the time it takes to recover from disruptive man-made or natural disasters.

9.2.2 Software security

Software threats are malicious pieces of computer code and applications that can damage your computer, as well as steal your personal or financial information. For this reason, these dangerous programs are often called malware (short for "malicious software.")

i. Mobile Software Threats

With an increasing reliance on mobile devices it is important to be aware of new and emerging software threats that target them specifically. Mobile viruses, for example, can infect one cellular phone and then spread to other devices via the mobile phone network. **Bluejacking** is the sending of unwanted or unsolicited messages to strangers via **Bluetooth** technology. It can be a serious problem if obscene or threatening messages and images are sent. **Bluesnarfing** is the actual theft of data from Bluetooth enabled devices (including both mobile phones and laptops): contact lists, phonebooks, images and other data may be stolen in this way. [1]

Mobile Viruses

Mobile devices can be infected by viruses that spread themselves via the mobile phone network. These have been a limited threat to date due to the fact that mobile phones use many different operating systems, but as a small number of systems (such as *Android* and *iOS*) become dominant, these viruses will be able to spread more widely. In all other respects these are identical to other computer viruses. [2]

Bluejacking

Bluejacking uses a feature originally intended to exchange contact information to send anonymous, unwanted messages to other users with *Bluetooth*-enabled mobile phones or laptops. In some cases this is used to send obscene or threatening messages or images, and it could be used to spread malware as well. [3]

Bluesnarfing

Bluesnarfing is the actual theft of data from *Bluetooth* enabled devices (especially phones). Like bluejacking it depends on a connection to a *Bluetooth* phone being available. A *Bluetooth* user running the right software from a laptop can discover a nearby phone and steal the contact list, phonebook and images etc. Furthermore, your phone's serial number can be downloaded and used to close the phone. Again, the only current defense is to turn your Bluetooth off by setting it to "undiscoverable". [4]

Security Tips

- In order to protect yourself from mobile viruses it is important to regularly update your operating system. Security software is also available for a variety of mobile operating systems, including *Android* and *iOS* (*iPhone* and *iPad*). Many of these are produced by the same publishers as popular security suites for desktop computers such as *Norton* and *McAfee*.
- The only way to avoid Bluejacking is to turn off your *Bluetooth* device or set it to "undiscoverable". To limit the risk of Bluesnarfing, only use *Bluetooth* devices in private.

ii. Malware

Email viruses

Most **email viruses** rely on the user double clicking on an attachment. This runs a malicious code that mails itself to other users from that computer. Any attachment that you open on your computer could contain a virus and infect your computer even if the extension appears to be safe (such as .txt, .doc and .jpg). Some viruses can infect users as soon as they open the email. These viruses may compromise your computer's security or steal data, but more often they create excessive email traffic and crash servers. [6] Viruses can also be spread by clicking on links in emails that lead to malware sites.

Macro viruses

This type of virus, also known as a **document virus**, takes advantage of **macros** (commands embedded in word processing and spreadsheet software that run automatically) to infect your computer. A macro virus can copy itself and spread from one file to another. If you open a file that contains a macro virus it copies itself into the application's start up files and infects the computer. The next file you open using the same program, and every file thereafter, will become infected; the infection can therefore spread rapidly across a network. [7]

Boot sector viruses

Boot-sector viruses are mostly spread through infected storage devices such as USB drives. When your computer is turned on the hardware seeks out the **boot-sector program**, which is the program the computer runs when it starts up. (This is generally located on the hard drive but can also be on a storage device such as a DVD or USB drive.) A boot-sector virus replaces the original boot-sector with its own, modified

version. Upon your next start up the infected boot sector is used and the virus becomes active. It can then read or modify any files or programs on your computer. [8]

Adware

This type of intrusive software displays advertisements on your computer. These usually come in the form of banners and pop-ups when an application is in use. Adware can become a serious problem if it installs itself onto your machine: it can hijack your **browser** (*Internet Explorer*, *Firefox*, *Chrome* or *Safari* for example) to display more ads, gather data from your Web browsing without your consent and prevent you from uninstalling it. The most common issues with **adware** is that it can slow down your Internet connection or render you computer unstable as well as distract you and waste your time. [9]

Spyware

While technically a form of adware, **spyware** has as its primary function the collection of small pieces of information without users' knowledge. One form of spyware, called a **keylogger,** actually monitors everything you input into your computer. In addition to monitoring your input and Internet surfing habits, spyware can interfere with your control over your computer by installing additional software, redirecting your browser, changing computer settings, and slowing or cutting off your Internet connection. [10]

Security Tips

- To avoid **viruses** you should run anti-virus software (*Norton*, *MacAfee*, and *Avast* are examples of reputable programs) and avoid clicking on unexpected **attachments**. Installing **patches** (a software "fix" designed to address holes and vulnerabilities in software) issued by software vendors can also protect you as they can close down vulnerabilities exploited by **viruses**. In particular, it is important to keep your **browser** (the program you use for accessing the Web, such as *Internet Explorer*, *Firefox*, *Chrome* or *Safari*) up-to-date, as browsers are one of the main targets of viruses.
- To avoid **email viruses** in particular, be careful about downloading attachments. You should only download an attachment from an email if you know the sender and are certain that his/her account has not been compromised. (Signs that an e-mail account has been compromised include a subject line that makes no sense and mass-mailings to all of the account's contacts.)
- Avoid opening any documents that are not from a sender you know and trust. If any of your programs begin behaving oddly, run a scan using your anti-virus software immediately.
- To avoid viruses and other malware carried on **storage devices**, use only storage devices that you have bought new. Before using any storage device, run anti-virus software on it, and do so again every time you plug a storage device into a different computer.
- Most antivirus software detects **adware** and labels it as "potentially unwanted applications". You can then authorize the adware or choose to remove it. There are also dedicated adware removal programs such as *Ad-Aware* by Lavasoft. A freeware version exists online, though it has fewer features than the commercial version.
- Similarly, most **anti-spyware** software will be included with a comprehensive antivirus program or you can opt for dedicated software.

General Tips - Most computers come with embedded security features including a **firewall**. This prevents unknown programs and processes from accessing the system but is not a replacement for anti-virus software. Your firewall can be located and activated from your computer's **control panel**. Some websites maintained by antivirus vendors offer free online scanning of your entire computer system, but be sure to verify the source: some sites which claim to scan for viruses actually plant malware on your computer.

iii. Cookies

A cookie is a small text file which is saved on your computer by a website, mainly used as a means for session management, personalization and tracking while surfing the Web. Some cookies can be beneficial, making for a smoother browsing experience: for instance, they can save small pieces of information into memory, such as your name, so that you don't constantly have to re-enter it on your most frequently visited websites. Cookies are essential to common features of websites such as "shopping carts" (which store your purchasing decisions while you browse an online commerce site such as *Amazon*). These cookies are usually deleted after you leave the website or within a few days of not visiting it.

Other cookies, however, can be far more of a nuisance. These cookies will recreate themselves after the user has deleted them. A script will then keep this information in some other location on the computer, unbeknownst to the user. Other kinds are able to closely track your online habits and can last up to a year on a given server. [11]

Understanding Cookies

There are several different types of cookies. Each has different properties:

Session Cookies

This type of cookie only lasts for the duration of your stay on a particular website and is deleted when you close your browser.

Persistent Cookies

This type of cookie is also known as a "tracking" or "in memory" cookie. These cookies can last up to a year from each time a user revisits the server.

Secure Cookies

These cookies are used when you are visiting a secure site (one where the Web address begins with "https" rather than "http"). These cookies are **encrypted** when being sent to and from your computer and the server, which means that they are more secure if someone intercepts or copies them.

Unauthorized Installation and Replication Cookies

This type of cookie, sometimes referred to as a "zombie" or "super" cookie, automatically recreates itself in some other location on the computer after a user has deleted it.

Security Tips

- Most browsers (*Internet Explorer*, *Firefox*, *Chrome* or *Safari*) are set to accept cookies by default. If you do not wish to use cookies, all browsers allow you to disable them. Some browsers also allow you to see which cookies you currently have on your computer and to delete those you do not want. There are also software tools, such as *CCleaner*, *WinBrush* and *QuickWiper*, that get rid of standard cookies and files as well as unwanted persistent and self replicating cookies that refuse to go away.
- Most browsers also have an option to browse without storing cookies (called **inPrivate Browsing** in *Internet Explorer*, **Incognito Mode** in *Chrome* and **Private Browsing** in *Firefox* and *Safari*). However, while this does prevent cookies from being saved to your computer it does not mean that there will be no records of your browsing saved on your computer or on the servers of the websites you visit.
- **Secure sites** (where the Web address begins with "https" rather than "http") encrypt any cookies you send to them. This makes it more difficult for the information in the cookies to be intercepted and misused. You should always use secure sites for anything that involves financial information (bank or credit card data, etc.)
- Because logins and passwords are often saved using cookies, you should periodically change your passwords on any sites you visit.

iv. Browser Hijacking

Browser hijacking is a malicious online activity where hijackers change the default settings in your Internet browser. Links may appear that point to websites you would usually avoid, new toolbars and favorites that you do not want may be added and your computer may slow down overall. Users will also often find themselves unable to return to their original settings once this is done. The purpose of this threat is to force you to visit a website. This increases the traffic and number of "hits" a website receives which allows it to boost its advertising revenue. (These websites may also contain malicious scripts or viruses.) Browser hijackers can be extremely persistent and if they can't be removed you may find yourself having to reinstall your browser or restore your entire system to its original settings. [12]

Security Tips

- As is the case with most other software threats, keeping your browser updated and using reliable security software and updates is your first defense. If you do become a victim of hijacking, you can reset your browser settings. How this is done depends on your browser:
  - In *Internet Explorer*, close your browser and then go to **Control Panel**. Select **Network and Internet** and then **Internet Options**. Click on the **Advanced** tab and then click on the **Reset** button under **Reset Internet Explorer Settings**.
  - In *Firefox*, open the **Start** menu and select **Run**. Enter "firefox-safe-mode" (without quotation marks) then select **"Reset all user preferences to Firefox defaults."**
  - In *Chrome*, delete the **First run** file. If you are using *Windows XP*, that file is at C:\Documents and Settings**UserName**\Local Settings\Application Data\Google\Chrome\Application (where "UserName" is your name); if you are using *Windows Vista* or later, it is at C:\Users**UserName**\AppData\Local\Google\Chrom\Application.
  - In *Safari*, begin by opening your browser and clicking on "**Safari**" in your **Safari menu**. Select **Reset Safari** and click the **Reset** dialogue button that appears.
- You can also disable your **add-ons** (a piece of software that enhances another software program, such as plug-ins for Internet Explorer) as a secondary line of defense. If all else fails you may have to restore your computer's state to an earlier point in time using a backup hard drive or the **recovery discs** that came with it.

v. Scripts

A **script** is a piece of code that is loaded and run by your browser. The most common type is **JavaScript,** but **HTML, Java** or **Flash** based plug-ins have similar effects. While scripts may enhance and enrich online experiences (and are often necessary to use the full functionality of a website) they can also be malicious. A **malicious script** can compromise your computer's performance and overall functionality by redirecting you to another site or loading malware onto your computer.

Security Tips

While you are generally safe from malicious scripts if you stick to trusted sites, there have been cases in which hackers installed malicious scripts onto legitimate sites. The only sure way of preventing script attacks is to control which scripts run when you visit a site.

- In *Firefox*, you may use a free add-on called *NoScript* (http://noscript.net/) which lets you select which scripts to run when you visit a site: you can select the minimum necessary to get the functionality you need.
- There are similar add-ons available for *Chrome*, which also allows you to block scripts by default by selecting **Options**, then **Under the Hood**, then **Content settings** and click **Manage JavaScript blocking**.
- In *Internet Explorer*, click **Tools,** then **Internet Options**, then **Security** and then **Internet.** Click **Custom Level** and set levels to "Prompt" wherever possible. Some antivirus software such as *Norton AntiVirus* also let you select which scripts to run.

vi. Internet-Connected Devices

An increasing number of electronic devices, from fitness trackers to cars to children's toys, are now connected via Wi-Fi in what's often called the "Internet of Things." One research firm estimates that there will be 26 billion connected devices by 2020. [13] Unfortunately, many of these devices are vulnerable in several ways:

- Many of them have poor security, which can allow hackers to infect them with malware, spy on them, or take control of them entirely.
- Because they typically connect through your Internet router, malware from an infected device can easily spread to other devices that use the same network.
- Because they often are designed to work with your online accounts, an infected device can also give hackers access to those (such as your email or social network accounts.)
- Even if the devices aren't compromised, many collect kinds of data that you may not be comfortable with – particularly ones such as fitness trackers that collect health information.

Security Tips

- Be cautious before buying an Internet-connected device: Security experts say that a majority of "smart" devices on the market today are not highly resilient to cyberattacks. [14] Be particularly wary of "cloud-based" tools that can only work when connected to the Internet. Do some research on the product you're considering buying to see if there have been any reports of security problems.
- Check the privacy policy: Make sure you have a clear idea of what happens to the data that the device collects, and what other data it can access by connecting to your online accounts or to other connected devices.
- Set a password: Make sure that every connected device in your home is protected by a unique password. Most connected devices allow you to set a PIN or password, but many don't prompt you to change it from the factory default.
- Use a guest network: Create a "guest" network on your Wi-Fi router and have your connected devices connect to that one, rather than your regular network. That way if they get compromised, they won't be able to access the devices that use your main network (like your computer.)
- Check for firmware updates: Like browsers and computer operating systems, makers of connected devices frequently release "patches" and updates to address new security issues they've discovered. Security experts suggest treating connected devices like smoke alarms, setting a date twice a year to make sure that everything is up-to-date.

Security Measures

Authentication

Every client computer should require a user to log in before using it. Whether the credentials are local to the computer or stored on an authentication server, nobody should be able to use a computer without logging in first. This stops everyone who is not an authorized user on the computer or the network from using a client machine for mischievous purposes.

Anti-malware Software

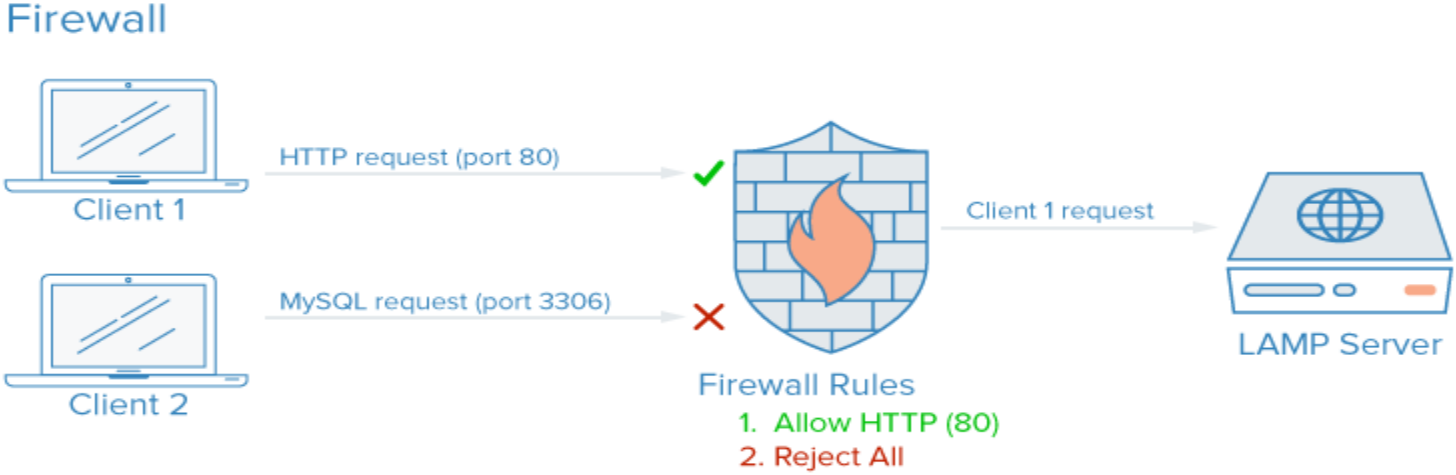
The richness of malware in the form of viruses, worms, Trojan horses and more requires the use of anti-malware software on every client machine. If one machine becomes infected, all machines on the network will become infected. Viruses and worms spread extremely fast, and it only takes a few minutes to infect every machine on the network, even if there are thousands of them. Large companies should deploy enterprise versions of an anti-malware product on all its client computers. Samller companies of a hundred computers or less may decide to deploy one of the many free offerings available, but should use the same software on all client computers.

Secure Protocols

Where possible, users of client computers should only connect with other computers and servers using secure protocols. One of these is HTTPS, or Secure HTTP, which creates a secure connection to Web sites. Another is Secure FTP, or file transfer protocol, which encrypts user ID and password information, unlike native FTP.

Firewall

The last line of defense for a client computer is a personal firewall installed on the machine. While an Internet firewall at the organization's Internet connection is the first line of defense, the personal firewall protects the client from attacks that get through, as well as attacks that originate from within the corporate network. *Both Windows and most Linux distributions have a client firewall included, and Windows' firewall is preconfigured for default protection.*



On a typical server, a number services may be running by default. These can be categorized into the following groups:

- Public services that can be accesses by anyone on the internet, often anonymously. A good example of this is a web server that might allow access to your site.
- Private services that should only be accessed by a selected group of authorized accounts or from certain locations. An example of this may be a database control panel.
- Internal services that should be accessible only from within the server itself, without exposing the service to the outside world. For example, this may be a database that only accepts local connections.

Firewalls can ensure that access to your software is restricted according to the categories above. Public services can be left open and available to everyone and private services can be restricted based on different criteria. Internal services can be made completely inaccessible to the outside world. For ports that are not being used, access is blocked entirely in most configurations.

Data encoding and encryption

One of steps necessary to protect the data is data encryption. Encryption is the process of transforming the data into some sequence of bytes using one of encryption algorithms. The primary goal of encryption is to hide the data from being visible and accessible without having the key. Very often protection of data is performed by making the algorithm, used to transform the data, unknown. In other words the author of such "protection" thinks that if the algorithm is not known, the data is properly protected. This is not encryption, but encoding. Revealing the algorithm makes such "encryption" defeated easily. And the algorithm can be discovered from the software that uses such encoded data. Sometimes it is possible to discover the data without even knowing the algorithm details.

Encryption is what is done with encryption algorithms. Those algorithms are well known and have been carefully analyzed by cryptography specialists and mathematicians. The strength of such algorithms is tested and proved again and again. The only secret part in encryption is the key, used to encrypt and/or decrypt the data.

The level of protection is determined not only by algorithm itself, but also in the way how the algorithm is applied. Internet security protocols, for example, take special care about how the keys are created and used.

Anti-Virus Software, and Anti-Spyware

Firewalls and anti-virus software offer the simplest examples of endpoint security software. Personal or desktop firewalls are software applications that protect single computers that are connected to the Internet. The connections are usually DSL or cable modem. Since these connections are always open and use static IP addresses, they are easy for intruders or hackers to break into. Firewalls work at the device level or link layer. This is between the physical machine and the transaction layer. It is the lowest level of Internet protocol, responsible for the physical connections between computers. It translates requests and responses into packets, decoding incoming packets by providing address and channel decoding. By acting on this level, firewalls control Internet connections, filter incoming and outgoing network traffic, and alert users to suspected intrusions.

Some of the top firewall products of 2007 are ZoneAlarm Pro, Outpost Firewall Pro, and Norton Personal Firewall. Anti-virus software is another example of simple endpoint security. It is a class of program that searches disk drives and other memory devices for computer viruses. The top anti-virus software applications for 2007 are BitDefender, Kaspersky, and F-Secure Anti-Virus.

Endpoint security is evolving to include other essentials such as the detection and prevention of intruders gaining access to a network, database, or workstation. Anti-spyware software is also increasing in popularity. Anti-spyware protects against programs that collect data on individuals or organizations without their knowledge for unknown uses. They can be secretly installed on computer through a new program or a virus. Some of the top anti-spyware products of 2007 include SpySweeper, CounterSpy, and Trend Micro Anti-Spyware

9.2.3 Network security

Security is often thought of only in terms of protecting software. However, any security plan should be implicated hierarchically at every level. Servers must be located in secure, access-controlled environments. Only authorized personnel should be allowed to supervise and administer it.

Essentially, server security is the controlling of access to the database server itself. The server must be attached to a stable power supply that provides backup up power if the there's a problem with the supply. This enables the server to shut down in a way that protects data and causes the least amount of damage. They should comply with business standards in password policy to protect database access.

Encryption also protects data through advanced DES (Data Encryption Standard) mechanisms or cryptograms. The degree of encryption depends on government standards. Database servers should not be visible to the world. (Web servers, however, are and require specific security measurements, since they support anonymous connections.)

For security and performance issues, the database backend should never be on the same machine as the web server with its open connections. To secure the database, the server should be configured to accept only trusted IP addresses. If the database is a backend for a web server, the IP address of the web server should be the only address that can access the database server. Another security gap in servers emerges from increasingly dynamic applications that allow on-line upgrades and can infiltrate the database server.

Networks are vulnerable to intruders who 'sniff' or eavesdrop on networks that can contain sensitive company information, passwords, and other potential company weaknesses. Secure networks should conform to four principles that form a 'trusted computing base' (TCB). These are:

1) identification and authorization,
2) discretionary control

3) audit, and
4) object re-use.

Identification determines the user's identity. The user is then authenticated through a password or the completion of a registration form or some other access-controlling barrier. Authentication also ensures the identity stays consistent across time. Authorization defines what the user is allowed to do, what processes users have access to. Discretionary access control (DAC) is a security system that gives users, processes, and devices specified permissions to gain access to system resources in clearly defined ways.

Audits are systematic evaluations of the security of a company's information systems. Audits examine the most secure physical configuration of hardware and software connections, how information is handled, and user practices. Object reuse takes a storage medium that contains one or more objects. It protects network security by ensuring that all residual data from previous objects is removed before the storage can be re-assigned.

Fundamentals of Network security,

- Principal methods of protecting Network (Encryption, Decryption, Encryption in network),
- Network organization (Firewalls and proxies, Analysis of the network infrastructure),
- DMZ,
- Types of Firewalls(Packet Filtering, State-full Packet Filtering Circuit Level Gateway, Application level/proxy),
- IPSec,
- VPN.

IPsec (Internet Protocol Security)

IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication.

IPsec provides two choices of security service:

- Authentication Header (AH), which essentially allows authentication of the sender of data, and
- Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

IPSec helps provide defense-in-depth against:

- Network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Administrative control of servers, other computers, and the network.

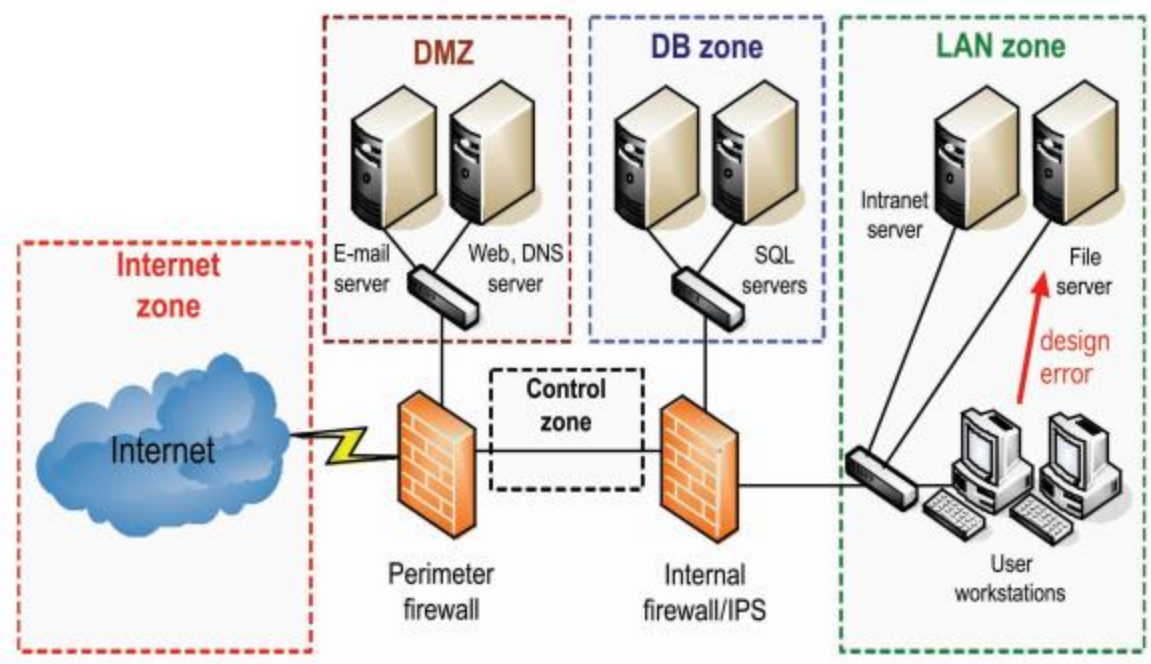
DMZ

DMZ is short for ***dem****ilitarized* ***z****one*, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Internal network is always preserved with the help of firewall and if external clients want to access internal resources, they can do that via DMZ since we can publish internal servers in DMZ so that external clients can access the internal resources such as servers and firewall admins can sleep in peace for just a few minutes

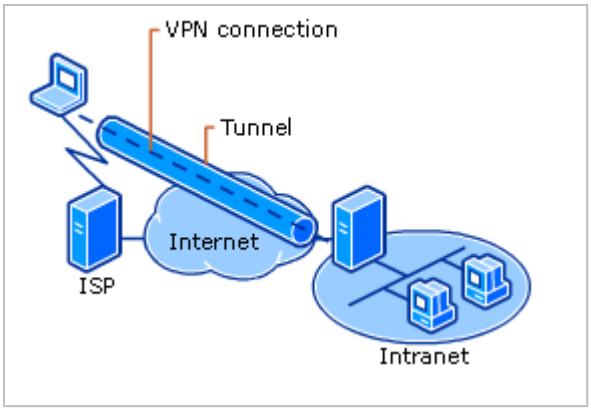
- Provide a dedicated subnet for publicly accessible machines so that if they get compromised, the rest of your inside network remains safe.
- Provides an administrative control point so that all machines entering the DMZ must meet a certain high security standard and be audited frequently.



VPNs and Private Networking

Private networks are networks that are only available to certain servers or users. For instance, in Digital Ocean, private networking is available in some regions as a data-center wide network.

A VPN, or virtual private network, is a way to create secure connections between remote computers and present the connection as if it were a local private network. This provides a way to configure your services as if they were on a private network and connect remote servers over secure connections.



How Do They Enhance Security?

Utilizing private instead of public networking for internal communication is almost always preferable given the choice between the two. However, since other users within the data center are able to access the same network, you still must implement additional measures to secure communication between your servers.

Using a VPN is, effectively, a way to map out a private network that only your servers can see. Communication will be fully private and secure. Other applications can be configured to pass their traffic over the virtual interface that the VPN software exposes. *This way, only services that are meant to be consumable by clients on the public internet, need to be exposed on the public network.*

Service Auditing

Up until now, we have discussed some technology that you can implement to improve your security. However, a big portion of security is analyzing your systems, understanding the available attack surfaces, and locking down the components as best as you can.

Service auditing is a process of discovering what services are running on the servers in your infrastructure. Often, the default operating system is configured to run certain services at boot. Installing additional software can sometimes pull in dependencies that are also auto-started.

Service auditing is a way of knowing what services are running on your system, which ports they are using for communication, and what protocols are accepted. This information can help you configure your firewall settings.

How Does It Enhance Security?

Servers start many processes for internal purposes and to handle external clients. Each of these represents an expanded attack surface for malicious users. The more services that you have running, the greater chance there is of a vulnerability existing in your accessible software.

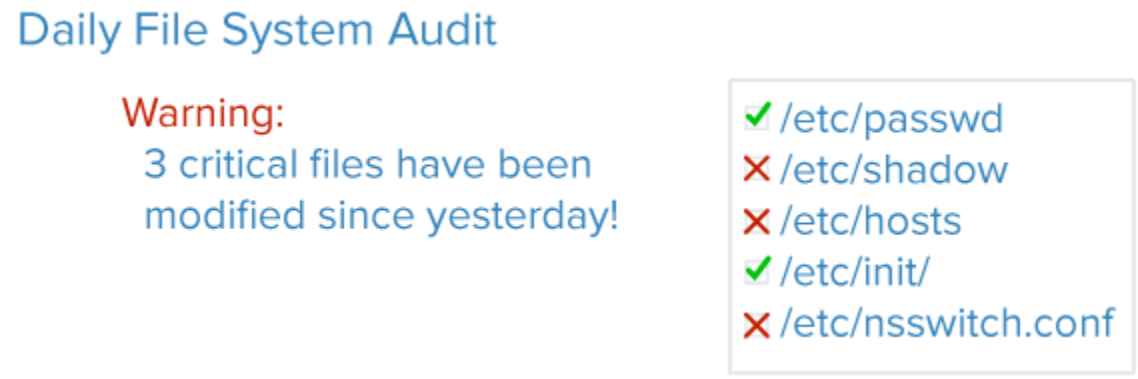
Once you have a good idea of what network services are running on your machine, you can begin to analyze these services. Some questions that you will want to ask yourself for each one are:

- Should this service be running?
- Is the service running on interfaces that it doesn't needs to? Should it be bound to a single IP?
- Are your firewall rules structured to allow legitimate traffic pass to this service?
- Are your firewall rules blocking traffic that is not legitimate?
- Do you have a method of receiving security alerts about vulnerabilities for each of these services?

This type of service audit should be standard practice when configuring any new server in your infrastructure.

File Auditing and Intrusion Detection Systems

File auditing is the process of comparing the current system against a record of the files and file characteristics of your system when it is a known-good state. This is used to detect changes to the system that may have been authorized.



An intrusion detection system, or IDS, is a piece of software that monitors a system or network for unauthorized activity. Many host-based IDS implementations use file auditing as a method of checking whether the system has changed.

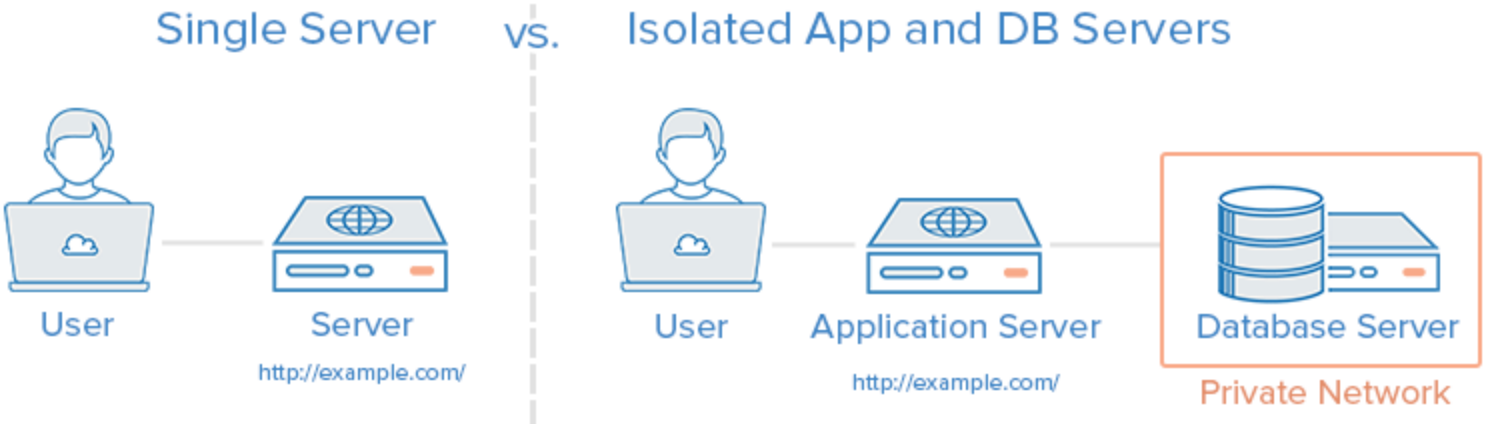
How Do They Enhance Security?

Similar to the above service-level auditing, if you are serious about ensuring a secure system, it is very useful to be able to perform file-level audits of your system. This can be done periodically by the administrator or as part of an automated processes in an IDS.

These strategies are some of the only ways to be absolutely sure that your filesystem has not been altered by some user or process. For many reasons, intruders often wish to remain hidden so that they can continue to exploit the server for an extended period of time. They might replace binaries with compromised versions. Doing an audit of the filesystem will tell you if any of the files have been altered, allowing you to be confident in the integrity of your server environment.

Isolated Execution Environments

Isolating execution environments refers to any method in which individual components are run within their own dedicated space.



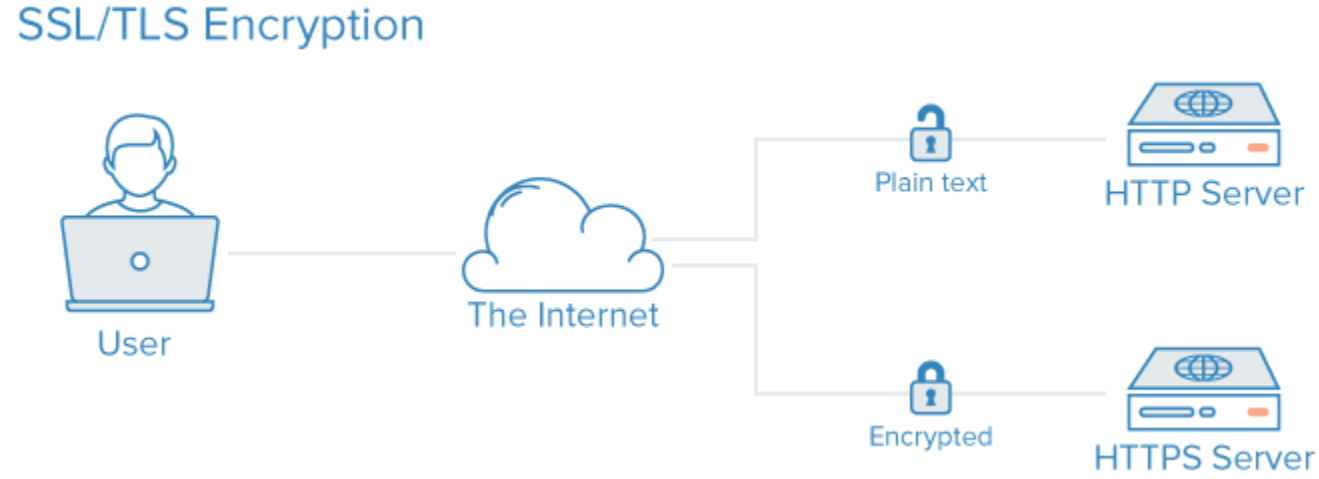
This can mean separating out your discrete application components to their own servers or may refer to configuring your services to operate in chroot environments or containers. The level of isolation depends heavily on your application's requirements and the realities of your infrastructure.

How Do They Enhance Security?

Isolating your processes into individual execution environments increases your ability to isolate any security problems that may arise. Similar to how bulkheads and compartments can help contain hull breaches in ships, separating your individual components can limit the access that an intruder has to other pieces of your infrastructure.

Public Key Infrastructure and SSL/TLS Encryption

Public key infrastructure, or PKI, refers to a system that is designed to create, manage, and validate certificates for identifying individuals and encrypting communication. SSL or TLS certificates can be used to authenticate different entities to one another. After authentication, they can also be used to established encrypted communication.



How Do They Enhance Security?

Establishing a certificate authority and managing certificates for your servers allows each entity within your infrastructure to validate the other members identity and encrypt their traffic. This can prevent man-in-the-middle attacks where an attacker imitates a server in your infrastructure to intercept traffic.

Each server can be configured to trust a centralized certificate authority. Afterwards, any certificate that the authority signs can be implicitly trusted. If the applications and protocols you are using to communicate support TLS/SSL encryption, this is a way of encrypting your system without the overhead of a VPN tunnel (which also often uses SSL internally).