Sn	Details	Pg
1.	SOCIAL ENGINEERING	2
2.	DIFFERENT TYPES OF SOCIAL ENGINEERING	4
3.	DEFENDING AGAINST SOCIAL ENGINEERING	6
4.	Information Security Awareness for Family	12
5.	CYBER SECURITY TECHNIQUES	21
	Windows Firewall	27

SOCIAL ENGINEERING

Social engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software present. It‘s the hardest form of attack to defend against because hardware and software alone won‘t stop it. It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system- the human being.

Social Engineering Attack Cycle

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. A broad view of social engineering attack life cycle has such phases:

research,
developing rapport and trust,
exploiting trust
utilizing information,
cloak activities,
evolve/regress.

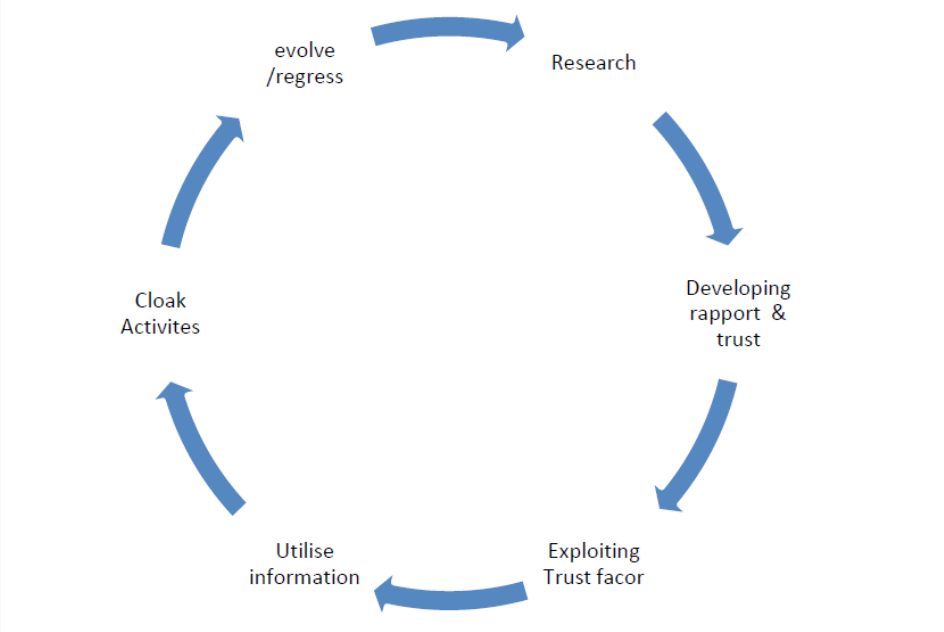


Figure 1: Social Engineering Attack Cycle

1. **Research:** It is an information gathering process where information about the target is retrieved. The attacker gathers as much information as possible about the target before starting the attack. Some methods are obvious and require no great cunning or planning,

while others require certain skill or knowledge. If industrial espionage is the aim, the attacker learns everything about the victim/ organisations with the help of all available resources, social networking sites etc. Typical information that may be gathered could be an internal phone directory, birth dates, organisational charts, personnel records, social activities, relationships, etc.

2. **Developing Rapport and Trust:** The social engineer capitalises on the psychological aspect of trust. The target is more likely to divulge requested information to an attacker if he trusts the attacker. Rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favors or gaining information through seemingly innocent conversations.
3. **Exploiting Trust Factor:** When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.
4. **Utilise & Execute:** The outcome of the previous phase is utilised to reach the goal of the attack or to move on to further steps which may be required to reach the goal. The execute-step is where the attacker does something that is clearly illegal or not allowed, for instance when the target is asked to submit his log-in information, or when the nefarious e-mails are sent.
5. **Recruit & Cloak:** Cloak is the actions performed after the execution, actions performed in order to hide the illegal activities. It can be to continue with the ―friendship‖ to normalize the actions, moves to make the victim seem untrustworthy, or more advanced techniques to hide the crime. In some cases the victim can be recruited to either work for the attacker or as an ambassador/reference for the attacker.
6. **Evolve/Regress:** This is where the attacker learns from the process and creates an internal justification for what has happened. There are basically two choices for the attacker here. Either the attack evolves, moving into another phase of the attack if the process has been successful up to this step. The other choice if the results to this point have been unsuccessful is to regresses, which can either be to stop the attack or to move to a more basic level of attack in order to be successful again. The gathered information can then be used to target and explore more deeper into the victim , until finally attackers convince their targets to divulge the information they need to achieve the goal.

DIFFERENT TYPES OF SOCIAL ENGINEERING

There are many types of social engineering attacks, but they can be broadly split into three categories:

- Physical social engineering,
- Remote social engineering
- Hybrid social engineering

In physical social engineering, the attacker attempts to gain physical access to a sensitive office or location, and in remote social engineering the attacker attempts to gain access to information or resources remotely, for example, over the phone or via email

Physical Social Engineering

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including :

- Piggybacking: Used to enter restricted area by convincing an authorised personal.
- Eavesdropping: Attacker can gain information by hearing a discussion between two people, or by reading emails and listening to telephonic conversation.
- Impersonation: The attacker acts like someone else to trap the victim
- Dumpster Driving: Valuable information can often be found on trash, printers and pieces of paper.
- Reverse Social Engineering: It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the attacker appears to be in a position of authority to ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre-attack research and planning, however if executed well it is more successful in attaining gaining quality information.

Remote Social Engineering

Remote social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging. This uses items planted to lure employees to run payloads.

Computer-based Social Engineering

Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.

Social Engineering by Email

Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the

email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

Phishing

Phishing emails typically take the form of fake notifications purporting to be from a well known organization (often banks, payment systems, Software vendors for possible upadate), asking for the recipient‘s personal information including user credentials, credit card numbers, or banking information. Some examples are an email looking like it's from your bank asking you to verify details or a phone call pretending to be from a company that you trust (including your own company) requesting you to divulge confidential information like a pin number.

Social Engineering by Phone

The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner, or applying pressure. The caller may purport to be from tech support or an anti-virus organization, a financial institution, or even a charity. In many business cultures, challenging someone‘s identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.

Mumble Attack

Mumble attacks are telephonic social engineering attacks targeted at call centre agents. The social engineer poses as a speech-impaired customer or as a person calling on behalf of the speech-impaired customer. Victims of the attack are often made to feel awkward or embarrassed and release information as a result.

Detailed description of the tool is out of the scope and the reader may refer to http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/ for further information.

Adopted from: http://www.infosecbuzz.com/social-engineering-attacks/
http://thewetwaregroup.blogspot.ca/p/other-methods.html

Defending Against Social Engineering

Successful social engineering attacks rely on the employees of an organization. To avoid such an attacks, employees must be well trained and familiar about common social engineering techniques, inform them about the value of information, train them to safeguard it. It is also important for organizations to establish a clear and strong security policy, including standards, processes and procedures to help eliminate the threat of social engineering. Aaron Dolan (2004) SANS(https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365) defines a good social engineering defense should include but not be limited to:

- Security awareness training
- Password policies
- Data classification
- Acceptable use policy
- Background checks
- Termination process
- Incident response
- Physical security

Continuous Security awareness training for employees

Organizational policies, procedures and standards must be taught and reinforced to the employees during orientation and during the employment on a regular basis. Security awareness events and activities, such as talks, awareness weeks, presentations, seminars, quizzes, and competitions, dedicated web-presence(an internal webpage , twitter handles, etc.) maintains the mainstream security current trends and issues and educate about the social engineering best practices. Points which should be highlighted in the employees training are:

- Data classification policy: This should describe what information is considered to be sensitive or confidential, how it should be marked, how it should be handled, and who it can be released to, as well as how to dispose of it. Example data classification levels might include the following:
  - Top Secret: Highly sensitive internal documents e.g. pending mergers or acquisitions, investment strategies, plans or designs, that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
  - Confidential: Data in this category may require certain levels of protection by law, for example, personally identifiable information, health information, certain employee data, certain business and financial data.
  - Restricted: Data in this category should only be accessible to certain roles or functions. For instance, it may be restricted to certain departments, such as employee information being restricted to the HR department or systems data being restricted to the IT department.
  - Internal Use Only: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but

where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

- Public: There is no expectation of privacy or confidentiality for data in this category. It could include public website information, press releases, and so on. Each category should include requirements for protection; describe how the data should be stored, who can access the data, and how it should be disposed of. Take every type of data that your organization processes, including customer data, user data, and supplier data, and assign it to one of your defined categories. All staff should know how to handle and protect each category of information

- Waste management This should include secure disposal of documents, electronic media, and so on, and should cover external as well as internal waste. Invest in shredders and have one on every floor: Your staff must fully understand the implications of throwing waste paper or electronic media in a bin. After this waste moves outside your building, its ownership can become a matter of legal obscurity.
- Acceptable use policy This should describe what is considered acceptable use of computer systems and equipment within the organization. It should cover system accounts, network use, electronics communications, use of non-company hardware or software, as well as monitoring of the same. d. Network access policy: This should cover wired and wireless network access, including IP telephony and mobile devices; it should describe who can access the network, how and from where, public access, guest access, and what is and is not permitted on the corporate network.
- Remote access policy: This should document remote access requirements, who can connect, requirements for connecting, termination of access, and so on.
- Physical security policy This should cover the various aspects of physical security, including visitor procedures and physical access logs.
- Electronic communication policy: This should describe how to handle email attachments, hyperlinks in documents, requests for information from both within and outside the organization, what instant messaging services staff are permitted to use, if any. Some policies may include examples of phishing attacks to help users to identify phishing attacks that they themselves receive.
- Checking in and checking out Visitors should be required to check-in and check-out in a dedicated area, usually the reception area. The process typically involves signing a visitors/contractors book and contacting the person that the visitor is meeting so he or she can escort them into the building. •Physical Security Policy: Visitors: Your physical security policy should, at a minimum, consider the following areas regarding visitors:
  - Identifying visitors Visitors should be required to present some kind of identification.
  - Escorting visitors Visitors should always be escorted by an existing staff member (not by another visitor or contractor) into the organization.
  - Visitor passes Are visitors required to wear visitor passes? If so, they should be required to return their visitor passes upon checking out. Some more security-focused organizations use different colored passes for different areas or different days of the week. Visitor passes should, at least, be dated. Employees should be encouraged to

challenge anyone not wearing an ID badge or a visitor pass. Visitor passes should be returned on leaving the building. Follow up on passes that have not been returned.

- Accessing the network Can visitors access the computer network, and, if so, where from and how? Can they connect their own devices to the network?

- Password Policies and Standards: For a social engineer, gaining access to a system can mean the difference between a successful or failed attack. A policy should exist for the delivery and creation of passwords. There must exist good and written password policy such as Not sharing passwords when asked(over phone also)

Information Security Awareness for Family

Internet has become a necessary tool for the Family. Home computers or Mobiles are often shared with every member of the family, including children and teenagers. The Internet can connect you and your family to all types of resources. Using computer with internet, you and your family can read the latest news, look up for information, do online shopping, do online booking of household items, listen to music, play games, buy things, or e-mail friends. The possibilities for learning and exploring on the Internet are endless. However, not all information and resources are safe and reliable.

How to make sure you and your family's experience on the Internet is safe, educational, and fun Both online shopping and the downloading of software or files need to be discussed with all members or supervised by adults to make sure your personal and financial information remains safe and secure.

The very nature of the Internet helps to connect to people and resources which have some risk of people intruding into your system. There are also other types of threats, such as companies that track what you do on the Internet. While there is no guarantee that you will be safe on internet, but there are many things you can do to protect yourself and family members while using the Internet. The Internet can be a helpful source of information and advice, but you and your family members can't trust everything you read. Anyone can put any information on the Internet, and not all of it is reliable. Some people and organizations may take the necessary steps and take care about the accuracy of the information what they post. In parallel, some may give false information intentionally.

When you and your family surf the Web it's important to keep the following in mind:

- Online information is usually not private.
- People online are not always who they say they are.
- Anyone can put information online.
- You can't trust everything you read online.
- You and your family may unexpectedly and unintentionally find material on the Web that is offensive, pornographic (including child pornography), obscene, violent, or racist.

Step 1 : Secure your home Wi-Fi network.

Step 2 : Consider Common Place for Computer to Children and Family

Step 3 : Set Family Rules for Accessing Internet

Step 4 : Understand the need and set boundaries for online safety

Step 5 : Sign for Agreement and Online pledge among family members for appropriate online behavior

Step 6 : Secure Your Computer

Step 7 : Keep your software up to date

Step 8 : Install Antivirus, Desktop Firewall solutions against malware and unauthorized access

Step 9 : Back up your system

Step 10 : Use separate standard user accounts for family members

Step 11 : Create strong and easy remember passwords for your accounts.

Step 12 : Secure your web browser before accessing Internet

Step 13 : Be careful online and don't click suspicious links

Step 14 : Ensure safe browsing for everyone, even for grand parents!

Step 15 : Download and install software from trusted sources only.

References:

https://infosecawareness.in/family/

CYBER SECURITY TECHNIQUES

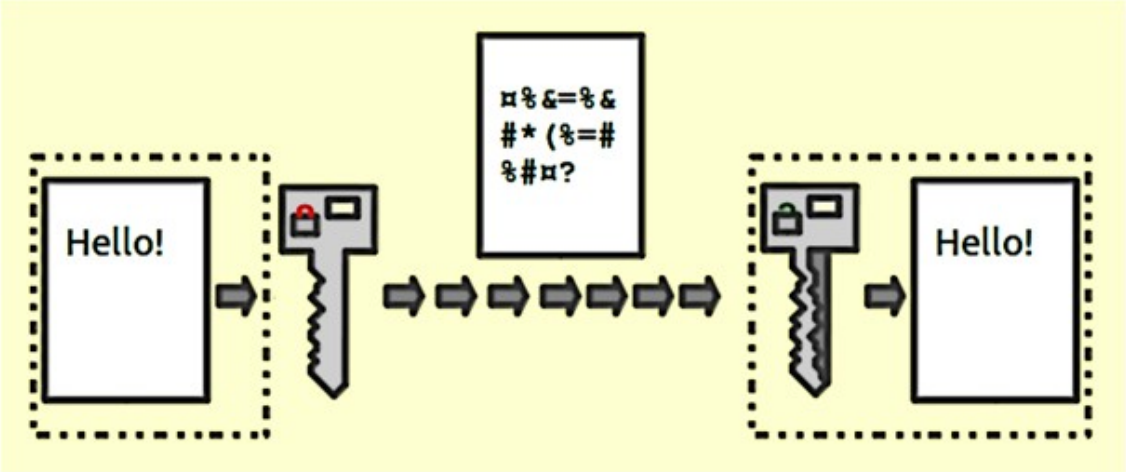
There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.



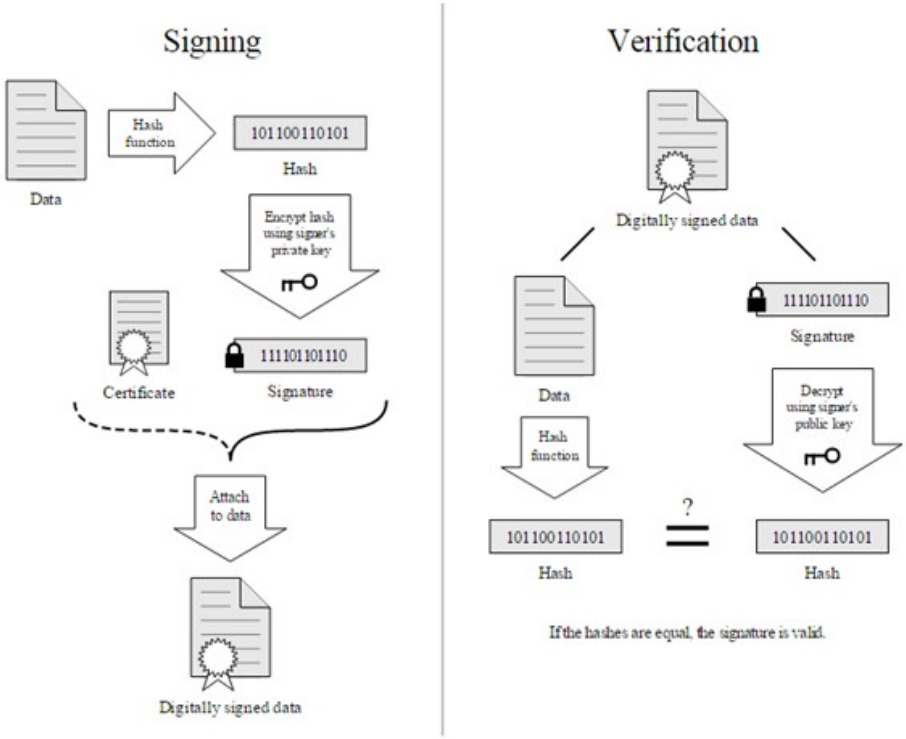
Encryption

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security

of key while transmission is itself an issue. E , is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse's two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B's public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.
As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.



Digital signature

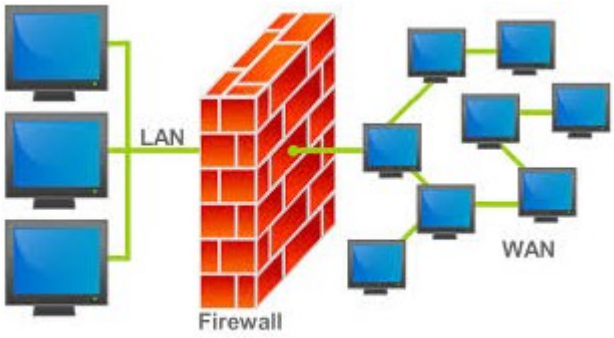
ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

Different antivirus available on the market

FIREWALL

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.



Firewall

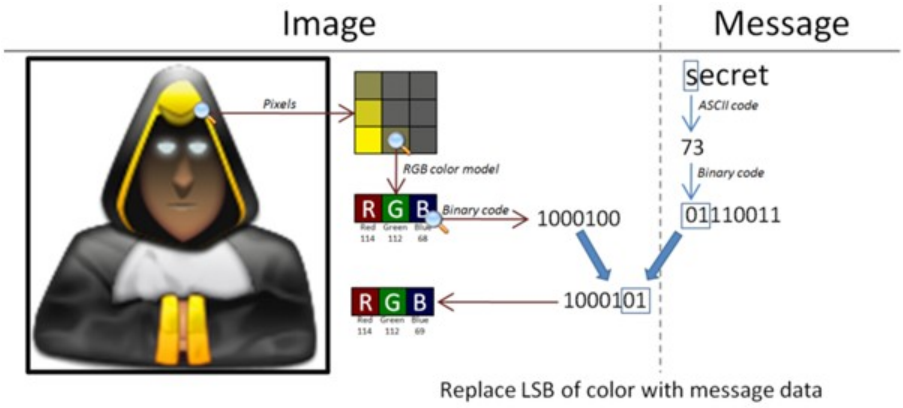
There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations' network.
- In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow "rules" and "policies" and based on these defined rules the firewalls can follow the following filtering mechanisms.
  - Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
  - Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.

- Stateful Inspection: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.
- The firewalls are an essential component of the organizations' network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

STEGANOGRAPHY

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.



Steganography

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

Let us discuss how the data is secretly embedded inside the cover file(the medium like image, video, audio, etc which is used for embed secret data) without being noticed. Let us take an example of an image file which is used as a cover medium. Each pixel of a high resolution image is represented by 3 bytes(24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embedded the data into it, will have unnoticible change in the image quality and only a very experienced and trained eyes can detect this change. In this way, every pixel can be used to hide 3 bits of information.

Similarly, introducing a white noise in an audio file at regular or randon interval can be used to hide data in an audio or video files. There are various free softwares available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

Windows Firewall

What is the Windows Firewall and how to turn it on or off?

Windows Firewall

The Windows Firewall is a silent tool that keeps our systems safe from all kinds of network threats and has been included in each version of Windows for the last decade. Because it is a silent ally, doing most of its work in the background, few users interact with it on a regular basis, and even fewer know what this tool is and how it works. That's why, in this article, we will

explain what the Windows Firewall is, what it does, how to find it and how to enable it or disable it, depending on whether you want to use it or not. Let's get started:

What is the Windows Firewall?

The Windows Firewall is a security application created by Microsoft and built into Windows, designed to filter network data transmissions to and from your Windows system and block harmful communications and/or the programs that are initiating them. Windows Firewall was first included in Windows XP (back in 2001), and since then it has been improved in each new version of Windows. Before 2004 it used to be named Internet Connection Firewall and, at that time, it was a rather basic and buggy firewall with lots of compatibility issues. Windows XP Service Pack 2 changed its name to Windows Firewall and introduced and improved core capabilities such as that of filtering and blocking incoming connections.

What does the Windows Firewall do for you?

Windows Firewall can provide your computer or device with protection against attacks from your local network or the internet, while still giving you access to the network and the internet. Because Windows Firewall filters the traffic that goes on your computer, it can also stop types of malicious software that use network traffic to spread themselves, like Trojan horse attacks and worms. Another useful capability is that it can filter both outgoing and incoming connections to your Windows computer and block those which are unwanted. The firewall uses a predefined set of rules for both types of network traffic, but its rules can be edited and changed both by the user and the software that the user installs.

Configuring Firewall on MAC system

How to Configure Your Mac's Firewall

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.

A firewall can help prevent *bad packets* from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

Turning on and Configuring the Mac OS X Firewall

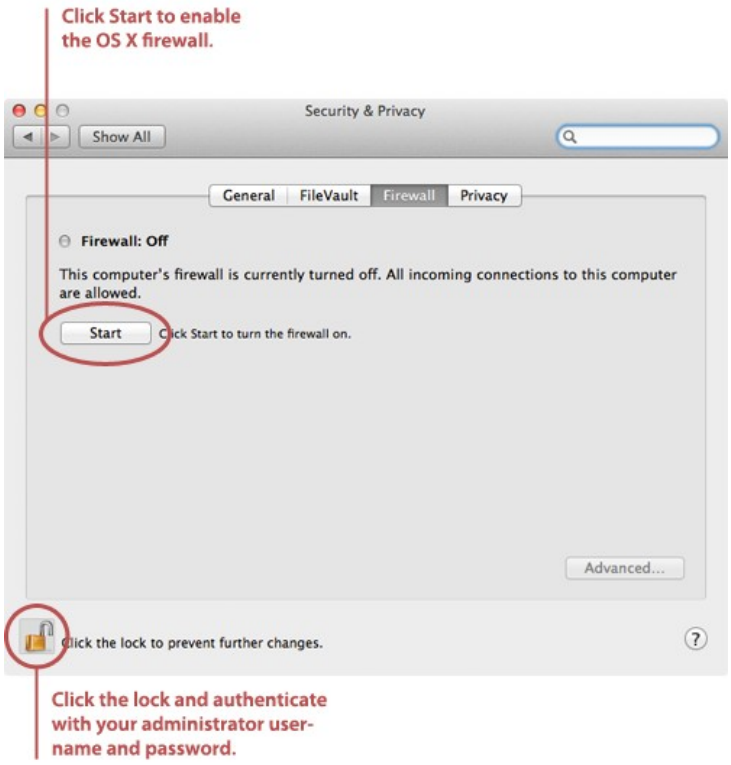
Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select **System Preferences**. The window shown below appears.

2. Select **Security & Privacy**.

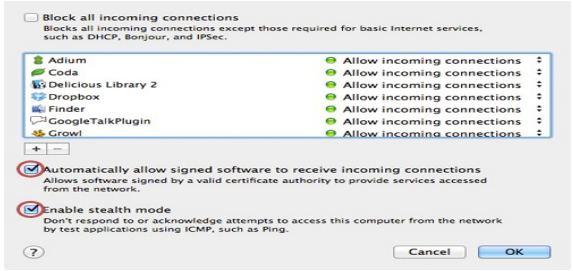
3. Click the **Firewall** tab.

4. Click the lock icon and authenticate with your administrator username and password. The window shown below appears.



5. Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message, as shown below.

6. Click **Advanced**. The window shown below appears.



7. Select the **Automatically allow signed software to receive incoming connections** checkbox. This allows the applications on your Mac to communicate with the

outside world.

8. Select the **Enable stealth mode** checkbox. This prevents your Mac from responding to port scans and ping requests.

9. Click **OK** to close the Advanced settings.

10. Close System Preferences. Your Mac is now protected by the built-in firewall!
