Savitribai Phule Pune University

Centre for Information and Network Security

Course: Introduction to Cyber Security / Information Security

Module 1: Pre-requisites in Information and Network Security

Chapter 2: Information Security Overview: Background and Current Scenario

Types of Attack

Phishing:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Phishing takes advantage of the trust that the user may not be able to tell that the site being visited, or program being used, is not real; therefore, when this occurs, the hacker has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes, and credit card numbers, among other things.

Example: *Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are the common tricks used by phishers. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to yourbank website; actually this URL points to a phishing site which looks as your original bank website. The user is then asked for his credentials by phishing website to gain sensitive information.*

Spoofing:

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.

Example: *Hackers will use spoofing mechanism to avoid getting tracked by routers while making an attack.*

Impersonation

It is an act of pretending to be another person for the purpose of fraud. It can be done via any communication mechanism like phone, email etc.

Example: *An Impersonator calling victim and claims that he is calling from the bank where victim has account. He will ask for account details, passwords etc. in claiming that he is asking for the information for verification. In reality he will use the information to make fraudulent transactions.*

Dumpster Diving

In the computer world, dumpster diving refers to using various methods to get information about a technology user. In general, dumpster diving involves searching through trash or garbage looking for something useful. This is often done to uncover useful information that may help an individual get access to a particular network. So, while the term can literally refer to looking through trash, it is used more often in the context of any method (especially physical methods) by which a hacker might look for information about a computer network.

Goals for Security

The following are the key security goals

- Integrity - Making sure that the behavior of the system under test cannot be changed maliciously
- Confidentiality - Making sure that the system does not leak sensitive information and does not allow illegitimate users to access the system
- Non-repudiation - Ability of the system to be able to "prove" that certain actions actually happened
- Availability - Making sure that the system continues to remain available in the face of attacks
- Access Control - Users should not be allowed to perform actions beyond their permitted role

E-Commerce Security

Ecommerce entails buying/selling of products over the internet and has gain popularity in the recent years. Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe ecommerce website:

1. Choose a secure ecommerce platform: Choose a strongly typed higher level language for the development. If open source tools/libraries are used then ensure that the frameworks does not create security holes in your application
2. Use a secure connection for online checkout--and make sure you are PCI compliant: Always use HTTPs protocol for all important transactions.
3. Don't store sensitive data: As part of the website, there is no need to store sensitive information like CVV number and other credit card information
4. Set up system alerts for suspicious activity: Build a system that alerts when an undesired event happens in the system. Multiple requests from the same IP for long periods of time can indicate malicious intent
5. Layer your security: Defense in depth is absolutely needed in ecommerce domain. Security features like multiple passwords and OTP helps in reducing the risk of hacking
6. Provide security training to employees: If the employees understand the importance of security then human error can be avoided
7. Patch your systems: New security loop holes are discovered on a daily basis. If the system is not up to date then risk of getting hacked increases exponentially
8. Make sure you have a Distributed Denial of Service (DDoS) protection and mitigation service: Have a mitigation strategy against network denial of service attack and block IPs that are sending lot of request to the system
9. Disaster recovery plan: Plan for unlikely failure of your system. In case of system failure ensure that sensitive data is not lost or corrupted by the system

Computer Forensics

Computer forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information

At a high level following are the guidelines used to process the evidence in computer forensic:

- Step 1: Shut down the computer. Considerations must be given to volatile information. Prevents remote access to machine and destruction of evidence (manual or ant-forensic software)
- Step 2: Document the Hardware Configuration of the System. Note everything about the computer configuration prior to re-locating
- Step 3: Transport the Computer System to A Secure Location. Do not leave the computer unattended unless it is locked in a secure location
- Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks
- Step 5: Mathematically Authenticate Data on All Storage Devices. Must be able to prove that you did not alter any of the evidence after the computer came into your possession
- Step 6: Document the System Date and Time
- Step 7: Make a List of Key Search Words
- Step 8: Evaluate the Windows Swap File
- Step 9: Evaluate File Slack. File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
- Step 10: Evaluate Unallocated Space (Erased Files)
- Step 11: Search Files, File Slack and Unallocated Space for Key Words
- Step 12: Document File Names, Dates and Times
- Step 13: Identify File, Program and Storage Anomalies
- Step 14: Evaluate Program Functionality
- Step 15: Document Your Findings
- Step 16: Retain Copies of Software Used

Where Computer forensic is used?

a. Criminal prosecution
b. Insurance companies
c. Law enforcement

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

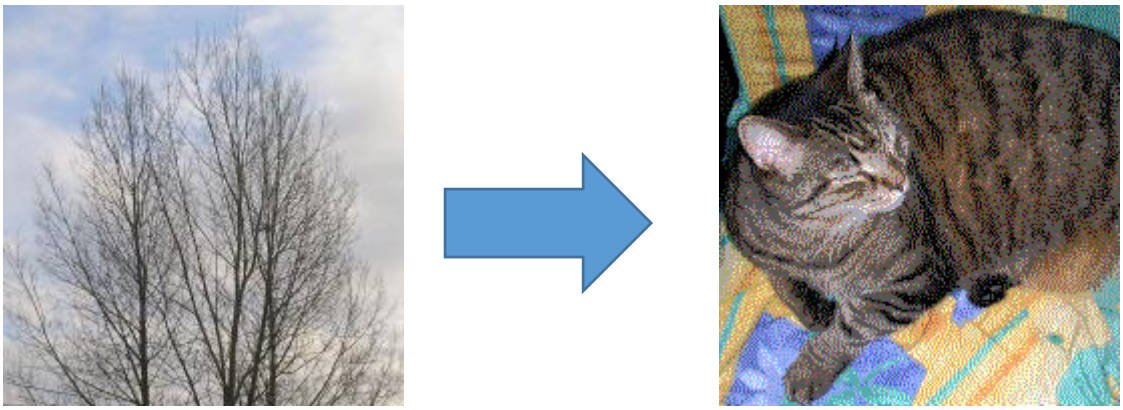
The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone,

steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Some of the earlier examples of steganography are:

- Hidden messages on messenger's body—also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and restrictions on the number and size of messages that can be encoded on one person's scalp.
- In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters in one typeface. Because of this, a message could be hidden using two (or more) different typefaces, such as normal or italic.

In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.



Source: https://en.wikipedia.org/wiki/Steganography

The above is a classic example of steganography where the left tree image is hiding the right image and the hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization.