In these notes, you will read how computer networks are vulnerable and the different system attacks that can occur.

Computer network security has reached a point at which it can be characterized by two seemingly conflicting statements: Never has network security been better than it is today, and never have computer networks been more vulnerable than they are today. This vulnerability stems from the world-wide access to computer systems via the Internet. Computer and network security comes in many forms, including encryption algorithms, access to facilities, digital signatures, and biometric authentication, such as using fingerprints and face scans as passwords.

As a result of a large number of attacks on computers and networks in recent years, many studies have been conducted to try to determine the standard methods of attacks. A form of attack comes in viruses. A computer virus is a small program that alters the way a computer operates and often does various types of damage either by deleting and corrupting data and program files or by altering operating system components so that computer operation is impaired or even halted. There are many different types of viruses, such as macro, boot sector, polymorphic, and file sector viruses.

Another form of computer virus is a worm. A worm is a program that copies itself from one system to another over a network. Worms usually propagate themselves by transferring from computer to computer via e-mail. Typically, a virus or a worm is transported as a Trojan horse. In other words, hiding inside a harmless-looking piece of code such as an email or an application macro.

Another common category of system attacks that became popular at the end of the 20th century was the denial of service attack. Denial of service attacks, or distributed denial of service attacks, bombard a computer site with so many messages that site is incapable of answering valid requests. Some common types of denial of service attacks include email bombing, smurfing, and ping storm. In email bombing, a perpetrator sends an excessive amount of unwanted email messages to someone. If these email messages have a return address of someone other than the person actually sending the email, then the sender is spoofing.

Smurfing is the name of a particularly nasty automated program that attacks a network by exploiting Internet protocol broadcast addressing and other aspects of Internet operation.

A ping storm is a condition in which the Internet ping program is used to send a flood of packets to a server to make the server inoperable.

Phishing is when hackers create emails that look like as if they are coming from a legitimate source when in reality the hackers are trying to get the users to give up ID and password information.

Pharming is another form of attack that involves tricking the user into supplying confidential information. The hacker redirects the unknowing user to bogus sites that look exactly like a legitimate company’s official website.

Two more tools that are used by hackers are rootkits and keyloggers. A rootkit is a program, or programs, that has been installed usually unknowingly in a user’s operating system. They are installed so deep within a user’s operating system that normal protection software does not even notice the rootkit virus.

A keylogger is a software system that secretly captures and records keystrokes made at a user’s keyboard.