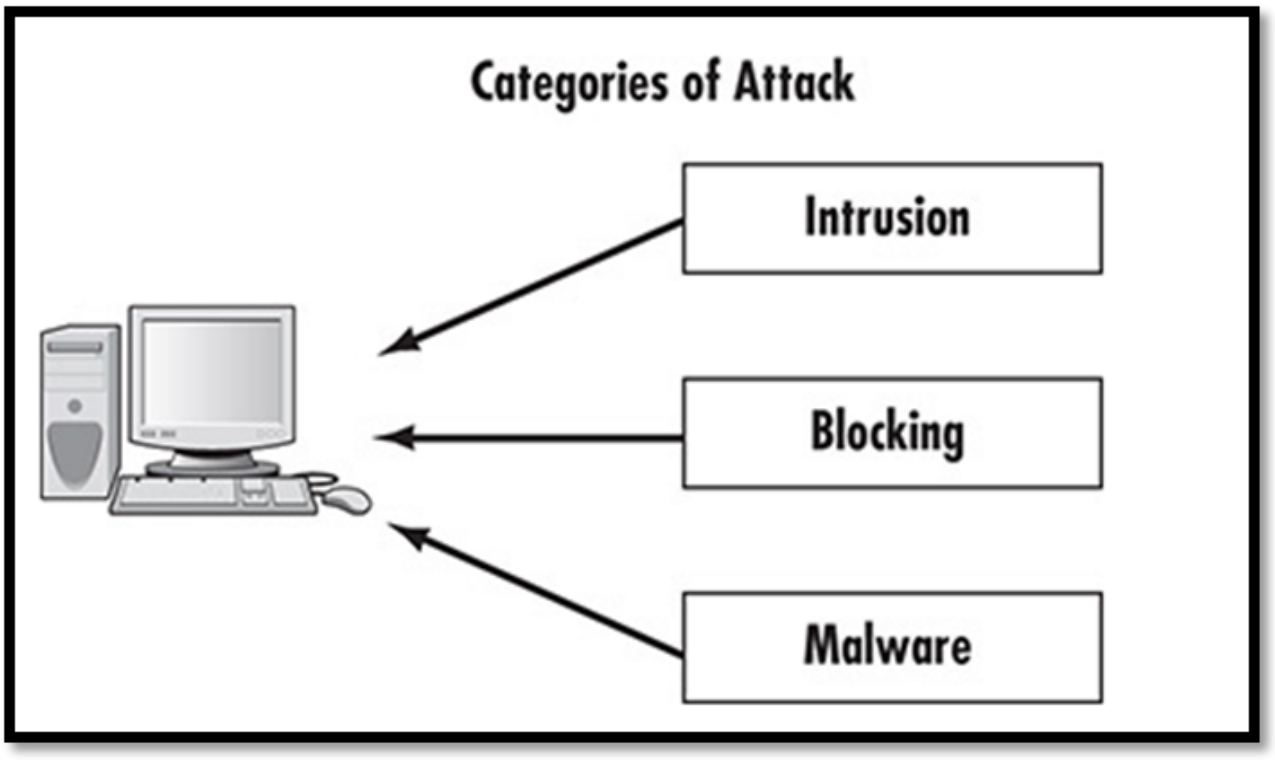
# 1.7 Threat Classification

Your network certainly faces real security threats, and these threats can manifest themselves in a variety of forms. There are different ways one might choose to classify the various threats to your system. You could choose to classify them by the damage they cause, the level of skill required to execute the attack, or perhaps even by the motivation behind the attack. For our purposes, we have categorized attacks by what they actually do. Based on this philosophy, most attacks can be categorized as one of three broad classes:

- Intrusion
- Blocking
- Malware

Figure 1-6 shows the three categories. The intrusion category includes attacks meant to breach security and gain unauthorised access to a system. This category of attacks includes any attempt to gain unauthorised access to a system. This is generally what hackers do. The second category of attack, which is blocking, includes attacks designed to prevent legitimate access to a system. Blocking attacks are often called denial of service attacks (or simply DoS). In these types of attacks, the purpose is not to actually get into your system but simply to block legitimate users from gaining access. The third category of threats is the installation of malware on a system. Malware is a generic term for software that has a malicious purpose. It includes virus attacks, Trojan horses, and spyware.




### 1.7.1 Malware

Malware is probably the most common threat to any system, including home users' systems, small networks, and large enterprise wide-area networks. Malware is designed to spread on its own, without the creator of the malware having to be directly involved. This makes the malware attack much easier to spread across the Internet, resulting into a wider spread.

The most common example of malware is the computer virus. You probably have a general idea of what a virus is. If you consult different textbooks you will probably see the definition of a virus worded slightly differently. One definition of a virus is "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." A computer virus is analogous to a biological virus in which both replicate and spread. The most common method to spread a virus is by spreading it across the victim's address book in his/her's email account. Some viruses do not actually harm the system itself, but all of them cause network slowdowns or shutdowns due to the heavy network traffic caused by the virus replication.

Another type of malware that it is closely related to the virus is the Trojan horse. The term is borrowed from the ancient tale. In this tale, the city of Troy was besieged for a long period of time, but the attackers could not gain entrance. They constructed a huge wooden horse and left it one night in front of the gates of Troy. The next morning, the residents of Troy saw the horse and assumed it was a gift, consequently rolling the wooden horse into the city. Unbeknown to them, several soldiers were hidden inside the horse. That evening, the soldiers left the horse, opened the city gates, and let their fellow attackers into the city.

An electronic Trojan horse works in the same manner, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer. In short, you have an enticing gift that you install on your computer, and later find out it has unleashed something quite different from what you expected. It is a fact that Trojan horses are more likely to be found in illegitimate software. There are many places on the Internet to get pirated copies of commercial software. Finding out that such software is actually part of a Trojan horse is not at all uncommon.

Trojan horses and viruses are the two most widely encountered forms of malware. A third category of malware is spyware, which is increasing at a dramatic pace. Spyware is software that literally spies on what you do on your computer. This can be as simple as a cookie, a text file that your browser creates and stores on your hard drive.

Cookies are downloaded onto your machine by websites you visit. This text file is then used to recognise you when you return to the same site. That file can enable you to access pages more quickly and save you from having to enter your information multiple times on pages you visit frequently. However, in order to do this, that file must be read by the website; this means it can also be read by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked.

Another form of spyware, called a key logger, records all of your keystrokes. Some also take periodic screen shots of your computer. Data is then either stored for retrieval later by the party who installed the key logger or is sent immediately back via e-mail. In either case, everything you do on your computer is recorded for the interested party.

### 1.7.2 Intrusions

Intrusions are types of attacks that are actually trying to intrude into the system. They are different from attacks that simply deny users access to the system (blocking), or attacks that are not focused on a particular target such as viruses or worms (malware). Intrusion attacks are designed to gain access to a specific targeted system and are commonly referred to as hacking. However, this is not the term hackers actually use. Hackers call this type of attack cracking, which means intruding into a system without permission, usually with malicious intent. Any attack designed to breach security, either via some operating system flaw or any other means, can be classified as cracking.

Using security flaws is not the only method for intruding into a system. In fact, some methods can be technologically easier to execute. For example, one security breaching method which is not technologically based is called social engineering. As the name implies, it relies more on human nature rather than technology. This was the type of attack that the famous hacker Kevin Mitnick most often used. Social engineering uses techniques to get users to offer up the information needed to gain access to a target system. The way this method works is rather simple.

The perpetrator obtains preliminary information about a target organisation, such as the name of its system administrator, and leverages it to gain additional information from the system’s users. For example, he might call someone in the accounting field and claim to be one of the company’s technical support personnel. The intruder could use the system administrator’s name to validate that

claim. He could then ask various questions to learn additional details about the system's specifications. A well-informed intruder might even get a person to provide a username and password. As you can see, this method is based on how well the intruder can manipulate people and does not focus on that person's computer skills.

Social engineering and exploiting software flaws are not the only means of executing an intrusion attack. The growing popularity of wireless networks gives rise to new kinds of attacks. The most common and dangerous activity is war driving. This type of attack is an offshoot of war dealing. War dealing means that a hacker sets up a computer to call phone numbers in sequence until another computer answers to try and gain entry to its system. War driving, using much the same concept, is applied to locate vulnerable wireless networks. In this scenario, a hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At DEFCON 2003, the annual hackers' convention, contestants participated in a war-driving contest in which they drove around the city trying to locate as many vulnerable wireless networks as they could.

### 1.7.3 Denial of Service

The third category of attacks is called blocking attacks, which is the denial of service attack (DoS). In this attack, the attacker does not actually access the system, but rather simply blocks access to the system from legitimate users. In the words of the CERT (Computer Emergency Response Team) "A 'denial-of-service' attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service." One often-used blocking method is by flooding the targeted system with so many false connection requests that it cannot respond to legitimate requests. DoS is an extremely common attack method.