List and describe in short various types of threats

**Identifying Types of Threats**

Most attacks can be categorized as one of six broad classes:

What is malware? Explain in detail.

■ **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks,

worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.

1. **Virus** – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. The most common method for spreading a virus is using the victim’s email account to spread the virus to everyone in their address book. Some viruses don’t actually harm the system itself, but all of them cause network slowdowns due to the heavy network traffic caused by the virus replication. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms** – Worms are also self-replicating in nature but they don’t hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine, they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan Horse** – The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the ‘Trojan Horse’ tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside. Their purpose is to conceal themselves inside the software that seem **legitimate** and when that software is executed. they will do their task of either stealing information or any other purpose for which they are designed. They often provide **backdoor gateway** for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include **FTP Trojans, Proxy Trojans, Remote Access Trojans etc.**

1. **Spyware** – It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection. One of the most common examples of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus, capturing interesting information like username, passwords, credit card details etc.
2. **Adware** – Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer’s desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
3. [**Ransomware**](https://www.malwarebytes.com/ransomware/) is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to regain access. Ransomware has been called the cybercriminal’s weapon of choice because it demands a quick, profitable payment in hard-to-trace [cryptocurrency](https://www.malwarebytes.com/blog/101/2017/11/cryptocurrency-works-cybercriminals-love/). The code behind ransomware is easy to obtain through online criminal marketplaces and defending against it is very difficult. While ransomware attacks on individual consumers are down at the moment, attacks on businesses are up 365 percent for 2019. As an example, the [Ryuk](https://www.malwarebytes.com/ryuk-ransomware/) ransomware specifically targets high-profile organizations that are more likely to pay out large ransoms. For more, check out the [Malwarebytes Labs Ransomware Retrospective](https://www.malwarebytes.com/blog/reports/2019/08/labs-quarterly-report-finds-ransomwares-gone-rampant-against-businesses/).
4. [**Rootkit**](https://www.malwarebytes.com/blog/glossary/rootkit/) is a form of malware that provides the attacker with administrator privileges on the infected system, also known as “root” access. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.
5. A [**keylogger**](https://www.malwarebytes.com/keylogger) is malware that records all the user’s keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker, who is seeking sensitive information like usernames, passwords, or credit card details.
6. [**Malicious cryptomining**](https://www.malwarebytes.com/blog/101/2018/02/how-to-protect-your-computer-from-malicious-cryptomining/)**,** also sometimes called drive-by mining or [cryptojacking](https://www.malwarebytes.com/cryptojacking/), is an increasingly prevalent malware usually installed by a Trojan. It allows someone else to use your computer to mine cryptocurrency like Bitcoin or Monero. So instead of letting you cash in on your own computer’s horsepower, the cryptominers send the collected coins into their own account and not yours. Essentially, a malicious cryptominer is stealing your resources to make money.
7. [**Exploits**](https://www.malwarebytes.com/exploits) are a type of malware that takes advantage of bugs and [vulnerabilities](https://www.malwarebytes.com/glossary/software-vulnerability) in a system in order to give the attacker access to your system. While there, the attacker might steal your data or drop some form of malware. A zero-day exploit refers to a software vulnerability for which there is currently no available defense or fix.

■ **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server… all the things you probably associate with the term hacking.

■ **Denial of Service Attacks**

In a denial of service (DoS), the attacker does not actually access the system. Rather, he or she simply blocks access from legitimate users (CERT, 2003). One common way to do prevent legitimate service is to flood the targeted system with so many false connection requests, that the system cannot respond to legitimate requests. DoS is probably the most common attack on the Web.

■ **Web Attacks**

By their nature, web servers have to allow communications. Oftentimes, websites allow users to

interact with the website. Any part of a website that allows for user interaction is also a potential point

for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language)

commands into login forms (username and password text fields) in an attempt to trick the server into

executing those commands. The most common purpose is to force the server to log the attacker on,

even though the attacker does not have a legitimate username and password. While SQL injection is

just one type of web attack, it is the most common.

■ **Session Hijacking**

Session hijacking can be rather complex to perform. For that reason, it is not a very common form of

attack. Simply put, the attacker monitors an authenticated session between the client machine and the

server, and takes that session over. We will explore specific methods of how this is done later in this

book.

■ **DNS Poisoning**

Most of your communication on the Internet will involve DNS, or Domain Name Service. DNS is what

translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses

that computers and routers understand. DNS poisoning uses one of several techniques to compromise

that process and redirect traffic to an illicit site, often for the purpose of stealing personal information.

* Describe Perimeter and Layered security approaches.

Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is.

In a **perimeter security approach,** the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely. Little or no effort is put into securing the systems within the network. In this approach the perimeter is secured, but the various systems within that perimeter are often vulnerable.

There are additional issues regarding perimeter security that include physical security. That can include fences, closed-circuit TV, guards, locks, and so on, depending on the security needs of your organization.

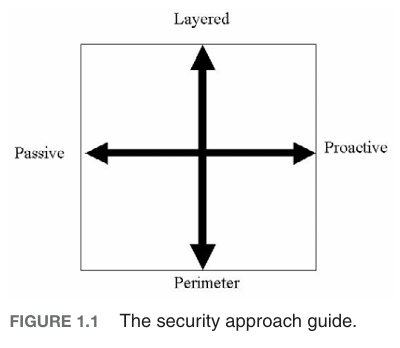
The perimeter approach is clearly flawed, so why do some companies use it? A small organization might use the perimeter approach if they have budget constraints or inexperienced network administrators. A perimeter method might be adequate for small organizations that do not store sensitive data, but it rarely works in a larger corporate setting.

**A layered security** **approach** is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method whenever possible.

You should also measure your security approach by how proactive/reactive it is. This is done by gauging how much of the system’s security infrastructure and policies is dedicated to preventive measures and how much of the security system is designed to respond to attack. A passive security approach takes few or no steps to prevent an attack. A dynamic or proactive defense is one in which steps are taken to prevent attacks before they occur.

One example of this defense is the use of intrusion-detection systems (IDS), which work to detect attempts to circumvent security measures. These systems can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. IDS can also be used to detect various techniques intruders use to assess a target system, thus alerting a network adminis trator to the potential for an attempted breach before the attempt is even initiated.

In the real world, network security is usually not completely in one paradigm or another; it is usually a hybrid approach. Networks generally include elements of both security paradigms. The two categories also combine. One can have a network that is predominantly passive but layered, or one that is primarily perimeter but proactive. It can be helpful to consider approaches to computer security along a Cartesian coordinate system, as illustrated in Figure 1.1, with the x axis representing the level of passive-active approaches and the y axis depicting the range from perimeter to layered defense.



The most desirable hybrid approach is a layered paradigm that is dynamic, which is the upper-right quadrant of the figure