In this presentation, we look at intruders and viruses on computer and network systems. The various intruders and types of viruses are examined along with possible countermeasures.

The many trespassers who continuously seek access to unauthorized systems have shattered the excitement over the benefits of distributed systems, especially the Internet. It is now common practice for an intruder to display unauthorized advertisements on users’ desktops as they surf the web. The different forms of trespassing can be categorized as 1) unauthorized login to a machine, 2) authorized users acquiring privileges or performing actions beyond those that have been authorized, and 3) software trespasses.

Let us more broadly examine these security concerns. Intruders come in different forms and are classified as a masquerader, misfeasor or clandestine user. The masquerader has no rights on the system, but penetrates a system's access controls to exploit legitimate users’ accounts. The misfeasor is a legitimate user on the system who accesses unauthorized resources. The clandestine user, on the other hand, can be an outsider or insider who seizes supervisory control of the system to achieve his or her goals.

Sometimes the trespassers do not have bad intentions, but in other cases, they may have serious goals to steal from or disrupt a system. More individuals than before do this for fun, because of the proliferation of password cracking and other software to assist them. The password file is a major target for the obvious reason that when crackers gain access to users with supervisory rights, they are then in a better position to gain access to the entire system or increase their range of privileges on the system. Existing techniques to counter these attacks fall under the one-way encryption and access control categories.

A number of intrusion detection products are also available on the market. They come with a number of benefits:

- If an intrusion is detected quickly enough, then the intruder can be identified and eliminated from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the lower the amount of damage and the quicker that recovery can be achieved.
- An effective intrusion detection system can serve as a deterrent against intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.
Systems can be trespassed using software in the form of viruses, worms, or Trojan horses. These malicious programs exploit vulnerabilities in computer and network systems. These programs can be divided into two categories: those that need host programs and those that are independent. Another way to view these threatening programs is those that do not replicate and those that replicate. Examples of the malicious programs are trapdoor, logic bomb, Trojan horse, worm, and zombie.

Viral infection comes in different ways, but they can be categorized as

1. Those initiated from user disks
2. Those initiated from vendor (manufacture of applications) CDs and disks
3. Those that begin across networking connections.

The most significant types of viruses include parasitic virus, memory resident virus, boot sector virus, stealth virus, and polymorphic virus. Some of the most recent viruses are the macro and e-mail viruses. Effort is constantly being made to counter the effects of these malicious attacks. There are currently many anti-virus products on the market to counter known malicious programs.

In this presentation, we discussed threats posed by individuals who trespass onto unauthorized systems. We pointed out that the intentions of these users are not usually pure, and that by bringing these threats to the forefront, countermeasures can be taken to deal with the threats. We also identified some of these counter measures.