target networks where UDP ports are open and allow unrestricted UDP traffic to bypass firewalls. Fraggle is considered a medium-risk attack and can be easily carried out by slightly tweaking Smurf code.

Fraggle attacks affect network management consoles by bypassing the installed firewall by having the internal system try to respond to external echo requests. These attacks prevent the network from receiving UDP traffic. A network administrator may not be able to distinguish between an inner system fault and an attack, due to missing syslog messages or SNMP trap alerts.

**Snork Attack**

In a Snork attack, a UDP packet sent by an attacker consumes 100% of CPU usage on a remote Windows NT machine. If there are several Snork-infected NT systems in a network, they can send echoes to each other, generating enough network traffic to consume all available bandwidth.

Windows NT 4.0 workstations and servers with service packs up to and including SP4 RC 1.99 are vulnerable to Snork attacks. Network administrators can easily detect these attacks by adding a filter in their firewalls with the following specifications:

- **Name:** Snork
- **Protocol:** UDP
- **Source Address:** Any
- **Source Port:** 135 (additional rules for ports 7 and 19, if desired)
- **Destination Address:** Any
- **Destination Port:** 135

**OOB Attack**

The OOB attack exploits a bug in Microsoft’s implementation of its IP stack, causing a Windows system to crash. Windows NT (server and workstation versions up through 4.0), Windows 95, and Windows for Workgroups 3.11 platforms are the most vulnerable to these kinds of attacks.

RPC port 135, also known as the NetBIOS Session Service port, is the most susceptible port for these kinds of attacks. When a Windows system receives a data packet with an URGENT flag on, it assumes that the packet will have data with it, but in OOB attacks a virus file has an URGENT flag with no data.

The best way to prevent such attacks is to configure firewalls and routers so that they allow only trusted hosts to get in, and in some cases NetBIOS Session Service ports can be blocked altogether to secure systems.

**Buffer Overflow Attack**

A buffer overflow attack is a type of attack that sends excessive data to an application that either brings down the application or forces the data being sent to the application to be run on the host system. This can allow the attacker to run malicious code on the target system. Sending e-mail messages that have 256-character file names is one common way to cause a buffer overflow.

There are two types of buffer overflow attacks: heap based and stack based. In a heap-based buffer overflow attack, memory space that is reserved for a program is filled with useless data and can allow malicious code to overflow and be written into adjacent memory space. In a stack-based buffer overflow attack, the program stores the user’s input in a memory object together with local variables on the program’s stack. This causes the return address to be overwritten and redirects the flow to allow a malicious user to execute arbitrary code.

**Nuke Attack**

In a nuke attack, the attacker repeatedly sends fragmented or invalid ICMP packets to the target computer using a ping utility. This significantly slows the target computer.

**Reflected Attack**

A reflected attack involves sending huge amounts of SYN packets, spoofed with the victim’s IP address, to a large number of computers that then respond to those requests. Requested computers reply to the IP address of the target’s system, which results in flooding.