# Network security solutions

A network Security Solution describe tools and policies employed by an organisation to track and thwart illegal admittance, abuse, alteration, or denial of the computer network service and network available resources. Network security entails safeguarding the network's internal resources by establishing protective boundaries immediately outside the organisation's network.

Such boundaries are intended to make the organisation's IT resources remain totally out of the way of intruders commonly referred to as ' hackers'. They are also key to protecting data assets from attacks, misuse, modification or outright theft by employees within the organization (Tipton & Krause, 2007).

In a network as big as that of Aircraft Solutions Inc, there are multiple threats that need a multifaceted solution approach. The best approach to securing such a vast network is to first remunerate the threats and then develop the mitigating solutions to the potential threats (Schiffman et al 2003). It is also practical to mention here early on that these kinds of networks are better protected by compartmentalization.

This is simply compartmentalizing the network with inbuilt internal boundaries, that is, separate networks for customers, contractors, suppliers and the company within one big network-Aircraft Solutions Inc. Virtual Private Network. It is vitally imperative to appreciate that good network security doesn't necessarily refer to the most fortified firewall. Every organisation must formulate a policy position that describes the approaches it will adopt in enforcing practices that will enable it to achieve better security for its IT resources (Yusuf, 2008).

For an individual to communicate over the internet, all he needs is a telephone line, a computer with an IP address. IP known as the Internet Protocol facilitate interaction between two hosts by first identifying the route to the destination host and hence carry packets of data, to and fro between the hosts. Therein lays IP security vulnerabilities. Attacks against IP are much probable.

IP security weakness stem from the fact that when two hosts are interacting, the two hosts do not authenticate the data packet header to ensure that it actually comes from the host on the other end of the connection, thus a hacker may introduce his packets of data with the intention of collecting information such as passwords and user ids for a later attack or simply flood the network with packets of data rendering it unusable-referred to as Denial of Service (DOS) attack.

To avert such type of an attack, the system administrator, can define router control access lists. These are lists that describe the hardware Mac addresses that are permitted to access the network resources such that if a packet originates from an alien Mac address, the router takes some sort of defined action-it stops the illegal packet or shuts down the violated port. This is popularly known as packet filtering.

DOS attacks can also be prevented by maintaining the latest software related security patches on the company’s hosts’ operating systems. It is also recommended that the company’s servers that are accessible from the outside are operated at levels that are not too close to capacity (Pohlmann et al 2009).

Another type of an IP attack is known as IP session hijack (Schiffman et al 2003). IP session hijacking attack occur when an attacker takes over and controls a user’s IP session. When the attack succeeds, the hijacker can proceed to do all that the user was doing, illegitimately. This sort of attack can be thwarted by simply using secure shell

(SSH) type applications since they are encrypted other than the telnet type applications that transmit data packets without encrypting the contents. In the event that an attacker hijacks a session, he wouldn’t be able to glean anything from it as the data is encrypted hence gibberish. He needs cryptographic keys to decrypt the data.

Unauthorised access refers to multiplicity of attacks where a hacker attempts to access a resource from a host that the host ought not to make available to the hacker. This could for example be a customers list on the customers’ server.

The server can be configured to authenticate that the request originates from a host that has the necessary privileges to obtain the list before, providing the command shell access to such a list (Mason & Newcomb, 2001). Execution of illicit commands on the company’s servers is another attack approach. This kind of attack is executed by people inside the network (Schiffman et al 2003).