Network Security Specification

Table of Contents

Introduction

This document is a specification for the design and configuration of the *System for Population Kinetics (Spk)* to provide a high degree of security against intrusion and attack via the Internet. As a practical matter, no system is absolutely safe. The goal of Spk, however, is to be at least as safe as major electronic commerce and web services sites. This is a reasonable expectation, because Spk and web commerce use the same technology.

Spk consists of a number of different processes running concurrently. Each type of process has its own security requirements. This document begins with an analysis of these needs. It then goes on to show how these requirements can be met with a straight-forward and inexpensive configuration of software and hardware.

High Level Requirements

These requirements address the security concerns of the user and of the service provider.

1. *Service Provider Authentication* Whenever a user accesses an Spk service, she needs to know that the service is authentic. She does not want to entrust her model designs or her data to a site which might be an imposter.
2. *User Authentication* An Spk service provider needs assurance that the user accessing the service has been authorized to do so.
3. *Security of Models, Data, Jobs and Results* A user needs to know that his information is secure from tampering, misappropriation and loss. It must be transmitted to and from Spk securely and its security must be assured while it is stored within the system.

Process Level Requirements

A functioning Spk consists of many independent processes running concurrently. Some processes or groups of processes of the same type require their own computer. Others can share a computer with different processes. In the following discussion, when we talk of *servers*, we do not necessarily mean that these are all hosted on

separate machines. A minimal Spk requires only two separate computers, in addition to client workstations and a gateway/firewall.

1. *Client Workstations:* Laptops, desktops, MDAs on which users run the Model Design Agent (MDA) subsystem.
2. *Gateway/Firewall:* a computer which provides a gateway to the public Internet while greatly restricting this access for security reasons.
3. *Computational Server:* the numerical computation engine that is the heart of the system. It normally consists of a processor cluster.
4. *Web Server:* the web interface for users, which is also the interface between the MDA and the rest of the system.
5. *Database Server:* provides the database by which all interprocess communication is performed and which contains a complete history of the service provided by this Spk.
6. *Application Server:* compiles model descriptions and job specifications from the MDA into the form required by the computational server.
7. *Administrative Server:* database backup; external access for system administrators and software developers.

Spk Network Security Requirements

Spk Development and Demonstration Network

The Spk network is attached to the public Internet via a dedicated computer that acts as a firewall and gateway. All network traffic into and out of the Spk network passes through the firewall.

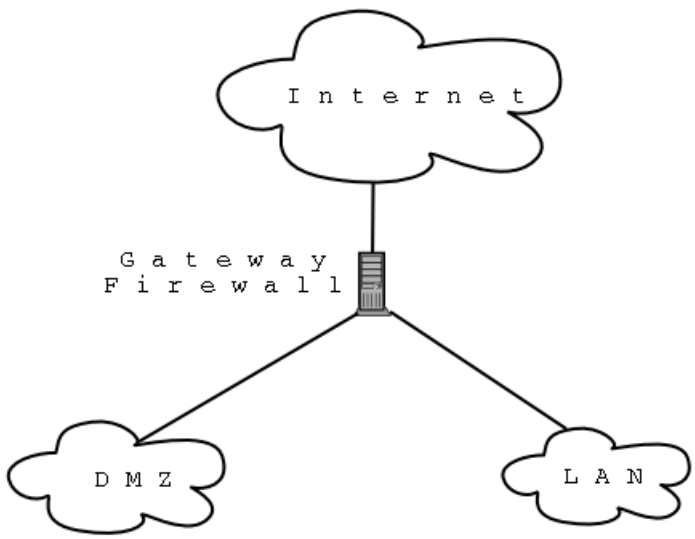

Figure 1. Spk Network

The Spk network consists of two subnetworks:

1. LAN (Local Area Network)
2. DMZ (Demilitarized Zone)

Of the two, the LAN is the more secure. Hosts on the LAN are not reachable from the Internet, because access is blocked by the firewall. In addition, all of these hosts have so-called *private* IP addresses, which are ignored by the routing and switching equipment of the Internet. These private IP addresses render the LAN invisible to the public Internet.

Just like the LAN, the hosts in the DMZ are assigned private IP addresses. Although these hosts are invisible to the Internet, a few of the services that they provide are not. Located in the DMZ are a web server and an ssh server. By virtue of an internet feature known as *port forwarding*, the firewall sends any requests for web service (http or https) to the web server, and any request for ssh connection to the ssh server.

The invisiblity of the individual hosts of the LAN and the DMZ shields them from external attack. All hosts connected to networks are capable of providing many services which are vulnerable, due to faulty software or to misconfiguration. In the Spk network, only two services are exposed to the public Internet, greatly reducing the chances of error. The two services offered correspond exactly to the set of services essential to the demonstration and ongoing development of Spk.

The table, below, lists the hosts on the two subnetworks.

Table 1. Hosts Located in Each Subnetwork

Subnetwork	Host	Description
DMZ	Public Web Server	Provides a web site, accessible from the public Internet, for users of the demonstration Spk system.
	Ssh Server	Although they cannot log into hosts on the LAN from the Internet, developers can log into this server in the DMZ and then can use it as the base for logging into hosts on the LAN.
LAN	Database Server	Spk Database resides here.
	Application Server	Aspk Compiler resides here.
	Computation Server	Cspk (eventually a cluster) resides here.
	Private Web Server	Used for development.
	Developer Workstations	Spk is developed on these hosts.
	General Server	Provides several functions: • Backup for all hosts on the network. • Shared file storage for development. • RFPK Projects Database and applications.