Network Security Specification

SPK is implemented on the user's workstation and a network of servers. Network security is important from the point of view of the privacy of data about human subjects, the proprietary nature of some PK models, and the reliability expected of a serious research tool. This document describes the specific network architecture that has been installed by RFPK to support the initial version of SPK. It is envisioned to become a model for SPK installations elsewhere.

Table of Contents

Introduction

Let us start by discussing some underlying assumptions and limitations.

1. *Physical Security*. The physical security of buildings and rooms in which computers are contained is an important component in the overall security of the network. At RFPK, the building and the lab are locked evenings, nights, and weekends. During normal business hours, however, anyone can walk in. This situation, which is appropriate for a facility that is involved in the education of students, is not ideal from a security viewpoint. Other installations might well choose to take additional precautions. This topic will not be mentioned further in this document.
2. *Level of Security*. Security is not cost free. In fact, it can be quite expensive. Absolute security would be infinitely expensive. The goal is to reach the right balance. The level of security that is right for one organization might be too high or too low for another. At RFPK, we have adopted a strategy for security similar to that for the technology we have chosen. SPK is a built on web-services technology which, although highly sophisticated, is available to us for free or very inexpensively because it is the technology of electronic commerce, rather than a special-purpose technology. Similarly, we have adopted the security model of e-commerce. We strive to be as secure as, for example, Amazon.com. Trying to be more secure would be difficult and very expensive.
3. *Compatibility*. The RFPK lab is situated on the campus of the University of Washington. Our network is part of the UW network. We have chosen a network security architecture which fits smoothly and nearly transparently into the UW network. Because the UW network is typical of what would be found at most universities and research organizations, we believe that our design has broad applicability. Enterprises with significantly different network infrastructure will, of course, make other choices.

The remainder of this document describes the specific architecture which RFPK has adopted.

Client Security

Users work on laptops or workstations, which can use any of the following operating system families: Windows, Macintosh, Linux or Unix. To work as part of SPK, a client machine must be connected to the public internet. Just connecting to the public internet introduces a level of insecurity, especially for users of Windows, because of the frequent attacks by viruses and worms. These risks can be minimized by employing anti-virus software, individual firewalls, by never opening executable email attachments, etc. This aspect of network security is the responsibility of the user. It should not be forgotten, however, that a compromised workstation may compromise the security of its user's participation in SPK.

Client software for SPK may be divided into four parts:

1. *Web Browser*. Any recent version of a popular browser should work, including IE, Mozilla or Netscape.
2. *Model Design Agent (MDA)*. The MDA is a component of SPK, which can be downloaded and installed securely, from the SPK web server.
3. *Java Runtime Engine (JRE)*. This software provides the java virtual machine needed to run the MDA. In some cases, a suitable JRE is already present on the client machine, because it is packaged with the operating system (for example Macintosh, Solaris, most varieties of Linux). In all other cases, it must be downloaded securely from a site operated by Sun Microsystems.
4. *Java WebStart*. This software is needed to download the MDA. It also automatically updates the MDA whenever revisions are available. In some cases, WebStart is already installed on the client, because it is packaged with the operating system (Macintosh, for example). In all other cases it must be downloaded securely from a site operated by Sun Microsystems.

The client software interacts with the web server to provide secure communications across the public internet:

- *Server Authentication*. The user starts a session with SPK by connecting to the SPK web server, using a browser. Because the Spk web site is a *secure* web site, the communication is via the *https* protocol, which provides the the user with a guarantee that the server is the genuine SPK web server and not an impostor. This validation is achieved when the server presents to the browser an authentication certificate signed by a certificate authority recognized by the browser.

- *SSL*. All communication between either the user's browser or the MDA on the one hand, and the web server on the other, uses a protocol known as the *Secure Socket Layer (SSL)*. All messages are encrypted using a 128-bit encryption key. This technology is identical to that used to protect credit card transactions at e-commerce web sites.

- *User Authentication*. In order to access the services of SPK, a user must log in by providing a username and a password. This communication is encrypted using SSL, as are all other messages. By logging in, the user provides SPK with proof that he or she is not an impostor.

- *WebStart*. The first time that the user clicks on the link for requesting the services of the MDA, WebStart downloads the latest version of the software from the server to the client machine. Each subsequent time that this occurs, WebStart downloads an update if a newer version is available, insuring that the user is always running the latest software. All downloads are encrypted.

- *MDA Authentication*. Since the MDA resides on the client's machine, it would be possible for a malefactor to modify the MDA to perform in ways that would jeopardize security. This is prevented by WebStart, however, which refuses to run an MDA that has been modified since downloaded.

Server Security

In the previous section, client security was discussed. The rest of SPK is provided by various servers. These servers are typically located in once place, hence the traffic between them does not pass over the public internet. Encryption is not a requirement. On the other hand, it is critical to protect them from external attacks, which could make them unavailable to users or could allow sensitive information to be stolen or tampered with.

Server Connection Security Requirements

Because their functions differ, the servers have differing requirements for connection security:

- *Web Server*. This is the only server that needs to be reachable from the public internet. With the exception of the database server, none of the other servers should accept connections from the web server.
- *Database Server*. This server should not be reachable from the public internet. It must, however, accept database connections from the web server. It must not accept connections of any other sort from the web server.
- *Application Server (ASPK Server)*. This server should not be accessible from the public internet. It must be able to establish database connections to the database server.
- *Computational Server (CSPK Server)*. Like the application server, the computational server should not be reachable from the public internet and it must be able to establish database connections to the database server.

It is not necessary that each of the above servers be hosted on a separate machine. All servers could reside on a single machine. It would be preferable from a security point of view, however, to have at least two machines: one for the web server and the other for the rest, because the web server is reachable from the public internet.

At RFPK, two machines and a cluster are used:

- The web server is a separate machine.
- The database server and the application server share a machine.
- The computational server is hosted on a cluster.

Firewall

The connection security requirements are satisfied by a triple-interface firewall. The firewall is a dedicated computer with three Ethernet interfaces:

1. Interface to the public internet.

2. Interface to a LAN known as the demilitarized zone (DMZ). Machines in the DMZ are reachable from the public internet, and from the protected LAN. DMZ machines cannot, however, access the protected LAN, except by special arrangement.

   Only the web server is in the DMZ.

3. Interface to a protected LAN, which cannot be reached from the public internet and can only be reached from the DMZ by special arrangement.

   All servers except the web server are on the protected LAN.

The firewall passes tcp/ip message traffic between the three networks according to the following rules:

- From the public internet, no incoming requests are forwarded to the protected LAN. Only requests to port 80 (http) and port 443 (https) are forwarded to the web server on the DMZ LAN.
- From the DMZ, no requests are forwarded to the protected LAN, with the exception of database requests directed to port 3306 of the database server.
- Requests from one host to another within the protected LAN are forwarded freely. In particular, this allows the application server and the computational server to access the database server without restriction.
- Requests are forwarded from both the protected LAN and the DMZ to the public internet.
- Replies to all requests previously forwarded are returned to the appropriate sender.