SPUC IT Working Group
(formerly MAPO Computer Security and Planning Committee)

Bob Loewenstein, chair
Michael Ashley
Chris Martin
Matt Newcomb
Clem Pryke
Darryn Schneider
Antony Stark

Introduction

Currently plans are being made to increase IT security at South Pole Station. The SPUC is concerned that the scientific community is not being adequately consulted in the design of the new plan. We certainly understand the need for swift action after a breach of security incident and believe that our community has a wealth of experience with networking, research, and security. Because of this, the SPUC has formed an IT working group representative of MAPO users and eventually other science groups at Pole. The first meeting of the working group was held, by phone conference on June 17, 2003, a few days after the SPUC meeting in Denver. A summary of the meeting and its recommendations is given below.

On Site

Firewalls have problems, but can provide a significant increase in security. In the past, the SPUC had voiced the opinion that science should have the choice to be behind the firewall or not; telnet would be replaced with ssh and while sftp and scp would also be used, there was still a need for ftp and passive mode. There was also need for various remote desktop login tools like VNC and Timbuktu as well as web mirroring between Pole and the continental United States (CONUS).

If it becomes necessary for all computers and peripheral devices to be behind the station firewall, science should have some role in specification of science requirements so that research is not hampered or restricted.

Concerning the plan for assurances that each computer brought to Antarctica has been anit-virused, patched, and perhaps even inspected, and software installed, we feel that this is almost an impossible task and very difficult to enforce; with thousands of types of computers and operating systems brought down each season, how will a handful of people have the knowledge base and time required to provide the correct software? No other research facility with which members of the committee are familiar inspects individual machines. As an example of how things can go wrong, a Viper Linux box at Pole this winter had patches installed without consulting the people on CONUS who

knew the system. The patches that were applied were not applicable for that version of Linux, resulting in the loss of the machine until a complete rebuild was performed.

Another plan brought up during the SPUC was to phase out older machines, including grantee computers. In many cases, this would require significant time and expense to rewrite working programs and purchase the new machines. In some cases, it could be argued, older machines are more secure than newer ones. Hackers target machines they know, and few target older machines or machines running obscure operating systems.

Off Site

While work on-site can likely be better facilitated, how the station network is managed and/or configured to provide off-station access is of major concern. It is *imperative* that authorized users off station have instant access to all machines they have accounts on. Authorization is defined by the science project. Very frequently it is necessary for remote experts to login from CONUS (and elsewhere) to help resolve problems and fix software problems, reduce data in order to reduce the size of the data to be uploaded to CONUS, and to install new software. There can be no delay in remote access; data will be lost. Any plan that is implemented must ensure instant access.

Currently the method for allowing scientists access to their South Pole machines is to allow specific IP addresses on one side of the firewall to access specific addresses on the other side of the firewall. This is not an ideal solution as it still exposes South Pole machines to security risks (in that any machine on a network between the authorized machine and the Pole can potentially impersonate, or "spoof", the authorized machine and thereby gain illicit access to the South Pole). In addition it still allows protocols with cleartext passwords to transit untrusted networks (another security risk).

In the event of a security issue with the current configuration the information logged is very sparse. At best one can say that a particular IP address was where the attack appeared to come from, but one cannot pinpoint to an individual machine or user from which the attack actually came.

Fortunately there are many possible solutions to the security problem. For instance, a popular solution for securing IP traffic across an untrusted network is to use IPSec. IPSec encrypts an entire packet, wraps it with an IP header and sends it off. It also includes packet level authentication so there is less concern about spoofing. This is not a complete solution because it does not authenticate network usage at the user level. But happily this problem also has potential solutions like the RADIUS protocol.

IPSec is commonly used to link two networks over an untrusted third network and as such it may be monetarily worthwhile to investigate using a Virtual Private Network to connect Denver to each of the Antarctic ground stations. That way Raytheon might not have to pay for a leased line from the ground station to Denver, but instead a leased line from the ground station to a local point of presence.

Many research facilities around the country operate in a reasonably open network architecture while still having government-approved security. We urge RPSC to look at how other facilities, both government and private, such as NASA Ames Research Center, NASA Goddard Flight Center, National Observatories, and Universities---all places where lively research is supported---in order to use them as models of how security and open research can coexist.

As an example, NASA Ames uses an encrypted VPN server to allow users to login behind the facility firewall. Cisco provides client software for users' computers so that the login is authenticated and all packets between the server and client are encrypted. This client software is available for essentially all machines which the science community might use to access computers at the South Pole. The accessing machines are more modern and standard than the special-purpose data acquisition machines at the Pole. Once behind the firewall, users have access to all machines they would have had if they had logged in from behind the firewall. Except for the commercial client on users' computers, the method provides a transparent process so that the user sees virtually no difference from being on-site.

Information on the Cisco encrypted VPN product may be found at the URL below:
http://www.cisco.com/en/US/products/sw/secursw/index.html

Recommendations:

1. Firewalls have security risks through backdoors. "Properly configured, a VPN tunnel will allow total and unrestricted access to the networks that the hosts are gateways for. When provided as a legitimate remote access tool for employees and business partners, VPNs can increase productivity, save time and reduce costs. When they are used to exploit gaps in the security architecture, they can have just the opposite effect." See http://securityfocus.com/infocus/1701 for more information. The firewall currently in effect for the South Pole is vulnerable to this security risk. We therefore recommend the use of a server/client connection with authenticated login and encrypted packet exchange for remote login to Pole. The science community is willing to run commercial client programs on computers used for remote access. Easy and rapid remote access to Pole is *essential* to fulfill the science mission at Pole. With encrypted packet exchange, this requirement can be met and network security can be enhanced at the same time.
2. If it would help to decrease the visibility of science machines, it might be a wise move to create another domain name for science that does not have spole.gov in its domain name.
3. Support the use of common utilities and ports for connections on and off site (e.g VNC, Timbuktu).
4. Utilize the science community's expertise in IT matters in the form of on-going consultation during the design of the new secure network.
5. Do not rely on individual computer inspections and forced compliance of security rules. This is likely to be unproductive and ineffective. Address the problem centrally, not individually.

6. If migration to new machines is required, grantees may need substantial supplemental funding to accomplish the task.