SLAC Remote Access Server Security Policies

Stanford
Linear
Accelerator
Center

SLAC Remote Access Server Security Policies

Approved by ADCC: August 9, 1996

Why do we need to Worry about Remote Access Security?

From time to time, SLAC users have expressed interest in setting up their own SLIP/PPP service or other remote access service (such as the Windows NT Remote Access Server) on one of their machines on the SLAC network in order to provide access to an offsite machine such as a home computer. This would allow a dialin connection directly to a server on the SLAC network, inside the protective Internet firewall screen and not subject to the normal SLAC firewall protections. Such a server could be a potential back door to the entire SLAC network. If not carefully configured, an onsite remote access server would be a serious security risk to all of SLAC's distributed environment.

Currently, SCS does not have the expertise or resources to configure, check, or otherwise manage such remote access servers, and we feel that it is better to put our resources into bringing up the new ISDN service, continuing to support Appletalk Remote Access (ARA), and providing pointers on how to use external SLIP/PPP services, e.g. through campus.

Those who wish to set up remote access servers must obtain prior approval from the Security Committee and meet reasonable guidelines. Such servers must be carefully administered, otherwise crackers may exploit weaknesses to gain unauthorized access to SLAC computers, networks, and/or file systems. In the worst case this could result in the release of sensitive information, modification or destruction of data stored on SLAC's computers, or even damage to apparatus controlled by these computers.

Government laboratories such as SLAC have proven to be tempting targets for crackers. In 1995 an intrusion into SLAC's network from the Internet resulted in SLAC having to sever its connection to the Internet for several days, inconveniencing many remote collaborators who were prevented from performing their normal work at SLAC. In addition considerable time had to be expended checking for and removing effects of the break-in and beefing up security to prevent similar intrusions in the future. Although this attack was probably not performed via a remote access server, it is to everyone's benefit to take reasonable precautions to prevent such intrusions taking place in the future.

The policies described below have been developed to minimize the exposure to remote access server breakins with an acceptable expenditure of effort /resources, while maintaining an environment in which the potential of remote access servers can be effectively exploited by SLAC groups. It must be understood that there is an implicit conflict between the requirements of security, the desire to exploit new technology for SLAC's research and adminstrative needs, and the limited manpower to support new technologies. Even with the implementation of the policies described here, it is not possible to completely assure the security of SLAC's network environment. The level of security described here is thought to be adequate for most of SLAC's current requirements, however it is probably not adequate for applications which deal with highly sensitive information or where human safety may be affected.

Policies

In order to provide reasonable security and availability, we recommend that:

- SCS provides support for a few ways to access nodes at SLAC via dialin. This should minimize the demand for non-SCS remote access servers. Currently this includes:
    - An Appletalk Remote Access (ARA) server within the firewall which requires username and password and in some cases dial back.
    - Documentation and/or pointers on how to access SLAC via SLIP/PPP services or Internet service Providers all outside the firewall.
    - An ISDN pilot with dialback where the "servers" are inside the SLAC firewall.
- Requirements for additional remote access servers should be documented and brought to the Security Committee for discussion and approval if appropriate. Guidelines for appropriateness will need to be worked out based on experience.
- No new remote access servers should be set up at SLAC without review and approval by the Security Committee and/or some higher authority.
- Any SLAC remote access server will be maintained by staff who will:
    - keep the operating system at a level supported by the vendor;
    - keep current with security patches, evaluate and expeditiously apply as appropriate;
    - have a thorough understanding of the vendor's remote access server system, and particularly those aspects which affect security;
    - ensure that the remote access server can be used only by persons authorized to use SLAC's computer and network resources;
    - ensure that the server properly restricts access to information;
    - ensure the administrator of the server, or a designate, will be available during working hours to expeditiously resolve problems;
    - keep and make available a current list of phone numbers where administrators or designates may be reached in a critical situation outside normal hours;
    - provide the ability to audit use via logs and to monitor exceptions;
    - If account/passwords are the chosen method of enhancing security then the user accounts and passwords must be well managed, this includes:
        - keeping a time stamped permanent record of all the accounts that have been created, together with access priviledges if appropriate
        - ensuring an account is removed or disabled when the owner should no longer have access to it (e.g. the owner is no longer associated with SLAC);
        - ensuring accounts are not shared by multiple users;
        - ensuring the passwords meet good practices.
    - If dialback is the chosen method of improving security, then the number to be dialed should be removed when a user should no longer have access.

- If all the remote accesses to a server are guaranteed to be restricted to the server itself (i.e. users connecting to the remote access server cannot access any other part of the SLAC network or the Internet by any means (e.g. FTP, finger, telnet, NFS)) then some of the above restrictions may be eased as we understand the issues more.

If an unauthorized remote access server is discovered, an attempt will be made to contact the owner(s) via phone and Email. If successful the owner will be appraised of the policies on remote access servers and requested to disable the remote access pending authorization. If the attempt to reach the owner(s) is unsuccessful or the user does not disable remote access, then measures will be undertaken to limit the effect (e.g. the server will be barred from the network pending authorization), and the Security Committee will be notified.

Acknowledgements

Much of the first section was derived from a similar section authored by Tony Johnson in the Web Security Document. We have had useful discussions with Dennis Wisinski on Windows NT Remote Access Services.

Les Cottrell and John Halperin