SLAC-PUB-8172
June 1999

NT Security in an Open Academic Environment

G. Daly et al.

Presented at 2nd Large Installation System Administration of Windows NT Conference, 7/14/99—7/17/99, Seattle, WA, USA

Stanford Linear Accelerator Center, Stanford University, Stanford, CA 94309

Work supported by Department of Energy contract DE–AC03–76SF00515.

SLAC–PUB–8172
July 1999

NT Security in an Open Academic Environment*

Gregg Daly, Gary Buhrmaster, Matthew Campbell, Andrea Chan, Robert Cowles, Ernest Denys, Patrick Hancox, Bill Johnson, David Leung, Jeff Lwin
Stanford Linear Accelerator Center, Stanford University, Stanford CA 94309

Abstract

Stanford Linear Accelerator Center (SLAC) was faced with the need to secure its PeopleSoft-Oracle business system in an academic environment that has no firewall. To provide protected access to the database servers for NT-based users all over the site while not hindering the lab's open connectivity with the Internet, we implemented a pseudo three-tier architecture for PeopleSoft with Windows Terminal Server and Citrix MetaFrame technology. The client application and Oracle database were placed behind a firewall, and access was granted via an encrypted link to a thin client. Authentication in the future will be through two-factor token cards. NT workstations in the business system unit were further secured through switched network ports and an automated installation process that included SMB signing and disabling LM Authentication in favor of NTLMv2. The hardened workstations then accessed the business system through the Citrix Secure ICA client. How these security measures affected our mixed environment (Windows9x, Samba, Transarc AFS clients, Pathworks, developers, researchers) is discussed.

Submitted to 2nd Large System Administration of Windows NT Conference Proceedings

* Work supported by Department of Energy contract DE–AC03–76SF00515.

NT Security in an Open Academic Environment

Gregg Daly, Gary Buhrmaster, Matthew Campbell, Andrea Chan, Robert Cowles, Ernest Denys, Patrick Hancox, Bill Johnson, David Leung, Jeff Lwin
Stanford Linear Accelerator Center

Abstract

Stanford Linear Accelerator Center (SLAC) was faced with the need to secure its PeopleSoft/Oracle business system in an academic environment which only has a minimal firewall. To provide protected access to the database servers for NT-based users all over the site while not hindering the lab's open connectivity with the Internet, we implemented a pseudo three-tier architecture for PeopleSoft with Windows Terminal Server and Citrix MetaFrame technology. The client application and Oracle database were placed behind a firewall, and access was granted via an encrypted link to a thin client. Authentication in the future will be through two-factor token cards. NT workstations in the business system unit were further secured through switched network ports and an automated installation process that included SMB signing and disabling LM Authentication in favor of NTLMv2. The hardened workstations then accessed the business system through the Citrix Secure ICA client. How these security measures affected our mixed environment (Windows9x, Samba, Transarc AFS clients, Pathworks, developers, researchers) is discussed.

1. Security in an Open Environment

SLAC has 3800 hosts running Windows NT (1400), UNIX (2000), Macintosh (350) and several other operating systems. The network is based on a highly redundant Gigabit Ethernet backbone implementing virtual LANs allowing hosts on the same subnet to be located anywhere in the Lab. All external network traffic to the Internet passes through a single filtering router.

Like most academic research environments, SLAC does not have a real external firewall. The High Energy Physics (HEP) community has a tradition of being very open – the strength of such an environment produced the World Wide Web. (CERN, where the World Wide Web originated, is another High Energy Physics facility, while SLAC itself was the first web site in the U.S.A.) Current HEP experiments can have more than a thousand experimental collaborators (distributed internationally), and collect hundreds of terabytes of data per year. The very size of the collaborations involving software development, hardware design, implementation, and data analysis require incredible amounts of open discussion, collaboration, and gigabit network bandwidth with as few barriers as possible. Physicists are creative people who tend to enjoy playing with the latest software releases (beta) and in solving puzzles (how do I get around this restriction?). Once these users have found a way around restrictions or become used to certain software "features," it can be extremely difficult and politically inadvisable to (re)impose barriers that might delay large projects. However, business application systems used within the Lab, and the Windows operating systems they run on (even Windows NT), are not designed for use in an open Internet environment.

In mid-1998 there was a major security incident at SLAC. More than 25 machines had root compromises and the intruders used more than 50 user accounts. In order to assess the damage and clean up the systems, SLAC dropped off the Internet with respect to interactive services for a one week period (incoming web access and bi-directional e-mail were still allowed). Needless to say, this incident caused a lot of attention to be focused on computer security issues. An example of a change in attitude was that the NetBIOS over TCP ports were finally blocked at the SLAC external router with only a grumble of protest.

1.1. Constraints

To protect the business systems, we needed to implement credible responses to what seem to be the major vulnerabilities: compromised passwords; and the combination of "scientist maintained" workstations and a mode of thinking that "PC" meant "*personal* computer". We had to balance the need for a secure, reliable computing and network infrastructure with the need for an open collaborative research environment. The bottom line at SLAC is, "The Physics must get done!"

1.2. Threat Analysis

SLAC's business data is stored on an Oracle database server. Over 200 users access the data via PeopleSoft applications running on NT workstations from both onsite and remote locations.

In terms of possible threats to the business systems, the major point of vulnerability was considered to be the Oracle database machine. The attacks we wanted to protect against were external network-based attacks or attacks involving unauthorized but authenticated users (compromised passwords, etc.). Additionally, we needed an architecture adaptable enough to respond to new threats over the next two years. In particular, it should include elements making it resistant to keyboard monitoring programs like Back Orifice and Netbus.

1.3. Corporate-world Solution

As we started doing our research, it was clear the "standard corporate model" was to build a fortress. Corporate networks were behind firewalls which allowed almost no protocols to travel through them and often used proxy servers for people inside the firewall to have access to Internet services. There might be a sacrificial web or e-mail server sitting outside the firewall, but that was all.

This was not a viable solution in an academic or research environment. An important factor in a research environment is to provide for the unexpected. Would the web have been developed without that kind of open environment?

1.4. Mini-corporate Solution

Another possibility was to treat the business services people as sort of a mini-corporation within SLAC, and place them behind the kinds of barriers described above (Fig. 1). While that thought made the physicists happy for a few minutes, only a little reflection was necessary to realize the business services people *support* the rest of the lab. To perform their mission, they have to communicate with the rest of the Lab concerning budgets, personnel, and financial issues. The senior research

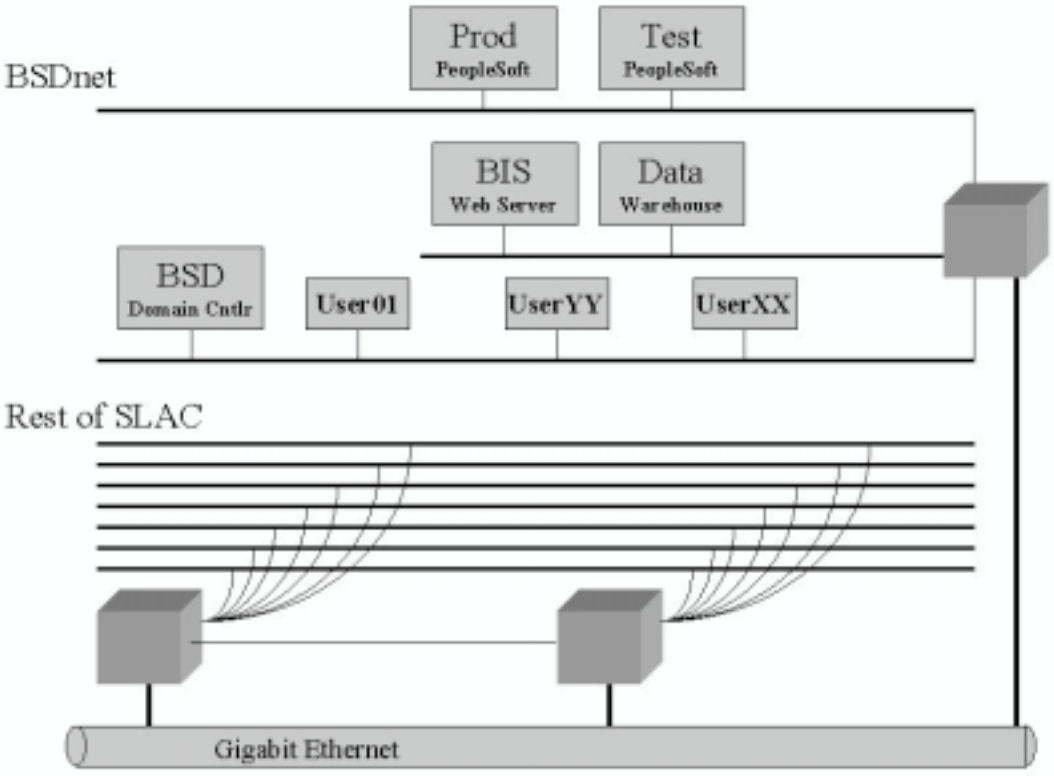

Fig. 1 Mini-corporate Solution

leaders are often heavily involved in financial aspects of the experiments and need access to current budget information, particularly near the end of fiscal cycles.

Another variation of this approach, with each business service user having two NT workstations – one secured and one configured for SLAC inter-operability – was also rejected. Besides the cost of additional workstations and networking equipment, the fear was that in the long run, users would bypass the security using either floppy disks, "yellow cables" or new ways of "piped" cross authentication (e.g., new web browsers) between the secure and not-secured systems.

1.5. Layered Solution

A layered solution finally survived a number of discussions and presentations (Fig.2).

1. Only the Windows Terminal Server/MetaFrame farm configured with PeopleSoft apps may access the database server (no direct workstation access).
2. Both the Oracle database server and this Windows Terminal Server/MetaFrame farm would be pulled into a subnet (BSD Extremely Private Network (EPN)) with very restrictive port filtering rules. Under normal operations, only these few machines would be behind this "firewall", and no personal workstations.
3. People directly using the business systems (as opposed to just viewing information through a web interface) would be required to access the PeopleSoft applications and the database server only via the MetaFrame 128-bit encrypted thin client.
4. Token cards provide two-factor authentication to this system.
5. Access to the MetaFrame servers must originate in the BSD subnet.
6. People directly using the business systems would also be required to have a standardized and security-hardened software configuration with basically interchangeable but fully functional workstations.
7. A few mission-critical users would have workstations limited to running only the business applications and not much else, and would be on the same BSD-EPN network as the servers.
8. Network and host-based Intrusion Detection Systems will watch network traffic and operations on the database server.

A major feature of this design is that during normal operations, the business users have full access to SLAC NT network resources. In times of response to an intrusion, two levels of "air gap" can be implemented to separate BSD-EPN and BSDnet from the rest of SLAC and the Internet, as shown by Fig. 3:

1. Mission critical functions can proceed with the few workstations on the same BSD-EPN network as the servers.
2. The 200 business users in BSDnet can be reconnected back to the servers on a priority basis after being revalidated. This subnet has its own domain controllers, SMS and home directory servers so it can exist as a standalone domain.

Selling the plan was simplified by two factors: the scientific researchers see no changes in their environment

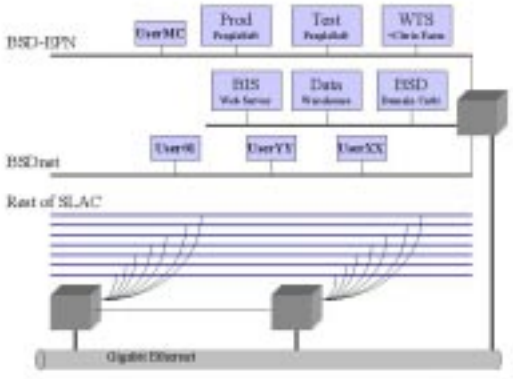

Fig. 2 Layered Solution

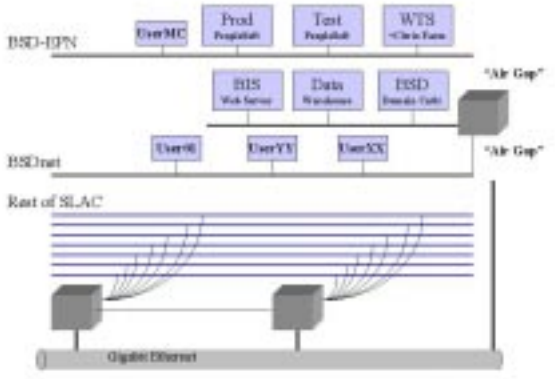

Fig. 3 Layered Solution during Intrusion

in the way of additional restrictions; and the "air gap" concept is easy for management to understand.

2. Configuring and Securing Windows Terminal and MetaFrame Server Farm

2.1 WTS/MetaFrame Overview

Microsoft's Windows NT 4.0 Server, Terminal Server Edition (commonly called WTS) is an extension to Windows NT Server which provides, in essence, a multi-user Windows system. That is, WTS allows multiple individuals "login" access to one Windows NT desktop, and attempts to keep each user separate from each other.

Citrix's MetaFrame product extends WTS in a number of areas. The most important features to SLAC were

- load balanced server farm
- Secure ICA client
- user drive remapping
- seamless windowing

The load balancing feature of MetaFrame allows administrators to publish an application, which will connect to the "least loaded" MetaFrame servers that supports that application – providing both load balancing and server failure recovery. (See Fig. 4) An added bonus for system administration is that a server can be placed "offline" for maintenance.

The Secure ICA client provides 128-bit encryption on the data stream. With password and session stealing the biggest threat to corporate networks, the ability to encrypt the entire session moves the complexity up one more level for a potential attacker.

Seamless windows allow an application to appear on the users' desktop as if the program was running natively.

Along with user drive remapping through the ICA cli-

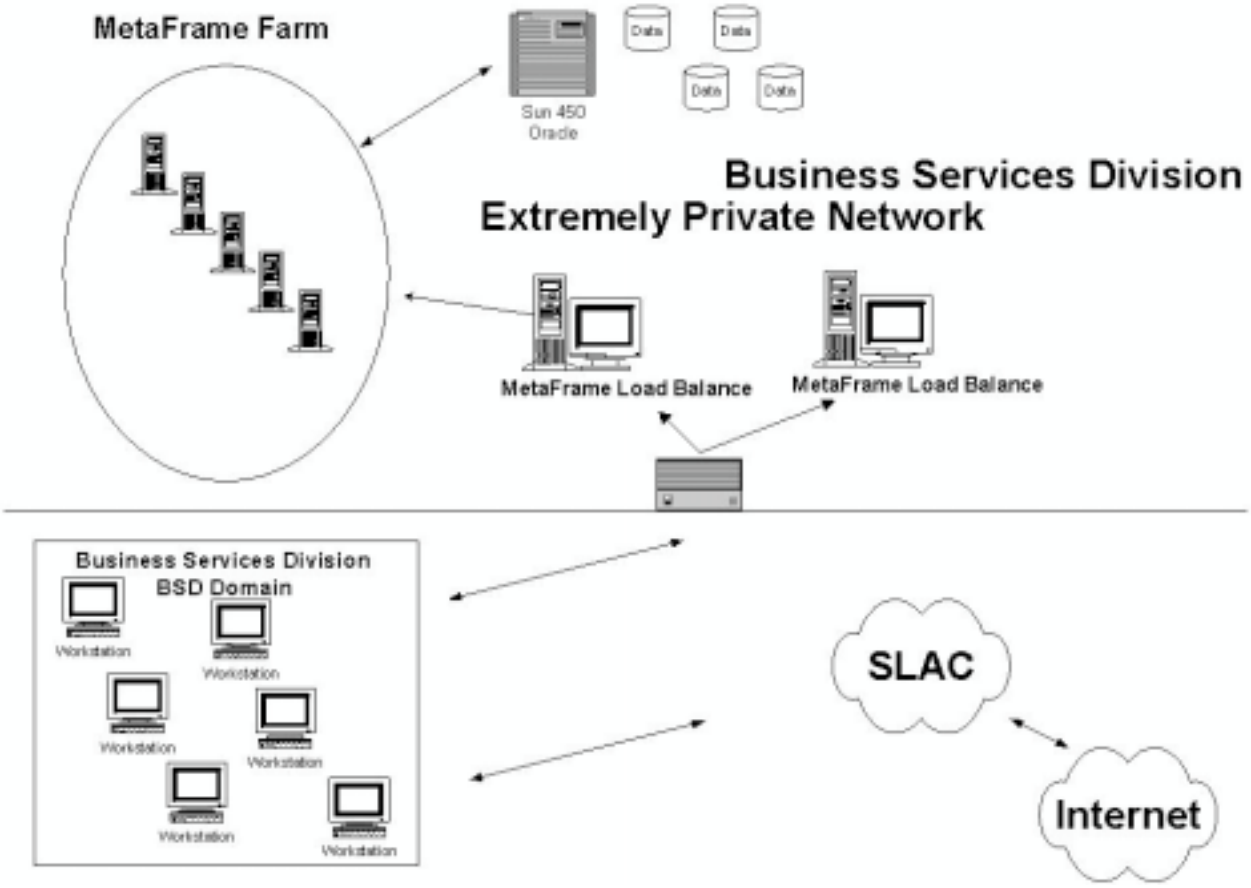

Fig. 4 PeopleSoft WTS/MetaFrame Farm

ent, the user's application has access to the local PC's resources when that is necessary.

2.2 Configuring Applications

Microsoft's NT solutions tend to be designed with the assumption that one and only one person will have a desktop on the machine at once. At logon, a number of things happen behind the scenes to "customize" the particular machine one is logging into. A system which allows multiple logins at once needs to isolate these "customizations" to particular users. This requirement has led to some challenges given the underlying architecture of Windows since the system and applications were designed to assume that only one user was logged on at once. Many (common) system directories contain configuration files for the currently logged on user. The NT registry, one of the central repositories of customization data, consists of both user and machine specific sections. While some newer applications are "WTS aware," or at least "WTS friendly," older ones can be complex to correctly configure.

PeopleSoft is a vendor of complete Enterprise Resource Planning solutions in the Human Resources, Financials, Manufacturing, and Student Administration System arena. SLAC is currently running PeopleSoft 6 HR and FS. PeopleSoft 6 is a classic 2-tier application, where the business logic runs on the client system communicating to a DBMS server. In addition, PeopleSoft comes packaged with a set of 3rd party applications such as Crystal Reports (a report writer) and SQR (a report and batch processing program). PeopleSoft has its own development tools and runtime processing environment. SLAC uses Oracle as the backend RDBMS for PeopleSoft.

As a classic 2-tier client/server system, PeopleSoft provides no protection of the data flowing across the network, nor does it in any way verify that the application connecting to the RDBMS is actually PeopleSoft, and will follow the appropriate business logic. The passwords in the PeopleSoft database are easily decrypted, which would allow someone to login to the application as a user with full authority on the entire database. PeopleSoft admits that this is a weak link in security and has addressed this in later versions of their product.

PeopleSoft, Crystal Reports, and SQR were designed and implemented long before WTS was introduced (SQR is a 16-bit application which are especially unfriendly to the WTS environment). As with most Windows products, they presume that one and only one user will run the application at a time. While PeopleSoft does let one configure the application dynamically, the changes are made to global files and registry entries.

Other problems existed – Crystal Reports, when invoked by PeopleSoft using PS/Query, requires registry entries in HKEY_LOCAL_MACHINE (HKLM), which is nominally a "shared" key. While it is possible to create user unique HKLM values in WTS, another solution was chosen. Since the HKLM key had the same value except for the environment (PSENV), the type of the variable was changed from REG_SZ to REG_EXPAND_SZ, which will expand environment variables before returning the string. For example, for a made-up key, the value before the change was

CRYSTAL\BINDIR=N:\HR600\CRYSTAL\BIN

To allow users to share the HKLM registry entries, the value becomes

CRYSTAL\BINDIR=N:\%PSENV%\CRYSTAL\BIN.

2.3 WTS User Interface

WTS (with the MetaFrame add-on) provides one of two methods to access the WTS farm. The first is essentially a desktop in a window on your normal desktop. The other method provides a "seamless" windowed application, where the application appears to be running on your desktop.

The seamless window was chosen for the BSD deployment for a number of reasons. First, the desktop, while it can be restricted somewhat, is a desktop. Not only can it be confusing which desktop one is using, the user can access applications which should properly be restricted. Using published, seamless applications, the WTS administrators decide what is appropriate and "safe." In addition, using a seamless window provides an interface that minimizes end-user training. The users are expecting to see an application window when they (double)click on the PeopleSoft icon. Using published seamless windows preserves, to a large extent, that experience and training.

2.4 Securing MetaFrame

Several departments within SLAC had prior experience with multi-user versions of Windows NT in the form of Ntrigue and WinFrame. It was necessary to retrain administrators because deploying applications and desk-

tops in the MetaFrame environment was significantly different.

Citrix's Secure ICA client provides from 40-bit to 56-bit DES to 128-bit RC5 encryption of the username and password as well as the data being transmitted and received during the session. This method of access provides the users with a secure tunnel to run the applications to/from the MetaFrame, providing a secured application environment to process sensitive financial and human resource data.

Installations of WTS using the default options do not result in a secure operating environment with respect to registry and file access. A basic method of securing an installation is to replace the access rights of both "guest" and "everyone" group. Replacing these rights with a more tolerable setting of assigned "authenticated users" or even restricting general access to the "domain users" group. This prevents common intrusion techniques and gathering information by anonymously reading system settings via the registry by unauthorized users. The file system should be modified to the most restrictive access possible without impacting the user's ability to run applications on the multi-user host. Since the every user in a multi-user setting must have the "log on locally" right, special attention must be taken with the access permission with the %SYSTEMROOT% (usually c:\winnt), SYSTEM and SYSTEM32 folders. Also due the "log on locally" right required for multi-users, physical security is even more important than in the client/server setting since any domain user may logon to a WTS server at the console.

3. Securing NT Workstations

3.1. Background to Network Install

The open academic environment of SLAC has historically led to departments configuring NT systems more or less as they saw fit, often with little concern towards standardizing the hardware or software or ensuring that systems do not adversely impact the functioning of the network and other systems. Over time, this created enormous management problems, such as tracking down or diagnosing system mis-configurations, timely replacement of failed equipment, and responding to network interruptions. In response to these growing problems, SLAC has worked toward standardization of NT systems by working with Dell to create recommended system bundles, and developing an automated software installation process.

The automated software installation process, or Network Install, began as a way to quickly and easily configure new Dell systems. Using the Network Install, NT systems can be configured in a fraction of the time it takes administrators to configure them manually. The automated process ensures that the operating system and applications are configured per SLAC's standards and brought up to the necessary patch levels, and that the system will work properly on SLAC's network. In an effort to standardize the software on existing, non-Dell NT systems, the Network Install was adapted to work with a variety of other hardware configurations as well. This allows administrators to quickly and easily redeploy standardized, reliable NT systems when rebuilding older systems or transferring them to new users.

The Network Install is a collection of scripts that utilize automated installation features of Windows NT, and several applications along with a variety of other software tools and utilities. It utilizes a modular construction allowing for easy modification of individual parts as software versions change, drivers are updated or service packs and patches are released. This modular construction makes it easier to update and maintain than a system image-based installation process, such as Ghost, which would require creating new images every time a hardware or software change is necessary. The Network Install is also able to support a much larger variety of hardware than would be feasible with system images. We have also tended to avoid cloning NT installs to preserve the unique machine SID generated during the installation process.

The Network Install consists of five main steps. First, the hard drive is erased, and a new FAT primary partition is created. Second, a script prompts the administrator for configuration information, such as the model and name of the computer, what types of video and Ethernet cards are installed, whether to use DHCP or a specific IP address and gateway, etc. Then, the network card is initialized, the system connects to a share on the network, and begins the installation of NT Workstation. After NT has been installed, the system re-connects to the network share to further configure the operating system and install the standard suite of applications and relevant software updates. Once this process has completed, the administrator need only perform a few final steps, such as installing any non-standard software and setting up printer connections, before the system is ready to be delivered to the user.

3.2. Secure Version of Network Install

In the spirit of SLAC's open environment, NT systems configured with the Network Install are largely default installations in terms of security settings on the registry and file system. Because the level of security required for the new BSDnet is significantly higher than for the rest of the lab, a new, separate version of the Network Install was developed.

The BSDnet Network Install incorporates a number of changes to the system installation and configuration that increase the security of these systems. These changes include:

- Restricting access to system files and directories and sensitive keys in the registry
- Replacing access rights granted to the "Everyone" group with the "Authenticated Users" group
- Removing access rights for the "Guest" group
- Enabling and requiring SMB signing
- Disabling the caching of credentials
- Enabling BIOS passwords
- Removing Dial-up Networking and Remote Access Service components
- Clearing the pagefile at shutdown
- Disabling clear text, LM, and NTLM authentication

Security practices already in place with the existing Network Install, such as requiring NTFS partitions, disabling booting from floppy disks, disabling anonymous connections, requiring complex passwords, renaming the built-in Administrator account and including a legal notice at logon were continued in the BSDnet version of the Network Install. Microsoft Office 97 Service Release 2 (SR-2) and post-SR-2 patches were added, as were patches for Internet Explorer 4.01SP1 and Windows NT 4.0 Service Pack 4 (SP4) and several post-SP4 hotfixes.

Computer Associates' InocuLAN 4.0, and Microsoft Systems Management Server (SMS), Citrix Secure ICA and Security Dynamics ACE client software packages were added to the list of standard software installed by the BSDnet Network Install. InocuLAN was picked to replace the existing anti-virus software because of its greater ability to be centrally managed. The installation of the SMS client greatly enhances the manageability of the BSDnet workstations by allowing administrators to troubleshoot systems remotely and automating the deployment of software updates.

Installation of the ICA client on all BSDnet workstations enables business system users to access PeopleSoft through the Windows Terminal Server farm from any BSDnet workstation, not just from their primary workstation. The Security Dynamics ACE client software is installed but dormant on all BSDnet workstations in preparation for the migration to two-factor token card authentication in the future.

The existing 200 workstations had to be re-installed using this secure Network Install. Most of this was done by a small team of NT administrators during after-office hours when the users were not using their workstations.

3.3 Compatibility with Lab Environment

The addition of the new security enhancements to the Network Install required significant testing and debugging. Requiring SMB signing and disabling all but NTLMv2 authentication initially created connectivity problems with NT servers in other parts of SLAC that had not been configured to enable these security enhancements. The result was that the standards for the rest of the lab were also raised.

Requiring SMB signing does not work with Macintoshes, Linux and other operating systems and services. This was an issue for users who rely on Samba or Transarc AFS client to provide connectivity to UNIX file systems. For these users, one of the SMB signing registry keys (HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Rdr\Parameters) had to be changed to not required.

Tightening the registry and file system ACL's proved to be particularly complicated, as most applications do not list the minimum access requirements they need in order to function properly. Application failures required numerous adjustments to the file system and registry ACLs, some of which created new failures that had to be fixed as well. Security scans revealed vulnerabilities that had been missed, which then had to be closed. Software standardization of the 'BSDnet' workstations also allowed for conversion from local to roaming profiles, which entailed further testing and troubleshooting.

The experience gained from developing and testing the 'BSDnet' Network Install security enhancements has enabled the incorporation of some enhancements into

the standard Network Install used by the rest of SLAC. This resulted in increasing the security of all of SLAC's NT systems while maintaining an open environment.

4. Other Issues

4.1 Remote Access (RAS/RRAS)

The routers were programmed to accept only Secure ICA connections from the BSD network to the MetaFrame servers. This prevents an unauthorized user from accessing the secured application set from any other segment of the network or the Internet.

For off-site access to the secure application set, users are required to use a 128-bit RC5 PPTP connection to a designated PPTP server, that provides the users with a BSD subnet address which will in turn allow a Secure ICA connection to the MetaFrame farm. PPTP-based access to the BSD subnet is filtering by the router that borders the SLAC network and the Internet. The router only allows the port (TCP 1723) and the underlying protocol (Global Routing Encapsulation (GRE) IP 47) to the BSD PPTP server and one other SLAC PPTP server. All others forms of off-site access have been blocked to add to the security of the BSD network.

4.2 Eliminating Reusable Passwords

In recent years, SLAC and Stanford University has experienced several publicized intrusions. In a few cases, the crackers comprised thousands of user accounts. Therefore, the NT and security staff reviewed the standard practice of reusable passwords in the BSD network. US Department of Energy's Computer Incident Advisory Committee (CIAC, www.ciac.org) has repeatedly stated that reusable passwords are the "weak link" in security at most DOE sites. The solution was to implement a two-phase, non-reusable password authentication system based on Security Dynamics Corporation's ACE/Server.

The use of two-phase authentication involves a user-defined pin code and a computer algorithm generated tokencode. Combining the pin code and the token code makes a single use passcode. Transmitting this passcode over a RC5 encrypted channel and using Microsoft's latest authentication hash, NTLMv2 provides a very high level of security for the username and passcodes. Even if an unauthorized user were to intercept the authentication packets, they would be forced to first decrypt session channel provided by Secure ICA, second decrypt the NTLMv2 hash to reveal the passcode then it would only provide an already expired passcode.

4.3 Network/System Intrusion Detection

In order to identify potential attacks against the BSD and BSD-EPN networks, SLAC is using the ISS RealSecure product to monitor the network for attack signatures. Since these networks are relatively closed, the attack signatures are set at lower thresholds than what might be acceptable on other, more varied, networks. On a system level, ISS System Scanner is used to detect changes to the system, and provide alerts.

5. Conclusions

Using MetaFrame servers meant the PeopleSoft and related applications ran on the NT Servers, not on each client workstation. This allowed for every module within the business application suite to be configured by an administrator. Once configured by the administrator, the application interface was "pre-configured" for the users when they logged into the application servers. Several benefits in configuring applications on MetaFrame:

- Fully encrypted 128-bit RC5 client connection using Citrix's MetaFrame Secure ICA client
- Administrator configured applications that presented a single, well-defined, secure application environment to every user.
- Provided a limited number of systems to monitor for suspicious activity. Since the applications only run on the server farm, only a limited number of NT systems actually contact the database servers over the standard SQL connection (TCP port 1521).
- Ability to "hide" connections by manually selecting a non-standard port(s) to connect the Secure ICA client to the MetaFrame servers. Sniffing standard connection ports, such as NetBIOS over TCP and the published Secure ICA would not provide information to a would-be cracker.

A filtering router blocked all normal access to the PeopleSoft application and direct connections to the database servers via SQL. Only secure shell access and client connections originating from the MetaFrame application servers are now allowed through the router. Any connection attempts through router on ports other than secure shell and Secure ICA are dropped and logged for later review by the networking and/or security groups. This prevents all but the most hardened

security threat from accessing the applications and database deemed secure by this project.

All of the MetaFrame servers were placed in an Extremely Private Network (EPN) with limited access within the EPN and limited access from BSD. All ports that were not used with the secure clients or designated host-to-host connections were blocked.

All systems within the BSD network are Windows NT Workstations 4.0 with a minimum of service pack 4 and several hot fixes. Each system on the BSD network was rebuilt using a specially configured boot floppy process. Each system was erased and loaded with a new; administrator configured version of NT Workstation and a list of standard applications for the desktop. In addition, the Secure ICA client and the Microsoft Point-to-Point Tunneling Protocol (PPTP) client were added to the managed workstations. These secure clients provide 128-bit RC5 encrypted access to the BSD subnet and to the EPN and the MetaFrame servers.

Work supported by Department of Energy contract DE-AC03-76SF00515; SLAC-PUB-8172

Acknowledgements: The work was performed by a collaboration from SLAC's NT Support Group, Security, Networking, Database Support, Web Support, UNIX Systems Group, PeopleSoft Developers and countless "BSDnet" users and SLAC users who gamely or sometimes un-gamely "collaborated" with us. Steve Chadly of Streamline Associates provided invaluable advice and scripts for running PeopleSoft applications in the MetaFrame environment.

SLAC Windows NT Web Site:
http://www2/comp/winnt/winnt.htm