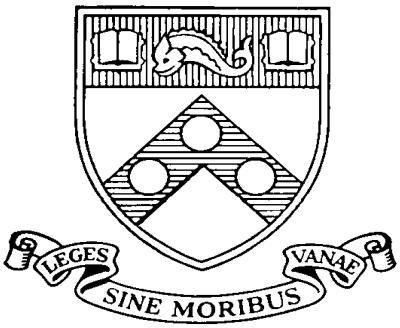

University of Pennsylvania

CAUSE 95

Assessing Risk: Developing a Client/Server Security Architecture

November 22, 1995

Dave Millar, University Information Security Officer (millar@isc.upenn.edu)
Noam Arzt, Director Information Technology Architecture (arzt@isc.upenn.edu)
Bill Ramirez, Systems Programmer (ramirez@isc.upenn.edu)

Introduction

The University of Pennsylvania's new Data Warehouse and Financial Systems are exploiting technology to bring to Penn flexible new ways to organize and manage data, making it readily-available for both operational and planning needs. Along with the benefits of the new technology, however come risks which the University must address to ensure the integrity of its information assets. The decentralization of data and computing, and the use of open networks, open systems and open standards exposes Penn to new vulnerabilities. Penn can no longer rely on the use of obscure operating systems and networking protocols to protect our systems and our information.

The Client/Server Security Standards Task Force was created to identify the threats to information security posed by the new technologies being adopted for the Data Warehouse and Financial systems. This report documents the threats which the group feels are most serious, and provides a rationale for the group's recommendations.

Bringing Together the Right Players

As Penn planned the implementation of Oracle-based Financial Systems and the Data Warehouse, it was apparent that careful thought would need to be given to how to assure the security of information in the new technical environment. For that purpose, the Client/Server Security Standards Team was formed, with the following mission:

> *Ensure that as Penn moves from mainframe-based computing to distributed, client/server computing, it can ensure the security of administrative systems and data.*

Care was taken to ensure that other planning efforts were taken into consideration, and were involved as necessary in the task force's work (e.g., campus-wide Distributed Computing and Network Architecture task forces).

Scope

Figure 1 shows that the initial focus of the team is on the implementation of Financial systems and the Data Warehouse; subsequently, attention will be given to the broader implications for administrative computing University-wide. The first phase of the Data Warehouse application was implemented in December, 1994, and additional phases will be implemented over time. Additional modules of the new Financial System are expected to be available in July of 1996.

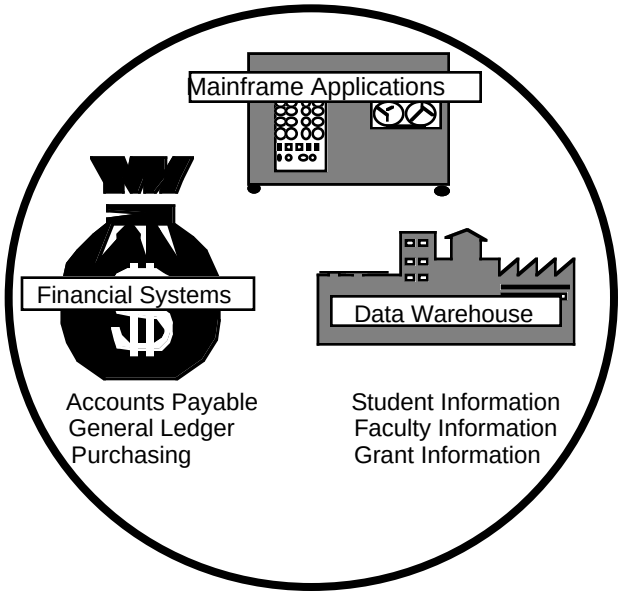

Figure 1 - Scope

While the group's charge did not initially include mainframe computer applications, the group came to believe that the following mainframe security issues should be included in the project scope:

- *Sniffing* To the extent that ethernet is used to connect to the University mainframe (about 40% of all mainframe connections), the legacy applications are no more immune to password or data sniffing than the new Financial Systems and Data Warehouse applications running on the server. Any data which travels over ethernet is subject to sniffing. The team felt that while the primary focus of the group is solving the problem of sniffing for the Financial Systems and the Data Warehouse, consideration should be given to how such solutions may apply to mainframe applications.

- *Single Sign-on* The new Financial and Data Warehouse applications will create new accounts and passwords for users to remember. The team felt that any recommendations for strong user authentication must include an assessment of the costs of mainframe integration, permitting a single sign-on for administrative system users.

Technical Environment

The technical environment for Project Cornerstone consists of a large, multi-processor Unix server connected via the campus' baseband enterprise network to a variety of desktop computers. Users will either connect via Telnet , or by making a client / server connection to an Oracle server using Oracle's proprietary SQL*Net client / server product via the TCP / IP protocol. Data will be exchanged between the Unix server and the mainframe. Financial system implementation plans and timing are presently under review.

Methodology

The team took the following approach to fulfilling its mission:

1. Survey other institutions for information
2. Identify trends in information security technology and practices
3. Identify the information assets we are trying to protect.
4. Identify the threats to those assets. Who might the actors be? How might threats be carried out? What are the implications of the threats.
5. Rank all of the threats. Consider only those threats which are credible and which could inflict significant harm to the University.
6. Validate the threat analysis with a knowledgeable focus group
7. Develop solutions to the credible/harmful threats.

Information from Other Institutions

Based on an informal survey conducted by Penn State in the Winter of 1993/1994 and reported verbally to members of College and University Information Security Professionals (no written report available) of eight private and five state educational institutions:

- 77% of the respondents have not updated their policies to address the migration to client/server architectures.

- 38% of the respondents require that all backbone-attached devices must have User ID/password or other authentication mechanism.

- 54% of the respondents are planning to migrate to more secure authentication mechanisms than passwords - rated from most to least important: Kerberos, tokens, encryption, signatures, DSS.

- 54% of the respondents required badging or card systems to gain physical access to telecommunications installations.

- 24% of the respondents are now using tokens or smart cards.

- 54% of the respondents are employing a firewall on at least some systems/networks. The effectiveness of firewalls was ranked as somewhere between "effective", and "somewhat effective" (the choices also include "ineffective").

- 77% of the respondents are not encrypting data in local LAN environments.

- 24% of the respondents are encrypting data between buildings and facilities.

- None of the respondents are encrypting data over WAN communication links.

Based on informal discussions with peer institutions, the following themes emerged:

- Some institutions which continue to run their administrative computing over SNA or similar proprietary protocols have not had to face the security challenges of open systems computing and may choose to wait for the solutions to catch up to the problems before wading in.

- Of those institutions facing the problem of open systems, client/server computing, many applications are still in their infancy, as are the solutions to the corresponding security problems. We spoke to a large number of organizations that were conducting limited studies or pilots, or limited implementations of security solutions. Concerns expressed about the solutions included scalability, performance, and the long-term viability of the solutions given confusion over what standard(s) will emerge.

Trends in Information Security Technology and Practices

The following trends were identified:

- Movement away from re-usable, plain text passwords to one-time and/or encrypted passwords using the following technologies:

    - DCE/Kerberos
    - Authenticator tokens
    - S/key - one time password algorithm
    - Public key digital signatures backed up with proof of authenticity "certificates"
    - Digital signature (and encryption technology) embedded in hardened PCMCIA-compatible smart cards: e.g. Fortezza card.

- Movement away from embedding security features (authentication, encryption, non-repudiation) in high-level applications (e.g. PGP, Kerberos) to lower, more pervasive levels in the Internet protocol, making security more transparent to users:

    - Secure Sockets Layer (SSL) from Netscape
    - Private Communication Technology (PCT) from Microsoft
    - SKIP (Simple Key Management for Internet Protocols)
    - Internet Protocol version 6

- Increasing use of firewalls

    - External firewalls

    - Internal firewalls
    - "Private" internets with firewall address translation

- Network-based tools for auditing host security

    - SATAN
    - ISS
    - Pingware

- We found no single, unified and comprehensive solution to the security problems posed by client/server computing in the heterogeneous technical environment we face. Organizations working on these problems are probably best served by accepting that problems may have to be solved on a piece-meal basis with solutions that may be obsolete in less than two years.

Assets and Threats to Those Assets

Figure 2 shows some of the assets that the Client/Server Security Standards team was charged to protect, and the threats against the assets. Information and infrastructure assets are at risk from threats which may originate either from within Penn, from the outside Internet, or which may simply be the result of an accident. The group was charged with developing recommendations for solutions to protect against the most credible and harmful threats.

The project team developed a complete list of the threats to the information assets. These threats were divided into three categories: **threats against the desktop** (7 identified); **threats against the server** (15 identified); and **threats against the network** (8 identified). A rationale was then articulated to explain the team's reasons behind its assessment. Finally, the threats were ranked along two dimensions: the **likelihood** that the threat might take place, and the **harm** that would be experienced if it *did* take place. Both these rankings were done on a "high/medium/low" scale.

The most credible and harmful threats include the following (rationale follows in italics):

1. Desktop Computer Data Disclosed: *Someone discloses sensitive information (e.g. payroll information, student grades), which was obtained without authorization from a desktop computer. As more data is available to be downloaded , and as it becomes easier to download, this risk will increase.*

2. Desktop Computer Data Altered or Destroyed: *Either intentionally (someone gains unauthorized access to a desktop computer) or unintentionally (hard disk crash, flood, fire, accidental file deletion by the user) , data is altered or destroyed. Since altered data is difficult to detect, it presents a special threat.*

3. Passwords Compromised by "Trojan Horse" Program on Desktop: *A "Trojan Horse" is a program that performs unknown, and unexpected as well as expected tasks. It is either placed on a system without the owner's knowledge, or it is placed there by the owner, ignorant of any harmful effects. One example is a program which logs the user onto a system (expected) while at the same time storing the password in a hidden file (unknown, unexpected) for later collection and illicit/inappropriate use.*

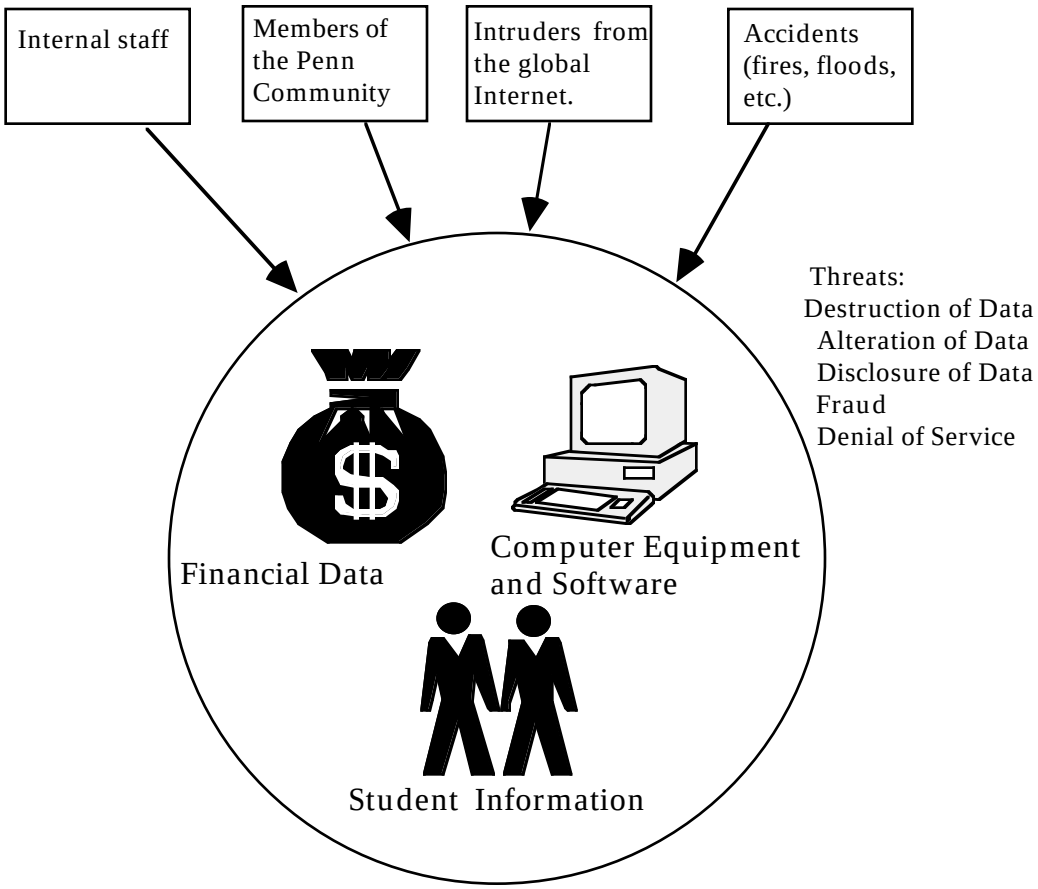

Figure 2 - Assets and Threats

4. Users Logged in on Unattended Desktop Computer: *Anyone who comes upon an unattended desktop computer , which is logged onto a server application, has all of the privileges of the user. This problem may become worse as the client/server architecture eliminates the incentive to sign off of mainframe applications to save on connect time charges.*

5. Employee Fraud/Sabotage: *Data or programs are altered, disclosed, or destroyed either by a properly-authorized employee abusing his/her access privileges or by an employee who obtains excessive access privileges. Such incidents are more common during restructuring/layoffs.*

6. Improperly Protected Server Accounts Used to Gain Access: *Privileged accounts on the server (those with broad capabilities normally only given to system administrators) are targets of intruders for obvious reasons. Poorly protected user accounts , though less powerful, also make tempting targets, since they provide a toehold to gain further privileges. Poorly protected accounts include those with easily-guessed passwords, or no password at all, accounts held by users who write down or script their password for easy sign-on, and dormant accounts belonging to inactive users. An intruder on a server can disclose sensitive information, destroy or*

alter data or programs, and leave behind hidden programs which steal passwords from unsuspecting users of the system, and which make future intrusions easier.

7. Intruder Exploits Server Vulnerabilities to Gain Access: *New security vulnerabilities in the Unix operating system and in Internet network services appear almost weekly. Detailed scripts for how to exploit these vulnerabilities are circulated widely within the hacker community, and patches to fix the problem are sometimes not available from vendors for months.*

8. Privileged Employees Accidentally Delete or Alter Data or Software: *In performing their duties, an application system administrator, a production control employee,, DBA or system administrator accidentally causes harm.*

9. Server Destroyed in an Accident: *Leaking pipes, power failures and equipment failures are not uncommon.*

10. Address Spoofing: *Someone spoofs network addresses to gain access to servers, and uses that access to read/alter data or set up future access. Someone "spoofs" a network address by using their host computer to "impersonate" a trusted computer, thereby improperly gaining special permissions and access that only the trusted computer should have.*

11. Sensitive Data Disclosed Through Packet Sniffing: *Someone uses a packet sniffing tool (software which allows a computer connected to the network to view data intended for another host computer on the network) to read sensitive data being transmitted over the network.*

12. Accounts Compromised Through Packet Sniffing of Passwords: *Someone uses a packet sniffing tool to capture accounts and passwords providing access to the server. In Spring, 1994, the Computer Emergency Response Team reported a high incidence of such attacks, including compromised accounts numbering between the tens and hundreds of thousands. CERT recommends that organizations stop sending unencrypted passwords over the network and move to encrypted, one-time password authentication schemes. Extensive harm could done with unauthorized access to numerous users' or system administrators' accounts.*

13. Network Unavailability: *Network connectivity unavailable due to accidents such as fiber cuts, flood, fires, power outage, etc.).*

After these threats were developed and articulated, a campus-wide focus group, consisting of both information technology professionals *and* functional managers responsible for the management of processes that use the information assets being protected, reviewed the threats and rankings in detail and suggested changes and additions.

Proposed Solutions

The following solutions were developed and proposed to try to mitigate the serious threats detailed above:

Policy: A comprehensive administrative information security policy should be developed which defines the information assets that the University wishes to protect, and defines the responsibilities of both computer users and computer administrators to ensure protection of those assets.

Server Protection: It is recommended that University administrative computing servers be protected by a firewall. This would allow Penn to better control how they are accessed and used.

Password Hardening: The Kerberos network authentication service was recommended for users of the Data Warehouse and Financial applications. A fair amount of time was spent looking for, testing, and evaluating Kerberos servers and client software. The project team was concerned about vendor support for these products, so commercial versions were evaluated wherever possible. In the end, the team was disappointed by what it found. Commercial products did not have even the most basic features required for a large-scale implementation among a wide range of users.

It was additionally recommended that privileged users will be required to supplement their Kerberos authentication with token authentication. In addition, some users unable to use Kerberos authentication (primarily due to insufficient desktop resources) will instead be required to use a token to authenticate themselves. A token generally uses either a challenge/response algorithm, or a clock-driven algorithm to create one-time passwords, which can not be re-used later, even if they are disclosed by network sniffing. A token authentication server provides token authentication services for the server.

The project team tested the SecureID token extensively and found that it met the project's needs for supplemental authentication. Given the poorer results finding Kerberos-enabled software, consideration is being given to wide-spread deployment of a token card to reduce password exposure even though it does nothing to enable data encryption.

In addition, warehouse users would be required to select strong Oracle passwords using the Braintree SQL*Secure software.

Data Encryption: An additional feature of Kerberized telnet products is the ability to encrypt the full stream of data during a telnet session. Since initially most users will be accessing the financial applications via telnet, this feature is highly desirable. Once again, however, the team could not identify products (commercial *or* public domain) to support these functions to their minimum specifications.

The warehouse users are accessing using client/server products. Oracle's Secure Network Services product is a piece of the Oracle product family that layers on top of SQL*Net and provides end-to-end data encryption with no modification of the client or server application. The project team hopes to deploy it as more financial applications migrate from host-based to client/server.

Desktop Computers: Users storing sensitive data on their desktop computers will be required to protect the data using desktop access control and encryption software unless the computers are otherwise physically secured. Policy should be developed to define the terms and conditions.

Lessons Learned

Be precise with scope: We faced a complex array of security issues to focus on. Product restrictions make it too difficult to select a single solution. Changing requirements blur the focus on the problem. All of the above factors combined demand constant focus on the scope of the project in order to limit the energy to the task at hand (securing the Cornerstone environment).

Stay on top of the vendors: Constant developments in products and technology offered requires constant review of available products that meet requirements. The configuration being secured differs from what other users implemented, hence the vendor requirements differ. This makes it hard to draw on the experience of others.

Limitations of Technology: The technology the project required is just not there yet. Products were usually inconsistent across vendors, and some product families were internally inconsistent. Limitations with the Kerberos components abound. On the other hand, new products are emerging constantly.

The process as an end in itself: Better understanding of how the tested security products work including their strengths and weaknesses. Increased awareness of network topology, network vulnerabilities, and Unix operating system vulnerabilities would be very helpful. The creation of the task force (made up mostly of technical people) and the focus group (made up mostly of business people) greatly increased the awareness of the risks of open systems and client/server computing. The process also helped introduce a risk management philosophy, informing business managers of the technical risks in terms they felt comfortable with. As a result, business managers responsible for applications and data are better able to determine acceptable levels of risk, and to make appropriate tradeoffs.

The recommendations have been presented to the project sponsors and have been accepted where there are products to implement them. Deployment of the firewall has begun. Use of token cards is still being assessed financially. Policy development will begin shortly.