



Case Study *Affordable IBM Midrange Software that makes you more productive*

Kisco's SafeNet/400 Secures the Intellectual Assets of Leading Educational Tool Developer

Historically, OS/400 Object Level security has been the benchmark of the computer industry. However, the rock solid architecture has been disturbed by recent changes to the iSeries computing environment that include the rapid proliferation of network connections, the facilitation of enterprise computing environments, and the addition of several new exit points for every operating system release.

There is cause to take note: The material losses suffered by companies who have had critical computer/data systems tampered with in unsecured environments are staggering. The Computer Security Institute, in conjunction with the San Francisco FBI's Computer Intrusion Squad, reported in March of 2001 that 85% of survey respondents associated with large corporations or government agencies had detected computer security breaches within the last twelve months. Furthermore, 64% acknowledged financial losses due to computer breaches. 35% of those respondents were able to quantify their financial losses resulting from system intrusions at \$377,828,700.



Computing Environment Changes Raise Concerns

Sunburst Technology has been using IBM midrange computers

since they were called mini-computers, starting with the System/32. Sunburst possesses a vast amount of hands-on experience with the platform, its applications and security architecture. Recent changes to Sunburst Technologies' enterprise computing environment raised concerns about system security as projected into the future.

Over the course of a several months, Sunburst replaced most of their twin-ax attached terminals

with Microsoft Windows based desktops and terminal emulation. That change created new security challenges from network access methods such as simple file transfer, ODBC, SQL, and DRDA. Linda Lettieri, Senior Programmer Analyst at Sunburst comments, "When we started implementing Client Access/400 and Windows desktops throughout the company, things changed dramatically." Like many companies, Sunburst's computer security strategy consisted of unique passwords and mandatory menus for the user community. Access was restricted by effective use of default menus. "The once closed environment of the AS/400 was now cracked open and potential security exposures were amplified," explains Lettieri.



Kisco Communiqué

By Rich Loeber

As the data processing environments of companies grow more diverse and complex, and reach beyond their internal information requirements, these systems grow more vulnerable to intrusions. To better serve the needs of IBM AS/400 and eServer, iSeries systems users, we have made several enhancements to SafeNet/400 in version 6, including better access controls, and we've introduced a new product to our suite of security solutions called ScreenSafer/400. Our objective is to make effective security solutions available to everyone, where the cost of implementation is not deterrent to effective security.

Sincerely,
Rich Loeber

For more information on SafeNet/400 and other Kisco software solutions, log in at www.kisco.com.

As the company moved away from SNA connections to TCP/IP, the added exposure from Telnet and FTP only complicated matters.

"When we started implementing Client Access/400 and Windows desktops throughout the company, things changed dramatically,"

Linda Lettieri,
Sunburst Technologies

Access restrictions based on menu controls and passwords fell far short of their security objectives. Virtually every desktop and remote session bypassed OS/400 security. Theoretically, any Sunburst employee could access any information on the system without being detected.

At Risk

Sunburst Technologies, a division of book publisher, Houghton Mifflin Corporation, creates innovative learning aids for the classroom teacher. One example is the PC/Mac based Math Arena product, an interactive game for multiple players that allows students to polish critical math skills. Sunburst relies on aggressive and sophisticated direct mail marketing to sell its products. The cornerstone of this process is their customer and prospect database. "Damage to this database would be catastrophic to Sunburst," according to Patti Glinski, Manager of Customer Information Services. "The company and its revenue goals would be severely impaired; some way had to be found to protect this crucial

asset," noted Glinski. The final straw that pushed Sunburst to look for a good permanent solution was the plan to connect the AS/400 to the Internet to support inexpensive telecommunication for their AS/400 programmers. With an Internet connection, all of the potential problems became greatly amplified.

Initial efforts to find a solution included investigating the use of IBM's exit point technology. Each data server function in the AS/400 provides for an exit point where custom programs can share data and functionality. Users can also write programs to block these exit points to enhance security. Sunburst carefully reviewed this alternative and shelved it because of the administrative overhead of writing and continually maintaining programs internally to keep up with new releases of the operating system and applications.

A search was then initiated for software from either IBM or a third party vendor. Lettieri's requirements for a minimally intrusive solution with simple installation and maintenance were compared with industry offerings including SafeNet/400 from Kisco Information Systems (www.kisco.com). SafeNet/400 is an AS/400 based-network access control system that uses the IBM exit points. Lettieri noted that Sunburst's current concerns were addressed both for securing their customer information and protection of other databases. Based on company claims, SafeNet/400 represented a very small footprint. Lettieri decided to take advantage of the free trial offer to assess the software's capability to close the holes

created by non twin-ax connected devices and other network connections.

Lettieri observed that installation of SafeNet/400 proved straightforward with one exception; it required an IPL. Rich Loeber, President of Kisco Information Systems explains, "Any product that integrates through exit points for any reason will require an IPL for installation. Since most companies have IPLs scheduled on a regular bases, we offer a flexible evaluation period to accommodate most companies needs." Once the initial installation is done, future release upgrades can be applied while the system is in Restricted State.

Lettieri noted that Kisco's delivery of new releases and fixes was as simple and straightforward as the installation procedure. New features introduced between release updates are available as PTF's that are delivered via e-mail along with bug fix PTF's. The Kisco website is kept current on changes to the product and provides information about the availability of new features and fixes.

"Damage to this database would be catastrophic to Sunburst. The company and its revenue goals would be severely impaired; some way had to be found to protect this crucial asset."

Patti Glinski,
Sunburst Technologies

After installing SafeNet/400, Sunburst then set it up in logging-only mode. This process allowed for a baseline of actual network

use to be built. After a few days, the access logs were checked to see who was accessing the system via network connections and what objects they were working with. Lettieri notes there were a few surprises that required management's attention. Most turned out to be illegal accesses to the system from Win 95/98/NT desktops that originated from curious employees and were deemed accidental. (Using current versions of Microsoft Windows and Network Neighborhood, the more adventurous user can click away at icons and gain unlimited access to what would otherwise be restricted AS/400 datafiles.) However, Lettieri mentioned a few instances in which employees were unable explain why they were working with restricted confidential files.

"Any product that integrates through exit points for any reason will require an IPL for installation. Since most companies have IPLs scheduled on a regular basis, we offer a flexible evaluation period to accommodate most companies needs."

Rich Loeber,

After running in logging-only mode for about two weeks, Sunburst took the next step, and locked down server functions on their AS/400. Each of the servers (there are more than 40 that SafeNet/400 controls) can be set to wide open (no restrictions, just logging), restricted by user, restricted by user and object, or closed (the server is disabled). Each current user's access

requirements were reviewed and rules were created for them within SafeNet/400. This was all set up prior to locking down the servers. Once all the users were set up, then the server levels were set to maximum protection and SafeNet/400 was fully activated.

At first, there were the usual missing rules and access denials that needed to be fixed. But once the initial missing access rules were entered, the number of calls to the help desk dropped off dramatically and the system was secured. Now, when SafeNet/400 detects an access violation the illegal access attempt is rejected, and SafeNet/400 automatically notifies several security officer user profiles so the infractions can be checked out immediately. If an access denial was made inadvertently, the rules can be updated on the fly.

With SafeNet/400 in place, Sunburst then looked to resolve the problem of Internet access for the programming staff that wanted to access the AS/400 from home. SafeNet/400 allows a Telnet session to be restricted so that only known IP addresses are allowed in. (The same rule holds true for FTP sessions.) Sunburst arranged for each telecommuting programmer to get their own IP address from their ISP and the rules were set up to allow only those IP addresses into the AS/400. A second problem came up with the sign-on sessions via the Internet in that the passwords coming in on the normal sign on screen were not encrypted. Using a feature of SafeNet/400, Sunburst was able to implement automatic sign-on, bypassing the need to

have an unencrypted password compromised.

SafeNet/400 Limits Access but Not Productivity
Sunburst is pleased with the level of added security provided by SafeNet/400. The original access problems have been resolved in a way that permits authorized users to get their work done while guaranteeing that unauthorized users will be kept out of restricted areas. The cost of telecommuting has also been significantly reduced since programmers no longer have to make long distance calls to a local controller to gain access to the AS/400.

Through this implementation, Sunburst's technicians learned much about how network connected devices access the AS/400 and are now conscious of its security shortfalls. There are several new connection points between users and AS/400 databases; visibility of these user connections is not always apparent. Implementing SafeNet/400 has shed a bright light on AS/400 network connections and has provided the controls necessary to elevate management's security comfort level.



**Kisco
Information
Systems**

344 Main St. Suite 204
Mt. Kisco, NY 10549
(914) 241-7233
Fax: (914) 241-9140
www.kisco.com
sales@kisco.com