DALLAS SEMICONDUCTOR

Application Note 98
A New Architecture for Distributed Security

INTRODUCTION
As PC LAN's become more popular for executing mission-critical applications, the issue of security is rising on many priority lists. Managing distributed information across many computers represents a real challenge when compared to the traditional centralized storage approaches, and until now there has been no real emphasis on security.

But the reality is that downswing efforts are in full swing and information managers are faced with porting their applications to potentially unsecured computer networks. Since no resources in the current PC configuration are dedicated to security, controlling access to the distributed data is much harder.

Two observations can be made when studying today's distributed security problems. Information managers need a cost effective scheme to control access to data, and software vendors need a cost effective approach to manage license distribution. Although these observations are under the umbrella of distributed security, they are separate problems.

DALLAS SEMICONDUCTOR'S DISTRIBUTED SECURITY ARCHITECTURE
Dallas Semiconductor offers a new technology called Buttons, which can be used as a basis for solving both data access control and license management problems. By solving both problems with the same technology, information managers can meet their own needs, and accommodate the needs of their vendors. In the process, the two solutions can co–exist without a major maintenance support effort.

The goals of the architecture then are as follows:

1. Provide a common medium which can act as a bridge for both solutions and to minimize incompatibilities.
2. Enable solutions for information managers and software vendors to be developed that can be offered at affordable prices relative to the cost of the PC.
3. Provide a path so that key pieces of the technology can be directly absorbed into the PC without forcing a major redesign or disrupting it's current pricing structure.

CONTROLLING ACCESS TO DATA
Information managers are often concerned with restricting access to data which is sensitive or critical to a business. Accounting data, transaction information, and certain product design information, all fall under this category.

Password Protected Schemes
Traditionally, this data has been protected by a simple password scheme, that a user requires knowledge of in order to gain access. Almost every mainframe or minicomputer-based software application requires a password for entry. The base assumptions that makes the password scheme effective are:

1. The data is stored centrally, in a controlled environment.
2. The operating system and (mainframe) hardware contain security hooks. The terminals deployed for users often had little or no independent processing capability.

Therefore, the number of feasible ways to gain access to the data was limited and controlled, so the password scheme was adequate to achieve reasonable levels of security.

Password Schemes No Longer Effective
However, the distributed topology changes the base assumptions:

1. No longer is the data centrally controlled.

2. The operating system used (i.e., DOS) contains virtually no security hooks
3. The terminal of yesterday has typically been traded for a PC, which has very powerful independent processing capability, and no security hooks.

These changes have opened access to the data in ways a simple password scheme can't effectively protect. The conclusion then is that a password only protection scheme can be easily defeated in a distributed environment.

Two-Level Authentication Now Required

In order to provide PC LANs with adequate security, adjustments must be made to the password scheme in order to compensate for the changes in the base assumptions. This paper advocates the addition of a hardware token, in addition to a password, be used to add possession to the criteria for access to data, in addition to knowledge.

Requiring possession is very powerful when compared to adding more knowledge, because a physically independent but related process must occur to gain access to the data. Additional passwords are not as effective, because the method essentially reiterates the original scheme. While it may increase the obscurity factor, it does not fortify the fundamental strength of the security, because it offers no solution for the problems created by the shift in the basic assumptions.

Two-level authentication is called in this paper "bring something, know something" security. It allows information managers to control the access to data because they can control distribution of the tokens, and yet manage their authentication centrally (at the LAN server), a controlled environment.

Using Buttons as a token in many cases removes the need for any security software to be resident on a client machine (or at minimum exposed for modification), and can be implemented independently from the host architecture or operating system.

Independence is the key to achieving adequate security, because a Button based scheme does not assume any security is provided by the operating system or PC hardware. Buttons provide solutions for the changes in the base assumptions, allowing the password to once again become effective for securing the data.

Bring Something/Know Something Traditionally Not Affordable

Two level authentication is not new. It has been attempted several times in recent years with little success. This is because the bring something part has been relatively unaffordable when compared to the cost per seat of the PC.

Security additions to mainframe systems were traditionally thought to be inexpensive, because the cost of implementation was incremental to the cost of implementing the system itself. Spending $100,000 for security represents only a 10% additional cost for a $1,000,000 mainframe system. However, spending $1,000 on PC security represents 33% to 50% additional cost when purchasing a $2,000 – $3,000 PC..

The massive decline in the cost per MIP (a measurement of computing power) that is in essence the very reason why the PC is becoming so popular, combined with the neglect of supplying security hooks in the PC, has left PC LAN security with only a handful of implementations. They are essentially ports from the mainframe topology, are expensive relative to PC pricing, and often awkward to implement. The neglect is a key issue, because it does not allow PC security solutions to emerge that can take advantage of the lower priced PC hardware.

The net result is that PC LAN security is often not affordable or not attainable. Lower priced PC security solutions have emerged recently, but they do not bring a substantial innovation that allows their security to integrate elegantly into the client server architecture, and only yield incremental security gains (most often inadequate for mission critical applications).

Button Based Bring Something Is Affordable

The key difference in architecting the Button based solution is that PC chip technology was utilized from the start. This enables Buttons and their readers to be sold at price points that are in line with PC price curves.

Buttons themselves are manufactured using the same semiconductor process used to make the PC chips themselves, so their manufacturing cost base is at the same level as the PC. In addition, economies of scale serve to lower costs over time as volume increases.

Another important feature that drives down cost is the innovation in 1–wire communication, pioneered by Dallas. Standardizing on a communication protocol, the functionality inside the Buttons can change without changes to their interfaces. This is an important feature for distributed security because it means that Buttons of different functionality can be distributed, and are compatible with the same Button readers.

The technology required to read and write to Buttons has also been dramatically simplified, because the communication work horse resides in the Button. To that extent, Dallas has engineered a reader solution that can be incorporated into current PC configurations for under $1.00 per PC, with virtually no impact to its design.

For the first time, PC vendors can absorb security technology into the PC hardware without requiring substantial premiums to resell the option. The elimination of the Button reader cost, coupled with its ability to be rapidly absorbed into the standard PC architecture, gives Button technology a tremendous advantage as a possible widely accepted standard. Effective security schemes can be introduced for very low costs.

Standardizing Button communication also allows today's Button based security schemes to take advantage of future Buttons products, because upward compatibility is maintained. Dallas Semiconductor plans over time to offer Button products to meet every security level that can be practically implemented using computer hardware.

Too Many Passwords

As a practical matter, downsizing does not often mean turning off the mainframe or minicomputer network and turning on the PC LAN. The reality is that the PC LAN is evolving into its destined role. For many companies, enterprise-wide computing means a conglomeration of PC LAN's and mainframe networks electronically hooked together, so that users can (somewhat) transparently access information from any system.

The consequence of hooking PC LAN's to older (legacy) systems is the rapid rise in the number of passwords which the user must remember in order to access the pieces of information from the different applications. In one sense, this is a product of the success of the password scheme, because the granularity of using password protection has migrated to the application level. As a result, many applications require their own passwords, and their authentication is independent of other applications that may exist on the same system.

The explosion of passwords is aggravated by the PC – LAN, which requires its own passwords, and typically allows users access to even more legacy applications, also increasing the number of passwords required. This phenomenon unfortunately places information management in a dilemma. Controlling access to data requires passwords, yet passwords themselves are making the networks harder to use.

Security is also compromised because to remember all the passwords, users write them down. This action weakens the security scheme, because the transfer of knowledge to an unauthorized user can become accidental..

While the computer vendors as a whole have been slow in offering solutions to this phenomenon, some progress has been made. In their defense, vendors must find a scheme which does not compromise any individual security, yet allows security management to be common across all applications. Since applications were not originally developed with this in mind, the problem is very complex.

Groups such as the Open Users Recommended Solutions (OURS) Security Task Force have brought together vendors and information managers to discuss these issues and provide practical solutions. Longer terms groups such as the Open Systems Foundation have worked with vendors to set future standards (such as DCE).

Dallas Semiconductor continues to participate in these activities. However, until these standards clearly emerge, Dallas SignOn^{TM} offers a solution today.

Dallas SignOn^{TM} is a Button based PC LAN security system that utilizes the simple concept of a centralized secure database for its authentication. This database (called the central repository) contains records that describe user access rights to files on the network. The record also contains Button ID's and login authentication information. Information managers can place entries in to the central repository and issue Buttons to users as a way of controlling login authentication.

The Button then becomes the "bring something" piece that is used with a password for login authentication.

The central repository also sets a foundation that makes additional passwords transparent to the user.

Application Programming Interfaces (API's) are available which allow either vendors or information managers to enter legacy system information into the central repository as part of a user's record, and provide security information to other applications during operation and transparently to the user. In this manner, the initial signon to the PC LAN can authenticate access to legacy systems without further user involvement.

The central repository concept is the key to relieving the users of multiple passwords. The implementation of a central repository is made possible by the Button technology, because login authentication has been raised to adequate levels.

For implementations which need extremely high security (often requiring the use of a cryptographic algorithms), future Dallas SignOn^{TM} updates will directly accommodate these needs. In addition, Dallas Semiconductor is actively working with key institutions and vendors who are implementing ticket based authentication schemes (i.e. Kerberos) in order to provide another migration path for Dallas SignOn^{TM}.

These ticket based servers typically require two procedures:

1. A procedure to authenticate a user in order to issue them a ticket for a service.
2. A procedure to access user information to help base its authentication.

The Button as a medium for user authentication represents a natural fit for ticket based authentication, because the foundation of the scheme is proper authentication of the user requesting a network service. Dallas Semiconductor is actively designing future Buttons to accommodate the ultra high security needs of such a token suited for this application.

The central repository also offers the database information required by ticket based security servers.

DISTRIBUTING SOFTWARE LICENSES

While information managers are concerned with access control to data, software vendor's are faced with license management issues. In centralized schemes, license management was far less complex. A central processor maintained the accounting necessary to control the number of concurrent users accessing the applications, and the sessions could be easily timed, because their effective execution was performed by the central processor.

However, once an application is distributed, it becomes more difficult to measure and control usage, because more than one CPU actually executes the application, and there is no way to accurately measure the individual execution of all processors on a LAN.

These issues pose a major challenge for software vendors, who make their living selling licenses. They manifest themselves in two areas, intellectual property protection and complex license management.

Intellectual Property Protection

Copy protection is really an issue of preserving the vendor's right to control use of the software. The mechanism most often used for authorization is payment of a license fee. Unauthorized use of the software represents a loss of revenue for the software vendor. As companies gear up for selling into a global economy, more and more emphasis is being placed on cost effective execution control in order to neutralize the variances in copy protection laws worldwide. In some cases, domestic use of copy protection products are already employed, because the value of the intellectual property is extremely high.

Copy Protection Can Be Expensive

A market has emerged for devices which basically offers a host–id for the PC. Software vendors can lock their software to a computer and effective control execution. Some of these products are called dongles.

However, since dongles essentially represent an external sub–system to the PC, there is a floor cost by which they can be offered. Traditionally, low price cannot afford to absorb the cost of the dongle (which resell for $20 –$50 each), and still retain enough profits to operate a business. Therefore, dongles often are not candidates for broad based solutions.

Button Based Protection Is Affordable By All Vendors

Today, Button based protection uses a Button and holder concept similar to a dongle. The Button functionality

is far superior to that of a traditional dongle, and typically cost less to implement (as an external subsystem). Therefore, Button protection on existing technology lowers the cost of implementing protection.

However, the real key to the Button solution is the absorption of the reader into the PC. Button Ready PC's represent a substantial shift in the floor cost for protection that is only realized by the elimination of the external subsystem hardware.

As information managers begin to purchase Button Ready PC's (to satisfy their access control needs), they are also in effect accommodating those vendors who use Buttons for intellectual property protection. If vendors can reliably assume a Button Ready PC is present at the customer site, they only need to absorb the cost of a Button (under $10 each) into their revenue stream to implement protection.

The end result is that any software vendor can afford intellectual property protection. To those who are familiar with the concept of the dongle, the inference is the eventual elimination of dongles (and Button Holders) from the security scheme.

License Management And License Server Technology

Another issue that becomes extremely complex for a software vendor in a distributed environment is supporting the varied license types now required. Since applications are potentially distributed across the LAN, the fundamental license structure must accommodate assigning the license permanently (fixed) or temporarily (floating). Management complexities arise as a result of the lack of sufficient tools to support license management (coupled wit h the lack of authentication capability as discusses earlier). And since the time source in the PC is user accessible (and can be changed almost at will), a guaranteed time source does not currently exist in a PC LAN configuration to meter use.

These issues have complicated license management. Several substantial efforts are currently underway to offer license server technology that in effect relieves the software vendor from managing the licenses at run time. By incorporating these servers (or requiring their presence on the customer system), varied license types can be administered.

The emergence of these license servers brings to bear the issue of authentication. Authenticating a user should be a natural part of the run time license process. In fact, many of the vendors offering license servers incorporate some form of authentication.

However, since the license servers themselves are distributed applications, they too can suffer from security breaches. This is why Dallas Semiconductor is working with the leading vendors to tightly couple Button solutions with license servers, and enhance the security of the license server software.

The requirement would be the inclusion of a Button Holder and Button attached (only to) the server that hosts the license server technology. If the server is Button Ready, the Button Holder is not required.

The other use for Buttons in these applications is the ability to introduce a tamperproof time source. Dallas markets a Button called the DS1427 which contains a real time clock. Having this resources available, license server vendors can build time based (metered) licenses into their portfolio of supported license types, knowing that there is a guaranteed time source that will ultimately determine the billings.

BUTTONS AS A COMMON MEDIUM FOR DISTRIBUTED COMPUTING

The above discussions expose several key messages with regard to the use of Buttons for distributed computer security:

1. The cost of technology has been sufficiently lowered to allow incorporation into a PC for little or no additional costs.
2. Having Button Ready PC's available lowers the implementation costs of data access applications for the information manager and license management applications for the software vendor.
3. Button Ready PC's benefit vendors and user of distributed computers.
4. The low impact of incorporating the technology presents a strong case for widespread adoption as an industry standard.

These messages show that the three objectives originally stated in this paper are met. In conclusion, the ar-

chitecture is very elegant, can migrate into the mainstream PC market with little engineering effort, and offers opportunity for the emergence of distributed security solutions that are both cost effective and reliable.

A Word About Physical Security

Efforts to use Buttons for physical security applications (building access, room access, parking lot access, etc.) are being undertaken by Dallas Semiconductor in parallel with its computer security efforts. The end objective is to someday merge the two applications, using the Button again as the common medium, so that one Button can authorize physical and computer access.