

MAGIC ACCESS CONTROL SYSTEM



The promise of the Internet or “Information Highway” is that information would be freely available to all Internet users. With the adoption of the Internet as the primary mechanism for commercial, industrial, medical, and government information transfer, realistic safeguards were required so that some information was only shared with authorized Internet users of this information. The definition of authorized users, however, expands and contracts based on corporate mergers and reorganizations, changes in government security policies, and new legislation defining the application of data access rights. This creates a dilemma for the designers of Information Technology and especially the designers and administrators of databases and large data repositories that are the core components of the technology supporting information access. How can Internet access to data within a database be effectively and efficiently controlled so that only authorized users have access while also allowing access rights to be expanded, contracted, and modified based on new operational and security requirements. This is especially difficult when information access requirements change suddenly and unexpectedly based on unforeseen events.

Such was the case for many Federal Government Agencies including the newly created Department of Homeland Security (DHS) that now had to find a way to effectively share sensitive data from many database sources as a result of the events of September 11th 2001. This is an extremely difficult problem when these legacy databases and repositories were never designed to allow secure interagency access and information sharing to the degree required by the new environment. The same problem exists at a lower level of urgency for corporate entities that want to expand remote information access to corporate partners or merged companies; financial institutions that wish to provide customers with new services requiring expanded data access; organizations that must expand data access based on legislation such as the Freedom of Information Act or restrict it based on proprietary or privacy rights.

The Multi-Category Access Guardian for Internet Communications (MAGIC) Access Control System developed by Secured Processing Inc. (SPI) under U.S. Patent No. 7,134,022, provides a low cost and low risk scalable data access control solution to this problem. It supports changing access requirements for existing relational database systems without requiring any modifications to the data, database structure, database hardware, software, or operating systems, or database user or administrator operations. In effect, this technology can be used in a transparent manner with any Relational Data Base Management System and any operating system and can be used to define access requirements for up to 65,535 categories of data and as many as 256 security levels. In addition, the MAGIC Access Control System is based on a well known and stable access control technology defined in Federal Information Processing Standard (FIPS) Publication 188, “Standard Security Label for Information Transfer” that is compatible with and transparent to the operation of Public Key Infrastructure (PKI) and IPsec Virtual Private Network (VPN) Systems.

The MAGIC Access Control System provides a transparent client-server access control system for controlling network access to a legacy database with multiple sensitivity level/category access requirements based on a remote users access rights and the access requirements or sensitivity attributes of the stored data. A drawing of the conceptual MAGIC Access Control System with a multilevel and multi-category labeling capability is shown in FIGURE 1, below. The depicted system is comprised of a Remote Client (1) with a network interface to a Label

Server (4) that is directly connected to a Database Server (2). The Remote Client includes the client labeling system software that generates user labels from user identification data provided by the Smart Card Reader (9) and also inserts them into the IP Header of data packets directed to the Label Server. Depending on the mode of operation of the Data Labeling System, user labels could also be stored within the Lightweight Directory Access Protocol (LDAP) Server (8) or a User Label Database (6) within the Label Server. Data labels are either generated by the Label Processor (7) from the accessed data records within the Database Server or are accessed directly by the Label Processor from the Data Label Database (5). A Firewall (3) is not part of the conceptual system but is shown as a possible security protection system for the Label Server and the Database Server.

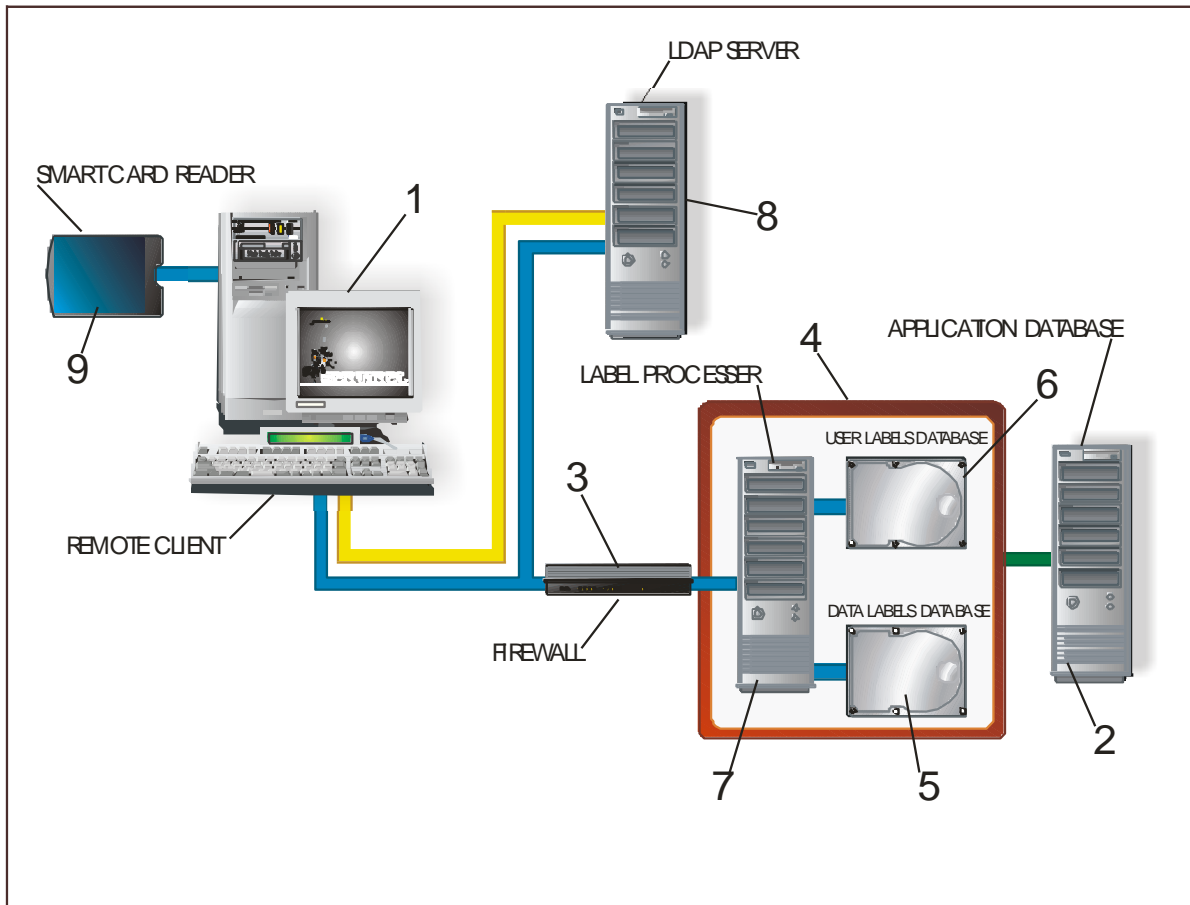


FIGURE 1. Conceptual MAGIC Configuration

There are several possible modes of operation for the MAGIC Access Control System shown in FIGURE 1 that utilize a subset of the depicted components. In the first mode of operation a user's data access attributes consisting of a digital representation of their access category and sensitivity level rights would be stored on their Smart Card or an equivalent user token. The Smart Card would be read by the Smart Card Reader, which would provide this data to the client labeling system software for conversion into a user label. To ensure that the user is actually the owner of the Smart Card, an Identification and Authentication (I&A) process will be implemented by the client labeling system software installed as an application on the Remote Client. The I&A process would require the user to enter a personal identification number (PIN) and password from the keyboard of the Remote Client that matches the values stored on the

Smart Card. Additional security could be provided by storing these values on the Smart Card as encrypted values that would be decrypted by the client labeling system software within the Remote Client. An additional security option would be to replace the entry of a password with user biometric data such as a fingerprint representation read and verified by a fingerprint reader system installed on the Remote Client. These security options are practical enhancements that are not part of the operation of the conceptual system

The user label can be any acceptable digital format as long as it supports the security attributes of potential users including the number of possible user sensitivity levels and data access category rights. A user label format must also be consistent with the data label format assigned to the data stored within the database server. This would require the label format to also support the number of possible sensitivity levels and data categories for the data within the database server. It is also desirable for the label format to be a recognized standard so that all remote clients can use it. The FIPS 188 Publication defines a standard label format for label types that support up to 256 sensitivity levels and 65,535 data categories.

The client labeling system software will open a Raw Socket and provide the generated user label to a Packet Editor in an Intermediate Driver. This driver will need to be developed as a Windows compatible Network Driver Interface Specification (NDIS) Intermediate Driver as defined in the Microsoft Developer Network (MSDN). The NDIS Intermediate Driver will be located between the NIC Driver below and the Transport Driver Interface, above. Its packet editor will copy the user label into a buffer for insertion into IP Headers of packets that are outbound to the Label Server. The Intermediate Driver will be responsible for filtering all outbound client packets based on the destination IP of the packets. If the packets are heading for the Label Server, the created user label will be added to the options field of the IP packet header. In order to perform this function the NDIS Intermediate Driver will be designed so that it can be layered over NDIS NIC drivers and under the Windows Applications, Network Protocol, and Transport Driver Interface layers, respectively. When the Intermediate Driver receives packets from an underlying NIC driver, it communicates with the above Protocol Layer Driver to determine if the Destination Address is that of the Label Server stored in the Windows registry. If the Destination Address is the Label Server, the stored user label will be inserted into the IP header. This allows the Intermediate Driver to monitor all outgoing packets and determine which packets will require the insertion of the user label.

When the data packets are received at the Label Server shown in FIGURE 1, the user label is extracted and stored in a buffer by the label processor. The Label Server passes the SQL queries to the Application Database within the Database Server for processing the data request. Data that is retrieved based on the data request is sent from the Database Server to the Label Server via a direct network connection through a dedicated line. When the retrieved data is received at the Label Server, it is immediately processed by the Label Processor to first determine if the retrieved data has a pre-assigned data label that is stored in the Data Label Database. The Label Processor will compare a predetermined attribute(s) of the retrieved data record with index data in the Data Label Database to determine if there is a link or relationship between a pre-assigned data label and the retrieved data. If there is no pre-assigned data label the Label Processor will utilize attributes of the accessed data record to directly generate a data label based on programmed algorithms.

The Label Processor will compare the stored user label with the stored or generated data label to determine if the accessed data can be transmitted to the Remote Client or if access will be denied. In the case of data labels that have a sensitivity level component, the user label must have a sensitivity level equal to or higher than the sensitivity level of the data label for access to be allowed. For data labels with a category component the user label must have the exact same category as the data label for access to be allowed. In those instances where the data label has both a sensitivity level and category component both of the above conditions must be met for data access to be allowed. If the Label Processor determines that access is allowed, the retrieved data will be transmitted to the Remote Client in a datagram with an IP Header that includes the destination address of the Remote Client. The required TCP/IP services will be provided via the socket interface of the Label Server operating system. If data access is denied a standard denial of access message will be sent to the Remote Client from the Label Server.

There is a variation on the first mode of operation that would use an LDAP Server to store the user labels instead of a Smart Card. In this second mode of operation the user could utilize a similar I&A procedure to that used in the first mode of operation to authenticate to the Remote Client shown in FIGURE 1. The encrypted I&A data stored on the user's Smart Card will be read by the Smart Card Reader of FIGURE 1 and decrypted by the client labeling software as was done in the first mode of operation. In addition, the user will also authenticate to the remote client to the LDAP Server by having the client labeling system use the socket interface of the Client Operating System and the services provided by the TCP/IP Stack to generate a datagram with the user I&A data and a data retrieval request for the user label matching that I&A data. The LDAP Server of FIGURE 1 will respond by sending the requested user label to the Remote Client 1. At this point the retrieved label will be processed by the client labeling software in the same manner it was processed when it was read from the user Smart Card in the first mode of operation. To secure the authentication process with the LDAP server, the data packets with the I&A data should be encrypted. If Public Key encryption is available as part of a Public Key Infrastructure (PKI), authentication to the LDAP server could be implemented via PKI user authentication.

The LDAP Server of FIGURE 1 provides an alternative source of user label data. It could also provide the primary source for those users who do not have a Smart Card. Such users could authenticate themselves through the entry of a PIN via the keyboard of the Remote Client 1 and a password or biometric data via the keyboard or a biometric sensor, respectively. This I&A data would then be compared by the client labeling software with the known user data stored within the Remote Client. Once the authentication was successfully completed, the I&A data would be used to authenticate the user to the LDAP Server and retrieve the user label as described above.

A third mode of operation that is very different from the first mode completely eliminates the need for the Intermediate Driver software at the remote Windows Client. In this mode of operation the user would authenticate directly to the Label Server using the same procedures used to authenticate to the LDAP Server including the possibility of using PKI. The authentication would be performed at the beginning of the user session with the client database application and the user I&A or PKI data would be used by the Label Processor within the Label Server to extract a user label stored in the User Label Database depicted in FIGURE 1. This user label will be stored for comparison with the data label that results from the database access

request in the same manner described in the first mode of operation. All other operations would be the same as the other two modes.

The MAGIC Access Control System is oriented towards controlling access rights to data in data repositories and not toward securing the data being accessed. In addition, the system design is based on a traditional method of authenticating users via a PIN and password at the client interface. However, one of the common characteristics of all three modes of operation is that the design is compatible and transparent to technologies that provide both user authentication and data protection capabilities such as the IPsec VPN and PKI technologies. This will allow the system to be coupled with any IPsec VPN for the protection of data transmittals to and from the Label Server. In addition, PKI and its utilization of Smart Card technology is also compatible with the MAGIC Access Control System design and can be coupled with the database application to provide strong user authentication between the client hardware and the label server. The overall result is a complete solution to controlling data access to shared data repositories while also securing the data being accessed and authenticating users to the data repository.