The 6th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, December 02-03, 2011

EMBEDDED SECURITY IN INDUSTRIAL MONITORING/CONTROLLING APPLICATIONS FOR MOBILE DEVICES

Professor, PhD eng. Daniel SORA

Regional Department of Defense Resources Management Studies, Brasov, Romania

Abstract:
Handling sensitive data often brings up security questions. Who should have access to the data and to which parts? Should everyone be able to modify the file or database? By defining the system needs up front, engineers can choose tools to help them to do this. LabVIEW with the Mobile Module enables engineers to define user profiles that limit access to different specific user interface controls on the application, as well as to different and sensitive sections of the data. This article describes the functionality provided by the LabVIEW Mobile Module to facilitate the implementation of security for LabVIEW project libraries, shared variables and front panel objects. This article also discusses how the security architecture separates user management and authentication from resource permissions.

Key words: *security, automation systems, mobile devices, monitoring and controlling.*

1. Introduction

The LabVIEW Mobile Module provides a set of powerful tools to facilitate security for LabVIEW project libraries, shared variables and front panel objects located on local and network systems. Security functionality is divided into two categories: user management and authentication, and resource permissions. User management and authentication is provided by the Domain Account Manager, so the developer can store all user information in a centralized location. With this architecture, distributed systems can access a single location for user information instead of storing the accounts on each computer. The Domain Account Manager also manages user authentication so distributed or networked systems do not need to implement the functionality themselves. The user information provided by the Domain Account Manager is used by LabVIEW project libraries, shared variables and front panel objects to assign permissions.

Distributed data logging systems have the most extensive lists of best practices:

- Reliable, efficient data storage
- Efficient tools for managing system-wide data
- Real-time and historical viewing of the entire system
- The ability to configure and log alarms and events
- Easy networking for different types of devices
- User interface security

2. Domain Account Manager

The LabVIEW 8 Mobile Module introduces the Domain Account Manager, which provides a more flexible, mature, and robust security solution than earlier versions. The Domain Account Manager serves as a central repository for managing local and remote user authentication and account management. You use the Domain Account Manager to create users and user groups, each with different privilege levels. Users can be added to any number of groups. This arrangement simplifies the process of assigning permissions to local and networked LabVIEW resources. Instead of having a single computer implement user authentication and store user or group information, individual computers communicate with a Domain Account Manager located on a remote computer. This remote computer then determines which users are trying to access a resource and to which group each user belongs.

3. Implementing Security with the LabVIEW Mobile Module

To launch the Domain Account Manager, select **Tools»Security»Domain Account Manager** from the pull-down menu in the project manager. In the Domain Account Manager, shown in Figure 1, right-click the **My Computer** icon and select **New Local Domain** from the shortcut menu. Then, enter a domain name and create an Administrator password. The Administrator is the default user that can add or remove users and user groups, change user permissions, modify user passwords, and so on. This functionality is limited to the Administrator and any users in the Administrators group. The other default groups include Operators and Guests.

Figure 1. Main Window of the Domain Account Manager

The Domain Account Manager has many security features, such as encryption, that increase the security of the computer on which it is deployed. The Domain Account Manager uses a challenge and response protocol to transmit passwords over the network. Because no clear text password is transmitted through the network, malicious eavesdropping techniques do not reveal the user's password. The Domain Account Manager also uses a one-way hash function to store passwords. Using this type of storage, applications can validate passwords with the Domain Account Manager, but these applications cannot determine the actual password.

To increase security, you can control access to the Domain Account Manager by assigning permissions to both individual computers and subnets. By denying access to the Domain Account Manager you are effectively denying access to any of the resources that use the Domain for user authentication. If a computer or subnet cannot access the Domain Account Manager, the requested resource cannot determine the necessary permissions.

You can use both individual computer names and IP addresses to control access to the Domain Account Manager. You also can use the "*" wildcard to control access by a range of computers or IP addresses. For example, granting access by "*.ni.com" specifies that all computers whose name ends with "ni.com" can access to the Domain Account Manager. Conversely, denying access by "10.0.0.*" specifies that no computer on the 10.0.0 subnet can access the Domain Account Manager. Figure 2 shows these settings of the **Domain Properties** window. You access this window by launching the Domain Account Manager, selecting **Edit»Properties** from the pull-down menu, and clicking the **Access Control** tab.

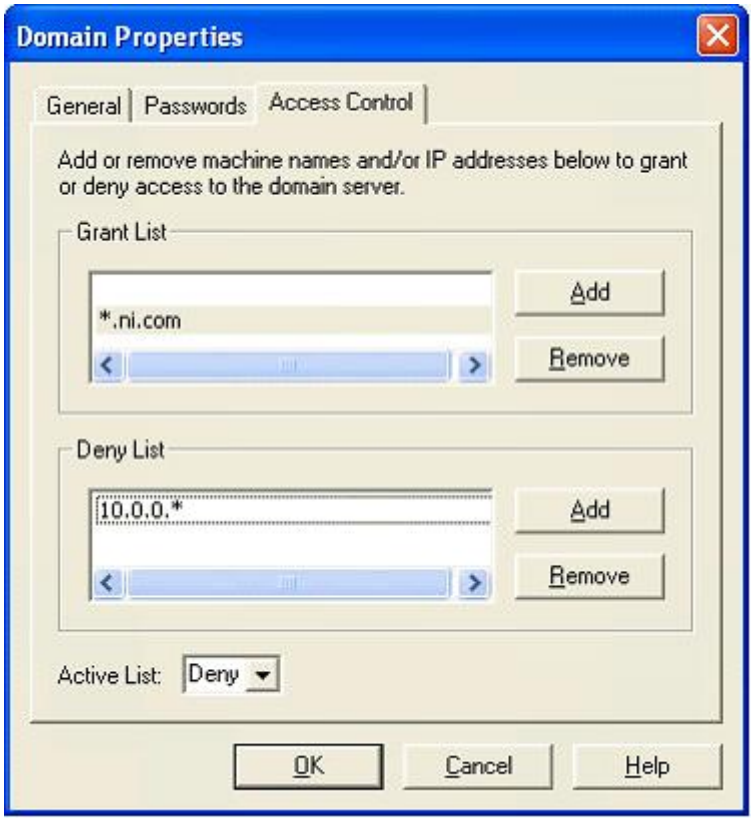

Figure 2. Domain Properties Windows/Access Control Tab

4. Project Library and Shared Variable Operations and Permissions

Project libraries and shared variables are two types of resources that use the security features provided by the LabVIEW Mobile Module. You can use permission levels to control read/write access to both of these resource types. The three permission levels are Grant, Deny, and Undefined. Table 1 describes these permission levels.

Permission Level	Behavior
Grant	The user or group can perform this operation
Deny	The user or group cannot perform this operation
Undefined	The user or group cannot perform this operation unless another permission statement specifies otherwise

Table 1. Permission Levels for Project Libraries and Shared Variables

Permissions are assigned hierarchically. The highest level of permissions is that which is defined at the project library level. By assigning permission to a library, you are assigning permissions to all project libraries and shared variables contained in that project library. The undefined permission can be overridden at the same hierarchical level or at a higher one.

4.1. Project Library Security

Once users and user groups have been defined in the Domain Account Manager, this user information can be used to determine the read/write permissions to perform operations on different resources. Notice the user has only read access to the project library.

4.2. Shared Variable Security

Shared variables use the Domain Account Manager user information and authentication functionality to set permissions much in the same way that the project libraries do. However, because shared variables reside inside a project library, there might be discrepancies between the permissions assigned to the project library and permissions assigned to the shared variable. In this situation, the most restrictive permission always is enforced.

To assign permissions for a shared variable, right-click the variable and select **Properties** from the shortcut menu. Then select **Security** from the **Category** list. Figure 3 shows the shared variable properties window providing the user read access and denying write access.

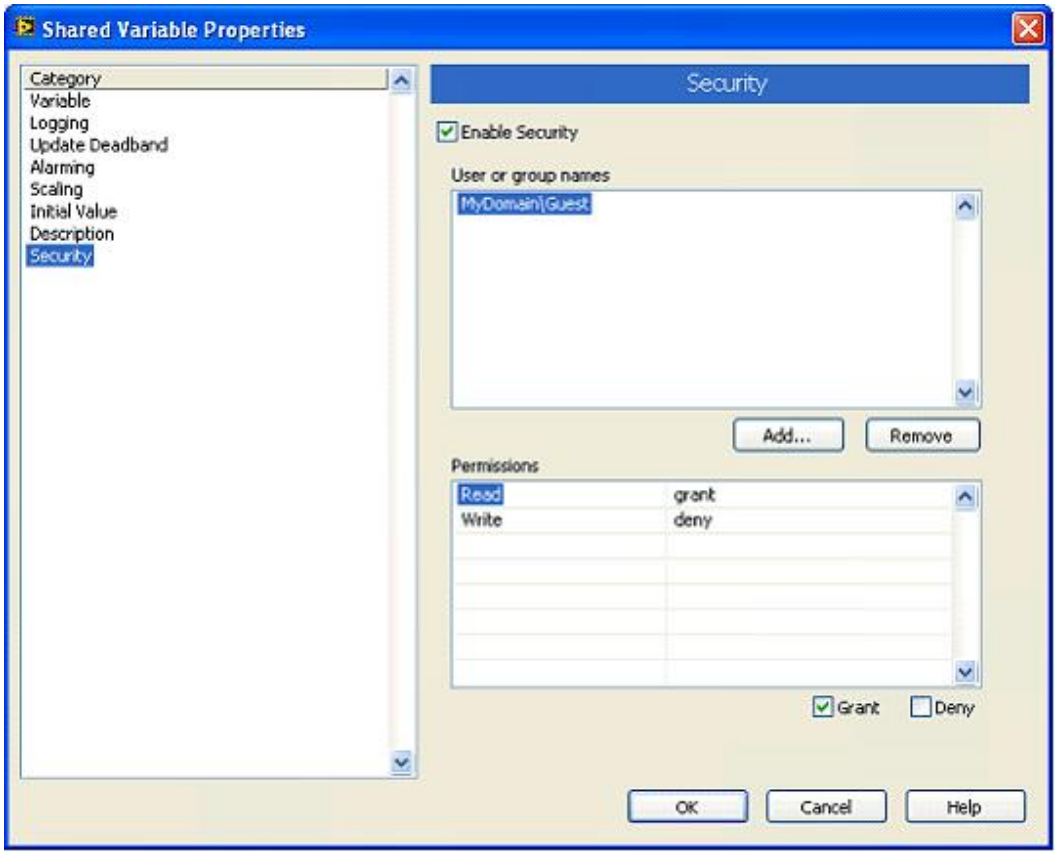

Figure 3. Setting Permissions for a Shared Variable

5. Front Panel Security

The LabVIEW Mobile Module also uses the Domain Account Manager to assign permission levels to controls and indicators on the front panel. You can assign the following four permission levels to front panel objects.

- **Full Access** – The user has unrestricted access to the front panel object.
- **Disabled (View Only)** – The user only can view the front panel object.
- **Disabled & Grayed Out** – Similar to **Disabled (View Only)**, but the front panel object appears dimmed.
- **No Access (Hidden)** – The user cannot see the front panel object at all.

You can use the following two procedures to assign permissions to front panel objects.

- Right-click the object and select **Properties** from the shortcut menu to launch the **Properties** dialog box. Then click the **Security** tab. Use this tab to assign permissions to that object.
- Select **Tools»Security»Front Panel Security** to launch the **Front Panel Security** dialog box. This dialog box, shown in Figure 4, lists all the front panel objects. Use this dialog box to assign permissions to more than one front panel object at a time.

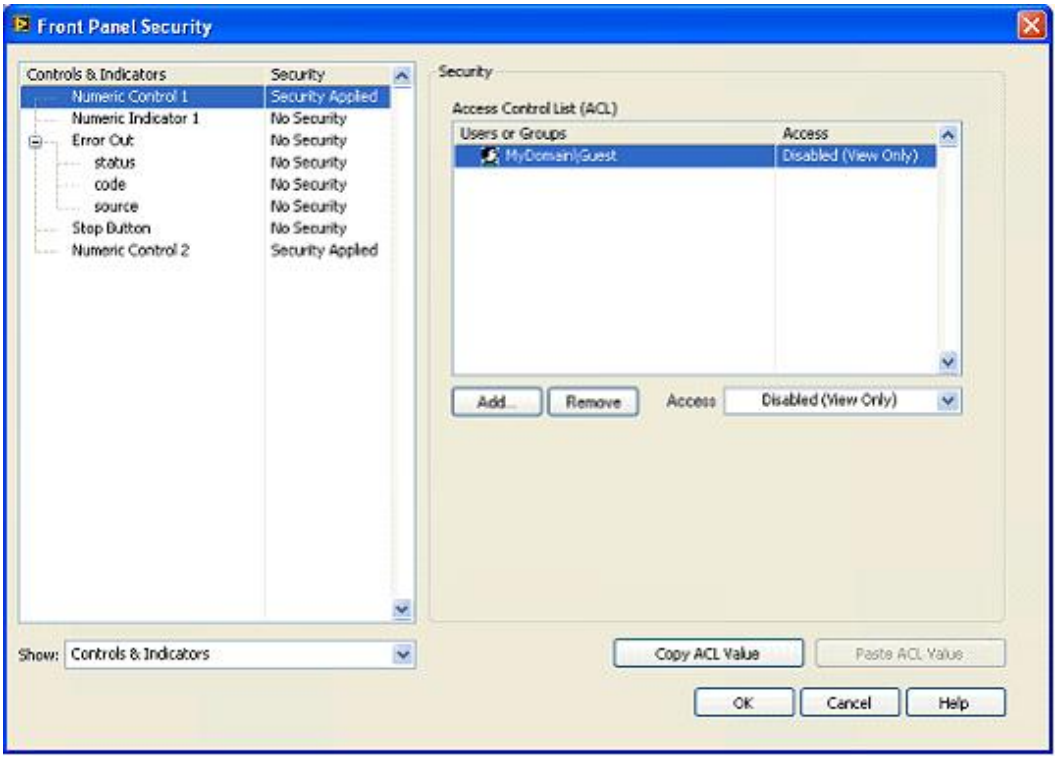

Figure 4. Front Panel Security Dialog Box

Using the **Front Panel Security** dialog box to assign object permissions is different from changing the object state using the Properties menu. Using the properties of that object changes the security of the object based on the user that is logged in to the front panel. Conversely, using the **Front Panel Security** dialog box keeps the security at the same level no matter which user is logged in. Also, permissions set by front panel security override the state defined for a front panel object by its properties. Therefore, no matter what the state of the object is set to, its behavior will be controlled by front panel security.

6. Conclusion

The LabVIEW Mobile Module provides a set of tools to facilitate the implementation of security for local or network resources such as LabVIEW project libraries, shared variables, and front panel objects. The security architecture of the DSC Module separates user management and authentication from resource permissions. User management and authentication is provided by the Domain Account Manager while the permissions assigned for users to access a resource are defined by the resource itself. The three resources that take advantage of the security functionality of the LabVIEW Mobile Module assign permissions in different ways. Project libraries can be used as containers to assign permissions to multiple shared variables or other project libraries contained in that project library. Although shared variables inherit permissions from the project library where they reside, shared variables can assign individual permissions as well. Front panel objects can also assign permission levels based on the user or group.