Securing SCADA Using Active Directory

A few months ago, we discussed how to store the PLC code of your organization, emphasizing the importance of saving it and securely managing the modifications and access to this PLC code. Today we will continue our focus on SCADA security by taking a closer look at something tangible; people. It is the people of our organizations that make decisions on how to operate our water systems and one of the tools to assist in the decision-making processes are our SCADA systems. SCADA systems can provide us critical process data, offer regulatory reporting, provide usage information for billing, and the capability to control physical equipment throughout our critical infrastructures. It is no question that our SCADA systems are extremely valuable and offer much control over our water operations but how do we secure such critical systems? In this article we will discuss one way to secure access to SCADA system software through a Microsoft platform called Active Directory (AD).

What is Active Directory?

The purpose of this article is not to dive into the technical details of how an AD works so for simplicity, think of AD as an electronic address book containing usernames and passwords for every individual in an organization. When opening an email inbox, for example, typically a login is required to gain access. As long as the user types in the correct username and password combination, access is granted. Otherwise, access is denied. What happens in the background is the username and password entered is verified against the organization's AD to ensure that the username exists, and that the password entered matches what is on file. Simple as that!

Now, the power of AD comes when multiple applications each require credentials. AD allows the same username and password to be used regardless of application being used. Similarly, if a user needs to be added to an application or a user's password needs to be changed, that change is only required in one place, the AD, and all other applications referencing the AD are simultaneously updated.

An example of this philosophy is similar to how some apps or websites offer access to them or allow account creation using your Google account rather than creating a separate username and password with just that app or website. Same concept as AD; one set of username and password to log into multiple applications.

Managing the Security of SCADA Applications

In my experience, I have seen very few organizations that use AD to secure their SCADA applications. In some cases, a shared, single user account is used for all SCADA control and everyone knows the password. My personal favorite is the sticky note with the username and password right on the screen of the SCADA computer (you know who you are! 😊). Consider the following scenarios and see how AD and having unique logins can be of great benefit:

- **Staff Addition** – With AD, an IT professional can add the new staff member into the AD address book, taking no longer than a few minutes, and instantly that new member has access to whichever applications he/she needs.

- **Staff Removal –** Whether it is a disgruntled employee, retirement, or someone who chose to leave, deleting the staff entry in AD instantly removes access to all applications and removes the risk of accidentally forgetting to remove that employee from a SCADA application.

- **Setting up a new application –** When setting up a new SCADA application, the System Integrators nor the IT professionals have to gather the list of usernames or passwords from all individuals to setup the new application. Instead, the new application can be integrated into AD and automatically inherit the ability to authenticate with the same credentials that have been used with existing applications.

- **Consistent Logins** – As mentioned before, if SCADA applications are all tied to AD, there is only one username and one password to remember per user.

The above examples are just a few instances where AD comes in handy. SCADA systems can benefit from AD integration and it will also make you IT professionals happy! I would encourage all of you to ask your Systems Integrators if your SCADA system's access is managed by AD. Start the conversation!

Our SCADA systems control the water operations of our communities and we owe it to our constituents to be good stewards of these systems. AD integration is just another way to better our cyber security stature. Thank you for reading!

Nicholas A Paradiso, PE
Lead Automation Engineer
Concentric Integration