Practical Password Management

Chris Anderson
June 7, 2012
The existing communications system was designed with a local security model in mind, with local shared accounts and pre-shared passwords. This was primarily because there was not a communications infrastructure to support centralized trust management controls. As a result, managing these local secrets is labor intensive, taking too much time and money to manually control.
Today there is a need for a password management solution that is automated and centrally located. Furthermore, it must support centralized access controls that provide individual accountability. This solution improves cybersecurity, change control, and compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements.
We all know that some things are the right thing to do; but sometimes life finds ways to make the right thing to do hard.
Let us look at an example of a small system to decide if it is economical or efficient to change local passwords.

If there are 50 sites to dial up and each site has an average of 20 devices, assume that each device has four passwords that need to be changed. This would result in 4,000 password changes.

The most efficient operator could probably change one password every minute, taking into account the connection management (dial-up connection, access commands, and change confirmations). Without any errors, it would take over 66 hours to change all 4,000 passwords. To meet the 24-hour NERC CIP requirement, there would have to be at least three people working 24 hours straight or, more realistically, nine people working almost a full 8-hour day.

However, this example neglects the actual change control aspect of password management. How are these password changes documented and communicated to the operations personnel that need them to perform maintenance? Change control is a very significant effort that probably costs more to manage than the actual process of performing the password changes in the first place.
So why is having a robust password system so hard?

Account management functions are typically built into application-specific embedded devices. However, because these devices are specialized in their application, the focus of the firmware architecture is to simplify the code base to minimize patch management. Therefore, these devices traditionally were not designed for enterprise access account management. This means that many of the technical solutions for centralized trust management cannot be used, which results in local accounts and passwords. Considering the number of these devices operating within and protecting the electric power system, there can be a lot of local accounts that need attention. Keep in mind that these devices also have a variety of management interfaces requiring their own tools or software to connect or make changes.
There needs to be a migration from shared passwords and local accounts to centralized accounts and passwords. This type of password system should be designed for reliability and take into account when central communications are not available. Another key task is to protect passwords in transit by securing communications. System changes are then performed centrally, which minimizes costly field changes.
Before implementing a centralized trust management system, draw on the experience of information technology (IT) personnel. Even though the IT environment is very different (with ever-changing systems and clients) compared with the system inventory (which is slow to change), IT personnel have knowledge to share about how to centralize trust management. Companies already have policies to tap into for user account creation and removal. There is no need to retrain employees when a company already has employees who understand how to administer user accounts. This helps to eliminate repetitive work and lower operational costs. However, this does not mean that IT takes over in all cases of user account administration. Both IT and operational technology (OT) personnel must understand and learn the business objectives relating to the required system operations.
When considering how to get to where we want to go from where we are today, it becomes clear that we need a solution that can sit in front of legacy devices. This device would perform the central account management functions and then be the proxy connection downstream.

Options to Get There

- Change out products $$$$$
- Firmware upgrades $$$
- Proxy $
Automate With Centralized Change

- Uses scripts to automate change
- Supports password checkout process
- Changes all passwords throughout system in 24 hours
- Provides successful change confirmation
- Communicates throughout wide-area system reliably

For the proxy to work, it needs to fulfill the main objectives of the system. Most importantly, if the proxy can relieve the need for the end user to know the local password, or have to use it, the security solutions help the operator get the job done more efficiently.
Once a local proxy is accomplishing the tasks listed on the slide, new devices that have central management capabilities can be integrated easily.
We must continue to improve power systems cybersecurity and try to stay ahead of attackers. We owe it to our investors and customers to find ways for these improvements to support overall company business objectives. When applied correctly, cybersecurity improves the efficiency of authorized utility operators.

NERC CIP compliance must be achieved and maintained and should result from implementing security systems to protect the power system. The total cost of ownership has to be evaluated, and trust management contributes a significant amount to this cost. Before deploying any cybersecurity system, evaluate the trust management capabilities and processes and ensure that they align with the desired architecture of the company.