License-based Protection Versus a Software Solution

Purpose:

There may have been a time when simply locking your home or car was the only method for securing your property. Now there are many additional safeguards available, such as security systems and cameras.

Industrial control systems are no different and have gone through the same security evolution. In the past, industrial control systems, like server rooms, data centers, and control cabinets, could only be accessed by a physical key and they were all separate entities. Today, these control systems are likely connected to other systems within the plant, and they need to be connected to the outside world for monitoring and analytical data analysis. Since the modern industrial control system is now connected and exposed to the rest of the world, it increases the risk of unintentional changes or malicious behavior, which can range from system control and destruction to stealing machine designs and intellectual property (IP).

Today's industrial control systems and machines need to follow a Defense in Depth security methodology, since a single key is no longer sufficient to keep your locked up contents safe. We will explore why a hardware root of trust provided by Rockwell Automation Licensed-based Protection is a higher level of security and can keep your valuable property safer than just keys and/or a password.

Background:

Roots of Trust (RoT):

The National Institute of Standards and Technology (NIST) conduct projects with a Root of Trust (RoT) methodology in mind. The following quote is from their website:

> Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trustworthy. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust. [1]

Rockwell Automation

WIBU – Trusted Computing Group

To further ramp up the versatility that characterizes its flagship technology, Wibu-Systems has joined the **Trusted Computing Group (TCG)** and offers CodeMeter as a **secure licensing platform** for all Trusted Platform Module (TPM) users to monetize their business. As part of this effort, Wibu-Systems is also expanding its hardware compatibility lineup to include support for TPM. CodeMeter features ever-growing support on multiple fronts: an unparalleled range of hardware platforms, including PCs, mobile devices, embedded systems, PLCs, and microcontrollers; a matchless lineup of secure elements that spans across dongles, memory cards, TPMs, cloud, and software-based repositories; and full integration with all major operating systems used in offices and industrial environments. [(2)]

Vulnerabilities:

This section describes vulnerabilities any Control System or IT Engineer has experienced in the past. The list is provided to bring attention to a software or hardware security method or lack thereof, expose the vulnerability, and provide a more secure solution. It is written from the perspective of an engineer either designing or running a control system using past or present development software and programmable logic controller (PLC) hardware solutions.

Development Software Vulnerabilities to Consider:

- Vintage Operating Systems (OS) and software packages had few embedded security features and could pose a huge risk to control system security. Many of these products only had Admin rights, meaning anyone with Admin rights had the ability to make changes.
- Out-of-Date OS and software packages may have had the ability to secure and protect control systems three to five years ago, but if the OS or software vendor has stopped updating their products, security holes in the products could eventually compromise the control systems.
  - Security Mitigation Path: Upgrade or replace these OS and software packages with a more modern and secure software solution. This can be easier said than done in some industries, but is very important to consider.
- Up-to-Date OS and software packages that use password authentication to protect Intellectual Property (IP). Although more secure than no password protection, these OS and software packages are still vulnerable.
  - Security Mitigation Path: Implement a procedure to change passwords frequently and apply expiration dates. Delete passwords that are no longer used or were assigned to personnel who left the company. Password maintenance can be tedious and time consuming, but is a necessary procedure.

PLC Hardware Vulnerabilities to Consider:

- Vintage PLCs had default backdoor passwords that helped a person access the PLC in case of an emergency, but now pose a huge risk to control system security.
- More modern PLCs, commonly known as Programmable Automation Controllers (PACs), are secure now that backdoor password capabilities are a thing of the past. These PACs continued to maintain password authentication capabilities to protect against Runtime Access and compromising of IP, but are still vulnerable to compromise.
  - Security Mitigation Path: Implement a procedure to change passwords frequently and apply expiration dates. Delete passwords that are no longer used or were assigned to personnel who left the company. Password maintenance can be tedious and time consuming, but is a necessary procedure.

Social Engineering Vulnerabilities to Consider:

A common theme stands out in the Software/Hardware Vulnerability section: password authentication and the tedious task of maintaining the process. You may think to yourself: "Passwords have always worked for me in the past. Why do I need to change my method of security? I have never given my passwords out to anyone!" This can be a common thought, but remember, people with malicious intent know this as well and have gotten quite creative in obtaining password information. Once a password for a control system has been compromised, people with malicious intent can monitor, control, change, damage, or steal IP. Here are a few points to consider.

- Convenience: Password authentication should be administered on an individual basis. Sometimes it can be more convenient to let someone "borrow" the password to make a quick change. However, by doing this, your only security method has just been compromised.
- Social Media: Using social media is great to keep in touch with friends and family. It is also used by people with malicious intent to gain your trust to eventually gain access to vital information.
- Phishing: Phishing emails are also used to gain your trust for the sole intent of exposing vital information, or worse, establish a physical connection into your network.
- Hacking and Scanning: Once the network has been compromised, passwords can be hacked in a matter of minutes using state of the art tools, or scanned using traffic-sniffer software.

License-based Protection Solution:

Rockwell Automation has been collaborating with the security specialists at Wibu-Systems to provide a robust security solution that is suitable for daily operations. The result is a solution called License-based Protection, part of the Rockwell Software Studio 5000 Logix Designer v30 software, which is based on the CodeMeter technology by Wibu-Systems. This method of security far surpasses the password authentication of the past.

Source and Execution Code Protection:

Multiple engineers, sometimes from different companies, often collaborate on the same machine project or application. How do you protect or lock down valuable IP from prying eyes? An OEM that builds machines and ships them all over the world must guarantee that the IP of each machine is secure. The machine's IP is what differentiates an OEM from the competition. Every machine needs to be as secure as possible. The answer is License-based Source and Execution Protection.

- License-based Protection generates licenses with cryptographic keys that encode and decode the Source code in the Studio 5000 Logix Designer software development environment and the executable programs on PACs. Standard ECC, AES-CBC and SHA-256 HMAC algorithms are all used for this executable protection.
- Source Code in the form of Routines (Ladder and Structured Text) and Add-on instruction (AIO) programming languages can be encoded to protect source code contents and decoded for users with the proper credentials.
- Access to protected content is restricted based on the principle of least privilege: The user is only granted the necessary access privileges for their work.
- The access privileges are stored as licenses in the secure CmDongle hardware by Wibu-Systems. A CmDongle is a piece of tamper and manipulation proof protective hardware with a built-in SmartCard chip.
- The CmStick/Cm USB secure hardware dongle, which gets inserted into a PC, prevents unauthorized reading, copying, and changing of protected source code, forces source code encryption during exporting activities, and permits new security configurations only for authorized participants in the Studio 5000 Logix Designer development environment software.
- The CMStick/SD secure hardware, which gets inserted into a ControlLogix or CompactLogix Controller, prevents an undesired upload of the program from the PAC controller and a subsequent download to another controller because the program is only allowed to run on authorized controllers.
- Additional options by CodeMeter can be used to control a user's access over time by applying an optional expiration date.
- Since the CmStick/Cm and CmStick/SD are physical hardware devices custom programmed with an individual's access credentials, there are no passwords to keep track of or worry about being compromised.

License
Source Protection

License
Execution Protection

- This new License-based Protection feature to protect source and execution code is only available for the ControlLogix 5580 and CompactLogix 5380, 5380S and 5480 PAC controllers.

Conclusion:

Licensed-based protection is an excellent addition to your company's Defense in Depth strategy and should be considered for your modern control systems and machines being shipped around the world. This will cause you to stay proactive, so that when (and not if) a password is compromised, you will not only save time and money, but also have the peace of mind that your system and valuable information are safe.

Cited Sources:

1. **https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust**
2. **https://www.wibu.com/solutions/software-licensing.html**

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 9324-WP002A-EN-P – January 2019