PHOENIX CONTACT
INSPIRING INNOVATIONS

Five Steps to a More Secure Control System

By Dan Schaffer and Dan Fenton

Executive summary

Cyber-security has been a headline-grabbing topic recently, both in the commercial and industrial worlds. Many control engineers, maintenance staff and plant managers would like to be proactive with security, but feel they lack the expertise to take on such a daunting task. And while it may be true that 100 percent security is a very difficult, if not impossible, task, there are some simple, practical steps that can be taken to immediately make your network more secure.

TABLE OF CONTENTS

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

Introduction

Cyber-security has been a headline-grabbing topic recently, both in the commercial and industrial worlds. In the last two years:

- Stuxnet crippled Iranian nuclear enrichment efforts
- Nitro and Nightdragon were found to be persistently attacking the chemical and energy industries – stealing gigabytes of sensitive data
- and Duqu – dubbed Son of Stuxnet – was discovered and is still baffling experts as to its authors and inner-workings.

As process and automation networks increasingly use Ethernet, wireless and TCP/IP for communication, and as this communication extends from the "isolated" industrial plant network to the office network and the Internet, securing that communications and protecting the critical assets on the plant floor becomes vital.

Many control engineers, maintenance staff and plant managers would like to be proactive with security, but feel they lack the expertise to take on such a daunting task. And while it may be true that 100 percent security is a very difficult, if not impossible, task, there are some simple, practical steps that can be taken to immediately make your network more secure.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Password Security

Passwords guard access to your data, your equipment and your programs. Without the use of good passwords, there is a significant vulnerability in your network infrastructure. Here are some simple password rules.

- Passwords are meant to be secret, so don't write them on a sticky note hanging on your monitor
- If they are for "shared" equipment, like a PLC that multiple people support, and one of those people who knows the password leaves (retires, quits, etc.), change the password — that day
- They should not be "password," "secret," "admin," "123456", "querty," etc. — that is, they should at least be moderately complex, so that they can't be guessed

A good way to make a secure, yet easy-to-remember, password is to first make a simple sentence you can remember, such as "I really want to program my PLC today." Next, use abbreviations to make a little pneumatic device out of it. "1rw2pmPt "is a really secure password[1]. It won't show up in the dictionary and is not the name of any of your kids or pets (hopefully). It contains both upper and lowercase letters and numbers, and you can even use punctuation if you want. Best of all, you can easily remember the simple sentence you used to create it.

Some guides recommend changing passwords every 30 to 60 days. Perhaps a better and more practical course of action may be to create a strong password (see above), memorize it and don't share it or write it down. If you keep it secret, the need to change it periodically greatly diminishes. In fact, frequent password changes is the number one reason people tend to write them down, defeating the purpose of having a password in the first place!

Top 10 Passwords

Hackers who steal passwords will often post those passwords or some "interesting" statistics for others to view. Here are the top 10 passwords used on popular sites[2]:

1. password	2. 123456
3. 12345678	4. qwerty
5. abc123	6. monkey
7. 1234567	8. letmein
9. trustnoone	10. dragon

[1] An eight-character password with upper and lowercase letters and numbers has more than 200 trillion possible combinations. Add in punctuation marks like *, @ or !, and you are well over 500 trillion.

[2] Forbes.com "25 worst passwords of 2011"

PHOENIX CONTACT
INSPIRING INNOVATIONS

Deny Access to the Internet from Critical Systems

The Internet is full of wonderful and useful information; it is also teeming with viruses, worms and other malware, often on otherwise benign sites (e.g., Facebook). Allowing control PCs, HMIs, etc., to access the Internet is playing with fire. Even if operators and technicians aren't supposed to use those PCs for surfing the web, sometimes the urge to check the news or post a status update is too great.

An even worse offense is allowing your control devices, for example an HMI, to have a "public-facing" address — that is, to be directly connected to the Internet, with an IP address that is public[3] and can be reached by anyone. Some users employ public-facing HMIs because it allows them the "convenience" of accessing and monitoring the HMI and connected control network from home, the road, etc. The cost of this convenience is compromised security. Public-facing devices are easy to find on the Internet. Once found, they are generally easy to compromise.

A recent example of the dangers of "public-facing" supervisory control and data acquisition (SCADA) equipment is the November 2011 compromise of water systems in South Houston, Texas. A hacker using SHODAN (see sidebar) or a similar free search tool was able to connect to a public HMI controlling the district's water system[4]. After connecting to the HMI, the hacker only had to guess a simple, three-character password to gain control of it. Fortunately, he did no damage, but instead posted screenshots of the system in an attempt to shine light on how insecure most control systems really are.

A safer, much more secure method is to use a "virtual private network" (VPN) to remotely connect to your network. IT personnel have used VPNs on the "office network" for decades. Today's VPNs come in many flavors and variations. All of them, however, utilize secure authentication to verify if access to a network should be granted. VPNs also use encryption to scramble sensitive data, such as programs and passwords, as it traverses the Internet. Many industrial VPNs are now available, including the FL mGuard line from Phoenix Contact, to combine network security with rugged hardware.

SHODAN – a Google for hackers

SHODAN (named after an evil artificial-intelligence computer in a popular video game) is a search engine first made public in late 2009. In the simplest terms, SHODAN scans public IPs to see what ports or services are listening (like http, ftp, etc.) and then indexes the header information that comes back. This header information contains some identifying details that can be used to find a lot about the system, such as manufacturer, operating system or firmware revision, etc. Someone with only modest hacking knowledge can use SHODAN to search for and discover PLCs, HMIs, etc. that publicly face the Internet and then try to compromise them with known vulnerabilities.

[3] "Private" addresses are not routed on the Internet and include any address starting with 192.168.x.x, 10.x.x.x and 172.16.x.x-172.31.x.x.

[4] http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-digit-password-secure-internet-facing-scada-system-112011

PHOENIX CONTACT
INSPIRING INNOVATIONS

Don't Be Fooled by "Wired Encryption Protocol" for Wireless

A wireless networking system is a boon to communications. Once completed, a well set-up wireless network can allow easy expansion, increased use of communication devices and lower infrastructure costs. But a wireless network can also be a very easy target for a person with malicious intent.

An unencrypted network means that someone does not even need to get a username or password to begin listening to data, which can include credentials to more important systems, such as a back office SCADA server or production database. Even basic encryption will barely hold its own. WEP, in particular, is merely an application download away from being cracked. A network name, or SSID, of "LinkSys" will clue the attacker in that the target is using a LinkSys router. Then the attacker could go onto the Internet and find the default username and password for that particular router and try typing it in. And yet, practices such as unencrypted or poorly encrypted networks, default network SSIDs, and unchanged default usernames and passwords proliferate.

In February of 2000, a disgruntled former employee of a system integrator decided to take revenge on his former employer and customer, the Maroochy Shire Water Treatment plant in Queensland, Australia. Driving around in the car, the attacker managed to infiltrate the remote SCADA systems for a multitude of stations. Over a three-month period, he caused more than 800,000 liters of raw sewage to be released into nearby parks, rivers and streams. Being an ex-employee, the attacker was able to use passwords that had not been changed, utilize a completely unsecured network and remotely manipulate the SCADA system for his own nefarious means. This led to a small environmental disaster. This attack was completely preventable.

Simple and easy steps can be taken to prevent breaches through the wireless. Almost all modern wireless-capable devices can use the WPA2 encryption protocol. The amount of time needed to brute-force attack a WEP network is the time it takes to download a program, and a malicious user will likely already have a program. On the other hand, the time needed to brute-force a WPA2-encrypted network is much longer. A good, strong password can make it impractical. Use the WPA2 protocol if at all possible, and no matter what, avoid using WEP.

Next, change the default name of the network. In fact, if the devices connected to the network support it, hide the SSID altogether. Not having a network broadcasting its existence may not stop many attackers, but it could mean some decide not to use that route, and there is no harm in this if the devices communicating with the network support it. This is especially useful to prevent workers from utilizing that network for unauthorized devices.

Finally, a username and password rotation policy is strongly advised. If this is impractical for any particular reason, at the very least change the username and password following the simple advice given above. While this may seem like a burden initially, in the long run a brute-force attack that requires six hours or more to run could mean the attacker will either look elsewhere, or be caught waiting to crack the network.

PHOENIX CONTACT
INSPIRING INNOVATIONS

USB Sticks Are Risky

With the popularity and convenience of USB sticks in our workforce – and the costly damage they can cause – what is the best next-step in protection?

As is the case with many things, total abstinence is the sure cure. However, as is the case with many things, the likelihood of that strategy succeeding in today's world is doubtful. Given the number of those in our workforce who use USBs, it's simply unrealistic to believe that self-restraint is the answer. USB sticks are simply too convenient for users to totally abstain from using them, even on a critical control network.

The next step of assurance might be for IT to institute a standard whereby a USB stick may be used, but only after the user stops by to "meet the parents" first – allowing IT to run the USB through a series of tests to determine its safety. Again, in today's fast moving world, this type of policy relies on each user adhering to the house-rules. And we all know the rebellious nature of many in our workforce. In addition, carrying out this type of process can cause a great deal of inconvenience for everyone involved: the user and IT.

A better solution may be to utilize a file monitoring and scanning program called Common Internet File System (CIFS) Integrity Monitoring. CIFS Integrity Monitoring is designed to alert the system of a change to the files it is watching, for example if an infected USB stick is introduced to the user's machine. While it will not prevent the threat from approaching, it will notify the proper personnel that a change has occurred since the last system check and request authorization before moving forward. In light of the well-known Stuxnet attack, the cost-savings are significant. While CIFS would not prevent the initial infection by Stuxnet or a similar virus, it will provide early detection and notification and, therefore, the opportunity to mitigate the problem. And because it does not require database or signature updates, like anti-virus solutions, you don't need to have Internet access to keep your protection current.

How to protect your system from the use of USB sticks is an issue that cannot be ignored – especially when you factor in the potential loss of time and money. In a world where total abstinence is a pie-in-the-sky strategy, CIFS Integrity Monitoring provides a level of protection and assurance that few other strategies can obtain.

PHOENIX CONTACT
INSPIRING INNOVATIONS

A Simple Firewall is Easy to Set Up and Provides Great Protection

A firewall is essentially a filter that allows some network traffic to pass, while blocking others. While there are several complex (and expensive) variants, a basic firewall is sufficient for most applications and a good place to start. Firewalls decide whether to "allow" or "drop" traffic passing through based on rules. These rules look at where a data packet is coming from (that is, the source IP or MAC address), where it is going to (the destination IP or MAC address) and what type of data it contains (Modbus, http, ping, etc.).

It's not hard to envision how a firewall can increase security on a control network; if a user or a device is not supposed to be able to communicate with your HMI or PLC, that traffic gets dropped. This greatly reduces the risk of compromise and even of accidental harm (for example, a virus infecting an office PC and that malicious traffic impacting or infecting control systems). Additionally, some firewalls – like the mGuard line – allow for named users to be configured with their own special rules. This makes it easier to allow technicians or engineers, who don't always have the same IP address, to authenticate to a firewall and be allowed to pass through, whatever their IP address may be at a particular time.

In 2011, a Brazilian plant was shut down due to a computer virus infection[5]. The infection started on the office network, but owing to a lack of firewalls, spread quickly to the industrial network. Here it infected Windows control PCs, and the additional traffic caused problems even with non-Windows devices. Firewalling the business-critical industrial network would have saved hundreds of thousands of dollars in lost time and production.

Investing a little time to install and configure a firewall will save a lot of trouble down the road. If you aren't sure what traffic you should allow, or what type of traffic is "normal," you can run most firewalls with "logging" or "learning" on. This will allow traffic to pass through while keeping a log of what it is. You can review this data to determine what rules you need to configure. This logging information is also useful for auditing who is connecting (or attempting to connect) to your network. This type of information is required for compliance with industry standards such as NERC-CIP and ISA99.

[5] PCWorld August 2011

PHOENIX CONTACT
INSPIRING INNOVATIONS

Conclusion

Security is incremental. It is not a binary of "totally unsecure," flip a switch and now you are "totally secure." Each step you take, from the above recommendations or other, more advanced steps, will help protect your network and environment. Additionally, many attacks, hacks, etc. are a matter of convenience. Each layer of protection makes a potential attacker's job more difficult and significantly increases the chance that he or she will look elsewhere for "lower hanging fruit."

We hope you take the time both to implement the above "5 Easy Steps" and also develop a deeper, more complete security plan in the future. Some recommendations for your "next steps" include Intrusion Prevention/Detection Systems, using logging and auditing to better monitor the events on your network, having a secure code repository for your programs and source code, and implementing an awareness or training program to help prevent social attacks.

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pa.

For more information about Phoenix Contact or its products, visit www.phoenixcontact.com, call technical service at 800-322-3225, or e-mail info@phoenixcon.com.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com