Safety practice

Isn't that IT's job?

Roger Barrett, Charles Taylor technical, UK

Summary

Mention 'cyber security' to many people and the image formed in their mind may be of an adolescent sat in a darkened bedroom breaking into computer systems many miles away. However threats can come from many sources and for many reasons. This paper highlights some of the main possible sources of threats to ICS security.

Keywords: cybersecurity, industrial control systems

Mention 'cyber security' to many people and the image formed in their mind may be of an adolescent sat in a darkened bedroom breaking into computer systems many miles away. As we'll see below, sometimes that is the case — but it is not always so. Threats can come from many sources and for many reasons. However, is it really an issue of concern to the owner of an industrial control system (ICS)?

The problem

The majority of ICS hardware in use in the process industry is either commercial Distributed Control Systems (DCS) or Supervisory Control And Data Acquisition (SCADA) systems. In the past, the difference between ICS software and hardware to that of general, business computing platforms, gave some level of security, even when the control system linked to the outside world. The underlying operating system and the computers on which it ran were quite different to the office PCs and software and any links to the outside world were probably over proprietary gateways.

Today the situation is much more blurred. The servers and operator stations are often customised versions of off-the-shelf hardware and are often Microsoft operating system based. In addition the network linking various components of the ICS and the links between the ICS and business systems are often standard Ethernet network connections.

The majority of ICS security incidents are probably not widely reported – in fact, the owner of the system may not even recognise some as security incidents. Of those that are reported, a number are well known and often quoted as examples of ICS security breaches. Some of these are briefly described below to give an idea of where the threat can come from and what damage it can cause.

The list opposite includes attacks from both inside and outside the companies involved. Whereas in the past, a process plant ICS may have been a standalone computer system, fairly secure, located in the middle of an operating plant, today they are often linked to other systems (ICS or otherwise) at remote sites. Parts of the ICS itself may also be distributed between sites, some of which may not be easy to secure physically. The threats can therefore come from a number of different sources. Below are some brief descriptions of just some of the possible sources of threats to ICS security.

Direct connections

Traditionally ICS hardware was maintained completely separate from the business network. However, with the growth of plant information systems and the use of real-time data in business, the links between the systems have increased. Potentially these can provide an access route to the ICS from the business network and, in the worst case, from the outside world.

Security threats can be caused by:

- malicious human intervention, e.g. from an external hacker or a disgruntled former employee;
- non malicious human intervention e.g. someone making a mistake;
- system faults (as in the Brown's Ferry example below);

1982 Trans-Siberian Pipeline[1]	This was reportedly malicious code planted by the CIA in stolen software, which resulted in overpressure to the pipeline and the largest non-nuclear explosion ever seen from space.
1999 Gazprom[2]	Hackers apparently infiltrated the pipeline system with the help of an insider and planted a trojan. Control of gas flows was reportedly lost for some time although Gazprom has always denied this.
2000 Maroochy Water Treatment[3]	A disgruntled former employee hacked into the system, took control of 150 pumping stations and released 1 million litres of raw sewage into local waterways over a 3 month period.
2003 Davis-Besse Nuclear Plant[4]	The SQL slammer worm apparently infected the plant systems and crashed the safety parameter display and plant process computer for several hours.
2003 PDVSA Oil Terminal[5]	During a period of extensive strikes and sabotage, the SCADA system at a marine oil terminal was apparently hacked into and the software on the PLCs operating the facilities erased.
2006 Brown's Ferry Nuclear Plant[6]	Excessive network traffic on the process control network apparently caused cooling pumps to shut down and forced a manual shutdown of the plant.
2008 Lodz City Tram System[7]	A 14 year old modified a TV remote control to be able to change points on the tram network resulting in the derailment of four trams.
2010 Iran Nuclear Processing[8]	The Stuxnet virus is suspected of causing damage to centrifuges used to enrich uranium in Iran's nuclear program.
2011 Duqu[9]	As yet, the purpose of this virus is unknown but it is suspected that it is being used to gather data on industrial control systems to be used for future attacks.

0260-9576/12/$17.63 + 0.00

- or even the inappropriate use of the control network by non-control traffic.

'Back-door' connections

Many sites have dial-up or VPN connections to the ICS from equipment vendors. It can be difficult to ensure the same level of protection on these connections as that between the business and ICS networks. Typically the computer being connected will not belong to the company who own the ICS but to the equipment vendor and often the connections are not known about by anyone other than the ICS engineer.

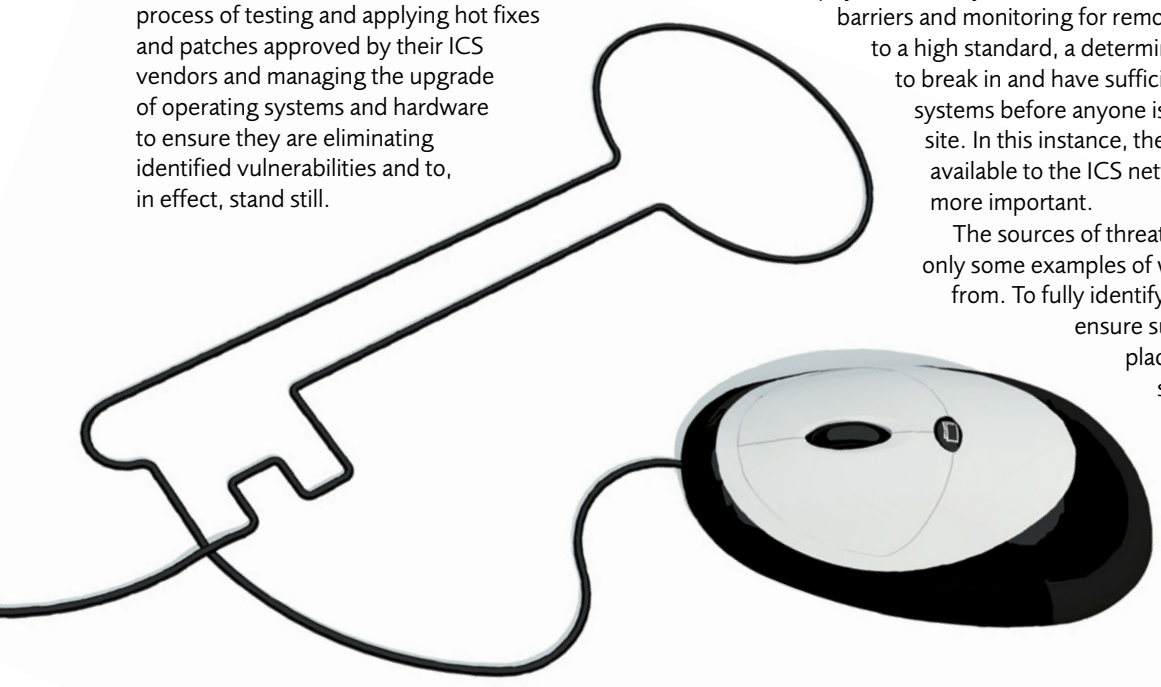
Portable devices

It has become common practice to use ICS data for troubleshooting and investigation on plants. Mostly, this data is obtained from the plant information system but sometimes it is necessary to extract data directly from the ICS (for example in order to extract data without any compression). The easiest way to achieve this is often to use a USB stick on one of the ICS servers. As you might expect, this is also one of the easiest ways to cross-infect machines with malware and is believed to be how the Stuxnet virus, which targets specific ICS systems, propagates.

Some sites prohibit the use of unauthorised USB sticks. However, there is little point having authorised USB sticks to use if they are used to transfer data between the ICS and 3rd party machines without being scanned on a 'safe' machine after every use. If you use the stick to transfer data to an infected 3rd party machine, the next time you use it on the ICS, the ICS can become infected.

Operating systems

Many ICS platforms now run on Microsoft operating systems. New versions of the windows server operating systems tend to be released every five years or so with standard support expiring within five years of release. This has resulted in some sites finding themselves in a continuing process of testing and applying hot fixes and patches approved by their ICS vendors and managing the upgrade of operating systems and hardware to ensure they are eliminating identified vulnerabilities and to, in effect, stand still.



Not doing this may leave the ICS with an operating system that is no longer supported and does not receive patches identified for security threats.

The amount of work involved in managing this process of patching and updating the operating systems safely should not be under-estimated. The implementation of hot fixes and patches will need to be coordinated with the ICS vendor and tested fully offline before implementing on a live ICS.

User security

On corporate business networks, no-one thinks twice about having individual usernames and passwords to log in. Typically, ICS logins have been role-based i.e. one login for operator, one for supervisors and one for engineers etc. Often the supervisor and engineer passwords quickly become public knowledge within the different groups as people feel much less inhibited 'lending' a common login to someone else than they would to giving someone their individual login details. In this situation, if passwords are not regularly changed, unauthorised groups of users can log on to accounts with elevated privileges. Anyone leaving the company would still have valid login details for the ICS if control processes were not in place to ensure that access rights are removed when someone leaves the business, or equally importantly transfers to a new role or location within the business.

In some cases support may be provided by the ICS vendor or a 3rd party. It may be difficult to enforce the same procedures regarding user security on these external companies. It is also essential that any default passwords used by vendors for installation and setup are changed or the accounts removed.

Physical security

For ICS hardware, general physical security tends to be good. The hardware is often in the middle of a process unit surrounded by dedicated security features. However for systems involving remote equipment such as pipeline controls, physical security is more difficult. Even if physical security barriers and monitoring for remote unmanned locations are to a high standard, a determined attacker may still be able to break in and have sufficient time to interfere with systems before anyone is physically able to get to the site. In this instance, the other forms of protection available to the ICS network and systems become more important.

The sources of threats described above show only some examples of where threats can come from. To fully identify the possible risks and ensure sufficient protection is in place requires a co-ordinated security management approach.

0260-9576/12/$17.63 + 0.00

Doesn't my ESD system protect me?

The Emergency Shutdown System (ESD) may be a completely stand alone and hard wired system but this is not the case on many plants, for example:

- the operator interface to the ESD may be via the DCS or SCADA system;
- some low level inputs to the ESD may be via an OPC (Object Linking and Embedding for Process Control) or other interface from the DCS or SCADA.

Even if the ESD system is completely hard wired, the engineering station for the ESD could be an accessible Microsoft-OS based PC.

So components of the ESD system can be subject to some of the same threats as the DCS or SCADA and should be evaluated in terms of cybersecurity, along with the rest of the ICS.

ICS security management

Just as an ICS is now rarely a standalone computer system, the security management of an ICS cannot be carried out in isolation. It will need to be closely integrated with the security systems and processes in place on a company's business networks. However, the security systems in place for the business networks are in themselves often not appropriate to be used on the ICS network and also focus on different priorities to those required for the ICS. For example, the security systems in place on a business network focus on the protection of information critical to the business whereas the security systems in place on an ICS should focus on the availability of the control system instead. The IT security systems and processes cannot therefore be implemented 'as is' on the ICS.

Some companies are already using ISO27001 as a framework to develop cyber security management for their business systems and a standard for cyber security for industrial control systems has also been developed by the International Society for Automation as ISA99 – Security for Industrial Automation and Control Systems. This standard is now being adopted as IEC 62443 by the International Electrotechnical Commission.

Other excellent guidance documents are also issued by the American Chemistry Council[10] covering the implementation of cyber security in the chemical industry and the US Department of Homeland Security, an example of which is Control Systems CyberSecurity: Defense in Depth Strategies[11]. This strategy is a technique of applying multiple controls to the same threat to reduce the risk of the ICS security being compromised. As an example, in order to prevent the infection of the ICS with malware, solutions using hardware, software and staff training are applied together.

As with any form of risk management, a suitable balance will need to be found between policies and procedures to maintain adequate security of the ICS and to allow adequate access to the system when required. How the policies are written and applied will impact their effectiveness. For example, forcing separate usernames and passwords to be used on multiple systems with frequent password changes may simply result in employees writing down their details so that they can remember them.

So if not IT, whose job is it?

When the ICS was a standalone system running on proprietary hardware and software, the responsibility for implementation and maintenance was largely within the 'control department'. As the ICS has become more integrated with other systems and can run on industry standard operating systems and communicate over standard network infrastructure, the skills required to implement and maintain the system have significantly changed.

In addition, the IT department may have been seen in the past as 'the enemy' by the control department, enforcing policies and procedures on the ICS to comply with company security requirements, without maybe fully understanding the implications of these on the ICS.

Today the skills of both control engineers and IT engineers are required to maintain an ICS and whether these skills are available within the control department or not, the control and IT departments will need to work closely together to ensure availability and security of the ICS is maintained.

As we have seen in some of the examples above, for an ICS, the traditional image of a cybersecurity threat – the hacker breaking in to a system from many miles away – is only one possibility and the sources of threats to the security of an industrial control system can be varied. In order to identify and control all the risks, the input of a multi-disciplinary team with access to the appropriate resources will be required.

The plant manager will need to ensure that he or she understands the nature and consequences of the risks and that an appropriate team with the required resources is in place to identify and control them, just as with any other form of process hazard assessment.

References

1. *The Farwell Dossier, New York Times, William Saffire, 02/02/04*
2. *In Bleak Russia, a Young Man's Thoughts Turn to Hacking, New York Times, John Varoli, 29/06/00*
3. *Slaying the Hackers, Brisbane Times, Penelope Debelle, 15/04/08*
4. *Slammer worm crashed Ohio nuke plant net, The Register, Kevin Poulsen, 20/08/03*
5. *CyberSecurity and the Pipeline Control System, Pipeline and Gas Journal, Eric Byres, 02/09*
6. *NRC Information Notice 2007-15: Effects of Ethernet-based, non-safety related controls on the safe and continued operation of nuclear power stations, US NRC,17/04/07*
7. *Schoolboy hacks into city's tram system, The Telegraph, Graeme Baker, 11/01/08*
8. *Stuxnet 'hit' Iran nuclear plans, BBC, 22/11/10*
9. *First came Stuxnet computer virus: now there's Duqu, Reuters, Tabassum Zakaria, 19/10/11*
10. *Guidance for Addressing Cyber Security in the Chemical Industry Version 4, American Chemistry Council, November 2009*
11. *http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf*

0260-9576/12/$17.63 + 0.00