The SCADA Threat Landscape

Michael Robinson
EADS Innovation Works
Celtic Springs
Coedkernew
Newport, NP10 8FZ
UK
www.eads.com
michael.robinson@eads.com

Nations around the world rely on the correct and continued functioning of industrial control systems (ICS) to keep economies moving and provide critical services such as electricity and clean water. This paper provides an analysis of the current threat landscape facing ICS. Discussion is provided on the actors involved, their motivations, and specific attack vectors they may use to reach their goals.

SCADA, ICS, Threat Landscape, Security

1. INTRODUCTION

Nations around the world are increasingly becoming reliant on the correct and continued functioning of critical national infrastructure (CNI). Stock exchanges and banking systems keep economies moving and allow every day life to continue, the power grid generates the huge amounts of electricity required to keep homes and businesses running, and water systems provide homes with clean water whilst safely treating waste. Around the middle to late twentieth century, security for national infrastructure was a minor concern that could be addressed by simple physical security measures such as a locked door. With no external connections and no internet, physical security was all that was needed. In many cases, even physical security was a luxury many facilities did without, simply because there was no imagined reason why anyone would want to enter.

With the arrival of cheap computing in the 70s and 80s, these critical infrastructures became increasingly computerised. As networking became more affordable and available, utility companies found cost savings by connecting facilities together and controlling distributed systems from a central control centre. Corporate divisions were also plugged into the systems, allowing direct access to various statistics and reports about global operations. Unfortunately, while the complexity and interconnectedness of these systems increased, security did not. Old systems designed without security in mind were now exposed to much more than just physical access issues. In the worst case, control panels for critical systems can now be directly accessed via the internet.

This paper surveys the current threat landscape faced by these systems, examining the who, why and how of attacking an industrial control system, from both the attacker and defender's perspective.

2. THREAT ACTORS

In today's world, there are a multitude of potential attackers, all with various ultimate goals. This section describes the main actors that may have an interest in attacking a SCADA system and their motivations. An estimation of their potential impact is also given.

2.1. Hostile Nations and Foreign Intelligence Services

During war and conflict, an enemy nation may seek to attack another by targeting the critical national infrastructure. By disrupting areas such as power, transportation and industry a nation can weaken another and bring a war or dispute to an early conclusion. An attack by a hostile nation is a high threat, since the resources behind the efforts will be substantial. These resources can be used to hire highly skilled hackers, who can operate without fear of prosecution in their home country. Highly skilled coders can also be hired, who can be tasked with coding advanced malware that avoids detection and delivers reliable payloads. Stuxnet was very robust

and highly obfuscated, and provides an example of what can be done with the resources of a nation state. In addition to the best coders and hackers, a nation state may have influence over vendors and convince them to insert backdoors into hardware. Nations are fully aware of this, and recent bans on awarding contracts to Chinese technology firm Huawei due to security concerns have confirmed an awareness of this threat Arthur (2012). Finally, the resources and status of a nation allow it to simply buy the hardware that another nation is using and test it locally for weaknesses, an ability that other potential attackers will not have (even if a hacking group managed to raise the funds, they are going to raise alarm trying to purchase nuclear centrifuges). Nations do not have to be at war to be interested in attacking the national infrastructure of another nation. Many nations have an interest in on-going information gathering on other nations, and seek to extract data from national infrastructure. The realisation that future wars may be held in cyberspace also encourages nations to keep up to date on each other's activities and test their ability to breach another nation's cyber defences. Again, with a nation's resources behind the attack, the threat is high.

2.2. Terrorist Groups

Critical national infrastructures are a tempting target for terrorist groups looking to cause fear, damage and loss of life. Air traffic control systems, nuclear power plants, the water supply and food production are just a few examples of areas where a terrorist group could target their activities. While lacking the resources of a nation state, terrorist groups may still be able to attract highly skilled hackers and coders due to an ideological appeal, rather than due to a financial reward. Terrorist groups may also have an extensive support network and unofficial support from their nation, somewhat shielding the attackers from the threat of prosecution.

2.3. Industrial Spies

Organisations themselves may also be potential attackers of SCADA systems. By breaking into a competitor's industrial control systems, trade secrets about production processes may be stolen and damage done to inflict financial harm or a drop in public confidence in the safety of their products. A large multinational will have the resources to hire quality hackers and coders, but the work will be clearly illegal with a risk of prosecution and damage to the organisation's reputation.

2.4. Criminal Groups

Criminal groups also have an interest in attacking SCADA systems. An organisation could potentially be held to ransom once a criminal group manages to gain control over its systems. Likewise, a nation could be held to ransom should a criminal group claim to have control over critical national infrastructure. The threat level of such groups may vary. Some may be amateurish attempts at extortion by one or two people, using simple Ransomware (malware that infects a machine and demands a payment to remove it and give control back). On the other hand, there is a potential that an already established criminal group could hire quality hackers, and launch a well-orchestrated extortion attack on an organisation. There is also the possibility for a truly high tech crime group to emerge. This group would differentiate themselves from traditional criminals by showing innovative methods of making money illegally through SCADA systems. An example of this may be acquiring false refunds on energy costs through a smart grid.

2.5. Disgruntled Insiders

Perhaps the biggest threat, disgruntled insiders already possess the knowledge of and access to an organisation's SCADA systems. An insider may include employees as well as contractors and business partners. In 2000, a sewage plant in Australia began to overflow shortly after it was activated, filling a river, park and nearby hotel with 264,000 gallons of raw sewage Tsang (2012). Operators struggled to locate the problem, but eventually tracked it down to a series of spoofed controllers, set up by a contractor who originally installed the control system. It was later determined that the contractor was intentionally making the plant overflow, in an attempt to make the company hire him to solve the problem. While their hacking knowledge may be low or zero, their knowledge of how the system operates and their privileged access to it makes the disgruntled insider a very high threat. Motivations can vary from revenge to being a part of a larger plan such as terrorism or extortion. An insider may act alone or be approached by one of the other groups discussed in this paper, such as criminal groups or a commercial competitor.

2.6. Hacktivists

Activist groups are increasingly becoming more active in the cyber world, using cyber-attack as a means of making a political or ideological point. Anti-nuclear groups may target the control systems of nuclear plants, environmental groups may seek to disrupt oil exploration attempts in the Arctic by disabling or damaging SCADA equipment on rigs. As with terrorist groups, high quality coders and hackers may be attracted by the ideology and personal beliefs.

2.7. Hackers

The final potential attackers are hackers. This group do not have an agenda other than proving that they can defeat defences and take systems over. There are generally two types of hacker, those that possess a good amount of knowledge and skill and those that simply run tools and scripts that are created by others. While the first type is obviously dangerous, the second type can still cause disruption and damage: especially when they may not realise the full effects of the tool or script they are running. The threat from a good hacker is high, since they possess a great deal of hacking knowledge and have a personal drive to defeat defences.

2.8. Comparison Table

Figure 1 below provides a visual overview of the potential levels of attack each actor could inflict and their related motivation for doing so. Note that only the highest potential attack level is shown for each actor. For example, nation states can achieve level five, and all levels below. The potential attack levels are defined as follows:

Attack Level	Description
1	The effects of the attack are minimal. Attacker may simply be snooping on operations or running scripts to little effect
2	The effects of the attack are limited. Disruption to one local facility with no wider effect. Possible data theft or tampering
3	The effects of the attack are wide-ranging. Disruption to multiple nation-wide services, acting as an inconvenience to daily life. Nation as a whole still able to run
4	The effects of the attack are extensive and sustained, bringing down at least one critical infrastructure, such as nationwide air traffic control. Lives put in danger. Attacker actively works to counter attempts to restore the infrastructure
5	The effects of the attack are sweeping and sustained, crippling multiple parts of a nation's CNI and bringing everyday life to a halt. Loss of life caused. Attacker actively works against defenders to sustain the attack

Table 1: *Potential Attack Levels*

Highest Attack Level	Political Motivation	Personal Motivation	War/Peacekeeping Motivation
Sweeping and Sustained (5)	Nation States		Nation States
Extensive and Sustained (4)	Terrorist Groups	Insiders Terrorist Groups	
Wide Ranging (3)		High Skill Hackers	
Limited (2)	Hacktivists	Hacktivists Med. Skill Hackers	
Minimal (1)		Low Skill Hackers	

Figure 1: *Actor Attack Level Table*

Note: This table is for a general overview of estimated attack levels and motivations that can be expected of the various groups. **It should be noted that it is always possible for an actor to cause much higher damage than expected due to luck** (e.g. a low skill hacker using a script which triggers a chain reaction could reach level 3).

3. ATTACK VECTORS

SCADA systems were developed at a time when the main concern of their users was to increase operator efficiency. By providing a centralised console, one operator was able to operate many distributed systems, allowing plant owners to make cost savings. With the internet not yet invented, the security of these systems was a minor concern that extended no further than ensuring that unauthorised people were not able to walk into a plant and use a terminal. Even as technology advanced, the design of SCADA systems lagged behind on issues of security, with assumptions made that air gaps would exist and unauthorised remote access would be unlikely. The fact that SCADA systems run critical infrastructure means they cannot simply be taken down and upgraded; even patching is difficult. For this reason, a modern day attacker can find multiple attack vectors that simply wouldn't exist on a system used in other sectors such as finance or defence. This section will explore these attack vectors.

3.1. Lack of protocol security

With the original focus on efficiency rather than security, a number of SCADA protocols still in use today have little to no security measures. Modbus, a popular SCADA protocol, is one that has no inbuilt security. A lack of authentication means that remote terminals will accept commands from any machine that claims it is a master. A lack of integrity checking or encryption means that messages may be intercepted, altered and forwarded on with no

mechanism to prevent it. DNP3, another popular protocol used in SCADA, also suffers from a lack of security. A malicious user may easily spoof replies from a particular outstation, making it appear to be unavailable and denying a master the opportunity to issue commands or collect data. Where passwords are sent across the network, it is not uncommon to see them sent in clear text. Attempts have been made to add security to protocols, as can be seen with DNPSecure. Putting these protocols into live environments is a difficult task however, since the kind of systems using them are critical national infrastructure in which any downtime is unacceptable.

Effects

The potential consequences of poor protocol security include:

1. Spoofing of requests and/or responses
2. Man in the middle/message tampering
3. Replay attack
4. Traffic snooping
5. Credential Theft

Effects 1-3 are significant and can lead to an attacker bringing down a SCADA system or causing a dangerous situation. While not an immediate threat, traffic snooping over a long period will provide an attacker with information on how the system runs and potentially allow them to better obfuscate a future attack by making it blend into normal traffic. In the case of CNI, it may also be a vector for espionage. As an example, country A may be very interested in building a profile of how country B's new smart grid system operates.

Red Team Perspective

In order to exploit a protocol's lack of security, an attacker must first gain access to the network that the protocol is being used on. This could be achieved by physical access (breaking into a facility, use of an insider) or by exploiting other attack vectors to gain remote access. Once on the network, tools such as Wireshark can be used to snoop on and capture samples of traffic. Packet crafting tools can then be used to either simply replay commands onto the line, or to first modify them to carry out some kind of malicious action.

Blue Team Perspective

From a defender's perspective, mitigating the impact of weak protocol security revolves around four approaches:

1. Preventing access to the network via good network security

The first step a defender needs to consider is the idea of perimeter control. In an ideal world, a sensitive SCADA system would be isolated and have no external connections. But in reality, that may not be the case. In cases where external connections exist, the perimeter of a SCADA network should end at connections to corporate networks, wireless access points, dial in/VPN connections and at connections to external parties such as business partners and backup services. Firewalls are the standard method to enforce a perimeter, and are an essential component in denying an unauthorised person from getting into the SCADA network. Defenders may also consider layering perimeters, whereby particularly sensitive networks are given a perimeter inside of the wider SCADA perimeter. This inner perimeter can be given very specific firewall rules that further protect it from an outsider looking to exploit the weak protocols used inside. IDS and IPS are additional valuable defensive tools to detect and prevent unauthorised access to the network carrying these weakly secured protocols. Data diodes are another option, physically enforcing one way communication out of the SCADA network.

2: Strengthening the security of the protocols

This approach to defence is a difficult one but research is advancing in this area. Researchers have developed new versions of existing protocols that add levels of confidentiality and integrity. While these protocols work in theory and in simulated environments, placing them into live environments is challenging since it would mean significant amounts of downtime and potential issues with systems that run critical infrastructures. Unsurprisingly, governments and utility companies are not scrambling to be the first to take down their national grid to beta test an improved protocol.

3: Redundant Systems

A potential way to mitigate the effects of weak protocol security is to simply have redundant systems. Should an attacker manage to get into your network and send a malicious message to shut down a system, a redundant system elsewhere would take over and ensure an uninterrupted service. By eliminating single points of failure, an attacker must perform a more complex attack to achieve something destructive.

4: Monitoring

A final mitigation that is essential in defending from weak protocol security is monitoring. Logs must be generated and monitored to alert staff that something abnormal may be happening. Without effective log monitoring an attack may go undetected

and post-incident investigation will be difficult. Security Information and Event Monitoring (SIEM) solutions are ideal for this task, raising alerts when abnormal network messages are detected. Adapting SIEM solutions to work seamlessly on SCADA networks is an ongoing area of research.

3.2. Erosion of Isolation

SCADA systems were originally isolated from the outside world. Sensors would simply monitor equipment and provide that information to a central control room. As networking has advanced and become more accessible, organisations have made decisions to integrate systems DigitalBond (2012). What were once isolated systems are now connected to corporate networks, allowing a head office to receive statistics and information from numerous remote sites. While protections such as firewalls are put into place, a physical connection to the outside world and the internet now exists. This opens the way for a determined attacker to leverage zero day vulnerabilities and social engineering to find a path through the corporate network to these once isolated systems. Aside from targeted attacks, there is also a constant threat of a path opening up by chance. Infected USB drives, infected websites and everyday social engineering that happens on a corporate network may open up paths to a SCADA network to the whole world.

Effects
The potential consequences of the erosion of isolation include:

1. Providing unauthorised remote access to a SCADA network

This effect is significant, since it provides the means for an attacker to exploit other attack vectors, such as weak protocol security.

Red Team Perspective
In order to exploit the erosion of isolation, an attacker must successfully locate and exploit vulnerabilities in the corporate network and ultimately build themselves a path to the SCADA network.

Blue Team Perspective
As with weak protocol security, the erosion of isolation can be defended against by having good network security. Layered perimeters defended by firewalls, IDS, and diodes, along with regular auditing of logs to detect intrusion attempts. Diodes can be particularly useful where network connections are required to send data out of a control network (e.g. statistics and monitoring) while still preventing traffic travelling back in. Where possible, authentication should be enforced with good password management at both perimeter devices and devices inside the perimeter. Staff awareness and the adoption of policies such as ISO27001/2 will also help mitigate the problems of eroded isolation.

3.3. Configurations: Convenience over Security

This attack vector exists due to the legacy of SCADA systems being isolated and the perception of air gaps. With the focus on efficiency and productiveness, it is common to find SCADA systems configured for convenience rather than security. Systems can be accessed with no authentication: if you can get to a terminal (either physically or remotely), you have full access. Where authentication is in place, passwords are often left as default or changed to something extremely weak, short and easy to guess. In some cases, passwords are actually hard coded into systems, meaning that they cannot be changed at all. Passwords can also be the same across multiple systems. With the growth of mobile computing, wireless networks are set up to give operators access to the SCADA network on the move. These wireless networks are again configured for convenience and may have weak passwords and poor or no encryption. Some older SCADA systems still use dial-up modems to allow remote access. In newer systems, VPN access has replaced this dialup access. Again, these systems can be potentially configured for convenience and not with security in mind.

Effects
The potential consequences of convenience over security include:

1. Unauthorised remote or local access to SCADA systems.

Red Team Perspective
In the case of insecurely configured wireless networks, the attacker needs to know which network to connect to and be in range with a device capable of connecting. For dial-up and VPN access, the attacker needs to know the telephone number or VPN details. To exploit poorly configured systems, the attacker needs either remote or local access to the system. Remote access can come from the erosion of isolation discussed previously. Local access can be achieved by exploiting failings in physical security at a site.

Blue Team Perspective
To defend against this threat, defenders must move away from a culture that emphasises purely convenience and towards one that balances convenience with security. Passwords should not be left at default and should ideally be subject to the

same password management policies that would apply on a corporate network. Unfortunately, due to the age and design of some SCADA systems, passwords may have to be changed at each machine manually or simply be hard coded, making password management difficult. Defenders should ensure that all external points of access such as wireless access points or dial in modems are properly protected. In the case of wireless access, MAC filtering can be applied to provide a whitelist of allowed devices, along with the use of WPA2 encryption. If these devices only support WEP, they should be replaced with modern devices. Dial in and VPN connections should challenge the connector for a username and password. Staff should be encouraged to lock workstations when not in use.

3.4. Weak Audit Trails

One of the main goals of IT security is to allow for non-repudiation. This is the goal of making it difficult for a particular person to deny sending a particular message or command. Somewhat related to the convenience over security issue, a system with shared logins such as admin present an issue in identifying which particular employee sent which command. If suitable logs are not kept, it may not even be possible to determine a time and date of a command being sent. This lack of accountability for actions on the SCADA network opens the way for a malicious insider to attack systems and remain undetected.

In addition to user actions, the actions of hardware also need to be audited. In 2012, the US blocked Chinese firm Huawei from being awarded certain telecommunications contracts due to national security concerns over its hardware Arthur (2012). This was due to suspicions that the hardware itself contained malicious code and hence could not be trusted. Therefore, auditing needs to focus on both usage by operators and the actions carried out by hardware with no user input.

Effects
The potential consequences of a weak audit trail may include:

1. Difficulty identifying who did what and when
2. Lack of hard evidence for a court case
3. Failure to notice abnormal activity before it becomes a security breach (brute force attempts on accounts, attempts to connect to systems etc.)

Red Team Perspective
From an attacker's perspective, weak audit trails are just a bonus that removes the need to spend time and effort covering their tracks. Connections can be made and commands sent with no record being kept. This allows the attacker to carry out more aggressive probing into the network without the worry of obvious trails being left in logs. In the case of a malicious vendor, the vendor simply needs to sell the device to a victim and have it installed into the infrastructure. Weak auditing will then allow the device to steal data or cause problems undetected.

Blue Team Perspective
The only real mitigation for weak audit trails is to add more logging and policies to review those logs. It should be noted that organisations may be reluctant to add logging since it may add delay or the potential for instability to mission critical systems. Defenders should check that all firewalls and IDS/IPS have logging enabled, and a security information and event monitoring (SIEM) program to monitor those logs and raise alerts.

To audit the actions of hardware, organisations can consider using a trusted third party who specialise in testing devices and detecting hidden or undocumented behaviour.

3.5. Vendor Back doors

Even if an organisation implements a very good security policy, attackers may still be able to find an attack vector through vendor back doors. Unlike a bug, a vendor back-door is a way into a piece of hardware or software that is undocumented and hidden. Vendors can use these back doors for remote support, to temporarily give admin rights to apply updates or as a last resort if an organisation gets locked out of their systems. In 2012, one such vendor back-door was discovered in Ruggedcom equipment widely used in perimeter defence. It was found that a hidden 'factory' account existed, with the password derived from the MAC address DigitalBond (2012). Once someone knows the existence of this account, they only need to discover the MAC address to gain unauthorised access to the device.

Researchers have for a long time suggested that computer chips made in China for the US military have contained such vendor back doors Business Insider (2012), raising fears that there are many more back doors out there that are sitting in critical equipment. Vendor back doors can be either intentional or non-intentional. Beyond that, they can be either malicious or non-malicious. Figure 2 below gives some examples of each characteristic:

	Intentional	Non-Intentional
Non Malicious	A backdoor intended for remote support	Test account used by developers accidentally left active
Malicious	Hidden account deliberately added by vendor to spy on the buyer	Rogue worker adds a personal backdoor for later use, vendor unaware

Figure 2: *Types of Vendor Back doors*

Effects

The potential consequences of vendor back doors include:

1. Unauthorised remote or local access to devices.

Red Team Perspective

By their very definition, vendor back doors are hidden and so are not immediately visible to a potential attacker. Information about these backdoors must either be leaked from the vendor or discovered in the same way that exploits are. To exploit a known vendor backdoor, an attacker must be able to communicate with the device in question. The erosion of isolation, weak physical security at the location or insecure wireless networks are potential paths to this goal.

Blue Team Perspective

To mitigate the effects of vendor back doors, organisations should aim to have multiple layers of network security. Should a back-door be found in one device, the next device will still provide an obstacle for the attacker. Using a trusted third party to test devices before putting them into use may also detect these back doors before they are exploited. Keeping logs and regularly reviewing them may also help to detect that a back-door is being used, although the device itself should not be trusted with this job since it may intentionally not log use of the back-door. Finally, defenders should ensure that their organisation has good supply chain management and knows where equipment is coming from and its history.

3.6. Interconnectedness

Critical national infrastructure is increasingly becoming more interconnected, with multiple distributed systems depending on each other to function properly. While important systems may have strong defences in place, the overall robustness of the system is only as good as the weakest link in the chain. A prime example of this is the national grid. In August of 2003, a bug hidden inside a General Electric management module triggered a chain reaction that took out power systems across Northern America, leaving eight US states and two Canadian provinces without power Farmer et al. (2005), Poulsen (2004). With knowledge of the level of interconnectedness seen in CNI, an attacker can focus on the weakest link and still achieve their goals.

Effects

The potential consequences of interconnectedness include:

1. Attacker can target weakest link and still achieve success.
2. An organisation can suffer problems due to a failing of another organisation.

Red Team Perspective

To exploit interconnectedness, an attacker must either get lucky and hit a device which has knock on effects, or carry out research to plan and specifically target a device which is likely to cause knock on effects. Once the chain reaction has started, the attacker does not need to take any additional actions.

Blue Team Perspective

Protecting against interconnectedness is a difficult task, since it is difficult to know what the knock on effects will be until it happens. Organisations should collaborate to discuss how their systems connect to each other and identify which systems are the most critical and interconnected. Plans can then be drawn up to provide extra security for that system.

3.7. Human Error

When looking at potential threats to a SCADA system, it is important to consider accidental damage as well as intentional attack. As SCADA systems increase in complexity and become more interconnected, the chance for human error increases. These errors can be the result of a simple mistake (i.e. entering the wrong value or forgetting to carry out a process), or due to a lack of training. Stuxnet was first introduced to Iranian nuclear facilities via a USB device used by an employee.

Effects

The potential consequences of human error include:

1. Damage to systems with potential knock-on effects to other systems.
2. Unintended changes to processes.

Red Team Perspective

In a scenario where an operator inputs a command and an undesirable effect takes place, there is no attacker, it is simply a mistake. Human error can be exploited in other scenarios however, such as leaving an infected USB stick on the floor outside of the facility. Out of curiosity, a worker at the facility may insert the USB into a system to see what it contains. At this point, malware can be automatically transferred onto the system. Human error may also provide opportunities for an attacker in the form of incorrect firewall rules, or rules that are added temporarily for testing but never removed once the testing is over.

Blue Team Perspective Human error is unavoidable but the threat can be reduced by having regular, up to date training of staff. In addition, checks should be in place to ensure that commands are entered correctly these can be automated checks using logging to flag potential errors or manual checks by another operator before an operation is permitted. In general, the organisation should have clear policies in place that limit the chances for human error to go undetected.

3.8. Unpatched Systems

Some industrial control systems need to be on 24/7 with no downtime. Once systems are up and running, organisations are reluctant to install updates to either the OS or applications. These updates may involve reboots and introduce instability or new bugs that could bring an organisation to a halt. For these reasons, organisations are much more inclined to simply leave the system as it is and avoid making any changes. For an attacker, this is extremely useful since no security updates will have been applied. This gives them the opportunity to exploit well-known vulnerabilities that are potentially years old.

Effects

The potential consequences of unpatched systems include:

1. Easy unauthorised access and control of systems.

Red Team Perspective

The attacker must discover at least one known vulnerability in the current version of OS or application being run on the target system. They must also be able to communicate with the system to exploit such vulnerabilities (e.g. secure wireless access or have access to the SCADA network via compromising another machine).

Blue Team Perspective

Having good network security will help to prevent an attacker from reaching an unpatched machine. Having redundant systems will also help in patch management. Should a patch introduce undesirable effects, the redundant system can take over until the patch is rolled back. Using an up to date intrusion detection system is also advisable, since it will have signatures for well known exploits and prevent such attacks from reaching the vulnerable system.

3.9. Malware

SCADA systems are just as (or even more) susceptible to malware as corporate systems, and the effects are potentially much more serious. To reduce potential instability and to ensure that the speed of the system is not hindered, SCADA systems rarely run any form of anti virus, firewall or IDS. This means that once malware has accessed a system, it is not going to be automatically detected and stopped. Malware infections into SCADA systems can be both general and targeted. As an example of a general malware infection, it was reported in 2011 that the USAF drone control systems had become infected with a key logger Naked Security (2011). This key logger did not specifically target the control centre, and could not communicate out, but its presence on the system was undesirable and its overall effect on the flying of drones was unknown. On the other hand, Stuxnet was coded to specifically target a very particular piece of Siemens hardware, and to perform a very specific action of changing the speed of centrifuges.

Effects

The potential consequences of malware on SCADA systems include:

1. Damage and impairment of systems.
2. Unauthorised remote access.
3. Data exfiltration.

Red Team Perspective

There are numerous ways a piece of malware can get into a SCADA network, ranging from USB drives to drive by downloads to coming preloaded on a new piece of hardware. Social engineering can be used to trick an employee into clicking a particular link in an email or by leaving a USB drive on the ground near a facility and hoping an employee inserts it into a machine out of curiosity. Once the malware is inserted into a machine on the SCADA network, it may attempt to call home and establish a connection with a command and control machine, allowing remote control or transferring data.

Blue Team Perspective

A SCADA system can never be completely secured from malware, but good security policies, the application of the principle of least privilege and host hardening techniques can be used to lessen the chance of infection. When an infection does occur, an organisation should have adequate logging in place to detect it, and a response plan to act quickly in its containment and removal. Good network security is also essential in preventing the spread of malware, along with staff training on how to avoid malware and redundant systems that can take over the running of systems should another fail. Making physical security teams aware of what items may potentially introduce malware (such as USB sticks or smartphones) and confiscating them before they reach a critical system is also important.

3.10. Adoption of Standards and Common Technologies

While the SCADA systems of the past often relied on proprietary software and technologies, modern systems are increasingly adopting more commonly accepted standards. Data is transported across TCP/IP networks; interfaces are displayed using a Flash or Java interface with an Apache or IIS webserver behind the scenes. These are also likely to be old versions: Either they simply can't be updated or the update process risks downtime, instability or loss of configuration. These common technologies are easier to use and implement since they are better understood, but this understanding is also possessed by attackers and can be used to help attack the system.

Effects

The adoption of standards has the following potential consequences:

1. Large number of known and zero day vulnerabilities, especially for old versions.
2. Attacker has advance knowledge of technologies being used.

Red Team Perspective

To exploit these common technologies, an attacker must be aware of a known vulnerability in a common technology such as Java or Flash, and be able to locate a suitably vulnerable version in use on the SCADA network. They must be able to communicate with the vulnerable piece of software in order to exploit it.

Blue Team Perspective

As with most attack vectors discussed so far, good network security is a key element of defending against vulnerable common technologies, since an attacker cannot exploit a vulnerability if they cannot access it. Improved logging would help to detect if an attacker was attempting to exploit a known vulnerability. If possible, security patches should be applied as they are released, but in a SCADA environment this may not be viable since downtime or instability may be introduced. Mitigation solutions such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET) may also have a role to play here, although extensive testing must be carried out before deployment since a product such as EMET changes the actions of processes to make them more secure. Having redundant systems is also a benefit, since patches can be automatically applied on one system while the redundant system continues operation. If the patched system performs identically to the unpatched system for a certain amount of time, the other system can also be patched. The best option is to avoid common technologies that regularly get breached, such as Java and Flash.

3.11. Lack of physical security

As the name suggests, distributed control systems can be distributed at multiple remote locations. Many of these locations are unmanned, simple structures where physical security may be limited to a padlock on a door. An attacker may break in and interfere with the SCADA equipment with little fear of being caught. Even at a larger, manned facility, an intruder may claim to be an engineer or contractor and be given physical access to sensitive equipment.

Effects

1. Unauthorised local access to SCADA equipment

Red Team Perspective

Attacker must locate remote equipment, and possess enough tools to break into the location or gain access through deception. A determined attacker acting as an engineer may make multiple visits to win trust. Once inside, they can cause problems simply by physically damaging the equipment. A more advanced attacker may possess the ability to do something more destructive, by sending or tampering with commands from the accessed equipment or changing configurations.

Blue Team Perspective

At a basic level, organisations should ensure that there is reasonable physical security at all locations

where SCADA equipment is present. Doors should be locked and not propped open; staff training and policies should reflect this. Policies should state a minimum level of physical security for all systems. For an organisation such as an electricity provider, this is obviously difficult since the systems are very distributed in nature with substations all around a nation. Organisations should also examine how traditional, physical security operations in their organisation work with cyber security operations. Often these two teams are unconnected and do not communicate to see the bigger cyber-physical security picture. Cyber-physical security can be defined as the integration of logical security, information security, physical and personnel security, business continuity, disaster recovery and safety risk management Slater (2011). By integrating all these security aspects, a number of benefits can be gained such as having a single point of contact for all security issues. This allows a security issue to be easily reported and solved by the collaboration of both physical and cyber security teams. As attacks on an organisation may involve both physical and cyber aspects, this collaboration is essential.

3.12. General Security Issues

This category covers security issues that are not specific to SCADA systems, but still present a threat. This includes software based vulnerabilities, such as buffer overflows and SQL injection. These can be present in web interfaces and will allow an attacker to crash the program or take control over processing. General network security is also an issue. Where they exist, firewalls and IDS systems need to be carefully configured with the principle of whitelisting (i.e. block everything, then only allow the minimum that is needed to carry out business). A firewall that is poorly configured can allow an attacker to pass through and exploit further attack vectors. Network administrators should also ensure that port security is upheld, unused network ports should be disabled and active ports should have MAC and IP address restrictions, to hamper a physical attack whereby an existing device is unplugged and replaced by a new one. These are all general cyber security issues that organisations should already be addressing, whether they use SCADA systems or not. US Cert provides extensive guides for anyone looking to secure their organisation from these general threats US CERT (2011).

Figure 3 provides a summarised overview of the discussed threats and associated controls.

	Improved Network Security	Improved Protocol Security	Redundant Systems	Staff Training	Policies	Improved Logging	Collaboration	Improved Cyber-Physical Security
Lack of Protocol Security	X	X	X			X		
Erosion of Isolation	X	X	X	X	X	X	X	X
Convenience over Security				X	X			X
Weak Audit Trails						X	X	
Vendor Backdoors	X					X	X	
Interconnected-ness							X	
Human Error				X	X	X		
Unpatched Systems	X		X			X		
Malware	X		X	X	X	X		X
Adoption of Common Tech	X		X			X		
Lack of Physical Security				X	X			X

Figure 3: *Attack Vectors and Controls*

4. ATTACK CHAINING

It should be noted that while these attack vectors are all significant, one alone is unlikely to result in a security breach. An attacker will exploit many of these vectors to carry out a complete attack. Figure 4 below gives an example of how an attack may take place by chaining together some of the attack vectors discussed in this paper.

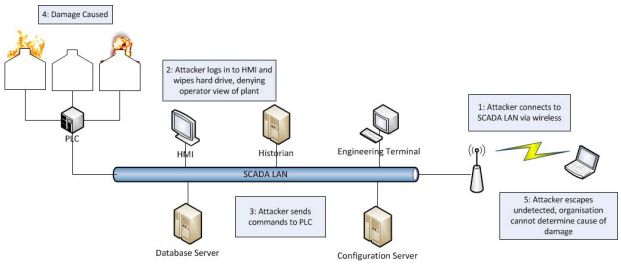

Figure 4: *Example Attack Scenario*

In this example, we can see that an attacker uses a wireless access point to connect to the SCADA network. They deny workers at the facility a view of the factory by disabling the HMI. Malicious commands are then sent to a PLC, which causes damage to the factory. The attacker is then able to escape undetected and the organisation is left wondering how this attack occurred, or even if it was just an accident. Figure 5 below shows how

the attacker was successful at each stage of this example attack:

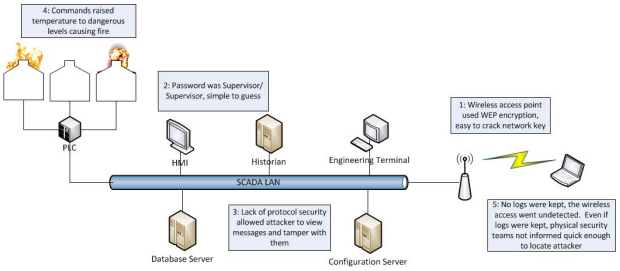

Figure 5: *Reasons for Attacker Success*

Firstly, the attacker exploits the erosion of isolation and the organisation's failure to update systems. The wireless access point did not use MAC whitelisting, and hence allowed anyone to connect. Once connected, the attacker was challenged for a network key. The use of weak and outdated WEP encryption allowed the attacker to easily determine this key beforehand. Once on the network, the attacker exploits convenience over security, by trying some obvious logins on the HMI terminal. They eventually guess supervisor/supervisor. This account has full administrative access to the machine, allowing the attacker to wipe the hard drive of the HMI. This leaves the supervisor with no view or control over the operation of the plant. The attacker then exploits weak protocol security by snooping on the traffic on the network. With some sample messages captured, the attacker can use a tool to craft their own messages containing commands to raise the temperature to high levels. The attacker disconnects, no logs are kept and the organisation is left mystified as to how this damage occurred. The problem of the insecure wireless point is not corrected, and the attacker may repeat their attack in the future. Even if a cyber security officer determined that the attack was coming via wireless, physical security officers are not informed quick enough due to a lack of cyber-physical security operations at the organisation and the attacker can escape the location.

Figure 6 below shows how the attack may be made more difficult by implementing some of the blue team recommendations made in this document and by having a secure architecture:

Here we can see a number of defences in place. Multiple firewalls provide perimeter security to multiple layers of perimeters, with particularly sensitive systems (highlighted in yellow, blue and green) given their own perimeters with deep packet inspection firewalls. Alongside these firewalls, one way gateways such as data diodes are used, to help ensure that data can only flow in one direction. A security operations centre (SOC) uses security information

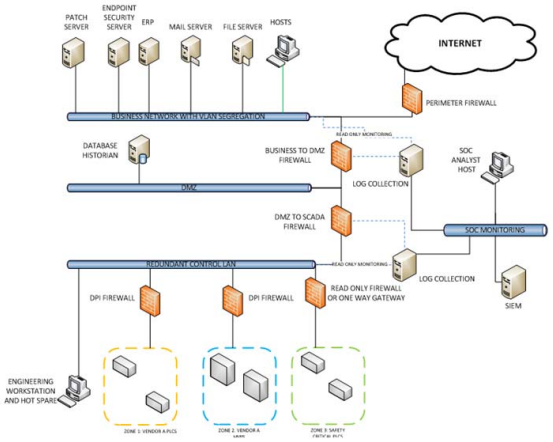

Figure 6: *A more secure architecture*

and event management (SIEM) systems to monitor logs and events from throughout the organisation.

5. RELATED WORK

This paper has suggested ways in which an organisation can develop policies to defend from a variety of SCADA threats. Aside from the advice in this paper, other efforts to develop best practice exist. ISA99 (2013), a standards development committee with a focus on industrial control systems is one such group also working to help protect critical infrastructure. NERC (2013), also focusses on developing standards, but specifically for power grid systems. In Europe, ENISA (2013) also provide a number of documents advising how best to secure industrial control systems.

6. CONCLUSION

This paper has looked at the SCADA threat landscape: The who, why and how of SCADA security. For each vector, red and blue team perspectives have been given, allowing an insight into both sides of the situation. The advice given to blue teams by this paper should be considered as pointers to help formulate an organisation's policies and to help support risk assessment procedures. Policy formulated from thorough risk assessment is the key to good security, and by ensuring current policies reflect the advice in this paper and other relevant works, blue teams can ensure that systems are protected by best practice.

REFERENCES

Arthur, C. (2012) Huawei contract ban stokes fear of cyber cold war. *Guardian*.

Business Insider (2012) Sergei Skorobogatov defends backdoor claims. *Business Insider*.

DigitalBond (2012) Ruggedcom backdoor revealed - fragile.

ENISA (2013) Protecting industrial control systems. Recommendations for Europe and member states.

Farmer, R., Anderson, G., and Donalek, P. (2005) Causes of the 2003 major grid blackouts in north America and Europe, and recommended means to improve system dynamic performance, IEEE Trans. Power Syst., 20 (4/Nov.). 1922-1928.

ISA99 (2013) ISA99 industrial automation and control security. Research Triangle Park, NC, USA: ISA.

Naked Security (2011) Malware compromises USAF predator drone computer systems.

NERC (2013) North American Electric Reliability Corporation.

Poulsen, K. (2004) Software bug contributed to blackout.

Slater, D. (2011) Physical and it security convergence: The basics. CSO.

Tsang, R. (2012) Cyberthreats, vulnerabilities and attacks on SCADA networks.

US CERT (2011) Governing for enterprise security.