The Top 20 Cyber Attacks Against Industrial Control Systems

Andrew Ginter, VP Industrial Security
Waterfall Security Solutions
December, 2017

Introduction

No industrial operation is free of risk, and different industrial enterprises may legitimately have different "appetites" for certain types of risks. Evaluating cyber risk in Industrial Control System (ICS) networks though, is difficult - for example, such evaluations can result in considering explicitly or implicitly up to hundreds of millions of branches of a complex attack tree modelling the interaction of cyber attacks with cyber, physical, safety and protection equipment and processes. Communicating the results of such risk assessments to business decision-makers who are not versed in cyber-physical risk-assessment techniques can be even more difficult.

One approach to communicating risk is a concept from physical security – the Design Basis Threat (DBT). A DBT document describes the most capable threat or attack that a site is required to defeat reliably. A recent whitepaper from Waterfall Security Solutions argues that cyber DBT is best modelled as a line separating a set of example attacks into two sets: one that is reliably defeated by an existing security posture, and the other that is not so defeated. The reason for modelling DBT in this way is the experience of Waterfall's customer-facing personnel that business decision-makers find it easier to work with attack scenarios than with more abstract risk metrics.

Top 20 Attacks

To this end, the Waterfall paper proposes twenty ICS cyber attacks across a wide range of attacker capabilities and attack sophistication. These attacks are proposed as a useful standard set of attacks that practitioners can use to compare security postures across a wide range of types of industrial sites. The attacks, in brief are:

#1 ICS Insider – A disgruntled insider with access to ICS equipment uses social engineering to steal passwords able to trigger a partial plant shutdown.
#2 IT Insider – A disgruntled insider with access to an IT network uses social engineering to steal passwords able to give them remote control of a copy of the HMI system on an engineering workstation.
#3 Common Ransomware – Accidentally downloaded to an engineering workstation and spreads to rest of ICS.
#4 Targeted Ransomware – Spear-phishing seeds a Remote Access Trojan (RAT) on an IT network, which is used to deliberately spread ransomware through an ICS
#5 Zero-Day Ransomware – Ransomware incorporating a zero-day Windows exploit spreads through IT/OT firewalls.
#6 Ukraine Attack – The now well-known first-generation Ukraine attack using spear phishing and remote access.
#7 Sophisticated Ukraine Attack – A variation of the well-known Ukraine attack – the variation targets protective relays and causes physical damage to electric substations and rotating equipment.
#8 Market Manipulation – An organized-crime syndicate uses known vulnerabilities in Internet-facing systems to seed RATs that are ultimately used to simulate random equipment failures, triggering commodities markets fluctuations.
#9 Sophisticated Market Manipulation – A similar attack targeting an ICS site's services suppliers as a means of seeding peer-to-peer RAT malware into an ICS and simulating random failures.
#10 Cell-phone WIFI – A combination of spear-phishing and a trojan cell phone app provides attackers with access to ICS WIFI networks.
#11 Hijacked Two-Factor – Sophisticated malware allows attackers to hijack remote desktop / VPN sessions after a remote user logs in with two-factor authentication.
#12 IIoT Pivot – Hacktivists pivot into an ICS via a poorly-defended cloud vendor.
#13 Malicious Outsourcing – A disgruntled employee of a remote services vendor configures a simple time bomb on important ICS servers on the employee's last day on the job.
#14 Compromised Vendor Website – Hacktivists use a compromised vendor's website to insert malware into a software update, malware that targets specific industrial sites.
#15 Compromised Remote Site – A physical breach of remote substation or pumping station hides a laptop at the remote site with a WIFI connection that is later used to attack the central SCADA site.
#16 Vendor Back Door – Hacktivist-class attackers discover a vendor's back door that provides the poorly-

defended vendor's website with remote control of ICS components in the name of "remote support."
#17 Stuxnet – A Stuxnet-class attack targets a heavily-defended site by compromising a services vendor for the site and crafting autonomous, zero-day-exploiting malware.
#18 Hardware Supply Chain – An intelligence-agency-grade attack intercepts new computers destined for an ICS site and inserts wireless, remote-control equipment into the computers.
#19 Nation-State Crypto Compromise – A nation-state-grade attack compromises the Public Key Infrastructure by stealing a certificate authority's private key, or by breaking a cryptographic algorithm, such as SHA-256, allowing them to falsify security updates.
#20 Sophisticated, Credentialed ICS Insider – An ICS insider is aligned with the interests of a sophisticated cyber attack organization, deliberately cooperating with the organization to create sophisticated malware and seed it in the ICS.

Water Treatment Plant Example

The Waterfall paper proceeds to evaluate an example security posture against these twenty attacks. The worked example is a water treatment plant protected with a "first generation" security system reflecting ICS security best practices published circa 2003-2013: firewalls, anti-virus systems, encryption, security updates, intrusion detection, and so on. The network structure is illustrated in Figure (1).

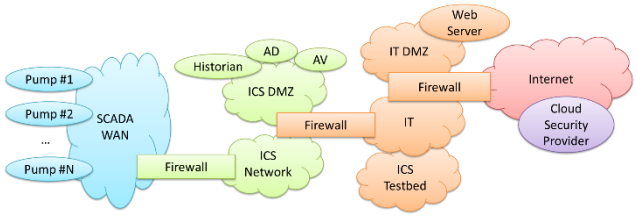

Figure (1) – Water treatment plant security system

This security posture is evaluated against the twenty attack scenarios and is largely found wanting. The security system reliably defeats very few of the attacks, as illustrated in Figure (2). The reason for the poor performance is the definition of "reliably defeats." To defeat an attack reliably means to prevent the physical consequence of the attack essentially every time this class of attack is launched. First generation security measures reliably defeat comparatively few attacks. Signature-based anti-virus systems for example, reliably defeat malware that matches their signatures, once those signatures are published. In the first few hours or days of circulation for a new malware strain however, no signatures exist yet. The anti-virus system, therefore, does not defeat common malware essentially every time the system is presented with a high-volume attack – the unlucky first few thousand victims are not protected.

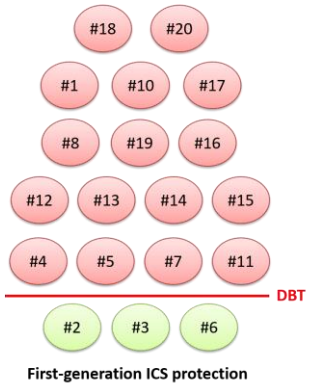

Figure (2) Risk assessment for first-gen system

The water treatment plan's business decision makers, seeing Figure (2), express dissatisfaction with the state of the security program. They may ask "what are these attacks that are not defeated reliably?" We as security practitioners need o explain why each attack is not defeated reliably. When we explain, we generally start with the simplest attacks not defeated, since attackers with a range of attack techniques available to them will generally choose the simplest, cheapest attacks that work.

Improved Security

To address management's concerns, the security team might seek to improve their security posture by:

- Deploying Unidirectional Security Gateway hardware and software to more thoroughly control network information flows,
- Deploying strict removable media controls, to control offline information flows, and
- Upgrade the ICS test bed to serve as a security test bed / sandbox, as well as a software reliability test bed.

The new system is illustrated in Figure (3).

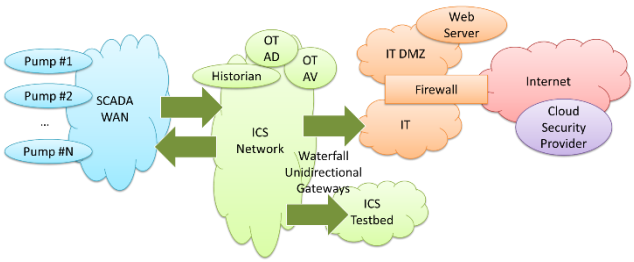

Figure (3) Modernized ICS security system

The corresponding risk assessment results are illustrated in Figure (4).

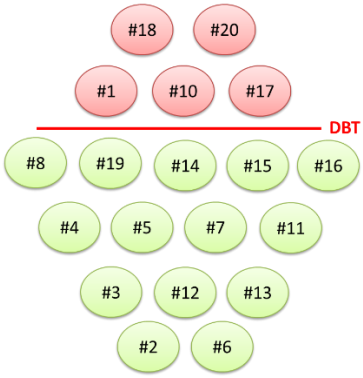

Figure (4) Risk assessment for upgraded system

The difference between the two security postures is easily visible. At this point we may be called upon to explain the residual risk – the attacks our security posture still does not defeat reliably. This is normal. The process may iterate another once or twice, with diminishing returns.

No security posture is infallible - there will always be attacks above the DBT line that we need to explain. Any practitioner who sees no such attacks for their security posture either needs to define more powerful attacks, or needs to think hard about whether they have mis-represented the effectiveness of their security posture.

Summary

A given security program/posture can only be evaluated if we have a clear understanding of the kinds of attacks that might target the protected industrial site. The Waterfall paper:

- Proposes a representative Top 20 list of ICS cyber attacks,
- Illustrates how to evaluate those attacks against a given defensive posture, and
- Illustrates how to communicate residual risk to business decision-maker as a Design Basis Threat line drawn through example attacks.

Nothing is ever completely secure - any DBT diagram should illustrate attacks that will breach the defensive posture under consideration. In any such set of not-reliably-defeated attacks, there is always a least-sophisticated or simplest attack or set of attacks with serious consequences. It is this set that should be the focus of communication with business decision-makers. Do such attacks represent acceptable risks?

When the answer is "no" we can evaluate attacks above the DBT line against proposed new security measures to see whether the line moves. In the water treatment system example, we see how a modest investment in modern ICS protection with Unidirectional Gateways and removable media controls produces a dramatic improvement in risk posture.

The full Waterfall paper, with more detailed attack descriptions and evaluations of attacks against security postures, is available at:

https://waterfall-security.com/20-attacks

About Waterfall Security Solutions

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall's products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, railway switching systems, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases and protocols in the market. For more information, visit www.waterfall-security.com

For More Information

For additional information on this topic or on any topic related to Waterfall products, please contact:

Waterfall Security Solutions
14 Hamelacha St.
Rosh Ha'ayin, 48091 Israel
+972-3-900-3700
www.waterfall-security.com

# # #