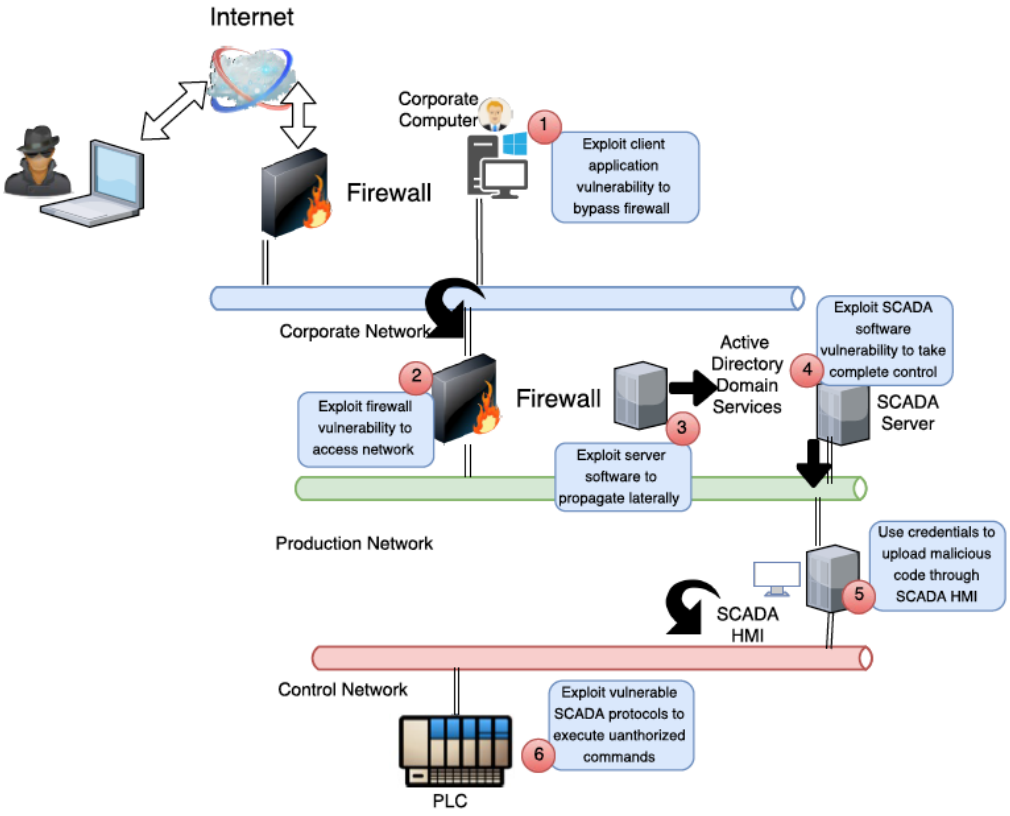
INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY STRATEGY, A NEW APPROACH



Author: **Annabelle Lee**
Nevermore Security

February 2018

ACKNOWLEDGMENTS

The author wishes to acknowledge the following subject matter experts for their technical contributions, many excellent suggestions, and recommendations to greatly enhance this white paper:

- Sachin Shetty (Old Dominion University)
- Shabbir Shamsuddin (Argonne National Laboratory)
- Virgil ‘Vic” Hammond (Argonne National Laboratory)

Table of Contents

Figures

Executive Summary

Threats to Industrial Control Systems (ICS) and Operational Technology (OT) that operate our critical infrastructure are now in daily news media. ICS controls provides automation of operating power plants, oil and natural gas flowing through pipes nationwide, and supports critical manufacturing of goods and pharmaceutical products for everyday use. Attacks on these systems can cause interruptions of major critical infrastructures, physical damage, and potentially threaten human health and safety.

The advances in technology and today's offerings of the Industrial Internet of Things (IIoT) devices today expands the attack surface of the ICS with the impact extending to all parts of the organization operating the critical infrastructures, the supply chain, and ultimately the end-use customers. Current cybersecurity solutions today cannot provide comprehensive protection against all the known and unknown threats of the automation components that operate the critical infrastructures, and specifically the energy sector. Particularly with the constantly changing threat and technology environments, this defensive approach results in the critical infrastructures constantly trying to play *catch up* in cybersecurity. Cyber attacks may be launched, for an example by malicious insiders, via supply chain, and/or by unauthorized remote access. Attackers only have to be effective once and defenders need to be effective 100% of the time. It is not realistic to be 100% effective in identifying and addressing all known and potential cyber attacks. In addition, with the increasing availability of attack tools and techniques, the end result is that the defenders keep falling further behind in addressing cybersecurity.

This white paper proposes an alternative to the current defensive paradigm. The paradigm proposed in this paper augments this defensive approach and considers cybersecurity from the attacker's perspective and includes identifying attack surfaces, attack vectors, and impacts. Because it is not possible to mitigate all potential cyber events, the objective is to identify the most common attack paths and mitigate the highest impact cyber events, independent of the specific attack method. This will include known and potential cybersecurity events. The *unknown* cyber events will be determined based on the impact to the ICS and the reliability of the grid. This paradigm will allow the energy sector to be more proactive in addressing cybersecurity and more resilient in the event of cyber attacks.

Introduction

Over the last decade, the rise in cyber attacks on critical infrastructures has resulted in cybersecurity becoming a central concern among industrial automation and control system users and vendors. These strategic attacks are aimed at disrupting industrial activity for monetary, competitive, political, or social gain, or even as a result of a personal grievance. Cyber threats are primarily aimed at industrial control systems (ICS) such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, and human machine interfaces (HMI) through loopholes which can range from unsecured remote access, to inadequate firewalls, to a lack of network segmentation. Such threats are not a new phenomenon. However, a spate of high-profile attacks over the last decade has brought this issue to center stage.[1]

ICS/SCADA systems were originally isolated from the outside world. Sensors would monitor equipment and provide that information to a control room center. As networking technology has advanced and become more accessible, organizations have made decisions to integrate systems. This integration is necessary to take advantage of the new technology that is being deployed. What were once isolated systems are now connected to corporate networks, allowing a corporate office to receive operational data and information from numerous remote facilities. While security protections such as firewalls, access controls, and user policies and procedures are put into place, a physical connection to the outside world via 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 from hardware and software vulnerabilities. Infected USB drives, websites, and everyday social engineering attempts on a corporate network may open up paths to an ICS/DCS/SCADA network for the adversaries as illustrated in Fig. 1.[2]

[1] Frost & Sullivan 2013, "Cybersecurity for Industrial Automation & Control Environments - Protection and Prevention Strategies in the Face of Growing Threats," URL: http://www2.schneider-electric.com/documents/support/white-papers/white-paper-cybersecurity-for-industrial-automation-control.pdf

[2] Michael Robinson 2013, "The SCADA Threat Landscape," URL: http://ewic.bcs.org/upload/pdf/ewic_icscsr13_paper4.pdf

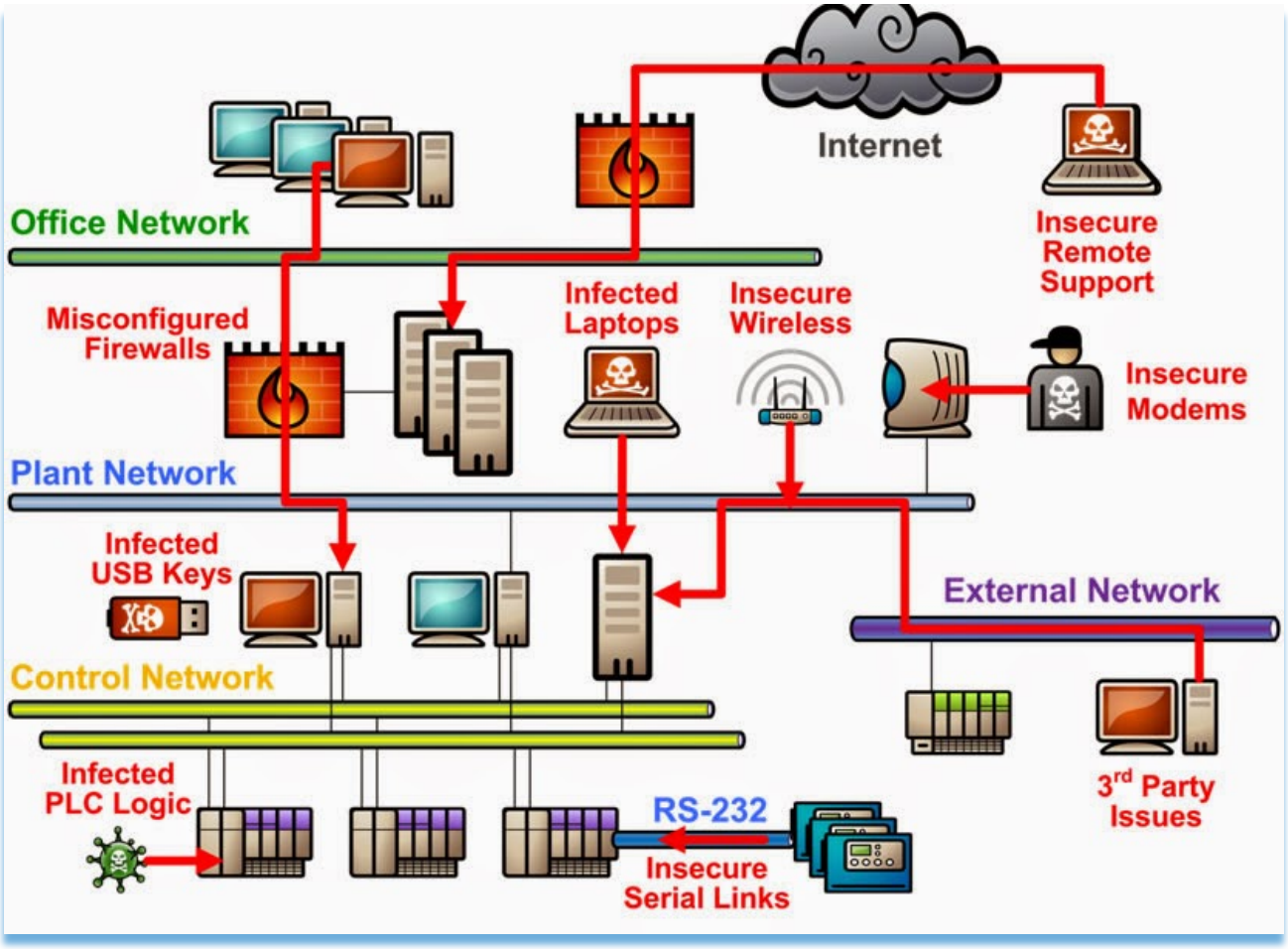


Figure 1 Attack Vectors to ICS
(Source: Lockheed Martin 2015)[3]

Threat Landscape

Corporate and industrial networks, which form a multilevel hierarchical infrastructure in modern industrial companies, are increasingly being integrated. The control systems in operation today are complex webs of old and new technology provided by a range of original equipment manufacturer (OEM) vendors. Historically, the use of proprietary technologies and isolation protected these control systems from Internet-based attacks that are so prevalent in common internet protocol (IP) communication technologies and commercially available IT software. As the industry looks to the future, however, operators seek to leverage the efficiency provided by these new communication technologies and are connecting these older systems to new systems. Enterprise Strategy Group, a leading consulting firm, published results of its 2015 survey for critical infrastructure providers that showed dramatic increases in the number of attacks. Sixty-eight percent of the providers claimed that they experienced one or several cybersecurity

[3] Lockheed Martin 2015, "Evolving Security in Process Control," URL: https://www.slideshare.net/Lockheed-Martin/evolving-security-in-process-control

incidents over the past two years; thirty-six percent said cybersecurity incidents led to a disruption of operations; and two-thirds of cybersecurity experts at critical infrastructure providers believe that the threat landscape is more dangerous today than it was two years ago.[4] Because cybersecurity awareness has been raised in visibility, some increase in reporting may be due to increased tracking of potential cybersecurity events. However, this does not account for all the increase.

Those who have interest in disrupting the critical infrastructures ICS systems (threat vectors) include:

- Nation state backed groups – Target ICS to achieve geopolitical goals.
- Criminals – Extortion of companies for monetary gain.
- Hacktivists – Promote social, political, and or ideological cause.
- Insiders – Inadvertently or maliciously cause disruption for personal gains.[5]

Recent high-profile attacks indicate that threat actors are using more sophisticated techniques such as multi-flow, and multi-vector attacks that exploit vulnerabilities in IT networks to penetrate into the OT systems. The 2010 attack on Iranian centrifuges that relied on complex malware known as Stuxnet and physically destroyed PLCs was introduced through a universal serial bus (USB) stick drive. Malware introduced via spear phishing and social engineering was used to cause severe physical damage to a German steel mill in 2014. Once inside, the attacker used captured credentials and IT connectivity to the plant's OT network to deregulate critical systems and cause physical damage. In the recent Black Energy attack on a Ukrainian power grid, increasingly networked OT environments opened the door for commodity malware to become a major threat.[6]

Nation-states do not fear reprisal and are likely to use ICS attacks as a component of a geo-political conflict. Alarmingly, offensive cyber tools are becoming commonplace, lowering the bar for rogue nations, jihadists, and hacktivists to get into the ICS attack game. And, cyber-criminals are figuring out that ICS networks are critical and therefore valuable, meaning it is only a matter of time until we see major ransomware trends in ICS.[7]

The recent ransomware's attacks on information technology has grown in 2015 and 2016. Ransomware generated an estimated $200 million for attackers during the first quarter of 2016, and researchers believe it is only a matter of time before critical ICS are compromised and held

---

[4] RKNeal Inc. 2016, "ICS Cyber Security," URL: at http://verveindustrial.com/wp-content/uploads/2016/06/An-Integrated-Approach-to-Protecting-Industrial-Control-Systems.pdf

[5] Booz Allen Hamilton 2016, "Industrial Cybersecurity Threat Briefing," URL: http://cdn2.hubspot.net/hubfs/407136/PDFs/Booz_Allen/Industrial_Cybersecurity_Threat_Briefing.pdf?t=1473881858278

[6] Fire Eye Inc. 2017, "Cyber Security Solutions for Critical Infrastructure and Industrial Control Systems," URL: https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/pf/ms/sb-critical-infrastructure.pdf

[7] Security Week 2017, "The Threat to Critical Infrastructure – Growing Right Beneath Our Eyes," URL: http://www.securityweek.com/threat-critical-infrastructure-growing-right-beneath-our-eyes

for ransom.[8] Ransomware payments in 2017 will hit a record $2 billion, according to new research from the cybersecurity firm Bitdefender.

To-date, no real ransomware attacks on ICS components have been publicly reported. Alternatively, the attacks have become a significant problem for patient data in hospitals and customer data in businesses. This emerging threat to ICS operators by infection of their OT devices and systems may cause disruption of service. ICS networks and systems usually have little valuable financial or personal data, but instead place the highest value on availability, equipment health, and safety to personnel.[9] Malware could potentially disrupt operations or prevent an operator access to OT devices and field locations.[10] Many OT devices have limited functionality and a cyber attack may result in the devices becoming "bricked", that is, no longer functioning. This is in contrast to IT devices that may continue to function, but in a degraded mode.

Industry Challenges to ICS Protection

Traditionally, industrial networks used to run on proprietary networks, used proprietary equipment, and were isolated from business networks and the Internet. This was the era of "security by obscurity" and "security by air gap." Over the last decade, however, industrial networks have been migrating from proprietary systems to commercial off-the-shelf (COTS) technologies such as Ethernet, TCP/IP, and Windows. Keeping today's ICS operating effectively may require a constant stream of updates from the COTS vendors and OT suppliers. The result is that the ICS networks now include open protocol communications activity and are no longer isolated from the Internet. Furthermore, devices such as Remote Terminal Units (RTU), Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCS) were designed with a focus on reliability and safety, rather than security. This makes many of the ICS, particularly older units, easy to exploit.

Since industrial control systems are often required to run 24/7/365 and withstand hazardous environments, many security policies are hard to or never deployed; since operational necessities and safety regulations overrule their application. Even traditional IT security strategies, such as patching, are often difficult or impossible to deploy due to conflicting industry-specific regulations and operational requirements. Today, ICS security is like playing a game with the advantage going to the attacker: millions of decades-old systems that were never designed to be secure, with increasing connectivity of SCADA and ICS, and a growing library of free tools and techniques available to the adversary to attack SCADA and ICS. A successful attack on an ICS could mean production losses, significant safety or environmental issues, or theft of intellectual

---

[8] Georgia Tech 2017, "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls," URL: http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls

[9] Georgia Institute of Technology 2016, "Out of Control: Ransomware for Industrial Control Systems," URL: http://www.cap.gatech.edu/plcransomware.pdf

[10] Booz Allen Hamilton 2016, "Industrial Cybersecurity Threat Briefing," URL: http://cdn2.hubspot.net/hubfs/407136/PDFs/Booz_Allen/Industrial_Cybersecurity_Threat_Briefing.pdf?t=1473881858278

property, including information obtained from the enterprise network. Indeed, an ICS network could be the simplest backdoor to a company enterprise network.[11]

A 2015 Tripwire survey of 400 executives and IT professionals across the oil, gas, utility, and energy sectors found that fewer than half believed their organization could immediately detect a cyber attack, although 94 percent believed they were a target. Furthermore, 83 percent believed that such attacks could do "serious physical damage". Although there has been an increased focus on cybersecurity in recent years, advanced persistent threats against IT and OT systems of the critical infrastructures such as the energy sector continue to go undetected for an average of six months. A study done by the Ponemon Institute found in 2017, on average, it takes 191 days for an organization to identify a data breach and 66 days to contain the data breach. In the 191 days, an insurmountable amount of data can - and will be - lost. In the US and Canada, the average cost of each record lost amounted to $225 USD.[12] A comparison between 2016 and 2017 showed that the amount of cyber-attacks were actually lower in number in 2017; however, the ability, strength, and maliciousness of the attacks had increased. Part of the reason for this is alert overload. Standard cybersecurity deployments generate hundreds of thousands of alerts per week, but most organizations only have the resources to investigate about six percent. With only 19 percent reliability, organizations waste millions of dollars a year chasing false positives or performing investigations with inadequate intelligence and insufficient expertise. As attacks against critical infrastructures occur through multiple stages and different vectors, organizations need higher fidelity and context from their security solution.[13]

Cybersecurity for the power industry should cover all issues involving ICS, OT, and communication systems that affect the operation of the electric grid. Currently, the focus is on implementing new technologies and equipment that can improve power system reliability (including availability). Until recently, communications and information technology (IT) equipment were typically seen as supporting power system reliability. However, increasingly the power sector is getting more dependent on the communication and IT as they are becoming more critical to the reliability of the grid. This was illustrated in the August 14, 2003, blackout, where a contributing factor to the power failure was issues with communications latency in control systems. With the exception of the initial power equipment problems, the ongoing and cascading failures were primarily due to problems in providing the right information to the right individuals within the right time period. Also, the IT infrastructure failures were not due to any terrorist or Internet hacker attack; the failures were caused by inadvertent events—mistakes, lack of key alarms, and poor design. Therefore, inadvertent compromises must also be addressed, and the focus must be an all-hazards approach.[14]

---

[11] Tofino Security 2014, "The Industrial Cybersecurity Problem," URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0ahUKEwjpzdPOpKLVAhUD8YMKHcnIAI0QFghQMAU&url=https%3A%2F%2Fwww.isa.org%2Fpdfs%2Fthe-industrial-cybersecurity-problem%2F&usg=AFQjCNEuVFlurCLSsr74YxWsORA7yZKDJA&cad=rja

[12] Sia Partners - Banking & Insurance, 2017 "The Biggest Cybersecurity Threats of 2017: The Need to Prepare," available at http://en.finance.sia-partners.com/20171024/biggest-cybersecurity-threats-2017-need-prepare

[13] Fire Eye Inc. 2017, "Cyber Security Solutions for Critical Infrastructure and Industrial Control Systems," URL: https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/pf/ms/sb-critical-infrastructure.pdf

[14] The Smart Grid Interoperability Panel 2010, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," URL: https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

Industry status on ICS Cybersecurity Research and Development

DOE and DHS with the help of the energy sector including owners and operators, commercial vendors, national laboratories, industry associations, academia, government agencies, and members of the international community developed a *Roadmap to Secure Control Systems in the Energy Sector* (2006 Roadmap) to enhance cybersecurity across the energy sector. The 2006 Roadmap was updated in 2011 and established a common vision and strategic framework for industry and government to develop, deploy, and maintain control systems that could survive an intentional cyber assault without loss of critical functions. The 2006 Roadmap started dozens of collaborative initiatives across industry, national laboratories, universities, and government. Many important, cybersecurity research and development efforts are still under way and are mapped to specific 2006 Roadmap milestones on the ieRoadmap.[15]

This paper provides another approach or paradigm shift in ICS cybersecurity and therefore complements the existing research and development activities by DOE, DHS, and industry.

[15] [15] Energy Sector Control Systems Working Group (ESCSWG) 2011, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," URL: https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

Strategy – Threat Paradigm Shift

The current defensive/reactive paradigm focuses on protection and detection and includes continuous monitoring and patching. This paradigm is important, but the end result is that the critical infrastructures are always playing "catch up." In addition, the current approach is not sustainable in addressing future cybersecurity events. The paradigm proposed in this paper augments this defensive approach and considers cybersecurity from the attacker's perspective and includes identifying attack surfaces and attack vectors. This is important because of the constantly changing technology and threat environments. For example, if OT devices are upgraded, the attack vector may remain the same – through a USB drive or remote access. This approach will allow the industry to define a high level mitigation strategy that is independent of a specific OT device. The goal is to increase the cost to the adversary. In addition, to effectively address an attacker's perspective, an active defense approach is needed. The goal of *active defense* is to anticipate cyber attacks and includes the collection and analysis of threat intelligence information and identification of the impact of cyber attacks. At a high level, the impact may be independent of the specific architecture configuration. As a result, an *active defense* approach should consider both existing and new attack vectors and support the resilience and reliability of the critical infrastructures. Cybersecurity resilience includes the following:

- Reducing the likelihood that incidents will occur
- Limiting the scope and impact of incidents
- Recovering from an incident
- Developing *lessons learned* for the future.

Resilience in control systems includes maintaining critical functions even if an attacker is in the system. *Reliability* assures the availability and integrity of the critical infrastructure and resilience (including cybersecurity resilience) should support reliability. Currently, there is little statistical data on likelihood related to specific attacks. As utilities become more sophisticated, they will collect statistical data that may be used in identifying mitigation strategies, but this is still examining past events, rather than looking forward.

Active defense has been proposed for many systems. In this white paper, active cyber defense and the attacker perspective are combined in an attempt to be more proactive. There are tools available to assist in this approach. Two are described below.

Attack Tree Modeling

There is a need for threat models to not only characterize the degree of exploitability from cyber attacks, but also quantify the financial or operational impact. A top-down modeling approach would be capable of using impact requirements to influence the development of the threat model. This approach will ensure that the threat model does not get bogged down into characterizing threat of exploits on assets which do not pose great financial or operational risk. This approach not only leads to efficient modeling, but also, ensures that the threats which pose the greatest financial or operational risk would be given priority during the mitigation process.

Several common attack subtrees were developed in the National Electric Sector Cybersecurity Organization Resource (NESCOR) project.[16] These are common branches that occur in several situations. The *common subtrees* are fragments of attack trees that were found to be repeated across many different trees as well as within attack trees. These common subtrees were developed in collaboration with utilities and research organizations. The intent was to provide useful guidance for the utilities. Unlike typical attack trees, these are read from top to bottom. Included in Figure 2 below is the attack tree notation.

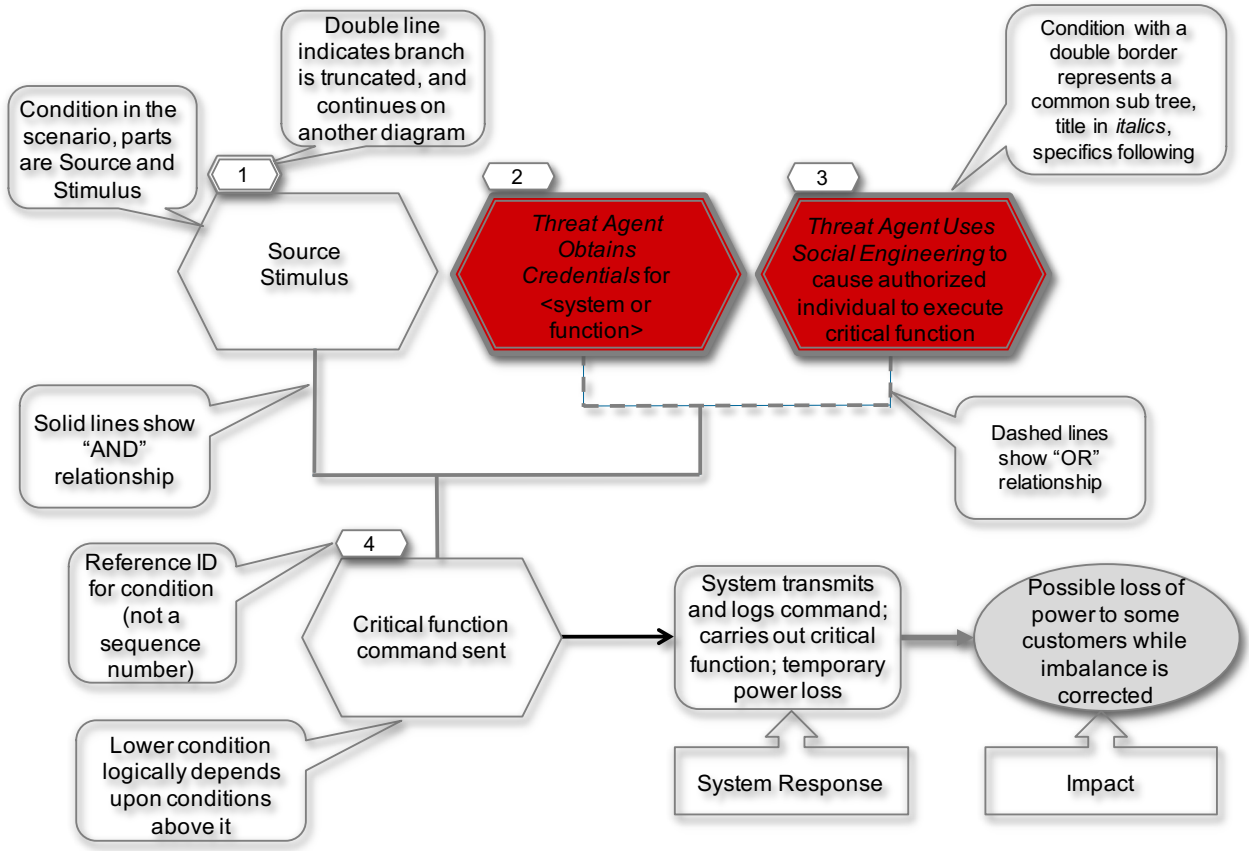


Figure 2 Common Subtrees
(Source: EPRI 2013)

Highlighted in red are two of the common subtrees. These are listed below. Included with each subtree is a description, assumptions, and mitigation strategies.

Threat Agent Obtains Credentials for <system or function>

Description

- A threat agent may gain credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing

[16] EPRI 2013, "Attack Trees for Selected Electric Sector High Risk Failure Scenarios NESCOR Version 1.0," URL: http://smartgrid.epri.com/doc/NESCOR%20Attack%20Trees%2009-13%20final.pdf

them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others (Figure 3).

Assumptions

- Credentials used are either any static piece of data (referred to as a password), biometrics, or a physical object (such as a key card/token).
-
- If multi-factor authentication is used such as a token with a PIN, the adversary must take additional steps to obtain all "factors" of the credentials.

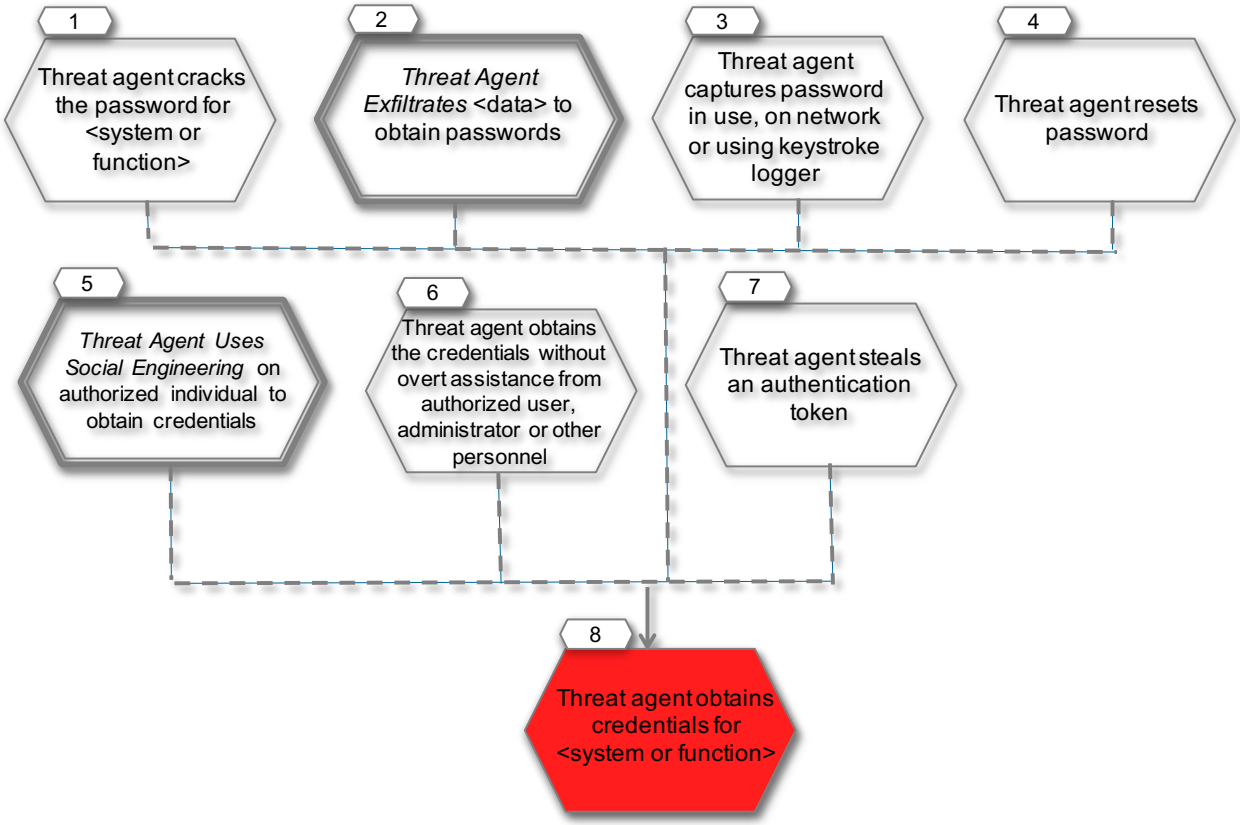


Figure 3 Common Tree: Threat Agent Obtains Legitimate Credentials <system or function>
(Source: EPRI 2013)

Listed below are the mitigation strategies.

Potential Mitigations

1 - Design for security by using strong passwords

2 - See mitigations for common sub tree *Threat Agent Exfiltrates* <data>

2 - Design for security by not recording clear text passwords in log files

3 - Test for malware on user devices

3 - Design for security by not sending passwords in the clear over the network 3 - *Encrypt communication paths* on the network

3 - Protect against replay on the network

4 - Design for security by using strong security questions and protect answers

5 - See mitigations for common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

6 - Design for security by using strong security questions and protect answers; *Require multi-factor authentication*

7 - Require multi-factor authentication such as using a token with a PIN

Threat Agent Uses Social Engineering to <desired outcome>

Description

- A threat agent uses techniques of social engineering to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent as shown in Figure 4. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT.

Notes

- The attack tree provides an overview of the use of social engineering, there are many varieties
- More details and common examples may be found at: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

Assumptions

- None currently identified

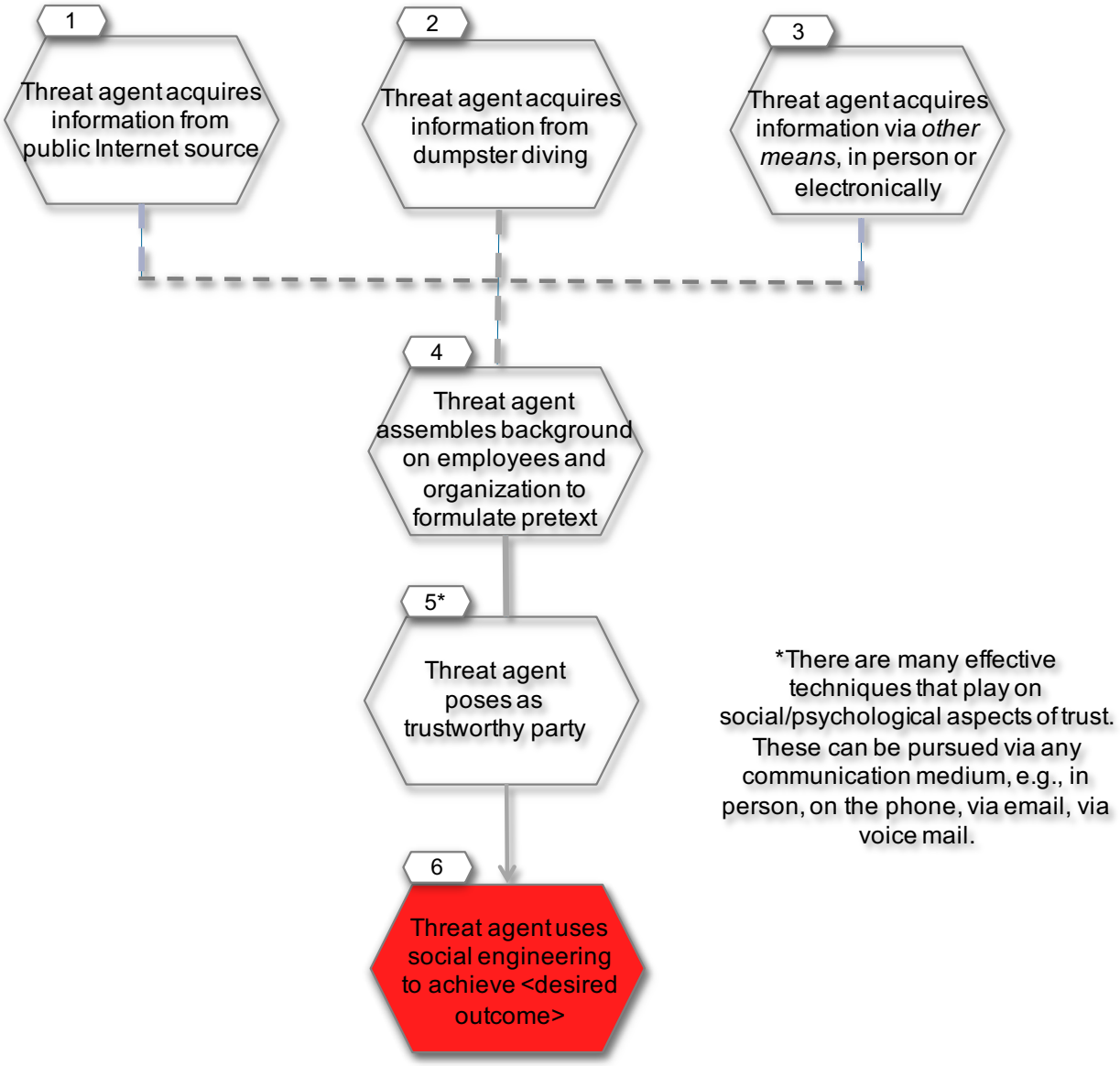


Figure 4 Common Tree: Threat Agent Uses Social Engineering <desired outcome>
(Source: EPRI 2013)

Potential Mitigations

1 - Define policy to minimize Internet disclosure, e.g., "do not make calendars public"
1, 2, 3, 5 - Conduct penetration testing periodically, posing as a threat agent (Conditions 1, 2, 3, 5)
2 - Define policy to minimize leakage of physical artifacts (e.g., shredding, locked receptacle)
5 -Train personnel that they are potentially targeted for these types of attacks and the consequences for the organization
5 - Train personnel to report social engineering attacks
5 -Track social engineering attacks and warn personnel
5 -Train personnel including users and administrators in procedures to foil threat agents,

e.g., always call back to the number in the directory

ICS Kill Chain

In 2011, Lockheed Martin created the Cyber Kill Chain™ to help the decision-making process for better detecting and responding to adversary intrusions[17]. This model was adapted from the concept of military kill chains. The ICS kill chain[18] was developed by individuals from the SANS Institute and augments the original kill chain and tailors it for control systems.

- To determine how to stop an attack
- For a better understanding of what is already protected
- For security gap and mitigation analysis
- To address OT threat scenarios and use cases

The goal is to be anticipatory and pro-active using a comprehensive risk-based approach. This includes identifying what is currently in place, what is in progress, and the gaps that need to be addressed. In contrast, the compliance approach is a minimum baseline that does not focus on emerging attacks.

The objective is to be proactive in identifying and addressing future risks and attacks. The use of the ICS Kill Chain focuses on the attacker and impacts of cybersecurity events as proposed in this white paper. The failure scenarios and attacks described above should be allocated to the various steps in the ICS Kill Chain. Based on the various attacks, mitigation strategies will be identified and deployed, if possible. The original cyber kill chain and the associated ICS Cyber Kill Chain are described and shown in Figures 5 and 6.

[17] Lockheed Martin Corporation undated, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," by Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, Ph.D., URL: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[18] SANS Institute 2017, "The Industrial Control System Cyber Kill Chain," by Michael J. Assante and Robert M. Lee, October 2015, URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

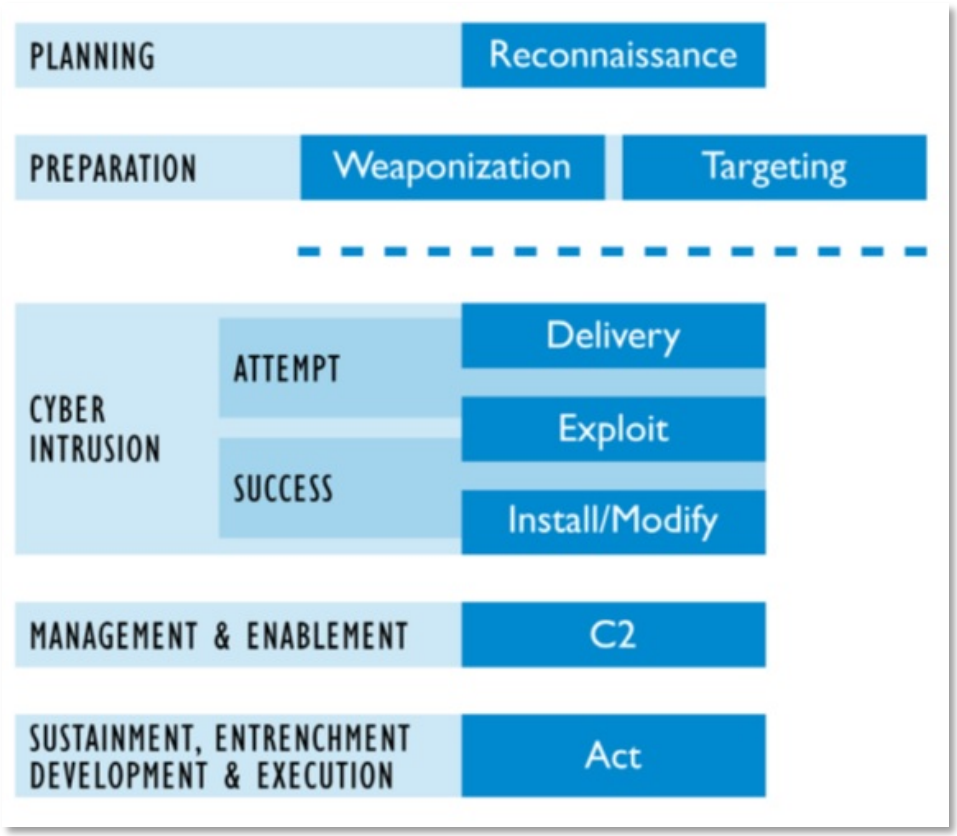


Figure 5 Cyber Kill Chain – Stage 1: Cyber Intrusion Preparation and Execution
(Source: SANS Institute 2015)

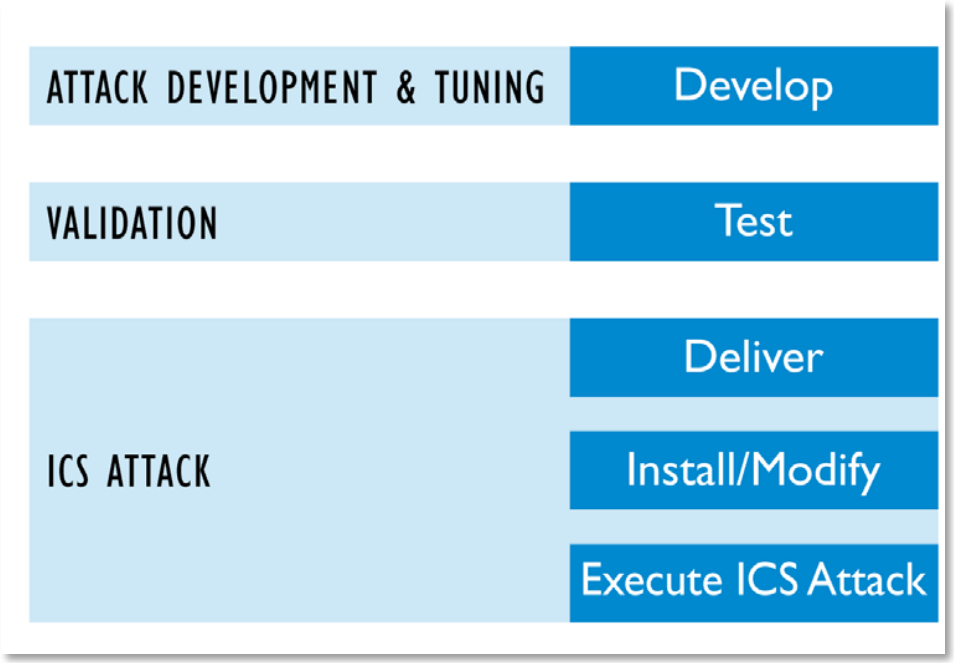


Figure 6 ICS Cyber Kill Chain – Stage 2: ICS Attack Development and Execution
(Source: SANS Institute 2015)

The steps in the Lockheed Martin chain are as follows:

- *Reconnaissance*: the attacker finds a gap in security of the social network
- *Weaponization*: builds a malicious attachment
- *Delivery*: and delivers it using social media or email targeting an employee
- *Exploitation*: the employee opens the file and the vulnerability is exposed
- *Installation*: malware immediately installs on the client
- *Command & Control*: the attacker takes control of the system
- *Actions on Objectives*: and is able to pinpoint and access critical data

The tailored ICS cyber kill chain includes the following steps and descriptions that are extracted from the ICS Kill Chain document[19]. This is an overview and additional details are included in the SANS document.

Stage 1: Cyber Intrusion Preparation and Execution

- ***Planning and Reconnaissance***: *Reconnaissance* is an activity to gain information about something through observation or other detection methods. The objective of the Planning step is to reveal weaknesses and identify information that support attackers in their efforts to target, deliver and exploit elements of a system.

- ***Preparation****:* Preparation can include weaponization or targeting. *Weaponization* includes modifying an otherwise harmless file, such as a document, for the purpose of enabling the adversary's next step. Targeting occurs when the adversary or its agent (such as a script or tool) identifies potential victim(s) for exploitation.

- ***Cyber Intrusion***: An *intrusion* is any attempt by the adversary, successful or not, to gain access to the defender's network or system. This includes the *Delivery* step, in which the adversary uses a method to interact with the defender's network. The next step, the *Exploit step*, is the means the adversary uses to perform malicious actions. When the exploitation is successful, the adversary will *install* a capability and may also, or instead, *modify* existing capabilities.

- ***Management and Enablement****:* Here the actor will establish *command and control* (C2). With managed and enabled access to the environment, the adversary can now begin to achieve his or her goal.

[19] SANS Institute 2017, "The Industrial Control System Cyber Kill Chain," by Michael J. Assante and Robert M. Lee, October 2015, URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

- ***Sustainment*, *Entrenchment*, *Development*, and *Execution***: In this step, the adversary *acts*. This can be a critical phase for the planning and execution of Stage 2 of the ICS Cyber Kill Chain.

Stage 2: ICS Attack Development and Execution

- ***Attack Development and Tuning phase***. The aggressor develops a new capability tailored to affect a specific ICS implementation and for the desired impact. This development will most likely take place through exfiltrated data.

- ***Validation***: Here, the attacker must *test* his or her capability on similar or identically configured systems if the capability is to have any meaningful and reliable impact.

- ***ICS Attack***: the adversary will *deliver* the capability, *install* it or *modify* existing system functionality, and then *execute* the attack. The security use cases vulnerabilities and descriptions may be allocated to the applicable ICS Kill Chain steps. This is useful in determining when the mitigation strategies should be implemented.

Testing

This white paper proposes that to stay abreast of threat vectors on industrial control systems, a virtual/physical test bed should be designed representing the energy sector SCADA/ICS architecture. The objective is to model various threat vectors against the system to understand the vulnerabilities and to gather information to drive stronger security standards, best practices, and the development of new SCADA/ICS system architecture that takes into account both legacy, present, and future design to protect the system from threats and failure.

To test this paradigm, this white paper recommends testing of the cybersecurity failure scenarios for the electric sector that were developed in 2013 and updated in 2015, by the NESCOR Technical Working Group 1 (TWG1). This includes testing the common attack subtrees discussed above. The failure scenarios can be allocated to the steps in the ICS Kill Chain.

The information about potential cybersecurity failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cybersecurity failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. These generic failure scenarios have been developed for generation, transmission, and distribution subsystems focusing on malicious and non-malicious cybersecurity events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,
- Human error,
- Interference with the equipment lifecycle, and

- Natural disasters that impact cybersecurity posture.

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence. [20]

Threat Modeling Requirements

The goal of any threat modeling is to perform quantitative assessment of exploitability and impact of attack surfaces within the cyber infrastructure. The following lists five key requirements for an effective threat modeling tool based on National Institutes of Standards and Technology (NIST) publications:[21]

(1) *Automatic discovery of vulnerabilities*: Due to constantly evolving attack surfaces, there is a need to discover the presence of exploitable vulnerabilities on a daily basis.

(2) *Lateral propagation analysis*: Adversaries exploit a chain of vulnerabilities to reach the attack goal, requiring analysis of the propagation of attackers through the chain of exploits. The analysis provides information on stepping-stones, pivot points, attack paths, vulnerable nodes, which in turn provides insights into potential strategies employed by adversaries.

(3) *Security metrics*: The quantification of attack surfaces based on exploitability and impact analysis is required to develop baseline security risk scores. These metrics aid the decision maker in developing effective risk management policies.

(4) *Prioritized mitigation plan*: The mitigation plan should provide an ordered list of vulnerabilities to patch or apply security controls to achieve a desired security score.

(5) *Compliance with a cybersecurity framework*: NIST provides a policy framework for organizations to assess and enhance their ability to prevent, detect and respond to attacks. Cyber risk assessment tools should take the recommendations of the framework in consideration for assessment of cyber risks.

---

[20] NESCOR 2013, "Electric Sector Failure Scenarios and Impact Analyses," URL: http://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf

[21] NIST (2011), NIST Special Publication 800-39. *Managing Information Security Risk: Organization, Mission, and Information System View*, from https://dl.acm.org/citation.cfm?id=2206253 , accessed 3 December 2017.
NIST (2012), NIST Special Publication 800-30. *Guide for Conducting Risk Assessments*, URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf , accessed 3 December 2017.
Ou, X., Govindavajhala, S., Appel, A., *Mulval: A logic-based network security analyze*r, In: USENIX Security Symposium, 2005
S. Jajodia, S., Noel, S., O'Berry, *Topological analysis of network attack vulnerability*, Managing Cyber Threats pp. 247–266, 2005
S. Jajodia, S., Noel, S., Kalapa, P., Albanese, M., Williams, *Cauldron mission centric cyber situational awareness with defense in depth*, In: Military Communications Conference. pp. 1339–1344, 2011
M.L. Artz, *Netspa: A network security planning architecture*, Ph.D. thesis, Massachusetts Institute of Technology, 2002

There are several cybersecurity risk assessment tools that provide a subset of the above requirements, but none satisfy all requirements. Tools such as Nessus, SAINT, OpenVAS, and Nikto only meet the (1) requirement. Core Impact, Nexpose, Metasploit, and Qualys meet the (1) and (4) requirements, while Bitsight and SecurtyScorecard meet (1) and (3). Attack graph engines such as, MulVal, Multi-host, Multi-state Vulnerability Analysis, Topological Vulnerability Analysis Tool (TVA) and NetSPA have been employed to characterize the attack surfaces.

Additional Tools

The NESCOR attack trees and the ICS Kill Chain do not include quantitative analyses. However, the NESCOR team developed a risk assessment methodology that is specific to the energy sector. The prioritization process has two primary criteria: impact and likelihood. There are 15 impact criteria and five likelihood criteria. The criteria are defined specifically for the electric sector and for utilities of all sizes – from very small municipalities to large IOUs. Figure 7 shows the highest priority attacks with the greatest impact and highest likelihood are in the upper right quadrant

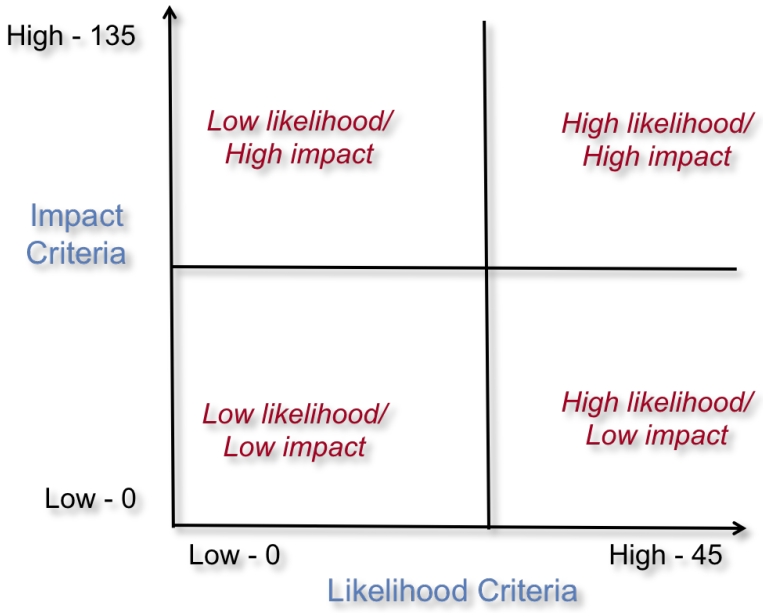


Figure 7 Impact and Likelihood Criteria
(Source: EPRI 2014)[22]

Bayesian Belief Networks (BBN)

Attack graphs are modeling formalism used to characterize the movement of adversaries through a chain of exploits. Each exploit lays the foundation for subsequent exploits and the chain is

[22] EPRI 2014, "National Electric Sector Cybersecurity Organization Resource (NESCOR) - Cybersecurity for Energy Delivery Systems Peer Review," URL: https://energy.gov/sites/prod/files/2017/02/f34/NESCOR_CEDS_Peer_Review_2014.pdf

called an attack path. All possible attack paths form an attack graph. Bayesian Belief Networks (BBN) have been applied to attack graphs to create Bayesian attack graphs that measure the exploitability of attacks. However, the Bayesian attack graphs only focus on exploitability of attacks and do not incorporate the consequences or impact of attacks. It is critical to incorporate both exploitability and impact of an attack to develop informed mitigation plans. If the organization's critical missions, operations, value, and location of sensitive assets can be incorporated within the Bayesian attack graph model, it will be possible to capture both exploitability and impact of specific classes of attacks.

Design Basis Threat (DBT)

Evaluating cyber risk in ICS networks 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 that models 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 reliably defeat. [23]

Moving Target Defense (MTD)

Taking a page out of the attacker's playbook, is it possible to randomize the systems and networks underpinning the cyber infrastructure in the power grid to reduce the future likelihood of cyber attacks and increase the degree of complexity for the attacker? It is well known that if the attacker is not successful in acquiring useful information about the target during the reconnaissance process of the cyber kill chain, the effectiveness of the attack is reduced by 50%.[24] An MTD based approach will ensure that the attacker will not be presented with same system configuration during the reconnaissance stage and the attack launch stage. Software Defined Networking can play a key role in achieving the randomization of network topology and configurations to achieve MTD at the network level. Within the system level, random instances of operating systems or virtualization software can ensure that the system configuration is randomized.

---

[23] Waterfall Security Solutions Ltd 2017, "The Top 20 Cyber Attacks Against Industrial Control ," URL: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

[24] Waterfall Security Solutions Ltd 2017, "The Top 20 Cyber Attacks Against Industrial Control ," URL: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

Conclusion

Current cybersecurity solutions today cannot provide comprehensive protection against all the known and unknown threats of the automation components that operate the critical infrastructures, and specifically the energy sector. Particularly with the constantly changing threat and technology environments, this defensive approach results in the critical infrastructures constantly trying to play *catch up* in cybersecurity.

This white paper proposes an alternative to the current defensive paradigm and considers cybersecurity from the attacker's perspective and includes identifying attack surfaces, attack vectors, and impacts. Combining the attacker's perspective and active cyber defense may be used by utilities in determining cybersecurity risk, particularly in the OT environment. Determining risk is necessary to ensure the reliability and resiliency of the grid. To get started, utilities may use the NESCOR failure scenarios, including the common attack subtrees, and the ICS Kill Chain described in this white paper. All these documents are publicly available. These tools are available to all utilities, from small municipalities and cooperatives to large investor-owned utilities (IOUs). The goal is to assist utilities in being more proactive in cybersecurity.
To advance this paradigm, further research is needed to provide tools and guidance that assist in determining the highest impact and exploitability cyber attacks. Two approaches, BBN and DBT, are discussed. Finally, MTD is proposed as a mitigation strategy. All of the techniques and tools described in this white paper should be tested in a laboratory environment.

Contact Information:

- Annabelle Lee: ablee@nevermoresecurity.com
- Sachin Shetty: sshetty@odu.edu

About Nevermore Security

Annabelle Lee is the founder and Chief Cyber Security Specialist of Nevermore Security - Annabelle's experience comprises over 40 years of technical experience in IT system design and implementation and over 25 years of cyber security design, specification development, and testing. Over the last 15 years, she has focused on cyber security for the energy sector. Over her career she has authored or co-authored many documents on cyber security, cryptography, and testing. She began her career in private industry concentrating on IT systems specifications, software testing, and quality assurance.

To adequately address potential threats and vulnerabilities, cyber security must be included in all phases of the system development life cycle, from the design phase through implementation, operations and maintenance, and disposition/sunset and address prevention, detection, response, and recovery capabilities. Proposed cyber security mitigation strategies must be evaluated based on the impact on reliability, performance, and cost. The approach of **Nevermore Security** is to identify the highest priority risks/attack vectors and the most effective cyber security strategies and solutions. This will include both technology and procedural solutions and may include accepting the residual risk. Ultimately, cyber security must not adversely impact the reliability of the energy systems.

For more information: https://www.nevermoresecurity.com/about/