Consequence-driven Cyber-informed Engineering (CCE)

Mission Support Center Concept Paper

Prepared by:
Mission Support Center
National & Homeland Security Directorate
Idaho National Laboratory
October 18, 2016

Idaho National Laboratory

INL/EXT-16-39212

1 Introduction

The Idaho National Lab (INL) is leading a high-impact, national security-level initiative to reprioritize the way the nation looks at high-consequence risk within the industrial control systems (ICS) environment of the country's most critical infrastructure and other national assets. The Consequence-driven Cyber-informed Engineering (CCE) effort provides both private and public organizations with the steps required to examine their own environments for high-impact events/risks; identify implementation of key devices and components that facilitate that risk; illuminate specific, plausible cyber attack paths to manipulate these devices; and develop concrete mitigations, protections, and tripwires to address the high-consequence risk. The ultimate goal of the CCE effort is to help organizations take the steps necessary to thwart cyber attacks from even top-tier, highly resourced adversaries that would result in a catastrophic physical effect. CCE participants are encouraged to work collaboratively with each other and with key U.S. Government (USG) contributors to establish a coalition, maximizing the positive effect of lessons-learned and further contributing to the protection of critical infrastructure and other national assets.

The CCE framework is built upon three distinct realities of cyber space. First, organizations must recognize the difference between targeted and indiscriminate attacks, and accept that if targeted by an advanced cyber adversary, they will be compromised. Second, traditional IT security is focused on cyber hygiene, which is only sufficient to repel non-targeted attacks. Third, and most importantly, coalition members must realize that critical infrastructure, and the complex systems created to control it, was designed to meet engineering requirements, not security requirements. These systems are based around failure mode analysis rather than security-minded, cyber-informed engineering. In order to incorporate an improved security posture within critical infrastructure, organizations must adopt a process that properly calculates the risk posed by specific cyber adversaries and groups, develops an understanding of the potential impact (including cyber-physical) of a cyber event, and promotes information sharing of actionable cyber security information and context.

> *"The deficiencies in the existing methods of cyber defense have been increasingly exposed as state-sponsored and state-run attacks have become more frequent and use more sophisticated and extensive resources."*
>
> ***-Richard J. Danzig, Former Secretary of the Navy (Surviving on a Diet of Poisoned Fruit)***

2 CCE Process

The enhanced and configurable capabilities of a modern ICS provide both significant benefits to the user and opportunities for malicious exploitation. This potential for malicious exploitation is a direct result of a design basis "trust," which assumes that digital system separation, and therefore protection from the cyber threat, can be maintained.

However, the reality is that the modern cyber threat is constantly evolving and there is no

separation method that can be maintained.

A well-resourced and experienced cyber actor drawing upon various skills can target a system and undermine the trust model at every level. They are goal-oriented and perform reconnaissance, conduct planning, develop customized tools, and test their attacks against frontline security solutions. They are also capable of human-enabled and supply-chain compromises that can bypass even the most sophisticated network defenses.

It is difficult to account for a threat that is co-adaptive (i.e. an intelligent human adversary) as the technology becomes the field of contest and can be used to defeat the underlying engineering design. Cyber incidents pose unique challenges and the appropriate response to a failure scenario will not account for a component or system behaving in a way for which it was not designed. Given enough freedom to operate and supporting resources, attackers will find ways to be successful. The degree of success will be a direct function of the knowledge, forethought, and planning of system designers and operators.

It has been proposed that new risk analysis and design methodologies must be adopted to account for co-adaptive nature of the hazard and devise potential mitigation strategies required for safe and secure operations. CCE at its core, is an engineering effort that eliminates the "trust" assumption and fills the existing cyber security gaps through a series of processes and procedures. These processes are divided into four distinct quadrants, each with a unique goal: 1) Consequence Prioritization, 2) System of Systems Breakdown, 3) Consequence-based Targeting, and 4) Mitigations and Protections. This combined process is intended to be completed in order from the first to the fourth quadrant.

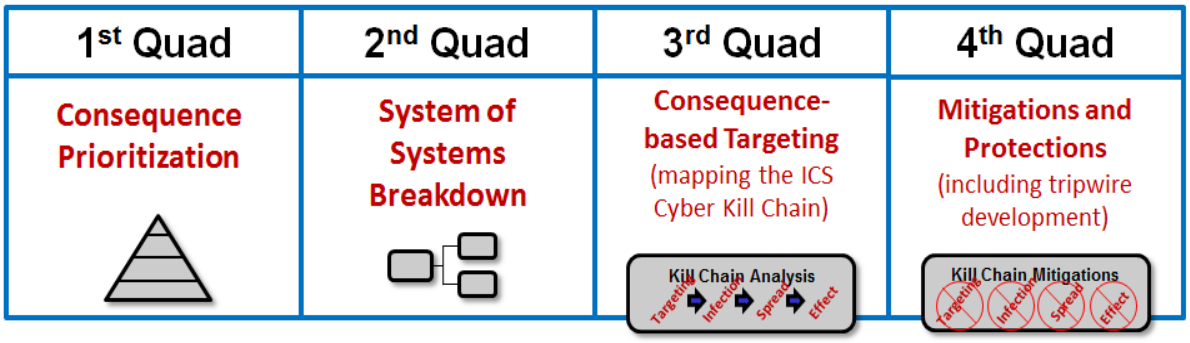

Figure 1: The primary processes of the CCE framework.

2.1 Consequence Prioritization

At the start of the framework process, Consequence Prioritization, organizations must define the most critical functions and services that allow them to accomplish their individual missions. Using CCE to distill High Consequence Potential events promotes a progressive risk management strategy that initiates with the required cyber hygiene and escalates to focus engineering-based preventative measures.

For example, a utility company must identify the functions and services that are required in order to provide electricity to their customer base. In some cases, there may be multiple critical functions and services. In order to prioritize these pieces, organizations should also identify the highest consequence events or thresholds that need to be protected against. In general, utilities are prepared for potential power outages such as those that occur as the result of bad weather. However, a utility might identify the highest consequence event as loss of electricity to a large section of their customer base for more than two days. Using this method, private industry can more clearly identify and prioritize critical functions and services. This is especially helpful in circumstances with limited resources.

The next logical step involves USG helping to identify the highest consequence events that pose a risk to national security. These problems are too large for any one business to protect against and therefore require federal efforts.

2.2 System of Systems Breakdown

In the second quadrant, System of Systems Breakdown, private industry evaluates their own infrastructure and operational processes in order to identify the critical systems, digital devices and components that impact the previously identified critical functions and services. This process can be thought of as an engineering analysis approach. Beyond the individual systems that support a critical function or service, private industry must be cognizant of any key information exchanges between these systems, the loss or compromise of which to an adversary would result in an operational failure. The government should assist in the development of the methodologies used to conduct a system of systems breakdown, however, in the long run; the burden of analysis will fall on private industry. Because of this, it is important that these methodologies be developed in consort with members of private industry, and the process validated in several sectors through pilot projects.

2.3 Consequence-based Targeting

The third quadrant, Consequence-based Targeting, uses an adversary approach to quantify "how" to achieve a specific impact against a target system. In order to expend private industry's resources efficiently, this process involves an assessment of the cyber adversaries' capabilities and methods. As an example, is there any way an adversary can achieve a desired, negative impact through cyber means? If that impact falls within the realm of the possible, then the next step is to map the adversarial progress against the ICS Cyber Kill Chain. The ICS Cyber Kill Chain is a high-level model that dictates the steps required for an adversary to be successful against a target system, from a cyber attack vector. Once this Kill Chain has been developed, this information should be shared with the intelligence partners of the coalition in order to baseline adversarial groups and better inform the risk mitigation strategy of private industry, within specific sectors. It can also be used to infer a more efficient and effective cyber defense effort at the utility.

2.4 Mitigations and Protections

The goal of the fourth quadrant, Mitigations and Protections, is to intelligently improve the security posture of private industry. Based on the work conducted in the other quadrants of

the framework, both public and private industry should better understand the goals, capabilities, and progress of a cyber adversary. This evolving resilience is bolstered by continued framework activities. For example, the information gained through the framework should inform the development of engineering design analysis documents that detail specific recommendations, mitigations, protections and tripwires. In some cases, the information will drive cyber-informed engineering changes to the infrastructure. For example, by employing a physical change in design or infrastructure that removes various digital devices or physical components from the cyber attack target deck.

3 Conclusion

INL designed the CCE framework to improve cyber defense and provide foresight within the new reality of cyber space, where organizations must prepare for compromise. The impact of CCE is substantial; employed at a major electricity producer it identifies:

- The critical functionality of a control system
- The applicability of an attack scenario against this functionality across the enterprise
- Additional insight from sensitive US Government reporting
- Key technical context for the organization
- Specific recommendations to harden the system and operations against sophisticated adversarial attack/manipulation

The CCE framework is intended to be an iterative process, allowing private and public industry not only to protect themselves against existing cyber threats, but also proactively prepare them for the next generation of emerging cyber threats. The CCE process revolutionizes the defensive strategy for potentially crippling cyber attacks, even in the event of complete adversary control over the IT environment.

4 Recommended Reading

[Paper | Robert Anderson, Joseph Price | *Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology* | 2015]

[Paper | Michael J. Assante, Tim Roxey, Andy Bochman | CSIS – Center for Strategic & International Studies | *The Case for Simplicity in Energy Infrastructure* | October 2015]

[Paper | Richard J. Danzig | Center for a New American Security | *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* | July 2014]

[Paper | Michael J. Assante, Robert M. Lee | SANS Institute | *The Industrial Control System Cyber Kill Chain* | October 2015]

[Article | David Sax | Bloomberg Businessweek | "In the Age of Cybercrime, the Best Insurance May Be Analog" | 10 March 2016]