Calhoun: The NPS Institutional Archive

DSpace Repository

Faculty and Researchers | Faculty and Researchers' Publications

2017

Modeling cyber conflict to inform critical infrastructure defense

Connett, Brian; Halloran, Bryan

B. Connett and B. Halloran, Modeling cyber conflict to inform critical infrastructure defense, Dynamic Systems & Control, March 2017, vol. 5, no. 1, pp. 7-10. Link http://hdl.handle.net/10945/57845

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

MODELING CYBER CONFLICT TO INFORM CRITICAL INFRASTRUCTURE DEFENSE

BY BRIAN CONNETT
CDR, USN, PHD STUDENT
BRYAN O'HALLORAN
ASSISTANT PROFESSOR

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

Imagine a naval strike group patrolling in the middle of a territorially challenged and electromagnetically controlled area of the world. The threats to that group are varied and wide ranging which require the group to employ all available defensive and offensive tools. While the physical kinetic threat to the group can be detected as an external event, it is not always easily detected when that threat presents itself inside the control network of the strike group. In this scenario, it is possible that the lurking threat is exercising data collection among the ships, or simply lying in wait to take over the navigation system without the users knowing. No known architecture or decision framework exists to inform a critical infrastructure or cyber-physical system (CPS) when it is best to defend against a possible attack. In addressing systems of systems (SoS) or families of systems (FoS), designers implement characteristics to describe the robustness of the system in terms of availability, reliability, reparability, etc. This approach may not be appropriate for the given scenario or those similar. Therefore, a framework and architecture must be introduced that supports the defense of a system to access most information, while being optimized to the characteristics of an attack. Often, those characteristics are not readily accessible, so an architecture is developed to analyze the attributes of an anomaly's timing, medium, intention and value. Here, the reader will find a methodical recommendation that develops the way defense of a cyber critical infrastructure can be most effective. First, historical background motivates the current political theme, followed by modeling theory that has been published. Classical systems engineering foundations are reviewed to adapt modeling environment to the current cyber conflict problem in a way that allows a systems owner to posture most effectively against anomalies across the network of communication nodes. Finally, the focus of both this paper and the authors' research is defining the attributes, and the common knowledge expected to be used throughout this field of research. Those attributes form the landscape upon which future research can be conducted.

BACKGROUND

The U.S. Critical Infrastructure Protection program of 1996 [1], and amplification in the Patriot Act of 2001, defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According to Presidential Policy Directive (PPD-21) [2] and the Department of Homeland Security (DHS) there are 16 critical infrastructure sectors. Those systems and assets within critical infrastructures were created and existed in a seemingly safe space away from exploitation or attack by adversaries with ill-intent. With increased complexity of CPS, vulnerability to cyber-physical attacks shows significant increase, if only validated by open source reporting like that of the attack on the Iranian Nuclear program, called Stuxnet [3]. In addition to the daily open-source reporting of infiltrations, this increase in activity is clearly demonstrated by the Federal Aviation Administration (FAA) Federal Registry report and Government Accounting Office (GAO) report citing belief

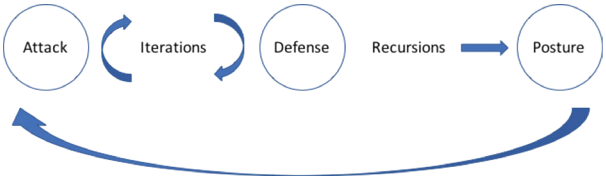

FIGURE 1
Integration Systems Model – Cyber Conflict.

that commercial aircraft contain significant risk for cyber-attacks through a common network of the avionics and entertainment system [4, 5]. Further, security breaches of well-known establishments emphasize the capability of such attackers. As a result, critical infrastructure has become a target.

Knowing that CPS exploits exist, with characteristics of patience, stealth, replication ability and the robustness never experienced before, system owners are obligated to maintain a high level of response-action posturing to protect their own resources. Regardless of the posturing, limited systems resources exist in computing, logic, and exploitation definitions, and contribute to an aggregated failure against multi-pronged attacks from multiple simultaneous attackers. Even when aligned in an apparent show of up-to-date defense, there exists the danger of unknown vulnerabilities and penetrations against such defenses. The key to success is having the knowledge to align critical infrastructure architecture in a manner that is responsive to the capability, willingness and timing of the attacker.

MODELING, ARCHITECTURE AND FRAMEWORK

Models currently exist that primarily demonstrate the dynamics of cyber-physical systems. In particular, Derler, et al., present a significant approach in "dynamics, the evolution of a system state in time"[6]. This model provides insight into the inherent difficulties of simply modeling the dynamic nature of systems of CPS. Few models, empirical or theoretical, exist to examine the value of both knowing attacker capabilities in the cyber realm and the strength of one's own system. Axelrod and Iliev [7] present a mathematical model that analyzes how the timing of using a cyber exploitation depends on the stakes involved and the characteristics of the exploitation itself. The reader is encouraged to reference this work in depth to understand three major assumptions of this model, leading to a balanced equation that defines value of an attack on a system. The implication of this model is that a protection posture can be estimated, and can quickly turn into a balanced engagement between the attacker and defender. The difficulty therein lies of knowing when to fortify a critical infrastructure against an impending attack.

To establish a framework that informs decision makers of when to defend critical infrastructures, critical architecture elements for several parameters are estimated. Understanding these parameter estimations uniquely positions the decision maker to posture having revealed the vulnerabilities of those parameters being estimated, an attacker's persistence, and stealth. A scalable framework designed to deliver optimal solutions to its user requires a broad-based methodology that can capture all aspects of the impending problem and the possible solutions. To that end, our current research works toward laying the foundational framework in four specific attributes, and tied into the aforementioned modeling efforts. The attributes of timing, intent, value of attack, and mediums will allow both a qualitative and quantitative tractability in the decision at hand.

As the framework is developed, consider the work of Langford who delivers a discourse on the differences in systems engineering versus systems engineering integration [7]. As relevant as it is in the classroom, the practices on integration from his industry point of view are even more relevant when applied against this problem of defending the critical infrastructure. Specifically, he highlights that the "usual desire for integration is for interoperability of objects and processes to achieve some effect in their intended operational environment," yet it is exactly this desire to integrate the parts of a system into a whole which make our modern cyber and physical systems vulnerable. Continuing to use Langford's emphatic position that systems engineering is quite different from systems integration, integration should not be relegated to that effort which results in a whole by following some set of best practices. "For systems engineering, a best practice is iterative development and improvement. For systems engineering integration, a best practice is successive approximation based on recursive thinking." [7] This approach to systems design and systems integration will be applied in a similar manner to the design of a proactive response to anomalies, rather than an iterative and reactive response. **Figure 1** is based on Langford's "high-level summary of the systems engineering process model" [7] where he addresses the "type of thinking required ... as the service progresses through development and into integration." Similarly, the cyber conflict framework and architecture introduced in this research claims the same progression. The attack of the critical system is interactive with the defense of the same system through iterations. The iterative relationship is the ultimate integration of understanding the attributes of the models described in Axelrod and Illiev [7], and help to develop the measures of success in the approach. Once the engagement is complete, or has settled to a steady state manageable for continued operations, the overall effectiveness of the integration of defenses is indicated by a forward-looking recursion to demonstrate the learned behavior within the decision framework. The recursive relationship forwarded to consequential posture of the system indicates the level of that learned behavior. The life-cycle of an attack and defend engagement is indicated by the closed-loop review arrow.

FRAMEWORK AS A DECISION MAKING TOOL

Decision making in defense of a critical infrastructure under a possible cyber-attack is rooted in the system owner's desire to maintain attributes of a system that are often found in broadly defined terms such as reliability, resilience, and stability. It is under these attributes that measurements of success can be assigned. While attributes found in these loosely-defined terms are generally understood, these attributes are not characteristics of this research being considered. Instead, the reader is encouraged to think of the optimal solution to an attack in terms of redundancy, which here describes the grouping of mechanisms (synthetic or natural) that replicate ability. As a result, failure of one means of ability will be recovered and continued

by the next. To increase the broad applicability of redundancy, this architecture decision framework is agnostic to how the physical or logical redundancy is presented.

The functions of redundancy encompass two sets of approaches to defending the SoS or the FoS, namely an iterative-based set versus a recursive-based set. These sets are respectively assigned to decision making based on rules or prior knowledge. The iterative process is purely reactive and allows an anomaly to have an initial effect on the system before the rules have an opportunity to adjust. Considering the Axelrod and Iliev model introduced earlier, a recursive (knowledge) based ruleset that does not wait for an anomaly to present itself, is introduced that considers the four attributes introduced in this piece as information to invoke redundant procedures throughout the SoS. This framework combines both of these approaches. This is a developing framework, yet it still needs to be stimulated by the attributes in some manner from an external source. The assumption of the ability to acquire the stimuli is made here, and will be left to other research to understand why or how that information is obtained. Still, we must start by aligning the work of Axelrod and Iliev to match the premise of response action being introduced.

Two attributes of the attacker, stealth and persistence, are most relevant in this framework. An exploitation or anomaly in a CPS or critical infrastructure will likely have some aggregation of these characteristics. Stealth is defined by earlier authors as a conditional probability describing that an exploitation will be able to transit a CPS undetected given that the attacker has activated the capability (Pr (exploitation surviving | activated)), and Persistence is defined as a conditional probability describing that an exploitation will not be detected given that the attacker has not activated the capability (Pr(exploitation surviving | not activated)) [8]. While this is consistent with the previous works, we will consider this as an attacker's 'intent', and for the research presented here persistence will be a redefined

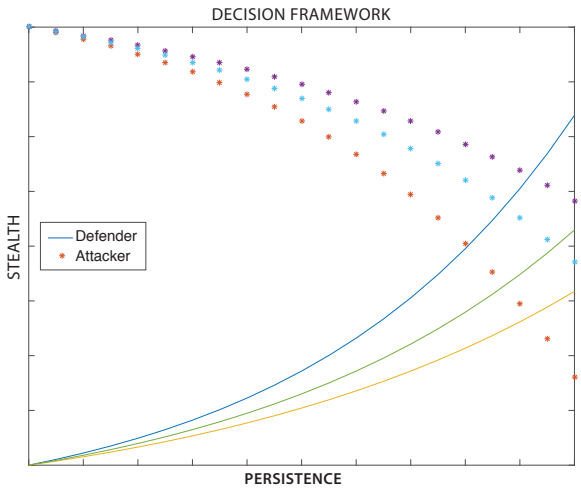

FIGURE 2 Decision Framework based on Threshold.

trait parameter to match the framework goal. Specifically, persistence will be the conditional probability describing that an exploitation will be able to transit a CPS undetected given that the attacker has increased its number of attempts at exploiting a system (Pr (exploitation surviving | increase in attempts to exploit)).

The next attribute informing the architecture framework is the value of the attack. Notionally, the value of the attack is a relatively-weighted item that fits into categories of destruction, data extraction, and behavior and social modifications. Because of the assumptions of stimuli introduced from a known external source, the weight of these values will be dictated by the current intelligence picture relative to the systems being targets. There are numerous examples cited throughout the government, industry and private

MEDIUM	PERSISTENCE	VALUE	STEALTH
Network Failure	M:1	0.05	1.00
Power Failure	M-(x_1) : 1	0.20	0.80
Malicious – Low	M-(x_2) : 1	0.40	0.60
Malicious – Med	M-(x_3) : 1	0.60	0.40
Malicious – High	M-(x_4) : 1	0.80	0.20
Kinetic Effect	1 : 1	1.00	0.05

TABLE 1 Taxonomy of Cyber Conflict.

sectors that build a growing intelligence picture with regard to cyber conflict. Specifically related to the fragility of critical infrastructure are examples of the electric grid blackout (2003) in the Northeast United States of America and Southern Canada, the ongoing failures of the Metropolitan transit lines in Washington, D.C., United States, private information breaches among super chains such as supermarket and retail product provider, Target, and hints at weak protection of avionics in commercial airliners that have received attention in recent memorandums from the U.S. Federal Aviation Administration. Still, knowing that these weaknesses exist, the weight of an attack value is dependent upon external source analysts.

The third attribute, when combined with the previous two attributes, reveals a taxonomy of attacking vectors that will ultimately inform the overall timing of the defense posture in the recursive methodology desired at the beginning of this work. The medium from which an attacker can deliver anomalies into a system is varied, but for the purpose of discussion, **Table 1** lists persistence, stealth and value for a range of mediums. As research to support the architecture framework matures, and modeling of the frameworks develops, arbitrary values will be modified to realize the potential effect of these attack characteristics. The mediums described are listed as those attack vectors that are expected to be encountered, from least destructive to most destructive. The persistence is described as an attempt-to-realization ratio. For example, in a Network Failure the attacker will be able to attempt access to a system many times before being caught (M:1), whereas a Malicious attack will have less attempts before being detected (M-(x_n):1). Finally, an attack with a kinetic effect will be attempted one time, and by the nature of its effect, will be known immediately (1:1). The last two columns are arbitrarily weighted values assigned to the attack in order to quantify the overall utility of the system and the stealth of an attacker. These are arbitrary values, and will be adjusted during modeling efforts using simulation techniques to measure various effects.

Finally, the fourth attribute determines the optimal timing of both the attacker and the defender. Using the taxonomy of the cyber conflict, a mathematical model will be derived to determine at what point it is best for a target defender to employ the recursive knowledge-based ruleset desired and illustrated in **Figure 2**. In **Figure 2**, a series of curves are used to demonstrate the dynamic nature of applying defensive measures. As stealth and persistence are measured along the axes, the posture of both the attacker and defender can be estimated. The model derivation will reveal an optimal time to employ the rules of the framework.

ABOUT THE AUTHORS

Commander Brian Connett, U.S. Navy, is currently stationed at the U.S. Naval Postgraduate School in Monterey, CA pursuing his Ph.D. in Systems Engineering. In particular he is examining concepts of cyber-physical systems and the complexity of decision making regarding its security. His education includes a M.S. in Systems Engineering, a M.S. is Space Operations both from the U.S. Naval Postgraduate School and the B.S. in Information Systems from Drexel University, Philadelphia, PA.

A career naval officer, Brian has recently been a junior faculty member at the U.S. Naval Academy in Annapolis, MD leading midshipmen in the classroom as a controls systems and cyber operations instructor. Prior to this classroom mission, his naval experiences include assignment to the U.S. Naval Air Forces, Navy Information Operations Command, Special Boat Team TWENTY and USS Lake Erie (CG70). His personal decorations include the Meritorious Service Medal, the Defense Meritorious Medal, the Navy and Marine Corps Commendation, and the Navy and Marine Corps Achievement Medal.

Bryan O'Halloran is currently an Assistant Professor in the Systems Engineering department at the Naval Postgraduate School. Previously he was a Senior Reliability and Systems Safety Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for hypersonic missile programs. He holds a Bachelor of Science degree in Engineering Physics and a Master of Science and Doctorate of Philosophy in Mechanical Engineering from Oregon State University. His current research interests include risk, reliability, safety, and failure modeling in the early design of complex cyber-physical systems.

Figure 2 is a theoretical representation of what the authors believe will represent that decision timing for both the attack and defender. All measurements within the graph are unitless and are meant to give an illustration of a relative magnitude of those attributes discussed. The solid curves of the graph show a relative magnitude value of defending against an attack, whereas the starred curves show a relative magnitude value of the attack. When stealth is at its highest, a deployment of defensive measures will have the smallest effect since it is not known if the anomaly exists. When persistence is greatest, it is known that an anomaly exists in the system, but now with lower stealth value. The intersection of the curves indicates when it can be both the best time to attack and to defend. The multiple curves show how the weighted values of the frameworks taxonomy can dictate that threshold of action. This is when the architecture framework lends itself to a decision framework.

CONCLUSION

Cyber physical systems are vulnerable to various anomalies. Some of those anomalies exist naturally, but when those anomalies are introduced by an actor with malicious intent, the intention and outcome can be devastating. In defense of the cyber-physical system there exist many methods and techniques to respond to an attack as it happens. The resources required to counter an attack can certainly be effective, but exist as a reactive measure. This paper presents a combination of known models and system design techniques that results in an architectural framework that is predictive. In turn, the prediction of the models serves as a decision tool for the physical systems owners. Further research of this predictive modeling and architectural framework will build upon current community contributions. Overall, the contributions from this community will address the tipping point of cyber conflict within the critical infrastructure of our hyper-connected society. Physical threats to the military, industry and private sector control systems are not easily detected, nor mitigated. Without architecture or frameworks in place to confront the issue, system owners will continue to struggle against the threat. When optimized within decision algorithms, data will exist to illuminate what process can be implemented in defense. Using classical systems engineering fundamentals, modeling & simulation, and proven mathematical approaches, this research seeks to support such implementation. ■

REFERENCES

1 W. J. Clinton, "Executive order 13010 on the presidents commission on critical infrastructure protection," United States of America, White House, 1996.

2 B. Obama, "Presidential policy diective - critical infrastructure security and resilience. PPD-21," United States of America, Washington, D.C., 2013.

3 K. Zetter, "WIRED," Crown Publishers, 03 11 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [Accessed 16 11 2016].

4 Federal Aviation Administration, "Airworthiness Standards: Transport Category Airplanes," FAA, Washington, D.C.., 2014.

5 U.S. Government Accountability Office, "Air traffic control: FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NEXTGEN," Government Accounting Office (GAO), Washington, D.C., 2015.

6 P. Derler, E. A. Lee and A. S. Vincentelli, "Modeling cyber physical systems," in *Proceedings of the IEEE*, 2012.

7 G. O. Langford, Engineering Systems Integration: Theory, Metrics, and Methods, CRC Press, 2016.

8 R. Axelrod and R. Illiev, "Timing of cyber conflict," in *Proceedings of the National Academy of Sciences*, 2014.

9 Federal Bureau of Investigation, "The Cyber Threat," 27 03 2012. [Online]. Available: https://www.fbi.gov/news/stories/2012/march/shawn-henry_032712. [Accessed 15 11 2016].

10 U.S. Senate and U.S. Congress, "Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act of 2001)," Unites States of America, Washington, D.C., 2001.