Mission Technologies division
HII.com

Automating Orchestration for Machine-Speed Cyber Defense

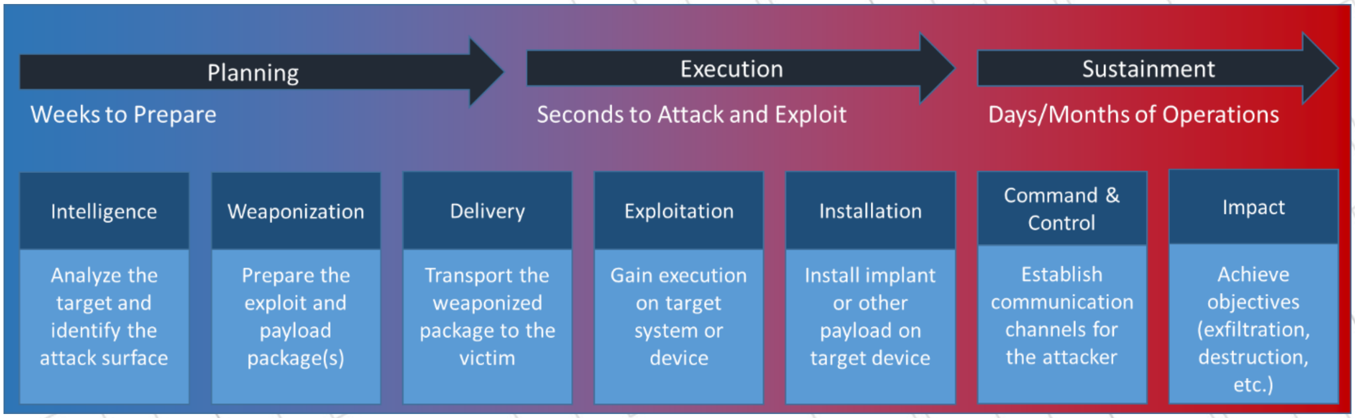
August 2022

Introduction

Military operations in the cyber and physical domains are often paralleled to provide a better understanding of the employment and effects of cyber capabilities. There are several similarities between the two domains, including the need for command and control (C2) of resources, situational awareness of the environment, and planning and preparation of the battlefield, to name a few. There are also substantial differences between them, two of which include our control of the domain and the inherent timescale within it.

First, cyberspace is a man-made domain unlike land, sea, air, and space, meaning that as the creators of the domain, we can better manipulate, more easily adjust, and even outright change the environment. Second, speed in the operations lifecycle is even more important in the cyber domain, as offensive operations may take weeks to plan and prepare, but they can be executed autonomously by machines in seconds (Figure 1). Contrast that timescale to an operation in the physical domain; movement of forces and engagement of the adversary may take days, weeks, or months, leaving ample time for the target to sense, react, and adjust to evolving operations. The cyber domain leaves little-to-no time for humans to adjust to autonomous adversarial actions, making automated and informed responses much more important. In this article, we will demonstrate how HII is changing the domain to enable "machine speed" reactions to defend against an adversarial cyber operation.

Figure 1 - Notional Timescale of a Cyber Attack



Planning
Weeks to Prepare

Execution
Seconds to Attack and Exploit

Sustainment
Days/Months of Operations

Intelligence	Weaponization	Delivery	Exploitation	Installation	Command & Control	Impact
Analyze the target and identify the attack surface	Prepare the exploit and payload package(s)	Transport the weaponized package to the victim	Gain execution on target system or device	Install implant or other payload on target device	Establish communication channels for the attacker	Achieve objectives (exfiltration, destruction, etc.)

The Immediate Benefits of Cyber Security Orchestration

Cyber security orchestration refers to the planning and execution of resources to defend a system from a cyber attack. For example, acting upon Security Information and Event Management (SIEM) alerts may include reconfiguring boundary protection devices, updating rules and policies, or patching systems. Due to the myriad of cyber security vendors and devices, these actions are typically performed through a coordinated effort of cyber security and information technology professionals. Because the process relies on manual interaction, responses can take excess time to implement, giving the attackers additional time to achieve their goals. Automation of orchestration is one area we can increase the speed of response to mitigate the effects of a cyber attack, and possibly even prevent them in the first place.

HII is one of the primary contributors to OpenC2, an open-source standard that automates cyber security orchestration regardless of the vendor or type of device. The Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit standards body supporting the development of OpenC2, in cooperation with cyber security vendors (Cisco, IBM, McAfee, etc.), government organizations (US Cyber Command and the National Security Agency), and HII. The OpenC2 standard will enable updating and reconfiguring of cyber security defenses at "machine-speed," leaving an adversary virtually no time to continue an attack on a vulnerable network. While Security Orchestration Automation and Response (SOAR) technology has the same goal, SOAR products are built to work with vendor-specific devices based on proprietary interfaces. OpenC2 expands the functionality of SOAR products via an open source, vendor agnostic machine language specification, allowing organizations to enhance their cyber security posture and easily share results with the rest of the community.

Incorporating Technology Advancements Into OpenC2

Automating cyber security orchestration is one way to mitigate an active cyber attack, but with future advancements, it may assist in preventing them as well. In the Office of the Director of National Intelligence's white paper on Cyber Threat Intelligence[1], the use of technology was identified as one of the tools that can drive change, specifically through Machine Learning (ML) and automation. As the implementation of highly effective ML models will process copious amounts of available cyber threat data and rapidly turn it into actionable intelligence, automation of cyber security orchestration will minimize the latency of human intervention in preparing and defending against an adversary's cyber operation. Imagine the power of an artificial intelligence system that can:

1) Analyze terabytes of cyber threat data in a matter of seconds,
2) Automatically process the data into adversarial capability and intent,
3) Instantaneously determine the optimal defenses to protect against the identified threat actor's capabilities, and
4) Autonomously send OpenC2 commands and messages to reconfigure security devices that will detect and stop the cyber threat from ever breaching the system.

Based on an increased capacity of actionable threat intelligence combined with a capability to immediately process and act on it, threat actors will be forced to plan and execute their operations in near-real-time since the target will have already deployed defense mechanisms to identify, detect and defeat employment of the adversary's capabilities. This approach also saves valuable resources assigned to detecting and recovering from attacks by preventing successful attacks from even happening and improves the overall cyber resiliency of these systems.

Summary

Whether we are referring to the cyber domain or any of the other physical domains, a successful defense is dependent upon the speed at which forces can react. In the cyber domain, the attacker typically has the advantage as the attack is often completed by the time the target's defenses have detected it (if they even did). Cyber threat intelligence helps organizations identify an adversary's capabilities and intentions, effectively providing a means for them to prepare for an attack. However, analyzing threat data to identify an actor's plans, and orchestrating defenses to prepare or defend against an attack, rely heavily on human intervention, at human speed. Advancements in artificial intelligence technology enable machine-speed analysis of cyber threat data, and implementation of the OpenC2 standards allows machine-speed orchestration of cyber security devices, eliminating the inherent advantage for attackers and greatly reducing the ability for adversaries to succeed in planning and executing cyber attacks.

Additional Steps

While automating cyber security orchestration is one mechanism to reduce the advantage attackers have in the cyber domain, other improvements are equally important to decreasing the number of successful cyber attacks in organizations. Increasing the speed and production of cyber threat intelligence, coupled with automating defenses, will help prevent adversaries from compromising their targets, but needle-moving improvements in cyber security cannot be achieved through a couple of changes. In future papers, we will explore other areas for improving the overall cyber security posture of an organization, including:

1) Enhanced sharing of cyber threat intelligence and mitigation techniques. As cyber threat intelligence production becomes faster and more effective, we need to quickly and accurately share adversarial TTPs and effective mitigation techniques that apply across organizations, tamping down any momentum an adversary may achieve through exploitation of vulnerable victims.
2) Improved cyber security hygiene, including application of best practices and standards. Dedicated application and maintenance of cyber security standards produced by organizations such as the National Institute of Standards and Technology, the International Standards Organization, and the Center for Internet Security ensures the most common and broadly spread attack vectors are neutralized. Eliminating the "ankle biters" shifts capacity to mitigate and defend against more advanced attacks that incur higher cost to organizations.
3) Demotivating would-be attackers through a government-based cyber deterrence program. The real and visible threat of inflicting cost on our adversaries can assist in preventing some attacks. Policies, politics, diplomacy, organization and technology are all required to deter advanced adversaries from inflicting damage to organizations. The US Government has the resources and authorities to achieve these goals, and an effective deterrence program will help us as we continue our endeavors to level the cyber playing field.
4) Increasing the pool of cyber security talent through education and training programs. A substantial talent gap exists in the workforce to address the requirements needed to improve security across industries and organizations. Programs at all levels (elementary school students through career professionals) will increase the available talent over time, while adding additional skills and capability to existing talent.