Chapter 12
A New Dynamic Cyber Defense Framework

Jim Q. Chen
DoD National Defense University, Washington, D.C., USA

ABSTRACT

Current approaches in cyber defense are flawed as they are fortress-based and generally static in nature. They are not flexible in dealing with variations of attacks, especially zero-day attacks. To address this issue, researchers have looked into dynamic cyber defense. However, the available approaches are either only about high-level strategies or only about specific tactics. There is no integrated approach that brings both levels together in a systematic way. This research article intends to address this challenge by proposing a new dynamic cyber defense framework that is systematic and cohesive, and that integrates strategic, operational, and tactical levels. It improves the research in dynamic cyber defense by employing game-changing elements such as a contextual analysis system and an intelligent decision-making system.

INTRODUCTION

There is a dilemma in cybersecurity. Significant investment has been made to protect computing devices, systems, and data. However, devices and systems still have been hacked and compromised, and data still have been stolen. What has gone wrong in cyber defense? An examination of the available apparatus utilized to defend cyberspace reveals that most solutions are static in nature; namely, computing devices, systems, and data are protected within a fortress, which has layers of defense such as access firewalls, intrusion detection and intrusion prevention systems, anti-malware software, access control systems, continuous monitoring systems, and log systems. To the outside world, it is obvious that assets are held inside the fortress. If one could bypass the layers of defense, one could get access to the jewels of information. The static characteristics are further consolidated with the implementation of static Ethernet addresses and static IP addresses, which serve as targets for search engines, such as Shodan, which discovers any devices connected via the Internet. In addition, the use of the TCP/IP stack may introduce other risks and unexpected consequences. Kovacs (2015) notes that the remotely exploitable TCP/IP stack vulnerability (CVE-2014-9196) "could allow an attacker to launch man-in-the-middle (MitM) attacks against

DOI: 10.4018/978-1-7998-2466-4.ch012

[the Eaton Cooper Power Series Form 6 recloser control and Idea/IdeaPLUS relay protection platforms] products that are accessible via the Internet". As explained in the MITRE CVE web site (2015), these power grid control and relay products generate "TCP initial sequence number (ISN) values linearly, which makes it easier for remote attackers to spoof TCP sessions by predicting an ISN value". In this sense, the attack surface is greatly increased if a device is connected to the Internet with an IP address, especially a static IP address. Industry control systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Internet/web cameras, and routers are good examples, as they are the popular search items in Shodan searches.

To reduce the attack surface, the mindset in defense needs to be changed. If a computing device is made to be a moving target, or at least seems to be, it increases the level of difficulty for attackers. The question is how to make it happen. In literature, it can be found that some researchers design obscurity methods, such as methods of making IP addresses anonymous or obscure as well as methods of hiding IP addresses. Other researchers invent dynamic addressing. All these methods obviously have their advantages over the static addressing methods, including the DHCP method. However, they have not been successfully implemented. It is odd to see these ideas are not put into use even though they have significant potential. This research article attempts to analyze, from different perspectives, the reasons for this odd phenomenon and to find out its root cause. This analysis leads to the exploration of an innovative solution that incorporates contextual analysis into dynamic defense in order to customize dynamic changes.

This article is organized as follows. In the first section, an introduction to the challenge is provided. Next, related works are examined. The current approaches and their limitations are also analyzed. In the next section, an innovative solution is proposed. Next, the proposed approach is further discussed and applied to a specific case. Its advantages are discussed. Directions for future research are also suggested. Finally, a conclusion is drawn.

RELATED WORKS AND CHALLENGES

Lamb, Ling and Hayes (2012) argue for dynamic defense in cyberspace, as "traditional approaches to cybersecurity are proving to be inadequate against today's increasingly sophisticated cyber threats". Furthermore, "too often, governments and businesses find themselves one step behind attackers, reacting to rather than anticipating each new threat" (Lamb, Ling & Hayes, 2012, p. 1). They maintain that "a new approach to cybersecurity is required, one that is proactive, dynamic, adaptive" (Lamb, Ling & Hayes, 2012, p. 1). They argue that four areas should be focused on: threat-vector intelligence, rapid response, evolutionary response, and integrated remediation (Lamb, Ling & Hayes 2012). This is a good strategy, but Lamb, Ling and Hayes (2012) do not specify how this strategy should be implemented at the operational level, especially how dynamic operations can be achieved. To implement this strategy, techniques such as Moving Target Defense (MTD) should be employed. According to Casola & De Benedictis (2013), MTD involves "continuously changing a system's attack surface" to thwart cyber-attacks (p. 22). This technique is "based on fine-grained reconfiguration at different architectural layers" (Casola & De Benedictis, 2013, p. 22), such as security layer and physical layer, to increase "the complexity for the attacker to successfully complete an attack" (Casola & De Benedictis, 2013, p. 28-29). Obviously, this technique can be effective only in an appropriate context under the guidance of an appropriate strategy.