Department of Homeland Security Innovation OTS Application Addendum

FINANCIAL SERVICES CYBER SECURITY ACTIVE DEFENSE (FSCSAD) TECHNOLOGIES

Application Date: February 22, 2017

Application Title: A Moving Target Defense for Data Storage Devices

Which TTA does this solution address: (Check all that apply)
☐TTA 1: Intrusion Deception | ☑TTA 2: Moving Target Defense | ☐TTA 3: Isolation and Containment

Executive Summary: Data storage devices are used to collect our nation's most sensitive financial information. And yet, it is a common misconception that these devices and the specialized conduits that connect them are somehow exempt from threats that permeate conventional networks. Nothing could be further from the truth. Cyber adversaries have the time and means to plan attacks at their leisure aimed at critical data storage devices. While recent international standardization efforts have begun to address the broad topic of storage security, much more can be done to actively defend against these threats. With this Phase 1 application, we offer an innovative Moving Target Defense that will provide critical protection for storage devices and networks.

New storage products often mention something about "security", but when you dig deeper, that usually means only one thing: encrypting the data on the storage media. Certainly, "data-at-rest" encryption is essential, but "data-in-motion" must be protected as well. Link-level encryption is one way to do that, but interoperability issues make it more difficult to implement on some storage networks than others, so vendors often leave it out. Another critical area that is neglected is the storage management interface. What if the only intention of a determined attacker is to simply turn off the power to one or more of these devices? If done at the right time, or on a large enough scale, that could result in a most devastating cyberattack on our nation's financial infrastructure. Our Moving Target Defense aims to protect storage *management* interfaces in addition to storage *data* interfaces.

This project is potentially revolutionary because it introduces active defense technologies to an industry that typically uses only passive techniques, such as encryption and authentication, if any at all. Storage virtualization techniques will be used to create multiple abstractions of a device that will confuse potential attackers and provide many possible "ports" or "channels" that may be used to communicate with the device. At any given point in time, there is only one port that is the "correct" or "active" port. By dynamically, or randomly, changing the configuration of the active port, we create a Moving Target Defense, not unlike that which may be found in today's software-defined networks (IP-hopping) and in yesterday's radio communications (frequency-hopping).

When complete, this project could potentially be of great interest to CIOs at financial services firms, as well as the many IT professionals specializing in data storage at those firms, not to mention the dedicated professionals at the Department of Homeland Security (DHS) and other federal agencies who safeguard much of our nation's critical data. The impact of this project would be felt in the commercial market for solid-state arrays, all-flash arrays, and purpose-built backup appliances. Over a period of six months, and with $194K in Phase 1 funding, we believe we can bring vital and revolutionary change by introducing our approach to utilize active defense technologies in an industry where either no security or dated techniques, such as passive encryption and authentication, have become the unopposed standard.

TECHNICAL INFORMATION

Technology Description: One of the most novel aspects of our solution is the use of *storage virtualization*, a type of *software-defined storage* that we have been pioneering for years. There are four essential elements to our technical approach. The first is to isolate the device from the host computer by changing the device type from "disk" to "unknown" inside a storage appliance that blocks access to the device from the host's operating system (OS) and applications. Next, we obfuscate the command set. Changing the command set for the device inside the appliance makes it more difficult for an attacker to access the device, but not impossible, as this is merely a "covert but static" approach at this point. A determined attacker could still monitor the interface and over time eventually infer the meaning of the commands. For greater security, we now implement a moving target defense. Changing the communications channel from one command to the next defeats the attacker who has taken the time to decode the custom command set. In addition, changing the command set itself from one command to the next makes the approach even more dynamic by changing two dimensions of the attack surface at once. Finally, we statically link the interface library to the authorized application on the host. Only that specific application will be able to access the device(s) presented by the storage appliance, not the OS and other applications. This step is potentially risky because it could negatively impact interoperability. It will work great for certain types of applications, such as backup apps, that typically talk exclusively to certain devices, but not for others that rely on general OS support. More direct customer engagement will allow us to better understand specific financial services customer applications and use cases. Our technology introduces minimal functional and performance impacts and provides the additional capability of gathering metrics related to both performance and security. Potential breaches will be detected and logged, but will not make the storage devices inaccessible to authorized users in order to preclude the possibility of having the technology used against us. One of our technical challenges is to ensure an adversary cannot simply flood the device with unauthorized requests for the purpose of generating a denial-of-service attack. That risk will be mitigated with appropriate code in the interface library.

Innovation: We believe our solution pushes the state of the art by adding active defense technologies to data storage devices and appliances for the first time. Current offerings provide "data-at-rest" encryption of storage media, password-based authentication for storage management interfaces, and signed firmware for storage devices. Our solution goes far beyond these passive techniques by adding active cyber defense technologies.

Homeland Security and/or Financial Services Sector Application: Our solution employs *randomization* in a manner that is understood by policies and algorithms known only to software on both the host computer and the storage appliance. This results in a solution that is *unpredictable by adversaries*, just as DHS has requested. Our solution closely mirrors the first *focal point* listed by DHS in the description of TTA #2 (networks – in this case, storage area networks) by randomly changing the Logical Unit Number (LUN) in a manner similar to IP-hopping. This results in a dynamic network configuration enabled by the use of *virtualization*. It most closely matches the first use case listed by DHS in TTA #2, in which randomization is used to self-modify the configuration of one or more devices, which in turn reduces vulnerability exploits by the attacker into denial of service for the attacker.

Prototype Maturity: We currently have a working prototype that demonstrates everything listed above except some aspects of the moving target defense. Specifically, we have a storage appliance that can successfully talk to disk devices on the "back-end" while presenting them as different device types on the "front-end", which can be either iSCSI or Fibre Channel at this point. We can change the device type to be something other than "disk" using storage virtualization, and we have the interface library running on the host computer that will be synchronized with code running on the appliance when the moving target defenses are implemented. All of the essential elements outlined above will be demonstrated at the conclusion of Phase 1 using iSCSI or Fibre Channel, or both.