Lockheed Martin and SCIT Technologies combine efforts to create a Moving Defense Cloud

Introduction:

In 2010 Lockheed Martin tested out a new level of security for its cloud based framework, LM ClearSky Cloud Command & Control Suite (LM ClearSky CC&CS). LM ClearSky CC&CS provides a reproducible cloud based enterprise data center solution that can be tailored or scaled to each engagement and quickly be brought online. It provides a secure, reproducible solution architecture that encompasses all facets for a data center. For outward facing applications, such as websites, additional technologies were sought to increase security against malicious attacks. SCIT Labs shifts the focus of intrusion avoidance to reducing the losses resulting from an intrusion. SCIT rotates virtual servers using fixed or random time intervals. As virtual servers move offline, they are scrubbed, removing any infectious software that has been placed there during an attack. By rotating these servers online again and removing others, the SCIT system is able to prevent long term attacks against an application. Lockheed Martin combined the capabilities of LM ClearSky CC&CS with the technologies created at SCIT Labs to design a cloud computing system that allows a web application to exist on the cloud but be protected by a moving defense of rotating virtual servers. The purpose of this project was to determine how a web application could be protected by both LM ClearSky CC&CS's capabilities and SCIT Lab's capabilities and how to productize such a system to allow a user to interact with the moving defense in the same way as a single server in the cloud.

Overview of LM ClearSky Cloud Command & Control Suite:

LM ClearSky CC&CS (formally NIMBUS) is a Lockheed Martin innovation that provides a secure, reproducible solution architecture / cloud based framework encompassing all facets of a data center. LM ClearSky CC&CS is web services enabled and uses a web 2.0 self service interface. The system facilitates the orchestration and automation of best practices across a myriad of COTS applications, management tools, and infrastructure devices to enable secure, self service, on demand delivery of IT applications, systems and services.

The value of LM ClearSky CC&CS is twofold. First, provide a reproducible cloud based enterprise data center solution that can be tailored and scaled to each engagement and quickly brought online. Second is to provide customer value by:

- Increasing agility across the full life cycle of development, testing, staging, production and coop

- Enhance end to end situational awareness
- Improve SLA management and security
- Streamline development, and improve overall service delivery in an elastic fashion
- Facilitate 'Green' IT practices and solutions

Overview of SCIT:

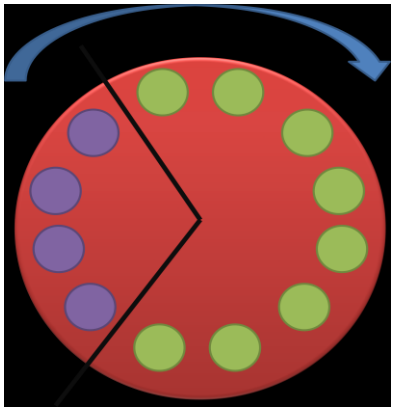

Figure 1: Visualization of the rotating SCIT architecture.

SCIT is designed to increase the security of virtualized and non-virtualized server environments. SCIT works by reducing the exposure of the server to the internet and nearly eliminating successful attacks. The system ensures that each virtual server is restored to a known pristine state at a pre-determined interval offering an attestation capability. SCIT can be set to restore the server to a known state every minute, deleting malware in the process. Although SCIT does not eliminate the vulnerability, by converting static systems to a dynamic system, SCIT makes it significantly more difficult for the attacker to exploit the vulnerability.

Using virtualization technology, SCIT rotates pristine virtual servers and applications at user specified fixed or random time intervals. In the graphic, five online virtual servers are processing transactions while three offline servers are being cleaned and restored to pristine state. Every cycle, a purple server is swapped out with a green server and the SCIT process begins again. SCIT design restores the system to a known state and thus recovers from an attack without user intervention. This is in comparison to the days or weeks in current systems taken to restore compromised systems.

Integration Effort:

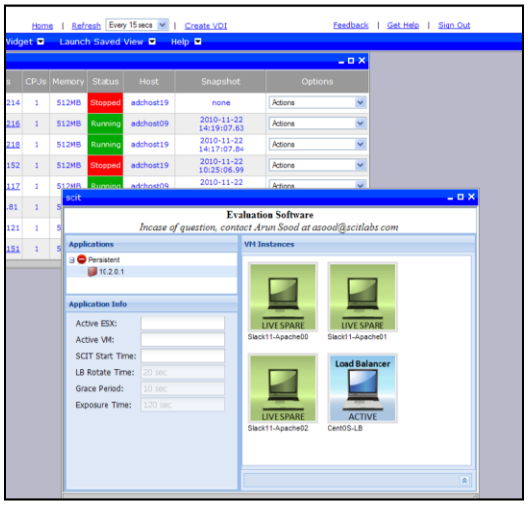

Figure 2: Embedded SCIT monitor inside the LM ClearSky CC&CS platform

Providing moving defense protection to a typical web framework requires multiple steps including duplicating the server's image across VMs and correctly configuring the SCIT server. Furthermore, it is necessary to separate the SCIT and LM ClearSky CC&CS controllers to prevent the possibility of SCIT controller being compromised. The LM ClearSky CC&CS / SCIT integration effort developed an architecture for automating the creation of new SCIT protected internet applications. Administrators can monitor the VMs hosting their system through the LM ClearSky CC&CS controller and can also view the status of SCIT protected VMs through its moving defense widget embedded in the LM ClearSky CC&CS

platform. By combining these systems, users are able to take advantage of the cloud computing services provided by LM ClearSky CC&CS and then deploy their system using the SCIT moving defense protection.