



**Conference Session Proposal:**  
NMCI Industry Symposium, June 20-23, New Orleans Marriott

**Speaker POC:**

Tom Resau, PR Manager, Public Sector  
703-668-8743  
thomas\_resau@symantec.com

**Topic concentration:**

“Security and NMCI”

**Session title:**

“Honey-pot Tactics for Threat Detection”

**Session Presenter:**

Wayne Selk, Principal Security Consultant, Symantec Corporation

**Presenter background:**

Mr. Selk is an expert on information security technologies and strategies. He currently serves as an on-site security consultant at Navy-Marine Corps Intranet (NMCI) operations centers, where he assists U.S. Department of Defense (DOD) authorities with security management across a large enterprise environment. In addition to consulting resources, Symantec Corporation provides NMCI with a broad range of security solutions across firewall, intrusion protection, content filtering, enterprise administration and virus protection technologies.

**Session description:**

*Adding “honeypot,” or decoy systems to the NMCI enterprise network will complement a defense-in-depth protection strategy in cost-effective fashion. Utilizing existing hardware, decoy systems provide an additional capability to slow attackers’ malicious actions – while capturing precious intelligence on who is seeking to compromise systems through various means.*

Malicious network-based attacks constitute a significant information assurance risk for NMCI. In defending against malicious code and novel intrusion attempts, care must be taken to address threats originating outside of the enterprise, as well as threats posed by insider error or abuse. As defense IT systems expand in size and capability, managing internal risks becomes more critical, particularly with respect to identifying threats in time to take mitigating actions and avoid a true system compromise.

This session, while addressing honeypot technology, will focus on networks of “virtual” massed honeypots, or “honeyd” as the logical choice for NMCI, since it merely requires

purchasing software and use of existing hardware. With the current rollout of Symantec ManHunt, a network-based intrusion protection system, at the B1, B2 and Transport boundaries, NMCI is currently optimized to detect external threats. A host-based IDS, Symantec Intruder Alert (“ITA”) complements ManHunt by monitoring individual computers, however it is slated to be removed from the desktop environment, leaving servers and Administrative workstations with optimal protection from intrusions specifically directed against workstations. Introducing honeypots at this tier of the network can protect IT assets from internal threats, the only other option for detection would be a honeypot cluster or a honeyd network.

Honeypots have existed for a number of years and offer a variety of tactical advantages. As decoy systems designed to be hacked; they can spare true IT assets from intrusion attempts. Further, since a honeypot has no “real” mission function, all traffic directed to it is inherently malicious, significantly lowering the occurrence of false positive issues. Honeypots also offer a compelling means to study adversaries and attack methodologies in-progress, to include identifying suspect internal actions.

Honeypots can assume various forms. Physical honeypots are real machines with their own IP address. They run multiple operating systems, services or applications. The configured services determine the avenues by which an attacker may choose to compromise the system. Virtual honeypots are attractive because they require fewer computer systems, which reduces maintenance and hardware purchase costs. They can give NMCI the flexibility to populate a network with hosts running numerous operating systems without increasing the physical population of servers. This “honeyd” approach can simulate the TCP/IP stack of the target operating system in order to fool TCP/IP stack fingerprinting tools like Nmap and Nessus.

This paper and subsequent presentation discusses honeyd’s design and will show how a Honeyd framework can help NMCI in many areas of systems security, e.g. detecting and disabling worms and distracting internal/external attackers, while capturing real-time documentation of their activities.