

Using Cyber Maneuver to Improve Network Resiliency

Paul Beraud, Raytheon
Network Centric Systems
Largo, FL
paul_f_beraud@raytheon.com

Alen Cruz, Raytheon
Network Centric Systems
Largo, FL
alen_cruz@raytheon.com

Suzanne Hassell, Raytheon
Network Centric Systems
Largo, FL
shassell@raytheon.com

Sonny Meadows, Raytheon
Network Centric Systems
Largo, FL
ledford_j_meadows@raytheon.com

Abstract— The Net Maneuver Commander (NMC) is a research prototype cyber command and control (C2) system which constantly maneuvers network-based elements preemptively to improve network resiliency in a cyber compromised environment. Similar in concept to a frequency hopping radio, Network Maneuver Commander transparently and preemptively provides a moving target defense to evade attack. It utilizes randomization algorithms for maneuver destination selection, providing randomized synthetic diversity of hardware platforms, operating systems and network segments. Network Maneuver Commander also improves resiliency through random and pre-emptive application and platform reconstitution with check-pointing, reloading and resetting, and through the support of deception and containment of malware.

The goals of the research were to increase the investment an attacker must make to succeed, increase the exposure of an attacker to detection as the attacker is forced to relearn the network and reestablish malware, increase the uncertainty of the success of the attack and to increase the overall survivability in the presence of attacks.

This paper describes the Network Maneuver Commander architecture as well as the resiliency techniques provided including moving target defense, randomization, reconstitution, artificial diversity and deception. Lessons learned are also addressed.

Keywords- Survivability; Resiliency; Preemptive Maneuver; Randomization; Artificial Diversity

I. SCOPE

In order to decrease the success of cyber attackers, new and proactive defensive strategies are required. Conventionally, defense in the cyber domain has relied upon a static, layered, “defense in depth” approach, with a focus on perimeter protection. Agile and resilient techniques such as the moving target defense, introduction of artificial diversity and reconstitution provided by Network Maneuver Commander are effective against 0 day vulnerabilities and insider threats with no known attack signature, because they provide a proactive defense rather than reactive defenses which are reliant upon attack detection and characterization.

Deployment of this agile defense increases the cost and chance of detection to the attacker and minimizes the effect of malware, thereby increasing the resiliency of networks. This increased resiliency enables mission assurance, even in a cyber compromised environment.

A. Overview

Proactive computer network defense must anticipate the emergence of new vulnerabilities, take action to avoid threat actors seeking to exploit these vulnerabilities, and disrupt the actions of successful intruders to increase their work factor and minimize their impact. The purpose of this paper is to describe the goals of the Network Maneuver Commander, the prototype developed, and the research conducted, to preemptively maneuver network elements to avoid cyber attack.

B. Background

A leading example of prior research in the area of dynamic defense is the DARPA-funded project called Intrusion Tolerance by Unpredictable Adaptation (ITUA) [1]. ITUA successfully demonstrated the feasibility of thwarting attackers by injecting pseudo-randomness in system response to attacks, but as a *post-attack reaction and response*. Network Maneuver Commander differs from this concept by proactively maneuvering resources during normal system operations and *prior to and independent of any attack*. Furthermore, compared to ITUA, the scope of cyber maneuver is broader and encompasses the full gamut of hardware and software through the creation of artificial diversity.

George Mason University pioneered a self-cleaning intrusion tolerance technology (SCIT) [2]. The SCIT Technology rotates transaction servers using load balancing and cleanses the ones that are offline prior to returning them. The Network Maneuver Commander concept is different in that although cleansing is also done, the primary focus is on the introduction of randomized artificial diversity, timing, and geographic destination. It is also not solely focused on transaction servers, and supports deception.

Information assurance (IA) defensive techniques today remain primarily passive and reactive. They focus on defending the perimeter, and as a result are vulnerable to insider and zero-day attacks. However, the need for resilient architectures that can ensure mission survival in a cyber compromised environment is now being recognized. As an indication of this change in thinking, MITRE hosted a Secure and Resilient Cyber Architectures Conference in McLean, VA, October 29, 2010 to discuss the goals, techniques and mechanisms recommended for achieving a Resilient Architecture [4].

The sections below encompass the work-to-date on the development of a cyber defense network maneuver commander. This work is the result of Internal Research and

Development (IRAD) funded by the Raytheon Company from March 2009 to 2011. This paper describes the implementation and usage of various cyber defense resiliency techniques supported by the Network Maneuver Commander.

II. DISCUSSION

A network maneuver approach that is capable of avoiding many attacks, even in the face of zero-day vulnerabilities, provides a proactive posture for the enterprise and increases the resiliency of the network. Recognizing that some attacks will succeed, the ability to disrupt a persistent threat, by requiring further attacker action to remap the network and re-establish malware command and control channels, not only makes the attackers work harder, but can increase the probability of attribution and detection due to the increased activity required of the attacker. The Network Maneuver Commander functionality morphs the “game board” on potential adversaries and significantly raises their stakes in this cyber warfare.

A. Hacking Process

The hacking process describes the steps a cyber attack must take in order to be successful. For the analysis and examples that follow, a hacking process as described in Hacking Exposed is followed[6]. This process can be thought of as a state diagram, and a possible depiction is shown in Figure 1.

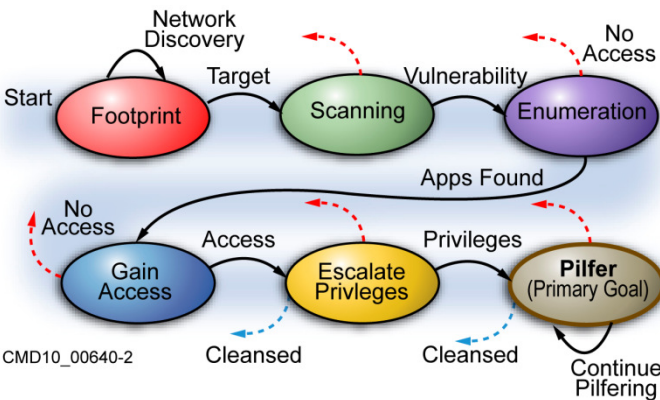


Figure 1. Hacking Process

As a cyber attack executes, it typically progresses through the steps, from the Footprint phase to the Pilfer phase. If a phase is reached where a cyber defense prevents access, the attack may revert to a previous phase. (In some cases this may be back to the Footprint phase.)

B. Cyber Defense Goals

There are three goals for the cyber defenses studied. These cyber defenses seek to:

1. Increase cost to the attacker
2. Increase uncertainty that the attack was successful
3. Increase chance of detection and attribution

The cost associated with execution of a cyber attack can be quantified as 1) the number of times a particular phase of the attack is thwarted and 2) the amount of time that is spent in the preparatory phases of an attack. For the cyber attacks analyzed, preparatory phases are those leading up to the Pilfer phase. A cyber defense is successful if there is an increase in both of these quantities.

The uncertainty associated with the success of an attack can be measured as a function the amount of time a threat spends executing its goal. For the cyber attacks analyzed, this is the time spent in the Pilfer phase. A cyber defense is successful if there is a decrease in this quantity.

The probability that a cyber attack is detected is proportional to the total time required for it to reach and execute its goal. A cyber defense is successful if there is an increase in this quantity.

Through the definition of these metrics, time becomes the fundamental measure of success and effectiveness. For further definition of the metrics, please refer to [5].

C. Moving Target Defense Decision Framework

The Network Maneuver Commander decision framework provides the necessary intelligence and configuration information to enable the maneuver of elements. Figure 2 shows the context diagram for the NMC. The network elements on which maneuvers are performed are shown in the lower left. Variants of executables may be deployed as maneuver destinations. The influencers of the randomized maneuver decisions are the threat information, predictions provided by model and real-time alerts and attack data received by the cyber command and control system from cyber sensors deployed in the network.

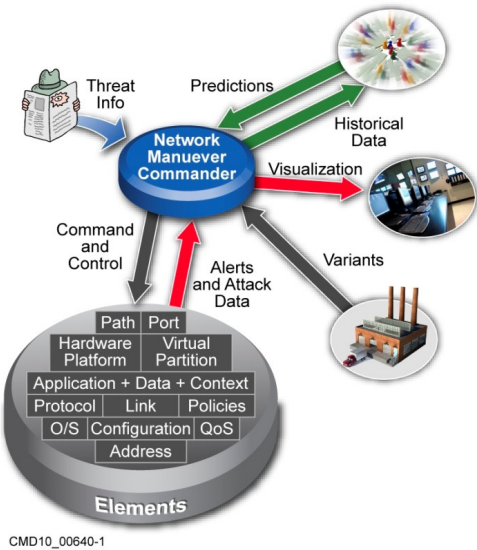


Figure 2. NMC Context Diagram

Identify applicable sponsor/s here. (*sponsors*)

The decision framework information contains three main elements used to make maneuver decision as illustrated in figure 3: introduction of artificial diversity, geographic destination, and move interval. Additionally, intelligence information is provided in the context of threat levels that impact the decisions made relative to all three main elements. Finally, consideration is given to a security zone constraint where the NMC will not maneuver elements between security zones.

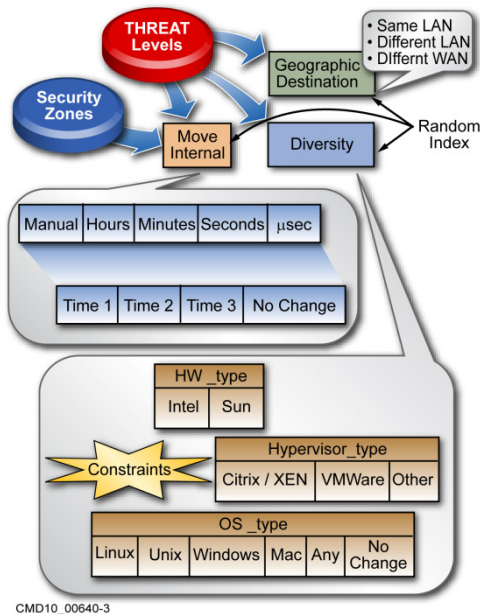


Figure 3. NMC Decision Framework

For example, the diversity element considers the hardware platform type, the hypervisor being used / moved to, the operating system type, and the applications that need to be moved. Any constraints contained within these elements are also considered. There are different move intervals as shown as well as multiple geographic destinations that can all be customized if desired. Destination selection algorithm influencing services also allow destination LANs to be specified as less or more desirable when network conditions change, and support avoidance of particular vendor operating systems, hardware platforms or hypervisors if unpatched vulnerabilities are known.

D. Reconstitution and Reloading

The objective of reconstitution and reloading is to enable the recovery of essential computing and network systems with immunity from errors and/or cyber attacks to ensure mission critical systems stay in the fight. Network Maneuver Commander supports two levels of reconstitution and reloading, a virtual machine level reconstitution and a complete hardware reconstitution.

As a new application destination is installed, it is loaded from a “gold image” virtual machine targeted to the operating system, hypervisor and hardware platform of the new destination. This ensures that no malware is resident in the application after the maneuver.

In particular, the use of hardware cleansing on different elements in the operating space allows for human independent regeneration of operational assets to survive disruptions..

- Hypervisors – Reloading of type 1 hypervisor systems onto an existing platform.
- Bare Metal Systems – This class of platforms includes what is typically referred to as a conventional server; it does not rely on virtualization and encompasses an application or set of applications running on an operating system loaded in a hardware platform.
- Network Components – This category entails devices such as firewalls, switches, and routers. While this group of platforms does not have as much data or state information as bare metal system, they do contain critical components of the mission; namely configuration settings and firmware.

E. Deception

After an application is maneuvered, its former destination may be removed/cleansed, contained and preserved for forensics or placed in a HoneyNet for real time observation. The Network Maneuver Commander HoneyNet capability is used for isolation, containment, monitoring and deceiving suspect applications and clients.

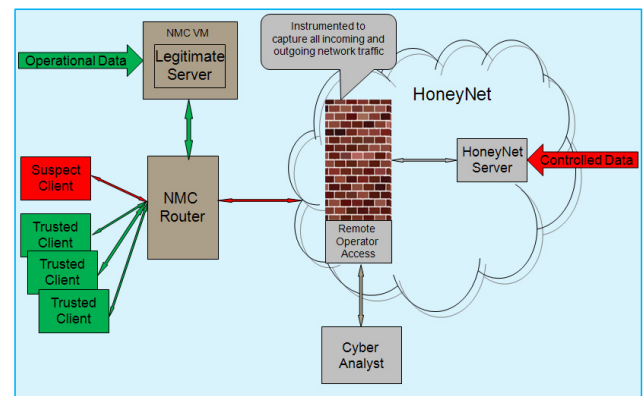


Figure 4. HoneyNet Configuration

The Network Maneuver Commander HoneyNet capability offers a novel way of protecting against potential

malicious clients. This feature, depicted in Figure 1, utilizes an instrumented host to achieve two main goals:

- Protection of Operational Data – Once a suspect client has been switched to the HoneyNet they will be provided with controlled data which is different than the operation data that the trusted clients are receiving. This controlled data can be such that it does not put at risk the mission even if it were to fall into the hands of adversaries.
- Enhances Attribution and Intent – Since all incoming and outgoing traffic is captured and can be access by an analyst, the likelihood of attribution of an adversary is increased. In addition, given that the suspect client will remain connected and consuming the controlled data, the intent of the operator(s) of the suspect client will be easier to ascertain.

The HoneyNet capability accomplishes these goals with the help of the prototype NMC Router that allows for dynamic re-routing of IP traffic without interruption to a client. The NMC Router enables external systems to switch from individual clients to entire ranges of clients to a desired destination without breaking the existing connection.

Once a suspect client is forwarded to the HoneyNet implementation, identical server software will provide data from a controlled source that is independent of the operational data that the trusted clients are receiving from the legitimate server. At any point an analyst can access the network data that was captured by the HoneyNet implementation in order to study the behavior of the suspect client and allow for further actions.

Maneuvering of IP addresses makes network appear larger than it actually is. IP addresses may be maneuvered independent of the other maneuver capabilities such as artificial diversity and reconstitution. Maneuvering IP addresses inside a network is useful in increasing cost for insider threats or advanced persistent threats that already have a presence inside the network, and is distinct from rotation of IP addresses at the perimeter of a network using NAT or other means.

The Network Maneuver Commander changes IP addresses of the destination at the time of the maneuver. This is typically done through use of high availability features like redundancy and load balancing, through use of the NMC router as described for the HoneyNet or through reconfiguration.

III. NETWORK ARCHITECTURE

A. NMC Architecture

The NMC architecture consists of an extensible collection of loosely coupled services. The services were developed to be standalone independent components conforming to a variety of interfaces including WSDL, Rest & JMS XML message based. The orchestration of the services was accomplished via the use of an Enterprise Service Bus (ESB). By leveraging the use of an orchestration engine, custom business logic for a particular deployment can be modified / extended via the rule configuration files. The NMC architecture includes a generic plug-in framework to provide wrappers for new applications to be plugged into the NMC system.

By leveraging a layered SOA architecture the NMC contains services at different service levels. The NMC provides high level business services to support mobility, variation and deception. The NMC contains both additional lower level specific business services that perform the core functionality as well as data services that insulate the consumer service from the underlying mechanism that was used to store the data.

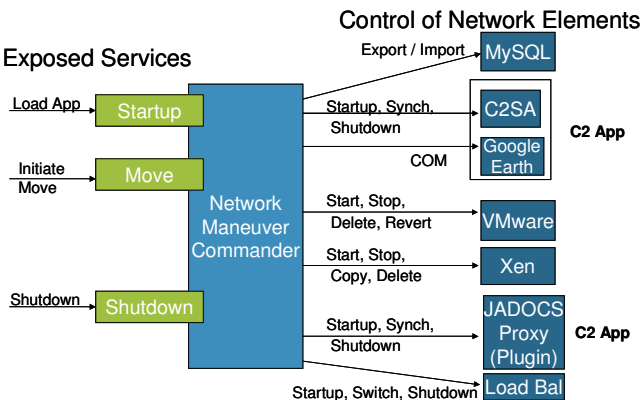


Figure 5. NMC Services Architecture

IV. MANEUVER MECHANISMS

A. Applications Maneuvered

The Network Maneuver Commander functionality has been demonstrated since 2009. Early demonstrations focused on maneuvering C2 systems and MySQL and Postgre databases, followed by maneuver of DNS, DHCP servers, web proxies and VoIP services.

For C2 system maneuvers, legacy systems were maneuvered as well as SOA systems. For the legacy systems, although data was not lost, the user situational awareness did experience a delay in updates viewed during

the short time (up to 2 minutes) that the client was reconnected, due to polling timeouts. This was not an issue for systems supporting high availability features.

The purpose of VoIP maneuvering is to reduce the likelihood of an attacker gaining access to critical VoIP components. VoIP components consist of an end unit which typically is an IP phone that connects to the local area network (LAN). The IP phone call control is performed by a call control manager, which performs the setup and teardown of calls. These components are vulnerable to attacks and malicious content such as malware introduced by Simple Network Manager (SNMP) exploits. To mitigate vulnerabilities of these components, firewalls, host based intrusion detection and other devices have historically been employed. VoIP maneuvering is a proactive approach to mitigate VoIP vulnerabilities. Most substantiation of VoIP networks consist of an enterprise solution with failover and redundancy included in the solution. Network Maneuver Commander leveraged this built in redundancy to maneuver call managers and gateways. Maneuvering of these components not only makes it harder for an attacker to gain access to systems that's dynamic in nature but is combined with reconstitution to remove resident malware from VoIP components without disruption to the end user.

B. Artificial Diversity

The artificial diversity for applications was primarily focused on hardware platform processor diversity (Xeon, HP) and hypervisor diversity (Xen and VMware). For applications that can run on different operating systems, the operating systems were also diversified. The advantage of the creation of artificial diversity was that typically malware is targeted at exploiting a vulnerability in a particular platform or operating system, rendering the malware unusable on other operating systems or platforms. The diversity and maneuvering to the different alternatives reduces the attack surface available to malware leveraging a particular vulnerability. Diversity was combined with cleansing to remove the malware that had obtained a foothold.

C. Mechanisms Used for Maneuvers

From a server, application or service perspective, maneuvers can utilize the organic failover/redundancy schemes if they are present. Similarly, maneuvers may take advantage of any inherent load balancing capabilities. Maneuvers were conducted using both VMWare and Xen bare metal hypervisors. It is important to note that we conducted maneuvers of applications residing within virtual machines and those that did not. Net Maneuver is not intended to be just a virtual defensive technique and there was a requirement to support legacy systems.

V. LESSONS LEARNED

A. Constraints

There are constraints that must be addressed when implementing a maneuvering strategy. We have grouped these into four main areas:

1. Environmental
2. Architecture
3. Network
4. Security

In the environmental grouping, constraints exist for components like memory, processing power and speed, as well as power requirements. Size, weight and power (SWaP) must be calculated into the maneuvering scheme as the architecture is designed.

The architecture grouping includes component relationship constraints, supported operating systems, hardware platforms, supported hypervisor types, network subnet requirements, etc.

The network grouping constraints exist for service level agreement (SLA) parameters such as latency, availability, throughput, and priority.

Finally, the security group addresses security zone constraints. The DARPA sponsored-BBN concept of security zones and known vulnerabilities was defined by the Designing Protection and Adaptation into a Survivability Architecture (DPASA) project [3]. Maneuvering should only take place within a contiguous security zone (e.g. the DMZ) and not maneuver from one security zone to another. If maneuvering across security zones is allowed, attacks could be transferred from one zone to another, which might open up vulnerabilities for the attacker to exploit that were not previously accessible. It is also advantageous to specify individual maneuver interval ranges per security zone.

B. Challenges

There are certainly challenges to implementing an active defense technology such as Network Maneuvering. A majority of modern technologies and software are not designed to support artificial diversity, and applications or services are often limited to running on a single operating system or hardware appliance. The increasing popularity of virtualized environments and cloud computing is improving this situation, and is making applications and services more maneuverable. Maneuver coordination is made difficult by the multitude of software interfaces within the applications and hardware that would be part of this strategy. There are no standard APIs for high availability capabilities, which are typically specific to each vendor. Network visualization and situational awareness is, and will continue to be, extremely challenging. Raytheon has defined measures of maneuver performance and success, which is the subject of a previously published metrics paper [5]. The current state of vendor licensing models presents a problem to maneuvering

schemes since maneuvering relies on using many instances (physical and virtual) and there is no licensing scheme that is designed to support this. However, this issue will be resolved as cloud computing deployment becomes more common. Use of high availability features for maneuvering increases license costs as this feature is typically more expensive. There is also a limitation that high availability (multiple simultaneous use) licenses for high availability deployments assume that a single operating system is supported.

There are both monetary and cultural barriers to entry in conducting network maneuvering. From a monetary standpoint, there could be significant infrastructure investment, depending on an organization's current posture and risk aversion. Culturally, network maneuvering increases vendor diversity, whereas most businesses are driving their information technology organizations to converge on standardization and support for a limited number of vendors, platforms and configurations. Concerns about supply chain integrity combined with the increased focus on resiliency help to support deployment of increased diversity of vendors and platforms in networks.

VI. RECOMMENDATIONS

A. Maneuvers

Based on testing we conducted in the laboratory and additional simulation, the resulting data showed that maneuvering, artificial diversity and cleansing, do provide improved intrusion tolerance as a lower percentage of attacks were successful and successful attacks took longer.

B. Other findings

1. The optimal maneuver frequency was to maneuver with an interval at least twice (2X) as fast as the fastest time it took an attacker to succeed in a stationary (non maneuvering) network scenario.

2. For a more robust performance, implementation of a client cleanup or complete virtualization scheme is recommended. This scheme has the added effect of eliminating any potential persistent threats on clients, as well as ensuring the clients return to a "known good" state periodically.

3. Maneuvering and artificial diversity in some cases can cause an application to move to a more vulnerable platform if an unknown (0 day) vulnerability exists on the destination platform or vendor type.

VII. SUMMARY

The network maneuver commander prototype described is an initial capability set to be used in the proactive defense of networks to increase resiliency in a cyber compromised environment. Figure 5 below illustrates the effect of cyber maneuvering on the Observe, Orient, Decide and Act (OODA) loop during execution of a mission. The blue forces represent network availability to execute the mission and the red forces represent the advanced persistent cyber threat

operating within the mission network to compromise the mission. During mission execution, the survivability and freedom of action required by the mission is increased due to the preemptive maneuvering, reconstitution and artificial diversity which make the attacks less successful and slow down the attackers. The attackers are more easily observed in the HoneyNet and through cyber sensors which detect their increasing activity. The attackers' freedom of action is hampered by the cleansing which removes the malware and the maneuvering of the botnet or malware command and control channels. The confusion and "noise" generated in the network by the maneuvering activity minimize the attackers' ability to observe the network, thereby increasing their cost and slowing them down.

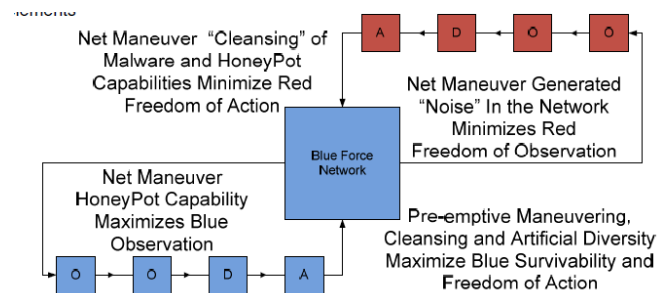


Figure 6. Network Maneuver effect on the Mission OODA loop

Raytheon is continuing to evaluate other candidate resiliency techniques, algorithms and technologies with ongoing research, and have 5 patents pending on this technology.

REFERENCES

- [1] "Intrusion Tolerance by Unpredictability and Adaptation", <http://itua.bbn.com/>
- [2] <http://cs.gmu.edu/~asood/scit>
- [3] http://www.bbn.com/technology/cyber_security/designing_protection_and_adaptation_into_a_survivability_architecture
- [4] Goldman, Harriet, "Building Secure, Resilient Architectures for Cyber Mission Assurance", Secure and Resilient Cyber Architectures Conference MITRE, McLean, VA, October 29, 2010. http://www.mitre.org/work/tech_papers/2010/10_3301/10_3301.pdf
- [5] Sandoval, Juan and Hassell, Suzanne "Measurement, Identification and Calculation of Cyber Defense Metrics", Military Communications Conference [MILCOM] 2010, San Jose CA, October 31, 2010 – November 3, 2010. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5680489
- [6] "Hacking Exposed 5th Edition: Network Security Secrets And Solutions", Stuart McClure et al. 2006
- [7] Hunt, COL Carl, Bowes, Jeffrey and Gartner, Doug "Net Force Maneuver", Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, West Point, NY