# 18 April 2012

MEMORANDUM FOR: AFIT/ENG

ATTENTION: MAJ BUTTS

FROM: 2d Lt Ryan Andrew Morehart (GCO-13M)

SUBJECT: Thesis Prospectus: *Malicious Traffic Detection through Internet Protocol Address Hopping*

1. A host of systems—including firewalls, proxies, and intrusion detection systems (IDS)—protect modern computer networks, yet attackers still routinely break in due to the inability to successfully detect every possible avenue of attack. The introduction of more dynamic methods of detecting malicious activity may offer additional protection. The goal of this research will be to test if the inclusion of network gateways that manipulate the Internet Protocol (IP) addresses and port numbers of incoming and outgoing packets allows the detection of malicious traffic. A comparison of correct traffic classification—on a per-packet valid/invalid basis—will be done on a network with such a system and one without. Time permitting, the integration of a honeypot system to handle malicious traffic will be explored.

2. Previous research into network address space randomization focuses on the confusion it presents to an attacker. This work intends to explore how it can be used to complement traditional network defense tools. The possible integration with other defense systems (IDSs and honeypots in particular) is mentioned in a few papers, but there is no work to determine whether such integration is viable or if traffic truly can be classified accurately.

3. A gateway-based IP hopping solution will be developed to perform experiments against. This system will include encryption between gateways, manipulation of network addresses and port numbers, a rapidly changing external IP, and require no changes to hosts inside the protected networks. Once this system is in place, a test network will be established with multiple gateways (each running the hopping system), hosts inside the protected networks, and hosts outside. Classification agents on all involved systems will record the number of valid and invalid packets they receive. Traffic on the network will come from generators that appropriately tag packets as valid or invalid, allowing easy detection on the receiving end. Several experiments will occur, with whether hopping is enabled or not as the primary variable. To perform this work, a network of at least six systems is required, although more would allow greater flexibility in testing: two gateways, one host behind each gateway, one malicious system outside the protected network, and one server outside the protected network. These could either by virtualized or physical, though the gateway systems ideally will have three or more cores available.

4. The anticipated outcome of these experiments would verify that the use of hopping gateways significantly decreases the amount of invalid traffic permitted into protected systems. If this occurs, it is safe to state that the introduction of IP address hopping would benefit networks. If it does not, it demonstrates that IP address hopping is less useful as a traffic classification measure. However, such a result would not invalidate previous published findings on the usefulness of hopping in confusing an attacker.

5. The protection of computer networks is critical to the military. This research will demonstrate if IP address hopping can be used to provide further safeguards.

6. Proposed thesis committee:

a. Dr. Barry Mullins, Chair / Thesis advisor \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(signature)*

b. Dr. Rusty Baldwin, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(signature)*

c. Dr. Timothy Lacey, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(signature)*

7. Sponsor: N/A

8. The coursework completed at AFIT has been planned to provide the foundation of knowledge required to successfully complete this thesis. Courses of particular applicability to this research topic include:

- CSCE 560 Intro to Networking

- CSCE 629 Cyber Attack

- CSCE 528/628 Cyber Defense

- CSCE 654 Computer Communication Networks

Additionally, four credits of special study focusing on previous network address space randomization research will provide necessary background.

Ryan A Morehart, 2d Lt, USAF

GCO-13M

1st Ind, AFIT/ENG

MEMORANDUM FOR AFIT/ENG

I approve/disapprove the above thesis prospectus and thesis committee. This prospectus will be maintained in the student’s file. The thesis should be prepared in accordance with the AFIT Thesis Guide. Good luck!

JONATHAN W. BUTTS, Maj, USAF

Chief, Computer Science and Engineering Division

Department of Electrical and Computer Engineering