

20 May 2016

MEMORANDUM FOR: AFIT/ENG  
ATTENTION: MAJ WOOLLEY

FROM: 2LT Matthew Aust (GCS-17M)

SUBJECT: Thesis Prospectus: Proactive Host Mutation in Software Defined Networking

1. Network scanning is the first step in almost every successful network attack. By determining the services on a network, an attacker can discover vulnerabilities they can exploit to gain access. To mitigate an attacker's ability to scan a network, I will build an application, which continues the work of a series of research papers concerning Random Host Mutation (RHM), that proactively mutates the IP address of critical servers to protect against enemy scanning.

2. Researchers from the University of North Carolina, Charlotte (Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan) have published a series of papers concerning their attempts at a Moving Target Defense (MTD) system. Their approach consists of creating a virtual IP address for each host and mutating it, either over time or based on scanning techniques, to reduce an attacker's ability to scan and map a network. I will be building on their research by moving past a proof of concept tested on a simulator, and creating an application that runs on physical hardware and enterprise-level systems.




3. To test the viability of my research I will be running experiments. As a control I will be testing three networks with the same number of hosts and switches. I will use the same hardware for all tests. First I will test a standard statically-configured network to set a baseline for its vulnerability to network scans. I will then test a network configured for RHM to determine its performance. Finally, I will be testing my system with the same method. I will be utilizing previously acquired servers and switches for all my experiments. I am also in contact with one of the members who conducted the original research to determine what methods they used as well as garner ideas for how to build my system. I will measure my progress based on the results of network scans and will know my research is successful if my system prevents a higher level of scans than the previous work.

4. The results of my experiment will be the number of hosts that can be accurately identified, i.e., an attacker is able to establish a TCP connection to a specific server. To portray my results in an accurate context I intend on conducting a statistical comparison of my results versus the previous research versus my baseline of a statically-configured network using either T tests or ANOVA.

5. This research can greatly increase the defensibility of any network utilizing Software Defined Networking. Given the sensitive nature of many Air Force and DoD networks, implementing my system will significantly reduce the ability of attackers to determine viable targets on a network and thus reduce their ability to launch attacks against them. My application can also force attackers to increase the rate at which they scan, increasing the likelihood of being caught, allowing DoD operators to more readily identify and prevent incoming attacks.

6. Proposed thesis committee:

- a. Dr. Barry E. Mullins, Chair / Thesis advisor
- b. Dr. Timothy H. Lacey, Committee member
- c. Dr. Michael R. Grimaila, Committee member

 (signature)  
 (signature)  
 (signature)

7. Sponsor: Undisclosed at this time

8. I will be utilizing several class offered by AFIT to further my knowledge to execute this thesis, to include

CSCE 686 Advanced Algorithmic Design

CSCE 725 Reverse Engineering

CSCE 554 Fundamentals of Performance Analysis and Experimental Design

CSCE 699 Finite Automata Independent Study

CSCE 699 Exploring Security in Software Defined Networking Independent Study

I will be using two servers, a Pica switch, a HP switch, and a Cisco switch on which to conduct my experiments.



MATTHEW E. AUST, 2LT, Air Force  
GCS-17M

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!

BRIAN G. WOOLLEY, Maj, USAF  
Chief, Computer Science Division  
Department of Electrical and Computer Engineering