# 9 June 14

MEMORANDUM FOR: AFIT/ENG

ATTENTION: MAJ DUBE

FROM: 2d Lt Zachary J. Zeitlin (GCO-15M)

SUBJECT: Thesis Prospectus: *Mitigating ARP Vulnerabilities using SDN*

1. The goal of this research effort is to demonstrate the feasibility of mitigating vulnerabilities found in the various network protocols using Software Defined Networking (SDN). Measured data from a simulated SDN environment will be compared with data from a baseline to evaluate the following: effectiveness in mitigating known vulnerabilities, latency effects, scalability, and overhead costs.

2. Prior research in the field of protecting network protocol vulnerabilities has been conducted, with several tradeoffs proposed. Current research exists in SDN security applications, however little research has combined both SDN with methods specific in securing the data link layer of the OSI model. Existing methods for securing the data link layer Address Resolution Protocol (ARP) include static entries, adding cryptography, port security, and Dynamic ARP Inspection, among others. All of the proposed methods have drawbacks inclusive to being too costly, incurring excessive administrative overhead, or incurring a loss of network efficiency. Research has not been performed using SDN to combine the benefits of each of these ARP vulnerability mitigation techniques, as well as other network vulnerability mitigation techniques.

3. A new SDN application will be developed which combines the techniques of previous research in the field of network vulnerability mitigation. This application will then be simulated in a virtual network using MiniNet, a vetted network simulator designed for rapid prototyping of network protocols and applications. Metrics to evaluate include latency changes, successful network attack attempts, and bandwidth performance. Comparing these metrics to a baseline provided by a standard network of similar size provided within MiniNet will provide a measurement of statistical significance that will reveal the proposed SDN application’s ability to effectively prevent various network attacks. The operating costs of this research is low considering tests will be performed in a virtual environment. A server capable of managing several virtual machines is necessary. Progress towards a successful simulation environment will be measured as each known data link layer vulnerability mitigation technique is transcribed successfully into software, allowing modular application of each technique. Success is determined based on a known network attack being rendered ineffective in the simulated environment, while basic networking services remain available.

4. Research results will include a comparison of the number of intercepted packets through ARP spoof techniques within the protected versus the unprotected environment, as well as a comparison for bandwidth and latency in the protected versus unprotected environment. This research will be expanded to apply to other network attacks (inclusive to denial of service attacks and other vulnerable network protocols). The expected results are to show that ARP attacks, and other network attacks are fully thwarted with little to no cost of network latency, bandwidth, or administrative overhead. Successful implementation will also show a reduction in network hardware costs, as specialized switches are replaced with programmable commodity hardware.

5. Results will be used as part of a determination of the feasibility of using dynamic SDN applications to replace custom and expensive switches designed with static capability.

6. Proposed thesis committee:

a. Dr. Barry E. Mullins, Chair / Thesis advisor \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. Dr. Timothy H. Lacey, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c. Dr. Kenneth M. Hopkinson, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Sponsor: (If no sponsor, put “N/A” here and remove subparagraphs a. through g.)

a. Name: Adam Wisely

b. Title: of sponsor POC

c. Organization: full mailing address

d. Section or Division: in words

e. Office Symbol:

f. Telephone number:

g. E-mail address:

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

- CSCE 526 Secure Software Design

- CSCE 528 Cyber Defense

- CSCE 560 Introduction to Computer Networking

- CSCE 689 Distributed Software Systems

- CSCE 629 Cyber Attack

Additionally, four credits of special study focusing on the fundamentals of SDN provided insight into the capabilities allowed within software defined networks. A course in performance analysis and design will assist in constructing an environment suitable for collecting research data. In addition to coursework, familiarity with Python and C programming is required to construct the various network vulnerability mitigation SDN applications, and has been gained through self-study.

ZACHARY J. ZEITLIN, 2d Lt, USAF

GCO-15M

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!

THOMAS DUBE, Maj, USAF

Chief, Computer Science Division

Department of Electrical and Computer Engineering