20 June 2013

MEMORANDUM FOR: AFIT/ENG  
 ATTENTION: DR MULLINS  
  
FROM: CAPT Nick Kulesza, USAF, USA, (GCS-14M) [Nicholas.kulesza@afit.edu]

SUBJECT: Thesis Prospectus: “Exploiting Alternative Behavioral Characteristics in Wireless Technologies to Establish Communication”

1. Wireless technologies provide a great deal of mobility to connect users to the Internet. The advent of various wireless protocols to establish communication between a user, wireless access point and the Internet offer a unique perspective on alternative communication. Pioneers of modern day computing seek to find innovative techniques of subterfuge to persist and maintain access while possessing the ability to pass commands. These alternative communication paradigms are more commonly known as “covert channels”. The goal of this research analyzes some of the latest developments in recent trends with wireless protocols to discover innovative new techniques and obtain alternative communication.

2. Computing breaks commands down into the atomic elements of true or false, more accurately depicted as either a one (1) or zero (0). The research required to obtain a successful covert channel requires the alteration of a seemingly ambiguous field that does not change the contents of the desired message. Recent trends with 802.11n indicate the possibility to explore the establishment of covert channels utilizing “lesser significant” fields. In addition, wireless technologies possess physical characteristics that present opportunities to alter the preamble leading up to active communication. The oscillation of ones and zeros before active wireless traffic begets an interesting proposition to omit or introduce extra ones or zeros and analyze the behavioral properties.

3. This research project consists of two phases: Phase I, Proof of Concept (802.11n) and Phase II, Exploratory Heuristics (802.11ac). The success of this research stems from the initial proof of concept. The current accepted industry standard wireless communication protocol (802.11n) provides a stable platform to demonstrate an alternative communication implementation. The advent of the next generation of wireless technology (802.11ac) provides the desired end state to introduce similar, if not identical, techniques and produce the same effect. Although already ratified by the Institute of Electrical and Electronics Engineer (IEEE), the 802.11ac wireless protocol introduces unique challenges to demonstrate proof of concept. The anticipated next generation of wireless technology currently operates on a very limited set of compatible hardware. Further, there is no guarantee that a technical solution that exists within the operational construct of 802.11n wireless protocols provides the same measure of effect with the new 802.11ac wireless protocols. These considerations have potential impacts on the exploratory heuristics associated with achieving alternative communication channels between Phase I and II.

4. A sound technical solution with the demonstrated capacity to achieve a cover channel offers additional tactical options for operators in the network attack and exploitation field. Covert channels augment a critical point of execution. Failure to maintain stealth and persistence leads to discovery, which compromises the attacker’s presence on the machine. The successful implementation of an alternative communication stream provides an extra layer of security for attack and exploitation operators. Furthermore, a successful demonstration of the proof of concept provides both network and attackers and defenders insight to recognize behavioral patterns associated with covert channels.

5. Proposed thesis committee:

a. Dr. Barry Mullins, Thesis advisor \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. Dr. Michael Temple, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c. Dr. Rusty Baldwin, Committee member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Below are the following courses that augment my research:

a. CSCE 560: Introduction to Computer Networking  
 b. CSCE 629: Cyber Attack  
 c. CSCE 725: Reverse Engineering  
 d. CSCE 625: Systems Security Analysis

7. Sponsor: Lemay Center, Maxwell AFB  
 a. Name: Mr. Steven Ellertson

NICHOLAS J. KULESZA, CAPT, USAF  
 GCS-14M

1st Ind, AFIT/ENG

MEMORANDUM FOR AFIT/ENG

I approve/disapprove the above thesis prospectus and thesis committee. The thesis should be prepared in accordance with the AFIT Thesis Guide. Good luck!

JONATHAN BUTTS, MAJ, USAF  
 Chief, Computer Science and Engineering Division  
 Department of Electrical and Computer Engineering