Introduction to HICCS-49
CyberWarfare: Offensive and Defensive Software Technologies Minitrack

Brian Hay
Department of Computer Science
University of Alaska Fairbanks
brian.hay@alaska.edu

Steven LaFountain
Distinguished Academic Chief for Information Assurance and Cyber
National Security Agency
s.lafoun@radium.ncsc.mil

This relatively new minitrack, CyberWarfare: Offensive and Defensive Software Technologies, is intended to bring together technical and non-technical cyberwarfare researchers, academics, and practitioners in related fields to discuss the mechanics and implications of offensive and defensive cyberwarfare activities. While the breadth of this field is extensive, the focus topics for this second offering of this minitrack include offensive and defensive technologies and capabilities, impacts of cyberwarfare, information warfare, collateral damage from related activities, as well as educational, legal, policy and ethical issues associated with the controversial topic.

This year there are four papers and a panel related to this topic that should promote discussion among the participants. In *Strategic Implications of Offense and Defense in Cyberwar,* Wade Huntley from the Naval Postgraduate School applies "Offense-Defense theory" to the domain of international cyber conflicts, and describes the implications that type of analysis has for strategic and tactical decision-making.

In *Defensive Cyber Operations in a Software-Defined Network*, Parker et al discuss the use of capabilities provided by modern SDN-enabled hardware and software to dynamically apply threat-specific responses to potential and actual malicious network traffic.

McDaniel, Nance, and Talvi describe a process in their paper *Mitigating 0-days through Heap Techniques* that can alleviated the impacts of newly discovered vulnerabilities through minor modification to the memory management components of modern operating systems, using Linux as a working example.

Finally, in *Mobile Konami Codes: Analysis of Android Malware Services Utilizing Sensor and Resource-Based State Changes*, Boomgaarden et al, describe how several common Android sandboxes can be fingerprinted, and then describe how they created Android applications to make use of this capability to evade analysis efforts when executed in such sandboxes.

As a relatively new HICSS minitrack, the chairs through it would be appropriate to bring in a panel of experts to discuss some of the issues associated with this important topic. The panel includes Steven LaFountain, Richard M. (Dickie) George, and Victor Piotrowski and is intended to promote discussion and guide the evolution of the minitrack for future years.

Mr. LaFountain is the Distinguished Academic Chief for Information Assurance and Cyber in the Associate Directorate for Education and Training (ADET) at the National Security Agency. Mr. LaFountain will be discussing the new National Centers of Academic Excellence (CAE) in Cyber Operations Program.

Mr. George is currently the Senior Advisor for Cyber Security at the Johns Hopkins University Applied Physics Laboratory where he works on a number of projects in support of the U.S. Government. He is also the APL representative to the I3P, a consortium of universities, national labs, and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States. He will talk about the threat/adversary model, what information is being targeted, and how cyber professionals can address the needs of the nation. The need today has shifted from rocket scientists to cyber warriors. He will go over some of those roles – red team, hunter, malware analyst, reverse engineer, and active defender - with the emphasis on the importance of building the workforce in this important area.

Dr. Victor Piotrowski is a Lead Program Director at the National Science Foundation (NSF) in Arlington, Virginia, where he is responsible for several programs in Cybersecurity. In particular, he oversees the CyberCorps(R): Scholarship for Service (SFS) program and Cybersecurity Education Perspective of the NSF-wide program Secure and Trustworthy Cyberspace (SaTC). He will discuss NSF portfolio related to CyberWarfare and potential funding opportunities in that area.

1530-1605/16 $31.00 © 2016 IEEE
DOI 10.1109/HICSS.2016.687