Towards a Framework for Building Maneuverable Applications

William Clay Moody, Amy W. Apon
Computer Science Division, School of Computing
Clemson University, Clemson, SC
{*wcm,aapon*}*@clemson.edu*

***Abstract*—This paper is an application to the PhD forum of the 2014 IEEE International Parallel & Distributed Processing Symposium (IPDPS) for William Clay Moody, Computer Science PhD candidate at Clemson University. The author is researching cybersecurity of distributed applications and systems through the introduction of the concept of military maneuver. The key attributes of cyberspace maneuver being investigated are in the areas of moving target defense and deceptive defense. Technologies used for these defense mechanisms include software-define-networking, live randomized workload migrations, and honey pot systems. Modeling of the maneuverable systems and stages of cyber attacks use Petri net models.**

***Keywords*-distributed applications, cybersecurity, maneuverability, Hadoop, Software Defined Networking**

I. Statement of Interest

A. Biographical Sketch

I, William Clay Moody, have been a PhD student for the past two years in the Computer Science program in the School of Computing at Clemson University, in Clemson, SC. I began working on my PhD in Computer Science in Fall 2012 and passed the PhD portfolio review in October 2013. I am an Advanced Civil Schooling student on a fully funded fellowship for the United States Army. In the summer of 2015, I will join the faculty of the United States Military Academy (USMA) at West Point, NY in the Electrical Engineering and Computer Science Department (EECS). My advisor is Dr. Amy Apon and I am member of the Big Data Systems Lab. My previous academic experience includes an BS in Computer Engineering from Clemson (1998) and an MS in Computer Networking from North Carolina State University (2009).

I have served in the Army for the past 15 years as Signal (Communications) Officer and as Telecommunications System Engineer. I have led Soldiers providing tactical command and control communications, controlled and managed a signal battalion network on multiple deployments for training exercises, supported a garrison network on one of the largest military installations in the world and been the communications advisor to an Infantry Battalion Commander in the most technologically advanced war fighting unit while deployed to Iraq. In my previous position, I served as an expert in cyber defense operations in support of defining the operational and technical requirements for the acquisition and development of situational awareness and command and control tools for the entire Department of Defense. In each position, I have been recognized for my unmatched technical expertise.

I chose to pursue a teaching position at West Point because of my intrinsic desire to help educate, train, and inspire the future leaders of the United States Army. I knew as a successful Army officer, I could be a positive role model for the Cadets at West Point. It was the honor of a lifetime to be accepted to fulfill one of these much sought after positions at such an distinguished institution.

B. Plans for the Future

Following my PhD studies at Clemson, I will join the faculty of the EECS department at USMA. During my three year assignment to West Point, I strive to develop a parallel and distributed computing curriculum for the undergraduate computer science cadets. Currently, the Army and DoD have a strong interest in high performance computing and a course in this important area will strongly support the objectives and the desires of our military. Furthermore, I desire to continue researching maneuverability in cyberspace. This principle of war is critical to the success of continued dominance in cyberspace for the United States. Following my military career, I desire to stay involved in research that benefits national defense.

C. Current Research Interest

My current research interest are in developing a framework for building maneuverable distributed applications and systems. The DoD defines maneuver as "employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy." There is substantial effort in government, industry, and academia on theoretically extending the concept of maneuver to the cyberspace operational domain, but little research has been conducted to actually design, build, optimize and study maneuverable applications. My PhD research is on focusing increasing the cybersecurity of distributed applications and systems through the introduction of cyber defense maneuver, specifically in the areas of moving target defense and deceptive defense.

D. IPDPS Student Program Participation

My objective for participating in the IPDPS student program is to enhance my research ability and technical knowledge in parallel and distributed computing. As I complete my dissertation, I will need to be exposed to the latest research in the field. The interaction with senior academic and industry leaders will open doors for potential collaboration not only at Clemson but at West Point in the future. Meeting some of the educators from leading universities will help me achieve my goal of establishing a parallel and distributed computing curriculum at USMA. The opportunity to present my research to peers will allow me to get critical feedback into my objectives, techniques, and results. These valuable interactions are not readily available outside of a venue such as IPDPS.

II. Poster Proposal

My poster for IPDPS is entitled "A Framework for Building Maneuverable Applications." I am the lead author with Dr. Amy Apon listed as second author and advisor.

A. Description of Work

The poster describes a framework for adding maneuverability to distributed applications. Apache Hadoop (version 1) is the specific application for the case study of the framework. The framework describes technologies and design considerations to add two aspects of defensive cyber maneuverability to the Hadoop platform. The framework utilizes Petri Net modeling to understand the improved survivability of the parallel and distributed application in the presence of a cyber attack.

The purpose of the framework is proving that applying different technologies can increase the network security and survivability of distributed applications through cyber maneuver. Specifically, I focus on moving target defense and and deceptive defense. Applied technologies include software-defined-networking, live randomized workload migrations, and honey pot systems.

Moving target defense is one of the fundament aspect of cyber maneuver defense [1] in which the targeted system is constantly modified in some manner to improve its defense. These techniques increase the effort and time it takes for an attack to compromise a parallel and distributed system. These increased effort and delay allows network defenders the ability to detect an advisories actions. Software-defined-networking can be used in multiple ways to provide a moving target defense. Randomly morphing internal IP addresses has shown an effective mechanism to protect systems [2]. In our previous work [3], we have shown how random movement of computation and storage nodes of a Hadoop cluster within a shared academic environment can provide semi-persistent parallel and distributed computational platforms. These same techniques can be further used to allow to constantly reorganize the membership of the a cluster to provide a moving target defense.

Deceptive defense is the act of presenting a seemingly vulnerable target for an attacker to compromise while unbeknownst revealing their intentions, techniques, or identities. This is normally done in information systems with the use of a "honeypot". Our work includes a version of a honeypot in which a subset of the systems in a distributed application are not actual computational nodes, but nodes to presenting vulnerable ports and services that attract attackers instead of operational nodes. Along with the moving target defense, nodes constantly transition between the two sets of operational and vulnerable nodes.

B. Abstract of Results

Anticipated results of the poster will include a formalized definition of the framework with its motivation, an update on the status of the technology integration into the Hadoop cluster, and significant findings of the Petri Net models. The models will include the fully operational system with and without added technologies and models for two different cyber attack methodologies. The models will focus on measuring and optimizing the mean time to system compromise, the probability of survive during a cyber attack, and percentage of systems available following a cyber attack. The theoretical models will be a foundation for comparing simulation and testbed results which will be deployed into close network cyber attack ranges at a later stage of the research.

III. Conclusion

This paper has introduced the primary author, William Clay Moody, and current research and work as a PhD student at Clemson University. We have highlighted his military career and goals at the United States Military Academy following his graduate studies. We have introduced research into cyber maneuverability as it applies to the defendability of distributed applications. Finally, we have described a poster to highlight this research as part of the PhD forum at the 2014 IEEE International Parallel & Distributed Processing Symposium (IPDPS).

References

[1] S. Applegate, "The principle of maneuver in cyber operations," in *2012 4th International Conference on Cyber Conflict (CYCON)*, 2012, pp. 1–13.

[2] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, ser. HotSDN '12. New York, NY, USA: ACM, 2012, p. 127132. [Online]. Available: http://doi.acm.org/10.1145/2342441.2342467

[3] W. Moody, L. Ngo, E. Duffy, and A. Apon, "JUMMP: job uninterrupted maneuverable MapReduce platform," *In Proceedings of 2013 IEEE International Conference on Cluster Computing*, Sep. 2013.