JDMS

Editorial

Journal of Defense Modeling and Simulation: Applications, Methodology, Technology
1–2

DOI: 10.1177/1548512911425125
dms.sagepub.com
SAGE

Special Issue on Cyber Defense: Methodologies and Techniques for Evaluation

J Todd McDonald[1] and Eric D Trias[2]

Welcome to this special issue of *Journal of Defense Modeling and Simulation* on 'Cyber Defense: Methodologies and Techniques for Evaluation'. The cyber domain has emerged as a strategic national domain of interest to both military and civilian sectors. The overlap between military and commercial networking resources and infrastructure complicates issues of protection, defense, and offense. The defense community is tasked not only with protecting our military information systems commercially procured, but also in protecting our nation's strategically vital enterprises. Homeland defense rests squarely on our ability to guard critical infrastructure control systems that have a wide range of exploitable vulnerabilities. In this issue we look at several publications that make contributions related to securing the cyber domain: (1) a formal model to capture human behavior in the cyber realm; (2) modeling results that capture efficacy of Global Information Grid awareness through Network Tasking Orders (NTOs); (3) performance modeling for virtual environments that aid in defensive training scenarios; (4) a model for attack analysis on underlying network control protocols; and (5) simulation results comparing centralization methods used in log-based security systems.

Robinson and Cybenko tackle the issue of capturing and analyzing human behavior related to observable actions conducted by users in the cyber domain. Little work has been done in modeling cyber-specific human behavior and their paper presents a novel extension to traditional topic modeling. Using their methodology, more precise data analysis activities may be conducted to extract quantitative information related to cyber security. By translating normal topic models related to document handling, they derive more cyber-appropriate characteristics such as users, sessions, activities, and behaviors. Using weighted probabilities and sampling distributions, appropriate matrices may be derived that are useful for classifying patterns of behavior and probabilistic models for predictive analysis. By analyzing user behaviors in such a way, a key layer of cyber situational awareness is created: changes in historical user behaviors may indicate telltale signs of insider activity or malicious corruption.

Cyber planners and operators, particularly in the DoD, face the problem of how to manage cyber assets to ensure synchronization of efforts and economy of force. Although air planners have longed benefited from the Air Tasking Order (ATO: a daily allocation of air assets to support current mission requirements), the cyber domain has no correlation. Compton *et al*. propose the use of a NTO to help allocate resources in the DoD's Global Information Grid, particularly for mobile assets that are part of highly dynamic network topologies. Although NTOs are not a new concept, Compton and colleagues use the concept to specifically optimize network resources as opposed to using them for supporting air missions themselves (the traditional use to date). By building upon the traditional structure of an ATO, this paper providers a clear translation to cyber-specific tasking and shows how a priori knowledge of network resources may be used in simulations during the NTO planning phase to support Quality of Service goals during execution.

A major area of research within DoD currently revolves around how to defend host machines and network resources themselves. Grimaila et al. compare methods for collecting, logging, and correlating events used for defensive analysis. Centralized logging, the traditional method for event correlation, comes with shortfalls because it does not scale well. Bandwidth and storage tend to be the

[1]School of Computer and Information Sciences, University of South Alabama, Mobile, AL, USA
[2]Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright Patterson AFB, OH, USA

Corresponding author:
J Todd McDonald, School of Computer and Information Sciences, University of South Alabama, Mobile, AL 36688, USA.
Email: jtmcdonald@usouthal.edu

limiting factors as network views become larger. Distributed event correlation, on the other hand may offer greater flexibility by distributing workload around the network. Event correlation itself revolves around identifiable relationships between two or more lower-level actions that occur. Security event log analysis and correlation offers the best approach to understand when intrusions and malicious activity occur. To lend credence to the superiority of decentralized approaches, the paper sets forth a simulation environment that can model effectiveness data collection and correlation activities. Grimaila et al. provide quantitative simulation results using sequences of experimental design where network, software, use cases, performance metrics, and experimental setup are determined beforehand. They present the efficiency results for distributed correlation techniques based on false-positive and false-negative results compared against actual detection rates. They present a compelling argument from the scalability perspective for adopting dynamic/decentralized correlation methods for network defense.

Along the lines of attack analysis, Butts, Rice, and Shenoi consider attacks on protocols where message exchanges are the fundamental process. In their approach, two attack mechanisms derive from an adversary's ability to either fabricate messages or block messages. When such attacks are successful, an adversary may compromise critical cyber infrastructure and take over system operations. A key contribution in this paper is a model to capture protocol operations via process calculi. The model may be exercised to represent message transactions, processes, concurrency, sequential operations, and termination. The paper also presents a nice summary of control protocol classification and the formalisms for modeling such communication paradigms. By extending the paradigm to include adversarial actions and attack vectors, Butts et al. show the fitness for calculi in representing real-world cyber threats in this realm. By using the real-world example of an oil pipe disruption, the paper also shows how the model can be exercised to conceptualize attacks, address weaknesses in protocols, and provide defensive avenues for national infrastructure.

Finally, we round out the special issue with a paper by Stewart, Humphries, and Andel that compares traditional virtualization techniques for representing cyber assets and domains. Such virtualization techniques are in high demand within the DoD so that cyber operators and administrators can train under realistic conditions using realistic attack/defense scenarios. Since duplication is resource prohibitive for such training environments, virtual environments provide the most realistic and cost-effective method in developing training scenarios. This paper provides a comparison of virtualization techniques and makes an argument for hybrid virtualization that combines lightweight and heavyweight techniques in combination. Stewart et al. setup a simulation environment to put different virtual environments under load and evaluate their performance characteristics. Though full virtualization may seem to offer the highest level of configurability for training, they show that hybrid environments offer comparable features with better performance. Based on their results, they show how complex training scenarios are supportable on a single machine such as a simple student laptop. Although more thorough statistical analysis is required for a definitive answer, their simulation results build the argument for utilizing hybrid virtualization for future cyber-warfare training simulation environments.

Acknowledgements

We thank Dr Jerry M Couretas, Ms Vicki Pate, Dr Bert Peterson, and the reviewers for their support during preparation of this special issue.

Author Biographies

J Todd McDonald received his PhD in computer science from Florida State University, Tallahassee, FL, in 2006. He served as an Assistant Professor in the Department of Electrical and Computer Engineering at the Air Force Institute of Technology from 2006 to 2010. In 2011, he joined the School Computer and Information Sciences as an Associate Professor at the University of South Alabama in Mobile, AL. He has published around 25 papers and journals related to software protection, cyber defense, and agent-based security. He is a retired Lieutenant Colonel in the US Air Force and served over 21 years as a communications–information/cyberspace operations officer specializing in cyber systems defense, research, and education. He is a member of the ACM, IEEE, Eta Kappa Nu, Upsilon Pi Epsilon, and a past member of the Military Operations Research Society.

Eric D Trias received his PhD in computer science from the University of New Mexico, Albuquerque, NM, 2008. He has served as an Assistant Professor in the Department of Electrical and Computer Engineering and as part of the Commander's Action Group at the Air Force Institute of Technology from 2007 to 2011. He is an active duty Major in the US Air Force and is currently deployed in support of Operation New Dawn. He has published more than 20 papers and journals related to database and information retrieval, information security, forensics, and cyber defense. He has been active in coaching cyber forensics competition teams and IEEE science fairs and has served in several in several educational outreach efforts. He is a member of the ACM and IEEE.