The Center for Autonomic Computing at Rutgers University

A National Science Foundation Industry/University Cooperative Research Center

http://nsfcac.rutgers.edu

Intrusion Detection – Analysis of Existing and Novel Techniques

Dr. Robert F. Erbacher

Army Research Laboratory (ARL) – Adelphi, MD

Abstract: This talk will discuss Dr. Erbacher's newly initiated research at the Army Research Laboratory related to computer security and areas of potential collaboration. The fundamental goal of the majority of the research revolves around the science of intrusion detection. This research is under the auspices of a larger program, also newly initiated, within ARL at large, on the science of cybersecurity. The goal of the science of intrusion detection research is to develop foundational knowledge that will lead to the development of intrusion detection techniques capable of dealing with real-world cyber security scenarios of the future. Future cyber security scenarios will necessitate moving away from strictly signature and pattern –based detection techniques. Dr. Erbacher has broad interests in this arena and is specifically interested in building collaboration activities and expanding ARL's research capabilities in the cyber security domain. Internally, specific projects Dr. Erbacher is working on include:

- Applicability, Impact, and Implications of Ensemble Techniques. Traditionally, anomaly detection techniques have fared poorly when evaluated. Given the need to move away from strictly signature and pattern –based techniques, we must understand why these techniques have performed so poorly. The goal is to determine how to develop anomaly-based techniques which will perform acceptably. To this end, our goal is to identify specifically what different techniques work well at and what they don't. Techniques will then be used together in an ensemble.
- Fundamentals of Visualization for Cyber Security. This project currently has two goals. First, with the extensive development of visualization techniques for cyber security why is there a severe lack of techniques actually deployed. More importantly, what are the requirements for ensuring such techniques are deployed and employed by analysts? The second goal is the design of novel techniques meeting these requirements.
- Novel Models for Cyber Security. The goal of this research is to explore models for the representation and modeling of cyber security and intrusion detection. This is akin to the developed models associating game theory to cyber security.
- Digital Forensics. The goal here is to develop techniques to aid in the identification, analysis, and legal admissibility of digital evidence. This type of evidence is usually obfuscated; thus we must assume we are being countered by anti-forensics techniques. Thus, techniques are needed to aid identification and analysis of obfuscated and outright hidden evidence. This need is applicable to both network traffic data as well as computer host-based data
- Automated Alert Correlation and Report Generation. This research consists of two phases. First, is to identify multiple alerts associated with a single event and correlate these alerts. Multiple alerts is indicative of the sophisticated persistent threats that are the primary concern to analysts. The second phase is to automatically generate reports for the naïve attacks such that the analysts are able to focus more attention on the sophisticated persistent threats.

Bio: Dr. Erbacher is currently performing computer security research at the Army Research Laboratory (ARL) in Adelphi, MD. Before joining ARL he was a senior principal scientist with the Northwest Security Institute (NWSI), a non-profit research organization based in Redmond, WA. Prior to joining NWSI, Dr. Erbacher was an Assistant Professor in the Department of Computer Science at Utah State University. Dr. Erbacher is an Associate Editor for the Journal of Electronic Imaging, Chaired the SPIE Conference on Visualization and Data Analysis for 13 years, is currently a steering committee member for the SPIE Conference on Visualization and Data Analysis, was general chair of the past two Workshops on Systematic Approaches to Digital Forensics Engineering and is now on the steering committee. He is also on numerous other program committees related to digital forensics, computer security, and visualization and performs extensive reviewing for conferences and journals in these areas. In keeping with his research interests in computer security and visualization Dr. Erbacher spent the summers of 2004 through 2006 at AFRL's Rome Labs developing visualization for intrusion detection techniques for the air force under their summer faculty fellowship program. Dr. Erbacher received his BS in Computer Science from the University of Lowell in 1991 and his MS and ScD degrees in Computer Science from the University of Massachusetts-Lowell in 1993 and 1998, respectively.

Friday, September 23, 2011, 10:00 AM
Place: Room 538, CoRE Bldg.
Busch Campus • Piscataway, NJ