Workshop on Research for Insider Threat
WRIT 2013

Workshop Introduction

Welcome to the 2013 Workshop on Research for Insider Threat, part of the IEEE Symposium on Security and Privacy Workshops. We are pleased to present the program for this year's workshop, which includes a broad spectrum of approaches towards the advancement of research in this critical area of information systems security. In only our second year, the workshop received 24 paper submissions, accepting 9 to be included in the event for an acceptance rate of 37.5%.

We organized the papers into three general categories: detection at the host, network and policy, and behavioral science and data. In the first group, we see an approach detailing how to detect behavioral inconsistencies in users across multiple information domains. Another paper explores system-level events to determine if a specific biometric signature of user behavior can be obtained. The third paper in this group applies several novel techniques to a large data set of observable user behaviors to detect anomalies and potential suspicious behavior.

The second group of papers, network and policy, includes an interesting approach for computing systems to covertly report suspicious behavior without user knowledge. We also include a paper that uses graphs to compare authentication activity between administrative and non-privileged users. A third paper proposes an approach that invalidates policies to identify potential insider threat attack paths.

The third group of papers, behavioral science and data, explores the human element of insider threat research, as well as generating data to represent user behavior. The first paper proposes a Bayesian-network model for identifying psychological predictors of insider risk. A second paper demonstrates a linguistic approach for identifying anomalies in user populations, as well as a method for measuring the impact of such tools in operational environments. The third paper outlines development of techniques for generating synthetic user data for use in insider threat research.

Overall, we have a very strong program this year, and are pleased to welcome authors and participants alike. Discussion is expected to be spirited and intense. In the end, we hope this workshop opens new doors for insider threat researchers, serves as a springboard for new ideas, and enables highly effective detection methods to combat this serious threat to information security.

Warmest regards,

Bill Claycomb **Frank Stajano**

2013 WRIT Program Committee Chairs