Inside the Insider Threat (Introduction)

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA, USA
mabishop@ucdavis.edu

Kara Nance
Department of Computer Science
University of Alaska Fairbanks
Fairbanks, AK, USA
klnance@alaska.edu

William Claycomb
Software Engineering Institute
Carnegie Mellon University
Pittsburgh. PA, USA
claycomb@cert.org

The insider problem is one of the most important problems in computer security, and indeed in all aspects of real-world security. Insiders have compromised many key societal systems and processes in domains such as government, finance, and even science. Many reports of insider attacks describe people trusted with access to sensitive information abusing that access to damage that information, compromise the privacy of that information, and collaborate with others (sometimes other insiders) to cause various kinds of failures, losses and serious harm. Indeed, the insider problem is also pernicious in the non-computer world; as the ancient Roman satirist Juvenal said, "Who will guard the guards themselves?" Any approaches therefore must have not only a technical aspect, but also a non-technical (social, political, legal, cultural, and so forth) approach. Insider attacks may be accidental or arise from conflicting policies that confuse the putative attacker. These unintentional insider attacks are as dangerous as deliberate insider attacks, but must be handled differently due to the lack of maliciousness. Understanding how to cope with unintentional insider attacks effectively is also a complex, difficult problem.

Analyzing and detecting insider threats involve both technical and non-technical approaches across many different disciplines, including human-oriented ones. This mini-track solicited papers emphasizing this cross-cutting work as well as papers that present case studies and experiences in coping with insider attacks or preventing them.

In their contribution *Demistifying Insider Threat: Language-Action Cues in Group Dynamics*, Shyuyan Mary Ho, Jeffrey Hancock, Cheryl Booth, Mike Burmeister, Xiuwen Lou, and Shashanka Timmarajus study the problem of detecting changes in the behavior of an online collaborator when that collaborator becomes deceptive. They hypothesize that after a successful insider attack, language-action cues will change significantly. They support their hypothesis with data gathered from an online game, and note that their work suggests it is feasible to develop a computational model of online deception to automate detection of some insider attacks.

The second paper, *Explaining and Aggregating Anomalies to Detect Insider Threats* by Henry Goldberg, Will Young, Alex Memory, and Ted Senator, examine the problem of analyzing alerts produced by an anomaly-based intrusion detection system. A perennial problem is to distinguish alerts triggered by unusual but legitimate activity from those that indicate some sort of insider activity. The authors examine these alerts, and provide more contextual information than is usual to help the human analysts distinguish between the unusual but legitimate and the unusual due to illegitimate use. They also aggregate anomalous user-days by users to identify insider actions.

In the paper *Reducing the Data Exfiltration Surface for the Insider Threat*, Bob Schlicher, Lawrance MacIntyre, and Robert Abercrombie tackle the increasingly prominent problem of data exfiltration. They define a ``data exfiltration surface'' analogous to an attack surface, but focusing on the removal of data from a network. They then present the Data Diode software and an architecture that uses it to reduce this surface, thus minimizing the avenues offered for data exfiltration by an insider.

These papers examine three very different aspects of the insider problem. Each focuses on both the technology and the people who use the technology. Two develop methods to detect insiders, one by examining the language and behavior of users and the other by looking at the context in which users trigger intrusion detection alerts. The third focuses on prevention, reducing the ways an inside attacker can send private data out of the organization. Their contributions advance the study of this critical, complex problem.