

Workshop on Insider Threats

Call for Papers

When equipped with insider knowledge, an attacker is a particular risk to an organization: they may know the policies and security measures of an organization and devise ways to subvert them. Such attackers can have a variety of motives and triggers that cause them to act against the organization's interests. Further, the mechanisms these attackers can use can range from unsophisticated abuses of their own authority to elaborate techniques to acquire unauthorized access. The duration of the attacks may be short or longer-term. Finally, the goal from these attacks can be simple exfiltration of information or even direct sabotage.

The Insider Threat has been identified as a hard, but important, computer security problem. This workshop broadly calls for novel research in the defense against insider threats. Relevant research may leverage operating systems, communication networking, data mining, social networking, or theoretical techniques to inform or create systems capable of detecting malicious parties. Cross-disciplinary work is encouraged but such work should contain a significant technical computer security contribution. Research in non-traditional systems, such as smart spaces, is encouraged as well as enterprise systems. Finally, while we discourage exploits of limited scope, we solicit generalized techniques that help an inside attacker evade modern defensive techniques.

Topics of interest include but are not limited to:

- Novel data collection of threat indicators,
- Detection of triggers and behavior modeling associated with insider threat development,
- Detection of malicious users acting within their own authority against organizational interests,
- Detection of unauthorized escalation of rights,
- Covert exfiltration of data and approaches to thwart such techniques,
- Automatic detection of high-value digital assets,
- Techniques to minimize false positives in insider threat detection,
- Advances in access control, data compartmentalization or administration of compartments,
- Detection techniques for resource constrained clients (limited processor, bandwidth, or battery capacity),
- Data and digital asset tracking, and
- Techniques to provide near real-time forensics.

Important Dates

All deadlines are firm due to publisher time constraints

- Paper Submission Due: June 28, 2010
- Acceptance Notification: August 6, 2010
- Camera-ready Due: August 16, 2010
- Workshop: October 8, 2010

Paper Format

Submissions must be at most 8 pages in double-column ACM format (note: pages must be numbered), excluding the bibliography and well-marked appendices and at most 10 pages overall. Committee members are not required to read appendices, so the paper should be intelligible without them. Submissions are not required to be anonymized. Only PDF files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. The authors of accepted papers must guarantee that their paper will be presented at the workshop. Accepted papers will be published by the ACM in a conference proceedings.

Paper Submission

All submissions are made through the Easy Chair Website: <http://www.easychair.org/conferences/?conf=wits20100>