2018 IEEE Symposium on Security and Privacy
Workshop on Research for Insider Threat

May 24, 2018
Hyatt Regency, San Francisco, CA USA

https://www.ieee-security.org/TC/SPW2018/WRIT/

Call for Papers

The threat of malicious insiders to organizational security has historically been one of the most difficult challenges to address. Insiders often attack using authorized access and with behavior very difficult to distinguish from normal activities. Today, insider attacks are further enabled by immense data storage capabilities, advanced searching algorithms, and the difficulty of comprehensive monitoring of networked systems. Because the actions that occur during insider attacks look much like normal user activities, this exacerbates the technical challenges of proposed solutions to reduce the high incidence of false positives. Furthermore, several recent high-profile attacks have been enabled by non-malicious, or unintentional, insiders fooled by exploits from external attackers.

The insider threat problem continues to receive attention from government agencies. Executive Order 13587 requires all US Government agencies handling classified information to implement insider threat programs to protect sensitive information, leading to a greatly increased interest among US Government agencies in advances in detection of insider threats. Additionally, upcoming changes to the NISP Operating Manual (**NISPOM,** DoD 5220.22-M) will require insider threat programs for potentially tens of thousands of defense contractors. In recent years, DARPA sponsored two programs (CINDER and ADAMS) aimed at Insider Threat challenges, and there is currently an insider threat program sponsored by IARPA, called Scientific advances to Continuous Insider Threat Evaluation (SCITE), supporting new research using active indicators to identify malicious insiders and development of inference enterprise modeling solutions to support insider threat assessment. Technical solutions are emerging, but there are still significant challenges:

- Data on insider attacks are difficult to obtain. One reason is that the rate of insider attacks is relatively unknown. Organizations suffering insider attacks are often reluctant to share data about those attacks publicly. Studies show over 70% of attacks are not reported externally, including many of the most common, low-level attacks. This leads to uncertainty that available data accurately represents the true nature of the problem. Furthermore, the behaviors of non-malicious users are also not available in large data sets. The ability to gather data that has external

validity is also hampered by the fact that research projects do not have access to actual insiders who are in engaged in committing insider exploits. While some data collection projects attempt to approximate insider threats through role-playing, this does not fully address the need for externally valid data that reflects the actions and motivations of true insider threats. However, researchers are beginning to make advances in this area, establishing productive partnerships with industry and government collaborators that allow data access while protecting the confidentiality and privacy of individual users. We hope to highlight these successful endeavors as examples for other areas of security and privacy research where data sharing limits meaningful advances.

- The insider threat problem is not well understood. In addition to the complex challenges surrounding collection, correlation, and detection of technical indicators, researchers must also understand underlying human motivations and behaviors. This is not a traditional area of study for IT security researchers; configuring technical solutions to monitor for human deception is challenging. However, ongoing work across several programs has shown significant advancements in this area as well.
- Another significant aspect to consider is privacy and security of users and data. Advanced insider threat detection programs often aggregate data from multiple sources, including sensitive personal information such as HR data, pre-employment screening or background checks, confidential communication, or self-reported issues such as substance abuse or severe financial difficulties. Protecting this data from theft or misuse is paramount to maintaining a credible and effective insider threat program, and new research directions should be highlighted to address this critical concern.

WRIT will focus on research that proposes solutions to the above challenges from diverse viewpoints, such as innovative approaches that integrate concepts from information technology, behavioral sciences, or criminology, as well as research that advances the state of art and practice in experimental methods for collecting data that addresses key challenges in evaluating and validating proposed models and solutions. The workshop will therefore be accessible to both non-experts interested in learning about this area and experts interesting in hearing about approaches being taken by others.

Topics of interest include but are not limited to:

- insider threat indicator development
- data collection, aggregation, and correlation for threat indicators
- data collection of baseline user data and behaviors
- analytic approaches that address key challenges such as reducing false positives
- novel techniques/new technologies for prevention, detection, and response to insider attacks
- predictive analytics for identifying potential indicators of insider threat
- linguistic approaches to identifying potential behavior of concern
- insider attacker behavioral models and analysis
- adversarial and game theoretic models of insider threats and attacks
- evaluation, experimentation and risk assessment of insider threat detection approaches
- mobile devices and insider threats
- social networking and insider threats
- identifying unknown insider attack patterns
- sociotechnical approaches to protecting against insider threat attacks
- biometric approaches for identifying potential insider threat behavior.
- application of solutions from other domains to address insider threats
- unintentional insider threats
- research directions addressing privacy and security

Paper Submission

You can submit your papers at: https://easychair.org/conferences/conference_dir.cgi?a=16542465. All submissions must be original work; the submitter must clearly document any overlap with previously published or simultaneously submitted papers from any of the authors. Failure to point out and explain overlap will be grounds for rejection. Simultaneous submission of the same paper to another venue with proceedings or a journal is not allowed and will be grounds for automatic rejection. Contact the program committee chairs if there are questions about this policy.

Authors are encouraged to use the IEEE conference proceedings templates. Papers must not exceed 10 pages total (including the references and appendices). If not using the IEEE template, papers must be formatted for US letter (not A4) size paper. The text must be formatted in a two-column layout, with columns no more than 9.25 in. high and 3.5 in. wide. The text must be in Times font, 10-point or larger, with 11-point or larger line spacing. Authors are encouraged to use the IEEE conference proceedings templates. Failure to adhere to the page limit and formatting requirements will be grounds for rejection.

Papers accepted by the workshop will be published in the *Conference Proceedings* published by IEEE Computer Society Press. The Workshop will use EasyChair for all submissions.

Important Dates

Paper Submission Due: January 10, 2018
Acceptance Notification: February 15, 2018
Camera Ready Version Due: March 1, 2018
Workshop: May 24, 2018

Program Chairs

Chair: Dr. Frank L. Greitzer, PsyberAnalytix, Frank@PsyberAnalytix.com
Chair: Dr. William R. Claycomb, claycomb@cert.org

Program Committee:

Chair: Frank Greitzer, PsyberAnalytix **Co-Chair**: William Claycomb, CMU/CERT Elshan Akhadov, Los Alamos National Laboratory Elise Axelrad, Innovative Decisions, Inc. Matt Bishop, University of California at Davis Sadie Creese, University of Oxford Zheng Dong, Microsoft Corporation Carrie Gates, Securelytix Michael Goldsmith, University of Oxford James Joshi, University of Pittsburgh Florian Kammueller, Middlesex University	Sjouke Mauw, University of Luxembourg Roy Maxion, Carnegie Mellon University Christine Noonan, Pacific Northwest National Laboratory Christian W. Probst, Technical University of Denmark Sal Stolfo, Columbia University William Streilein, MIT Hassan Takabi, University of North Texas Ilsun You, Korean Bible University Allison Watkins, University of South Florida St. Petersburg Shannon Wasko, Johns Hopkins Applied Physics Lab