Introduction to the Special Issue on Insider Threats

One of humanity’s most perplexing and persistent security risks is the threat of harm from those we trust. Various descriptions and definitions of this insider threat have been offered. The US Cybersecurity & Infrastructure Security Agency (CISA) defines insider threat as “the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department’s mission, resources, personnel, facilities, information, equipment, networks, or systems.” The CERT National Insider Threat Center defines it as “the potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.” The various definitions differ slightly in specifying who an insider is, what actions are of concern, and why the individual took those actions. To some extent, the functional definition of insider threat may be unique to a particular context, such as with respect to the organization’s mission, or focusing on a particular type of crime.

Simply stated, we can describe the insider threat most generally as “the risk of misuse of trust to cause harm.” This removes qualifications about who is the insider and what trust was violated through what means. Encompassed within this broad definition is the current or former employee, trusted business partner, or even a piece of poorly written or exploited software or a malfunctioning server; this description also acknowledges the insider threat risk posed by a regular customer with access to a company’s web portal. Most importantly, this definition of insider threat focuses on trust in people and in systems and includes impacts such as physical damage to assets, reputational harm, financial loss, and injuries to people.

As Zimmer, Burkert and Federrath point out in their article, “Insiders Dissected—New Foundations and a Systematisation of the Research on Insiders,” in order to establish a rigorous, functional definition of insider threat, it is necessary to more clearly specify the nature of insiders. Their article addresses this need by systematically breaking down the concept of insider, with a careful discussion of defining characteristics of insiders and the relationships among these constructs. The resultant taxonomy of insiders represents a major contribution that may be applied to further inform not only the definition of insider threat used in research and practice, but also to inform and facilitate a more systematic representation of insiders in current insider threat knowledge bases, taxonomies, and ontologies.

Research on detection, deterrence, and mitigation of insider threat risk generally falls into several focus areas. The first area focuses on the “who” and “what.” That is, identifying the entities that have access to an organization, and what assets they have access to. A second area focuses more on the question of “why?” This includes social and behavioral science research that explores the motivations and underlying psychological aspects of insiders. A third focus area considers “how” insiders attack, including the mechanisms, capabilities, and pathways insiders might utilize in an effort to cause harm, and how an organization can mitigate and minimize those opportunities. While each focus area is interesting on its own, very exciting results emerge when the three areas overlap. For example, consider the differences in how a behavioral scientist and a computer scientist might approach the insider threat problem. With the behavioral scientist’s interest on individual

ACM Reference format:
Bill Claycomb, Frank Greitzer, Stephanie L. Jaros, and Carrie Gardner. 2022. Introduction to the Special Issue on Insider Threats. Digit. Threat.: Res. Pract. 3, 1, Article 1 (January 2022), 3 pages.
https://doi.org/10.1145/3477501

© 2022 Copyright held by the owner/author(s).
2576-5337/2022/01-ART1
https://doi.org/10.1145/3477501
motivations to do harm, the challenge is to observe meaningful indicators of these motivations prior to the attack. On the other hand, the computer scientist may focus more on detecting misuse of IT systems or other physical assets; here, solutions are sought to either prevent that misuse or to enable early warning systems that mitigate the risk. Significantly, the merging of behavioral science and computer science approaches offers important advantages: technical observables from IT systems can be used to identify behavioral risks (e.g., a person’s email communication shows signs of extreme disgruntlement or stress); behavioral observables can be used to identify and prevent potential technical (or physical) risks, such as by suspending certain privileges (e.g., handling nuclear material, flying airplanes) when extreme individual stressors are detected.

A major challenge facing the development of insider threat detection systems is a lack of empirical data with ground truth, which is necessary to evaluate and validate threat models. An article by Williams, Abbott, Shoman, and Charlton demonstrates how actual data collected in a nuclear facility over nearly a twelve-month period, comprising tens of thousands of access control data points and thousands of intrusion sensor data points, could be used to recognize operational patterns of behavior and detect off-normal behaviors of concern. In their paper, “Results from Invoking Artificial Neural Networks to Measure Insider Threat Detection & Mitigation” Williams, Abbott, Shoman, and Charlton describe the use of artificial neural networks to analyze patterns of behavior rather than individual observables. Data that are already accessible in nuclear facilities—such as access control data, intrusions sensor data, camera video, area radiation monitoring data, personal radiation monitoring data, and material control data—are analyzed to detect deviations from “normal” patterns to reveal unwanted behaviors, including possible malicious insider acts.

Unfortunately, it is not always possible to rely on real-world, operational data with ground truth. Even when real-world data are available, ground truth may be lacking to protect personally identifiable information. For example, organizations might anonymize personal information or completely redact this information: this restricts the availability of distributional statistics, such as means, marginal distributions, and correlations, which are necessary to evaluate proposed threat models. In that case, researchers need to be able to recover some of the individual distinctions from these aggregated data, and/or to reliably simulate organizational behavior given certain technical controls. This approach to inference enterprise modeling enables the use of powerful statistical modeling methods to evaluate and measure confidence in model outputs. The article by Sticha, Diaz, Axelrad, Vermilion, and Buede entitled “Simulating Organizational Data from Redacted Input for Inference Enterprise Modeling” provides a fascinating look at a novel way to approach that problem.

Another approach to addressing the lack of ground truth data, as well as the challenge of detecting potentially malicious activity in near-real-time, is described in the article by Zheng, Yuan, and Wu, titled “Using Dirichlet Marked Hawkes Processes for Insider Threat Detection.” In a novel approach utilizing advanced statistical models, the authors propose a solution that addresses the dearth of ground-truth data and the challenge of real-time threat detection. The paper also demonstrates how the analytic techniques can derive likelihood estimates of combinations of indicators in terms of activity type and time, with the resulting improvement in accuracy of risk assessment that comes with combining insider threat indicators. Importantly, since the latter approach of using sophisticated modeling methods to detect combinations of indicators applies to the analysis of behavioral as well as technical data, the methods and findings of studies in one focus area can be generalized for use by multidisciplinary approaches.

In summary, the articles in this special issue on insider threats offer a broad range of studies across several disciplines and applications of insider threat research that hold promise for advancing research on insider threat detection and mitigation. We believe that these papers will be of interest to researchers and practitioners by informing approaches for enhancing insider risk mitigation programs or by providing inspiration for the next round of innovative insider threat research. We would like to thank all the authors who submitted papers for
consideration, as well as the Editors of the ACM Journal of Digital Threats: Research and Practice for the opportunity to share the research results represented in these articles with the broader research community.

Bill Claycomb
Frank Greitzer
Stephanie L. Jaros
Carrie Gardner

Guest Editors