Guest Editors' Introduction

Addressing the Insider Threat

As users, managers, researchers, or administrators, we often worry about outsiders attacking our systems and networks, breaking through the perimeter defenses we have established to keep out bad actors. But we must also worry about the *insider threat*—people with legitimate access who behave in ways that put our data, our systems, our organizations, and even our businesses' viability at risk. Such behavior might not be malicious; it might be well-intended but still have unwelcome consequences.

Shari Lawrence Pfleeger
RAND Corporation

Salvatore J. Stolfo
Columbia University

Considerable research has been done to examine the nature of inappropriate insider activity, with the goal that eventually organizations can reduce the threat. Beginning in 1999, RAND conducted a series of workshops to generate a research agenda for addressing this problem.[1–3] In parallel, the US Department of Defense (DoD) outlined a set of policy changes and research directions for reducing the insider threat.[4] And the Software Engineering Institute's Computer Emergency Response Team (CERT) has been working with the US Secret Service to understand convicted insiders' motivations.[5] From these and other efforts, a rich literature illuminating various aspects of the insider threat problem is emerging.

The Scope of the Insider Threat

But how real is the insider threat? Many recent anecdotes about cybercrime suggest that often the threat to an organization's computer-based assets is greater from those within the organization than from without. In a 2007 Computer Security Institute survey about computer crime and security,[6] 59 percent of respondents thought they had experienced insider abuse of network resources. About one in four respondents said that more than 40 percent of their total financial losses from cyber attack were due to insider activities. However, the 2008 survey had significantly different results:

> As noted in last year's report, a great deal is made of the insider threat, particularly by vendors selling solutions to stop insider security infractions. It's certainly true that some insiders are particularly well-placed to do enormous damage to an organization, but this survey's respondents seem to indicate that talk of the prevalence of insider criminals may be overblown. On the other hand, we're speaking here of financial losses to the organization, and in many cases significant insider crimes, such as leaking customer data, may not be detected by the victimized organization and no direct costs may be associated with the theft.[7]

Credible data describing the scope and impact of unwelcome insider actions are hard to come by, for two reasons. First, many organizations are loathe to reveal the nature and magnitude of the cyber incidents they've experienced for fear of reputational harm. Second, most cyber surveys are convenience surveys; it's impossible to know what population the results represent. This paucity of data is challenging for insider threat researchers, who need good data with which to build models, make predictions, and support good decision-making. The large-scale, carefully sampled National

Computer Security Survey[8] suggests that the threat is real and the consequences significant:

- Forty percent of all incidents reported by the 7,818 respondents (representing 36,000 US businesses) were attributed to insiders.
- Seventy-four percent of all cyber theft was attributed to insiders, including 93 percent of embezzlement incidents and 84 percent of intellectual property thefts.

For the past few years, the Institute for Information Infrastructure Protection (I3P) at Dartmouth College (with funds from the US Department of Homeland Security) has supported a project exploring ways to understand and address the insider threat. With researchers at Columbia University, Cornell University, Dartmouth College, MITRE, Indiana University, Purdue University, and RAND, we've examined not only how technology can reveal the threat's nature and magnitude, but also how it's influenced by the environment in which the insiders operate. The overall goal is to suggest appropriate responses to the insider threat; after all, the response to an insider accidentally selecting the wrong menu entry should be different from the response to an ex-employee trying to exact revenge.

In our project's early days, it became clear that many ideas exist about what "insider" means and what unwelcome behavior constitutes an "insider threat." For example, insiders are more than just employees or ex-employees—they can be business partners, auditors, consultants, or other people and systems who receive short- or long-term access to an organization's systems. Without a unifying framework, we have difficulty recognizing emerging insider problems, comparing incidents, or dealing with them appropriately. For this reason, Joel Predd, Shari Lawrence Pfleeger, Jeffrey Hunker and Carla Bulford[9] developed a taxonomy of insiders and their actions, which Figure 1 shows. The taxonomy doesn't prescribe a uniform definition; rather, it provides a consistent vocabulary for describing clearly which aspects of the insider threat problem the research and practice address. It also provides the basis for discussing, comparing, and contrasting the various possible responses to different kinds of insider behaviors. The framework takes into account the roles of the organization, the individual, the IT system, and the environment in enabling unwelcome behavior.

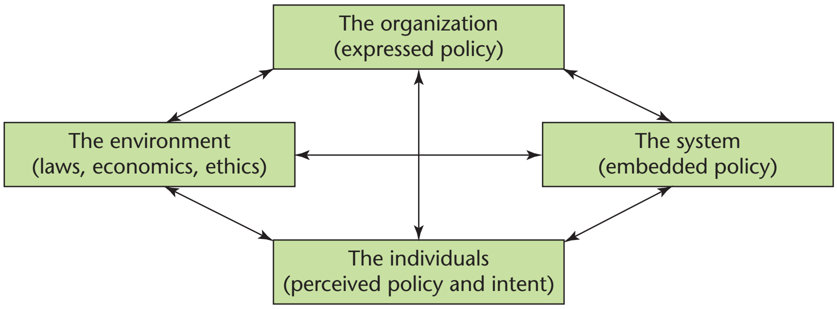

Figure 1. Framework for taxonomy of insiders and their actions. This taxonomy provides a consistent vocabulary for describing which aspects of the insider threat are being addressed, and takes into account the roles of organizations, individuals, IT systems, and the environment in enabling insider threat behavior.[9]

Because not all insiders are alike, we must distinguish among the different types of insider threat, differentiate problems we can address from those we can't, and determine the roles technology and policy play in crafting responses. Policy is a particularly thorny issue because the stated policy (called the *de jure* policy in the taxonomy) isn't always the same as its interpretation and enforcement (the *de facto* policy). For example, most organizations forbid the use of their computer systems for personal use: the *de jure* policy. But in actuality, most organizations look the other way for some personal uses: the *de facto* policy. Sometimes, the *de facto* policy is stronger than the *de jure*, as when a security guard challenges a worker in the office at 2 a.m., even though the worker is wearing a proper badge.

Promising Insider Research

In this special issue on addressing insider threats, articles by three different research groups illustrate how technology and policy can inform both our understanding of the insider threat and how to respond appropriately to its effects. In "Detecting Insider Theft of Trade Secrets," Deanna D. Caputo, Marcus A. Maloof, and Greg D. Stephens describe how they used their Elicit system to observe the relationship between insider intent and action. Their approach is based on technology that looks for violations of *de jure* policy, and they perform a carefully designed experiment to see whether malicious insiders have different behaviors from innocent users. Their research is important not only for illuminating the nature of malicious behavior but also for illustrating how to perform high-quality empirical cybersecurity research.

In "Designing Host and Network Sensors to Mitigate the Insider Threat," Brian M. Bowen and his colleagues at Columbia University also investigate real users' insider behavior. Based more on *de facto* policy, the collection

Table 1. Applying a framework for responding to insider threats.

	ORGANIZATION: NO EXPRESSED POLICY	SYSTEM: NO EMBEDDED POLICY	INDIVIDUAL: NO MALICIOUS INTENT	ENVIRONMENT: LAWS, ETHICS APPLY
Detection		Embedded decoys; watchful monitoring		
Prevention	Create organizational policy	Embed organizational policy	User training, incentives, reminders, access control	Remind users of legal implications of their actions and of costs to organization
Mitigation	Update related policies			
Punishment				Apply legal punishments
Remediation	Update related policies			

of detectors acquires online event data created by computer systems and applications while insiders (users who misused privileges) or masqueraders were impersonating a user whose credentials they stole. The authors use the descriptive and behavioral data that their system captures with machine learning algorithms to identify and model abnormal search events. Then, they augment this information, describing how users actually behave, with strategically placed decoys that report to a central location when documents and data are misused. The Columbia researchers' goal is to understand unusual behavior and misuse of decoy information so that systems can reliably detect insider attack.

The MITRE and Columbia articles offer different but mutually supportive views of modeling insider behavior. MITRE approaches the problem by specifying up front what are considered to be *de jure* policy violations as defined by subject matter experts. By contrast, the Columbia work proposes technology to identify unusual or bad behavior by learning over time about normal and abnormal use. Both articles present technology to provide insight into insider threats and to address the dearth of study data available by generating some of their own. In each case, their rich data sets have information not only about observed behaviors but also about the context in which the behaviors occurred. Each article provides a roadmap for generating data to test and evaluate proposed technology solutions.

Such data sets can support the kind of modeling used in the third article. In "Building a System for Insider Security," Felicia Durán and her colleagues at Sandia National Laboratories use technology to model outcomes. Representing the employee life cycle with a system dynamics model, they analyze employee interactions with insider security protection strategies. Using a scenario involving prehiring screening and security clearance processes, they assess important interactions, interdependencies, and gaps in insider protection strategies; the results should lead to a more effective set of responses to the insider threat.

Indeed, the goal of much insider threat research is to make more effective the prevention, detection, mitigation, remediation, and punishment of unwelcome action by the people and systems that have legitimate access to our networks. It's not enough to expect technology to prevent insider misdeeds. Instead, we need a multifaceted set of strategies that address all elements of the taxonomy: the organization (including its culture and goals), the system (including the completeness and correctness of its implementation of *de jure* policy and its ability to learn *de facto* behavior), the environment (including legal restrictions on monitoring and analysis), and the individual (including motivation and intent). Table 1 illustrates how the taxonomy, coupled with goals of prevention, detection, mitigation, remediation, and punishment, can suggest sensible and effective response options.

As technologists, we often hope to use our skills to monitor behavior and predict the new threats our systems will face. But the dynamic threat environment, coupled with continuing technological advancement, make it impossible to predict with certainty what our systems will look like and what features and functions they'll provide. That same uncertainty makes it difficult to predict what insiders will do and when and how they'll do it. However, the substantial literature on "workplace deviance"[10] tells us with certainty that insiders will continue to behave badly, using our computer systems as a means or as a target. Thus, insider threat detection and mitigation will continue to be a vexing and persistent security—and very human—problem. □

Acknowledgments

This material is based on work supported by the US Department of Homeland Security under grant award numbers 2006-CS-001-00000 and 2006-CS-001-000001-02 and the Army Research Office under grant ARO DA W911NF-06-10151. The views and conclusions contained in

this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the US Department of Homeland Security or the Army Research Office.

References

1. R.H. Anderson, *Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: Results of a Three-Day Workshop*, research report RAND CF-151-OSD, RAND Corp., 1999.
2. R.H. Anderson et al., *Research on Mitigating the Insider Threat to Information Systems #2, Proc. Workshop Held August 2000*, research report RAND CF-163-DARPA, RAND Corp., 2000.
3. R.C Brackney and R.H. Anderson, *Understanding the Insider Threat: Proceedings of a March 2004 Workshop*, research report RAND CF-196-ARDA, RAND Corp., 2004.
4. *Final Report of the Insider Threat Integrated Process Team*, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), US Dept. Defense, 24 Apr. 2000.
5. M. Keeney et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," US Secret Service and CERT Coordination Center/SEI, May 2005.
6. R. Richardson, "2007 Computer Crime and Security Survey," Computer Security Inst., 2007, pp. 12–13, 15; http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.
7. R. Richardson, "2008 CSI Computer Crime and Security Survey," Computer Security Inst., 2008; www.gocsi.com/forms/csi_survey.jhtml.
8. R. Rantala, *Cybercrime against Businesses, 2005*, special report NCJ221943, US Bureau of Justice Statistics, Sept. 2008; www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf.
9. J. Predd et al., "Insiders Behaving Badly," *IEEE Security and Privacy*, vol. 6, no. 4, 2008, pp. 66–70.
10. S.L. Robinson and J. Greenberg, "Employees Behaving Badly: Dimensions, Determinants, and Dilemmas in the Study of Workplace Deviance," *Trends in Organizational Behavior*, C.L. Cooper and D.M. Rousseau, eds., vol. 5, Wiley, 1998, pp. 1–30.

__Shari Lawrence Pfleeger__ is a senior information scientist at the RAND Corporation. Her research interests include software engineering, cybersecurity, and risk management. Pfleeger has a PhD in information technology and engineering from George Mason University. Contact her at pfleeger@rand.org.

__Salvatore J. Stolfo__ is a professor of computer science at Columbia University. His research interests include computer security, intrusion detection, machine learning, and parallel computing. Stolfo has a PhD in computer science from New York University's Courant Institute. Contact him at sal@cs.columbia.edu.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*

computing now
ACCESS | DISCOVER | ENGAGE
Let us bring technology news to you.
http://computingnow.computer.org
Subscribe to our daily newsfeed