

The Cyber Enemy Within ...

Countering the Threat from Malicious Insiders

Panel Moderator:

*Dick Brackney,
Advanced Research and Development Activity*

Panelists:

*Terrance Goan, Stottler, Henke Associates
Shambhu Upadhyaya, University of Buffalo
Allen Ott, Lockheed Martin, Orincon Information Assurance*

Panel Theme

One of the most critical problems facing the information security community is the threat of a malicious insider abusing his computer privileges to modify, remove, or prevent access to an organization's data. An insider is considered *trusted* (at least implicitly) by his organization because he is granted access to its computing environment. Whether or not that insider is in fact *trustworthy* is a question that lies at the heart of the insider threat problem. Complicating this problem is the fact that there is no "one size fits all" description of a malicious insider. Motivations, objectives, cyber expertise, system privileges all can and do vary from one case to the next.

Any comprehensive solution to countering insider threats must consider a wide range of technical problems, many of which still exist largely in the research realm. Examples include automated real-time detection of anomalous behavior; another is originator control over electronic document handling (e.g., dissemination, copying, printing, etc.) The Panelist are all actively engaged in insider threat research for the US Intelligence Community and will provide their own unique perspectives on the current state of the art, gaps in current capabilities, and recommendations on what needs to be done to shrink the gaps. The Panelist will also cover visionary (what do we want?) as well as practical (what is achievable in the next

few years?) issues regarding insider threat solutions.

Panelist and Their Issues

Terrance Goan: Making progress in insider threat detection will require reconsidering some basic concepts. First, we as a community need to consider new means of evaluating behaviors over months or even years, and for incorporating non-traditional evidence (e.g., personnel reports). Second, these more comprehensive systems will need to be able to generate summary reports that can be digested by managers/supervisors because the computer security staff may not be in a position to make adequate assessments. Third, in order to cut down on the number of alerts, new systems must be able to learn through feedback that anomalous behavior is truly suspicious (although not necessarily intrusive) and which is simply due to the vagaries of everyday honest work.

Shambhu Upadhyaya: Insider threat is a very complex problem requiring a multi-faceted approach with radical solutions and paradigm shifts. Preventive measures harden a computational environment, making it tough for an insider to launch a successful attack without being noticed. However, since no technique is 100% secure, detection and a tamper-resistant logging and trace-back mechanism must be in place so that essential details about the attack and the feedback to refine the security policies

can be collected should an attack succeed. The “jewels” that insiders may pursue are usually documents of high value such as intellectual property, confidential information and military intelligence. We present a sequence of steps – Threat Models, Decentralized Accountability, Prevention of Tampering, Pollution and Information Falsification, and Finer Access Controls and Event Logging to mitigate the insider threat.

Allen Ott: Most existing information security systems are designed to prevent remote entry from external hackers. Sophisticated professionals, meanwhile, gain initial entry through the acquisition of passwords or via insiders – disloyal casual or full-time employees - and then do damage. Many insider actions can appear to be completely authorized and legitimate while; in fact, they are part of a sophisticated attack. I will discuss the research being done in the following areas, which, I feel, is vital to addressing the malicious insider threat:

- the use of automated technology to gather network and insider information
- modeling users and networks
- advanced reasoning techniques to identify sophisticated attacks