Panel: The Insider Problem Revisited

Matt Bishop
Dept. of Computer Science
University of California at Davis
Davis, CA 95616-8562
+1 (530) 752-8060
bishop@cs.ucdavis.edu

ABSTRACT

The "insider problem" is considered the most difficult and critical problem in computer security. But studies that survey the seriousness of the problem, and research that analyzes the problem, rarely define the problem precisely. Implicit definitions vary in meaning. Different definitions imply different countermeasures, as well as different assumptions.

1. INTRODUCTION

The "insider threat" or "insider problem" is cited as the most serious security problem in many studies. It is also considered the most difficult problem to deal with, because an "insider" has information and capabilities not known to other, external attackers. But the studies rarely define what the "insider threat" is, or define it nebulously. The difficulty in handling the "insider threat" is reasonable under those circumstances; if one cannot define a problem precisely, how can one approach a solution, let alone know when the problem is solved?

Definitions of the "insider threat" have some common elements. For example, a workshop report [1] defined the problem as *malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems*[i]. Elsewhere, that same report defined an insider as *someone with access, privilege, or knowledge of information systems and services*[ii]. Another report [3] implicitly defined an insider as *anyone operating inside the security perimeter*[iii].

Each of these definitions seems reasonable. Consider the following three scenarios.

1. A manager at a military base learns she is about to be dismissed. She enciphers critical files on the system, and offers to provide the deciphering key if the contractor pays her $10,000 as severance pay, and agrees not to prosecute her. The contractor agrees. Here, the manager did not damage information on the system; she simply denied access for some time. Without access to the system, and knowledge of which files were critical, the attack would have failed. This is an example of an "insider attack" [4] satisfying the first definition.
2. A system administrator at a bank accesses a financial system that she is responsible for. She notices that $10,000,000 was transferred from account 1011 to account 6734. The account of a close friend is number 6834. She moves the money to her friend's account, alters the original log file entry to change the number to that of her friend's account, and deletes the log entries showing the money being moved from account 6734 to account 6834. This seems to qualify as "unauthorized access by an insider," which is one of the types of misuse reported in the 2003 FBI/CSI Computer Crime and Security Survey [2]. This also satisfies the second definition.
3. A janitor at a large company takes papers with the social security numbers of employees from the trash and uses this information to commit identity fraud. This satisfies the third definition.

The differences among these definitions illuminate the different interpretations of the "insider threat." In the first, the attacker has access to information and/or resources, and is trusted in some way, presumably not to abuse that information or resource. Note the abuse may arise from violations of the security policy, or for actions not covered by the security policy but covered by the trust; we shall elaborate on this later. The second definition broadens the notion of an insider to include anyone who knows something specific about the systems and services under consideration, whether they have access or not. The third definition covers anyone within the security perimeter, regardless of their level of privilege. Presumably, access is required; but access may be only to one entity within the security perimeter, and need not be the system under discussion. A janitor, for example, may have physical access to the console of a system when he cleans a room.

This panel explores the nature of the insider problem, and of the effects of different definitions on assumptions of trust in systems and people, as well as on the countermeasures to be taken.

NSPW 2005 Lake Arrowhead CA USA

2. REFERENCES

[1] R. Brackney and R. Anderson, Understanding the Insider Threat: Proceedings of a March 2004 Workshop, RAND Corp., Santa Monica, CA (Mar. 2004).

[2] CSI/FBI Computer Crime and Security Survey, Computer Security Institute (2003).

[3] J. Patzakis, New Incident Response Best Practices: Patch and Proceed is No Longer Acceptable Incident Response Procedure, Guidance Software, Pasadena, CA (Sep. 2003).

[4] E. Shaw, K. Ruby, and J. Post, "The Insider Threat to Information Systems," Security Awareness Bulletin No. 2-98, Department of Defense Security Institute (Sep. 1998); available at http://rf-web.tamu.edu/security/secguide/Treason/Infosys.htm

---

[i] [1], p. xi.

[ii] [1], p. 10.

[iii] The report contrasts insider threats with "problems that originate from outside the perimeter, such as denial of service attacks, worm infections, and website defacements" ([3], p. 3).