Aspects of Insider Threats

Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop

Abstract The insider threat has received considerable attention, and is often cited as the most serious security problem. It is also considered the most difficult problem to deal with, because an "insider" has information and capabilities not known to external attackers. 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? This chapter presents some aspects of insider threats, collected at an inter-disciplinary workshop in 2008.

1 Introduction

The "insider threat" or "insider problem" has received considerable attention [2, 13], and 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. However, the term "insider threat" is usually either not defined at all, or defined 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? It is noteworthy that, despite this imponderability, definitions of the insider threat still have some common elements. For

Christian W. Probst
Technical University of Denmark, e-mail: probst@imm.dtu.dk

Jeffrey Hunker
Jeffrey Hunker Associates, e-mail: hunker@jeffreyhunker.com

Dieter Gollmann
Hamburg University of Technology, e-mail: diego@tu-harburg.de

Matt Bishop
University of California, Davis, e-mail: bishop@cs.ucdavis.edu

C. W. Probst et al. (eds.), *Insider Threats in Cyber Security,*
DOI 10.1007/978-1-4419-7133-3_1,

example, a workshop report [4] defined the problem as malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems. Elsewhere, that same report defined an insider as someone with access, privilege, or knowledge of information systems and services. Another report [12] implicitly defined an insider as anyone operating inside the security perimeter—while already the assumption of only having a single security perimeter may be optimistic.

In 2008, a Dagstuhl seminar on insider threats brought together researchers and practitioners from different communities to discuss in a multi-national setting what the problems are we care about, what our response is, which factors influence the cost of dealing with insider threats and attacks, and so on. In a time where we barely understand which factors cause insider threats, and our solutions are scattered all over communities, areas, and instruments, this coordinated action between the involved communities seems to be needed more than ever.

This chapter presents some of the results of that workshop, where also the idea for this book was born. Many of the aspects identified in this introductory chapter are touched upon throughout the book. An earlier version of this chapter, as well as more information on that seminar, is available from [9].

2 Insiders and Insider Threats

One of the most urgent quests for communities dealing with insider threats is identifying the characteristic features of an insider. One approach for doing so is to look at recent insider threat cases, and try to find individual or common properties. This is an important step, since insider threat cases can be rather diverging—take for example cases such as Binney vs. Banner [1], a message flood created as consequence of a security bulletin [11], spies that stole secrets for the Chinese Army [7], or a tax authority employee who used her influence to embed backdoors into taxation software [10] (see boxes below for short summaries). While these cases could not differ more, they serve the purpose of illustrating the widely differing characteristics of insider threats.

The wide range of properties that can characterize insider threats recently has led to the development of taxonomies, which are discussed in Section 2.2. Especially Case 2 (message flood) is interesting, as it seems unclear whether this really is an insider case, and if yes, whether it was the deed of a single insider, or a confluence of several actions by insiders. Case 4 (taxation software), on the other hand, seems typical for an employee who is an insider, but needs to "break into" the system to reach certain goals.

To be able to deal with cases so divergent, one clearly needs 1) a common vision of how insiders can be categorized; and 2) security policies for countering insider threats, and ways to evaluate the impact of alternative security policies.

From analyzing cases such as the above, several approaches to identifying an insider can be developed: