The Dark Side of Security Extensions and How to Handle it

Hans Hedbom
Department of Computer Science
Karlstad University
SE-651 88 Karlstad, Sweden
Hans.Hedbom@kau.se

Abstract

Securing computer systems is an increasing concern as more and more systems are connected together in large networks. Traditional operating system based protection mechanisms have failed to fully meet the demands of this new situation. To overcome some of the shortcomings of these mechanisms new types have been developed with the intention to stop or reduce the impact of the new threats. We would like to call these new mechanisms security extensions, since they are not usually part of the core operating system. However, security extensions often contain sensitive and vital information that also needs to be secured. Usually they are dependent on the security mechanisms of the operating system for their own protection, i.e., they are dependent on the security of a mechanism whose insecurity they are supposed to patch. This is clearly an unwanted situation. Due to this fact, we argue that security extensions actually adds risks and vulnerabilities to the system if the underlying system is insecure or if they are not capable of handling their own security by themselves. Making these types of systems distributed or introducing cooperation between different types of security extensions aggravates the situation. In this talk, we discuss and analyze possible vulnerabilities in two types of security extensions, i.e., firewalls, and intrusion detection systems. We will also give some suggestion on how these problems could be handled. And finally we will discuss the concept of graceful degradation in connection with security mechanisms and present the some of the requirements that must hold in order to achieve this.

Keywords: protection, defence mechanisms, intrusion detection, firewall, privacy