Security Laboratory Design and Implementation

Linda V. Knight
DePaul University, USA

Jean-Philippe P. Labruyere
DePaul University, USA

INTRODUCTION

Security laboratories provide controlled environments that simulate enterprises' infrastructures. Such laboratories allow technical professionals to test the effectiveness of different hardware, software, and network configurations in warding off attacks, as well as to experiment with and learn about various security devices, tools, and attack methods in a controlled manner that insures benign consequences. These laboratories typically include an extensive and sometimes complex networking environment.

This paper identifies the critical issues that make the design and implementation of a simulation environment difficult, and provides ways to address these concerns through a checklist of nine critical security-lab design features. Design and development principles and technical and engineering requirements proposed here theoretically can be of use to businesses or universities seeking to build a security laboratory. They can also provide a useful checklist for managers charged with the IT function to use when discussing their security laboratory with their lab's technical designers and support staff.

Historical Perspective

As organizations depend more heavily upon their information resources, and these resources are more commonly attacked, security laboratories become increasingly important. The number of attacks reported to Carnegie Mellon University's CERT Coordination Center (CERT, 2004) grew from 6 in 1988 (the year it was established) to 21,756 in 2000 and 137,529 in 2003. By 2004, automated attacks had become so prevalent that CERT stopped publishing the number of incidents. Such attacks are costly. According to the 2004 FBI and CSI survey (Gordon, Loeb, Lucyshyn, & Richardson, 2004), the 269 respondents who provided costs estimates on the damages estimated that losses reached $14,496,560 in 2004. Yet, the CSO Magazine, U.S. Secret Service, and CERT/CC 2004 E-Crime Watch Survey (2004) found that 32.4% of their respondents did not track monetary losses due to electronic crimes or system intrusions. According to the U.S. Secret Service special agent in charge of the Criminal Investigative Division, "Many companies still seem unwilling to report e-crime for fear of damaging their reputation" (CSO et al.).

BACKGROUND

The most obvious goal of the security-laboratory environment is to provide a suitable setting for experimentation with computer and network security. Such a laboratory can be used to assess the effectiveness of different configurations against security attacks, as well as to allow laboratory users to experiment with and learn about various tools and attack methods. The difficult question is how to design, deploy, and maintain such a nonproduction or laboratory environment. Key issues revolve around how to provide full functionality without allowing the laboratory to be misused, threatening the security of its parent organization or of outside entities.

Security laboratories may be broadly classified into two types: enterprise and educational. For business enterprises, the security laboratory should mimic the organization's security infrastructure production environment. The lab generally should replicate the organization's core security set and configurations while providing access to data that is fundamentally the same as production data, but without the vulner-

ability that using actual production data would incur. Within an educational environment, the lab should be designed to follow either the most common or the best-practice recommendations for enterprise security. Such an educational lab is particularly likely to be set up to allow experimentation with a variety of configurations.

Despite growing interest in computer and network security, little research centers on the design of security laboratories for business enterprises. However, several papers do address various aspects of designing security laboratories for university students. Mayo and Kearns (1999, p.165) described a lab where "…students are given complete (root) control of systems with essentially unrestricted access to the Internet." This was accomplished by insuring that clients within the network appear as outside systems, lacking the ability to interact directly with departmental systems. A guiding principle for this design was that students be able to do no more damage than they might from their dorm room. In a related work, Hill, Carver, Humphries, and Pooch (2001) described implementing an isolated laboratory where students in a specific class were divided into two groups: one group with the goal of protecting its computers, and one group with the goal of compromising the other group's computers. A similar situation was detailed by Wagner and Wudi (2004) when they described using a closed network for cyberwar exercises. Matei (2003) offered extensive advice and resources for those wishing to develop a lab-based course on Internet security. This lab also was isolated, with the exception of specific controlled connections to the department's server. In yet another work related to educational security laboratories (Frank, Mason, Micco, Montante, & Rossman, 2003), a five-member panel who had attended a National Science Foundation (NSF) sponsored cybersecurity workshop shared their thoughts on how they applied what they learned to their courses. Themes that emerged in the panel discussion included moral and ethical considerations, the need to isolate laboratory functions, and the need to formally assess risk. These themes were further developed in work by Labruyere and Knight (2004) that is believed to be the first to center upon the design of both enterprise and educational security laboratories. Key principles from this work are incorporated throughout this paper.

CRITICAL ISSUES

The greatest challenges involved in implementing and supporting the security-laboratory environment are, for the most part, the result of seemingly conflicting functional requirements. In particular, the lab must allow the implementation and utilization of dangerous tools while protecting the production environment and Internet-accessible host from such tools. The lab hosts must have access to outside resources for downloading updates, patches, or documentation, and yet the lab must be protected from outside-initiated attacks. Strict logging of all activities must be implemented for control purposes, but the privacy of the lab user must be maintained. The lab must be able to be reinitialized relatively quickly to a stable and secured state, yet support and maintenance resources are likely to be scarce. Finally, the lab must closely mimic the production environment, but no live data must be present and the lab must be set up in a fashion that will not give an intruder useful information concerning the actual production setup and infrastructure.

DESIGNING A SECURITY LABORATORY

Conflicting functional requirements can be addressed by implementing a combination of nine critical technical design features, as described in the text that follows.

Implement Strict Activity Logging

A strict, auditable system is required to control access to laboratory resources. A copy of all activities must be kept on a real-time basis and logged to a repository that is not directly accessible from the lab environment. All communications between the lab devices and the logging facility should be done via out-of-band connections, that is, connections that are not used by the lab or production facilities and that are protected from disruptions and attacks. When logging activity, actual data payloads may be kept or discarded, depending on the organization's legal and ethical requirements. The logging system must include the sending of null-message heartbeats