IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4881

Designing a Controlled Environment for the Simulation of an Enterprise Security Infrastructure

Jean-Philippe Labruyere and Linda V. Knight
DePaul University, 243 South Wabash Ave., Chicago, IL 60604, JLabruyere@cit.depaul.edu, lknight@cti.depaul.edu

ABSTRACT

Despite a growing emphasis upon computer and network security, little attention has been paid to how business enterprises or universities should approach the design of security laboratories. Such laboratories allow business professionals or students to test the effectiveness of different 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. This paper pinpoints the critical issues that make design and implementation of a simulation environment difficult, and recommends ways of addressing these concerns through a three-step design process. Design and development principles and technical and engineering requirements proposed here can be of use to businesses or universities seeking to build a computer and network security laboratory. They can also provide a useful checklist for managers or administrators charged with the IT function to use when discussing their security laboratory with their lab's technical designers and support staff.

INTRODUCTION

For testing and educational purposes, a realistic security laboratory infrastructure that can closely simulate production or "real life" environments is required. The "test" or "lab" environment then can be used to assess the effectiveness of complex security setups. The difficult question is how to design, deploy, and maintain such a non-production 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 other outside entities.

Despite the continuing interest in computer and network security, little prior research deals directly with this issue. Much has been written concerning the development and operation of generalized student laboratories, yet just three relevant papers were uncovered by the authors that dealt specifically with security laboratories. None of the three directly addressed the needs of enterprise environments. All made specific contributions within a subset of the overall question of security laboratory design for university students. Mayo and Kearns (1999) addressed the specifics of how to implement a Linux student laboratory with three basic goals: do not allow students to do any more damage than they might have done using other computers; isolate each student's work; protect student work from system crashes on a client or the server. In a second work, Hill et al. (2001) described their experiences in 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. In the third prior work related to security laboratories (Frank et al. 2003), a five-member panel who had attended an 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 provide a foundation that is further developed in this paper.

GOALS OF THE SECURITY LABORATORY

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.

A security laboratory must mimic an enterprise security infrastructure production environment. In the case of an enterprise laboratory, the lab generally should mimic the organization's core security set and configurations. Within an educational environment, the lab should be designed to follow either the most common or the best-practice recommendations for enterprise security. Such a lab also might be set up to allow experimentation with a variety of configurations.

This paper details a three-step process for designing a security laboratory: (1) Develop clear functional specifications; (2) Bring in human resource, legal, and administrative experts to address legal, ethical, and risk analysis issues; and (3) Evaluate the soundness of the proposed lab design against a checklist of critical design features.

Step 1: Develop Functional Requirements

To be valuable, the security lab environment must fulfill functional requirements while taking into consideration several constraints to protect against misuse. Table 1 presents these requirements and the reasoning behind them.

Table 1: Functional Requirements for a Security Laboratory

Desired Functionalities	Reasoning / Threats Addressed
1. The lab provider must allow the safe implementation, use and testing of security auditing tools.	Tools can be dangerous if used against an outside target. Organization may be liable for providing the tools if misused.
2. Lab resources must be available and restricted to legitimate users only.	Lab resources must be protected from outside attacks and unauthorized use.
3. Production environment must be protected from lab environment.	Sensitive data must not be present in the lab. A production environment should not be accessible from the laboratory.
4. Restrict Internet bandwidth available to lab resources.	The lab must not be a facility that can be used to launch Denial Of Services (DOS) attacks. This is a particularly important consideration in academic environments.
5. Provide for easy reloading / resetting of configurations.	Experiments / tests will modify lab setup and structure. A trusted secured environment must be available for quick deployment.
6. Privacy of lab users must be safeguarded.	Accountability for user's action must be enforced but its privacy safeguarded.
7. Promote ethical awareness and conduct.	Legal liabilities and ethical considerations may require an organization to enforce an Acceptable Use Policy and/or a Code of Ethics.

Step 2: Consider the legal, ethical, and risk implications

Legal, ethical, and risk analysis issues typically result from conflicting goals and values.

Privacy v. Strict Logging

The dilemma: Just as in a production environment, the privacy of the security laboratory user must be preserved. Unfortunately, this privacy requirement clearly conflicts with the need for an audit trail, with strict logging of all activities and accountability for all actions taken.

The solution: The definition and documentation of the exact logging and privacy policy must be part of the design of the lab environment and must take into consideration the organization's unique legal, ethical, and regulatory requirements and policies. Thus, each organization must find its own balance between privacy and logging requirements. This solution may be grounded in regulatory requirements, the organizations' employee manual, or its Acceptable Use Policy (AUP).

Although it is impossible to give a generalized solution to the logging vs. privacy dilemma, at a minimum, the lab user must receive clear warnings that all activities are monitored and logged. This should be done by making the lab user sign a "Laboratory acceptable use policy" as well as by displaying warning banners and dialog boxes for all devices accessed by the lab user.

Limited Resources v. Increased Needs

The dilemma: Typical production environments often lack some support and administrative resources. A business laboratory environment, often patterned after a parallel production environment, but without the priority of a production setup, typically would suffer further from a lack of resources. Similarly, university laboratories are notoriously short of resources. This shortage of resources is in direct conflict with the fact that, since a security lab provides its users with potentially dangerous tools, the need for close monitoring and support is increased.

The solution: The limited resource v. increased needs dilemma can only be solved by carefully taking these considerations into account when designing the lab environment and specifying the support and maintenance mechanism for it. Such efforts are facilitated by the fact that a lab environment often does not include all the complexity and dynamics of a production environment. At the very least, downtime consequences are usually benign in a lab environment.

Legal and Ethical challenges

The dilemma: An organization that deploys a security laboratory has to take into account many legal and ethical considerations that are often not present in a standard production environment. Since the security lab could be used to perform attacks and might allow a user to gain expertise and skills that could be used later for malicious purposes, legal, ethical, and human dilemmas must be analyzed.

- Does the organization have any liability for providing the tools and infrastructure that might be used in an attack?
- How can an organization promote the ethical use of security auditing tools?
- How can an organization preserve the privacy of users while enforcing accountability for the actions taken?
- Should a lab user be required to adhere to a code of ethics? Should such an agreement be formally signed? Can or should it be legally enforceable?

The solution: The answers to these critical legal and ethical questions require a proactive, multi-faceted study that includes an organization's Human Resource and legal departments. This type of broad study requires considerable time, and can be particularly problematic for smaller organizations without extensive in-house resources readily available. However, it is critical that legal and ethical issues are studied before a security lab is designed. Legal and ethical policies and guidelines first should be established by careful examination of the issues, and then later should be technically implemented within the framework of the lab environment.

When an organization skips the step of requiring a careful up-front analysis of the human and ethical factors by those most skilled in these areas, it is likely to end up having its policies determined by those who are relatively untrained in human, ethical, and legal considerations, the technical staff who design and build its security laboratory.

The enterprise laboratory may have to comply with different legal requirements for privacy and security than the university laboratory. Some of these requirements will be the result of regulatory rules and guidelines, while most will be the result of the fact that lab policy must be consistent with the overall organization's security policy. This security policy typically includes privacy and logging policies that will carryover to the security laboratory. On the other hand, in an academic environment, the security laboratory may be considered a research facility and may have separate requirements.

Step 3: Evaluate the Technical Design

The greatest challenges involved in implementing and supporting the security laboratory environment are, for the most part, the result of seemingly conflicting functional requirements:

- The lab must allow the implementation and utilization of danger ous tools, while protecting the production environment and Internet accessible host from such tools.
- The lab hosts must have access to outside resources for download ing updates, patches, or documentation, yet the lab must be protected from outside-initiated attacks.
- Strict logging of all activities must be implemented, but the privacy of the lab user must be maintained.
- The lab must be able to be reinitialized to a stable and secured state, yet the support and maintenance resources are expected to be scarce.
- The lab must closely mimic the production environment but no live data must be present and it must be setup in a fashion that will not give an intruder useful information on the actual production setup and infrastructure.

Such conflicting functional requirements can be addressed by implementing a combination of seven critical technical design features, as listed in Table 2 and described in the text that follows.

Implement laboratory access control and 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: i.e. 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. This will depend on the organization and its legal and ethical requirements. The logging system must include the sending of null message heartbeats, to alert the lab administrator when a resource cannot perform the real time logging.

Typically the lab environment will use the same Internet connection as the production environment. Access controls must also be implemented to ensure the lab resources can not access the production environment.

Enable restriction on outbound traffic type.

The lab hosts must have access to outside resources for downloading updates, patches, or documentation. At the same time, outbound traffic that is malicious or non-authorized must be prevented. This can be achieved by setting up strict restrictions on the type of traffic and destinations allowed. The remote logging of all activities described earlier can ensure that such controls are in place, functional, and not bypassed. Even organizations that do not routinely store data payloads may wish to do so for outbound traffic. The feasibility of keeping such copies will be determined by the amount of traffic generated, the capacity of the logging facility and the privacy requirements.

Table 2: Checklist of Critical Security Lab Design Features

Critical Design Feature	Enterprise security laboratory	University research or student lab
1. Implement access control and strict activity logging.	yes	yes
2. Enable restriction on outbound traffic type.	yes	yes
3. Enable bandwidth limitation on outbound traffic.	yes	yes
4. Implement an efficient configuration management and restoration system.	yes	yes
5. Ban all production data from the security laboratory.	yes	May not apply
6. Implement only the minimum software needed.	yes	May not meet educational or research needs
7. Promote the ethical use of information security resources.	yes	yes

Enable bandwidth limitation on outbound traffic.

Very often, a security laboratory environment is connected to the main Internet link of an organization. That bandwidth is likely to also transport production or mission-critical traffic, along side the security lab traffic. In the case of a major university or a large enterprise, that Internet link may have high bandwidth capacity; however, the amount of bandwidth allowed to leave a laboratory must be limited. It is extremely challenging to prevent DOS attacks based on overwhelming a victim with high traffic levels. This is because such attacks can be carried via legitimate traffic. High traffic levels generated from the lab can also deny regular, production traffic the ability to access the Internet link. To prevent these threats, traffic bandwidth policy or artificial bottlenecks must be introduced to limit the traffic levels leaving the lab environment.

Implement an efficient configuration management and restoration system.

Since the security laboratory environment will be changed through experiments with alternate setups and test configurations, the security laboratory administrator must be able to restore the lab in a fast and secured fashion to a known state, in order to allow other lab users access. That known state or baseline will be very dynamic as new patches and configuration changes will be frequent. Thus, an efficient system must be setup to perform such restoration and manage changes in the baseline.

Ban all production data from the security laboratory.

Such a ban may not be particularly meaningful for university research or student security laboratories; however it is critical for an enterprise laboratory to avoid all risk that production data might be compromised by banning all production data from the security lab. Further, the lab environment, setup to mimic the production environment must not give a lab user (or a successful intruder) any useful information on the actual configuration or setup of the production environment.

Implement only the minimal software needed.

In an enterprise environment, the laboratory environment should only implement the minimal software needed to address functional requirements. Adding powerful security tools that are not critical to the lab's charter poses an unnecessary risk. For example, a front-end logging system might be implemented, but the complete functional application should not be made available if it is not part of what is being tested. In a university environment, more than minimal software may be needed to provide a rich educational or research environment. In this case, the institution's managers or administrators should be called upon to make a conscious decision, balancing the added risk against the added educational benefits. Although the technical staff can be an important resource in quantifying the amount of risk involved in including various features in the lab, risk analysis should not be left to their discretion. This is consistent with the recommendations made earlier for making key decisions in the legal and ethical areas.

Promote the ethical use of information security resources.

To facilitate the ethical use of information security resources, an organization may implement mandatory self-paced training and/or require all users to sign a code of conduct agreement before being granted access. In any case, an individual should be designated as the key person responsible for promoting ethical use of the laboratory.

DEPLOYMENT AND EVALUATION

Based on the proposed methodology, we are implementing a security laboratory in an academic environment. One important aspect of this endeavor is to allow us to validate or criticize our proposed approach. However, proving the soundness of our approach, or even of any one deployed laboratory environment, is in fact not possible. One can demonstrate that a given deployed environment failed by mitigating its integrity. However, the only evidence that such an environment achieves its goal comes from verifying over time that it has not been compromised. Such evidence cannot be considered proof of the soundness either of the laboratory or of the methodology used to design it. Furthermore, the compromise of an established laboratory environment does not necessarily mean that the methodology followed for its design is flawed. While the compromise may be caused by a defect in establishing the functional requirements, it is even more likely to be caused by a defect in implementation and configuration. Thus, as is often the case in the security domain, the methodology proposed here cannot be proven, however evidence of its soundness and of its weaknesses can be expected to emerge over time as it is used to design actual security laboratories. The methodology can be expected to develop further over time as such evidence emerges, and as new technologies and external threats continue to emerge.

CONCLUSIONS

The implementation of a security laboratory environment provides many benefits to both business enterprises and universities. Chief among these are the ability of lab users to increase their skills by experimenting with the methods and tools typically used by intruders, and the ability of the lab to be used to test a configuration or a system for security weaknesses before production deployment. The implementation of a security lab does however introduce complex threats and many aspects and requirements must be closely considered during the design. The major areas of concern to address are: how can malicious activities be prevented from originating in the security lab environment; how can the lab environment be protected from attacks and from being compromised; how can the privacy of lab users be maintained while implementing the necessary logging and auditing system to enforce accountability; and what tools and methods can be used to facilitate simple, trouble-free management of the lab environment.

The answers to these concerns include technical solutions, policy decisions, and procedural solutions. While the specific solutions will vary with the organization, some critical principles can be applied across-the-board. First, organizations seeking to develop a security laboratory should first develop clear functional specifications. Table 1 provides a guide to key considerations during this process. Second, before the technical design is completed, human resource and legal experts should be brought into the discussions to develop and interpret policy regarding the legal and ethical issues involved in implementing the lab. At the same time, the institution's managers or administrators must become involved in risk analysis. This is the opportunity to address

the issues of whether various desired functionality warrants the risks involved. Finally, before the security laboratory design is finalized, the checklist of critical design features in Table 2 should be used to evaluate the soundness of the proposed lab's design.

While every organization is unique and each security laboratory must be specifically designed to meet the unique needs of its parent organization, there are nonetheless key principles that should underlay the design of any security lab. By organizing these principles in one paper, this research provides a guideline for those seeking to develop a secure and yet effective security laboratory.

REFERENCES

Frank, C., Mason, S., Micco, M., Montante, R., Rossman, H. "Panel Discussion: Laboratories for a Computer Security Course." The Journal of Computing in Small Colleges. 2003, 18:3, 108-113.

Hill, J.M.D., Carver, C.A. Jr., Humphries, J.W., and Pooch, U.W. "Using an Isolated Network Laboratory to Teach Advanced Networks and Security" The Proceedings of the Thirtieth SIGSCE Technical Symposium on Computer Science Education. 2001, 36-40.

Mayo, J. and Kearns, P. "A Secure Unrestricted Advanced Systems Laboratory." The Proceedings of the Thirtieth SIGSCE Technical Symposium on Computer Science Education. 1999, 165-169.