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

ITB12818

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2*
edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

A Framework for Teaching Information Security Laboratory Projects with Open Source Software

Mariana Hentea, Southwestern Oklahoma State University, Dept of Computer Science & Info. Systems,
Weatherford, OK, mariana.hentea@swosu.edu

ABSTRACT

Although traditional lecture approach dominates the current teaching of information security, by combining traditional lecture approach with laboratory projects, students become more interested and active in analyzing problems. The security laboratory projects are building on practical and problem solving skills as well as flexible designs and easy implementations of security architecture. This paper discusses a framework for teaching Information Security in Computer Science and Information Systems programs using laboratory projects based on Open Source Software/Free Software (OSS/FS). The freedom to experiment with various OSS/FS products for security laboratory projects stimulates student's learning and creativity. The framework for security laboratory projects based on use of Open Source Software/Free Software could have a positive impact for many educational institutions that are looking to introduce Information Security Assurance in their education programs.

WHY OPEN SOURCE SOFTWARE/FREE SOFTWARE?

The use of open source software/free software (OSS/FS) has been a trend for the past years and "the popularity of OSS exploded among consumers and developers" (St. Amant & Still, 2005, pp. 791). OSS/FS source code is publicly available and developers can reuse the code and refine it to create more complex and better software. Open source movement is one among other environments or "societal institutions where most software is developed" (Shah & Kesan, 2005). Other environments include universities, firms, and consortia. Open Source movement has developed software such as Linux operating system, Apache web server, MySQL database management system, the scripting language Perl, and the popular email server Sendmail - that rivals with commercially available software. OSS/FS became "even superior approach to using their proprietary competition" (Wheeler, 2005). OSS/FS is "changing the way the software code is produced" (Jin, Robey & Boudreau, 2005).

OSS/FS is a new business model that is appealing to non-profit and government entities that established policies to adopt OSS whenever possible. OSS/FS is used successfully in a university environment to set-up a Web based online conference (Halstead-Nussloch & Lu, 2005) or to support Web information management (Cartelli, 2004). The impact of Open Source Initiative approved licenses on commercial applications is discussed in (Cuellar, 2005). OSS/FS research is mainly focused on the development. However, research is emerging in use (Jin, Robey & Boudreau, 2005) and application software for business applications (Brandon, 2005). Organizations are building complex applications at a fraction of the initial cost and ongoing cost associated with proprietary software products.

The characteristics of OSS/FS such as no cost, easy availability, portability, relevance to state of the art software techniques, relevance to emerging technologies, open standards based, methodologies, and ease of learning are distinct attributes that are preferred in an education institution when compared to commercial software products. Also, reports indicate that OSS/FS for security protection are often more reliable than commercial software. Linux is the operating system which is superior in base security, application security, and open standards compared to Microsoft Windows (Wheeler, 2005). Many organizations report significant savings when using OSS/FSS. For example, Apple is using open source code for the operating system (Apple, 2005). Additional advantage is that OSS/FS products can be modified by users and protect its users from the risks and disadvantages of single source solutions. Many countries around the globe (i.e. Brazil, China, France, Germany, Japan, South Korea, Peru, etc.) already established special projects to help organizations to transition from proprietary software to OSS/FS.

Performance, scalability, and security are better features with the OSS/FS products than with commercial products. For example, OSS/FS vulnerability scanner Nessus was found to be the most effective tool among other seventeen tools that were evaluated (Vulnerability, 2001). Also, OpenSSH, the Secure Shell (SSH) protocol is used to securely connect to computers and control them remotely (using either a text or X-Windows graphical interface) and it is the Internet highest implementation compared to proprietary implementations.

OSS/FS has been proposed in the revised Information Technology Curriculum (Mallick & Subrahmanya, 2004) in terms of tools, laboratory software and ingredients for learning. The movement to create OSS and applications for higher education from course management systems to ERP financial systems is "rapidly gaining momentum" (Gandel & Wheeler).

OSS/FS USE IN INFORMATION SECURITY EDUCATION

Teaching Information Security in Computer Science and Information Systems programs is often based on traditional lecture approach. However, skill building is facilitated by combining traditional lecture approach with laboratory projects because students become more interested and active in analyzing problems. A combination of traditional lectures with laboratory projects supports teaching security skills ranging from basic to advanced levels. Students learn how to analyze and solve security problems. In addition, laboratory projects with OSS/FS for teaching Information Security concepts provide students with the advantage of learning the most current technologies and trends. Emerging patterns of growth in the Information Security disciplines must be identified through research, and then promptly integrated into curriculum. Higher education institutions have to update curriculum in response to corporate, government, and home users needs. This results to ongoing process for the development of an Information Security education program to ensure "that it remains up to date with international standards and practices as well as with the expectations from industry" (Smith, 2005). The strategy of designing and changing laboratory projects continuously can become expensive. The use of OSS/FS resources allows to quickly start an Information Security Program in higher education institution even when the budgets are limited (Dhillon & Hentea, 2005).

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

The security laboratory projects are building on practical and problem solving skills as well as flexible designs and easy implementations of security architecture. The freedom to experiment with various OSS/FS products for security laboratory projects stimulates student's learning and creativity. The next section discusses a framework for teaching Information Security in Computer Science and Information Systems programs using laboratory projects based on OSS/FS.

SECURITY LABORATORY PROJECTS BASED ON OSS/FS

The laboratory project series is based on three courses which sequentially increase student skills from the introductory level to higher and advanced level. Students enrolled in Computer Science or Information Systems programs have to take INTRODUCTION TO INFORMATION SECURITY course and perform the laboratory projects suggested in the category Part 1 in the second semester of the freshmen year. If the student specializes in Information Security, then the laboratory projects of Part 2 and Part 3 support the topics covered in the following courses: SECURITY ARCHITECTURE AND DESIGN and INFORMATION SECURITY MANAGEMENT. The suite of the laboratory projects is described in (Hentea, 2005). The courses and laboratory projects allow students to understand the impact of organizational changes (for example, new business, new missions, new factors such mobile workers) to security architecture.

Advanced theories of computer protection have established the foundations of security systems. When applying information security, we need to go beyond the analysis of individual security protocols and consider how they are used within distributed systems, software applications and services. The approach is to extend the theory and analysis of security protocols towards a modeling approach for describing, analyzing, and simulating security aspects of systems. This involves using software that is specifically designed to explore the security facets of systems (Monahan, 2004). Simulators allow students to play "what if" scenarios with their configuration to make sure the design can hold up firm against all positive and negative conditions. Modeling an environment leads to systems designed to achieve a specific and rewarding goal and application of these results has improved the quality of the security systems that is being protected (Bishop, 2005).

The security laboratory is equipped with adequate resources to provide an environment to students for executing the laboratory projects. The security laboratory is equipped with security technologies hardware and software. Software security technologies include both commercial and free open source products. The free software from open source and demonstration versions make it possible to maintain an up to date security environment which requires changes due to the dynamic and emerging security technologies. In addition, this option allows freedom to choose a variety of tools without any costs. Open Source Software is used for the important components in the laboratory projects such as operating systems, simulators, security software, and tools for configuration, verification, maintenance, emulators, and management tools. The security laboratory is equipped with computers on which both operating systems, Microsoft Windows and Linux, are installed. Currently, simulators are used mostly by enterprises. Examples of costly free products from software manufactures include firewalls, and OPNET simulator (OPNET, 2005). OPNET offers embedded expert knowledge about how network devices, network protocols, applications, and servers operate. Other simulation tools such as Ns and nam are provided by the Virtual InterNetwork Testbed (VINT) project (Breslau et. al., 2000) and are publicly available (Ns, 2005). These tools help in the design and deployment of new wide area Internet protocols. Simulation is used to evaluate network protocols under varying network conditions.

The suite of laboratory projects is organized to support a series of three courses in the Information Security Program. The evolution of techniques from simple to more complex security architecture supports a gradual learning and reinforcement of prior knowledge and skills. The first set of laboratory projects (section Laboratory Projects Part 1) focus on learning different approaches and technologies for security protection. The second set of laboratory projects (section Laboratory Projects Part 2) teaches students to apply various techniques to more specific security architectures that were ultimately designed to address one organization's specific needs. The third set of laboratory projects (section Laboratory Projects Part 3) allows a student to search for broader solutions that include managerial decisions, design, and development of new tools. The suite of laboratory projects covers important and emerging technologies required to be used by a security professional. These laboratory projects can be performed only in a Windows or combination of both Windows and Linux environments. Also, the security laboratory is equipped with routers, firewall appliance, and software firewall. The specific product from a vendor is not significant. Any device can be substituted with a device from any other vendor.

Laboratory Projects Part 1

This suite of laboratory projects are based on theoretical concepts introduced in the course INTRODUCTION TO INFORMATION SECURITY**.** Students are required to meet the prerequisites such as familiarity with Operating Systems (UNIX, Linux, and Windows). The laboratory projects cover the basic security technologies and techniques for the information security assurance. Table 1 summarizes the subset of laboratory projects that are required to use OSS/FS resources.

Laboratory Projects Part 2

This suite of laboratory projects are based on theoretical concepts introduced in the course SECURITY ARCHITECTURE AND DESIGN**.** Students are required to meet the prerequisites Computer and Network Security Fundamentals and suite of laboratory projects Part 1. The laboratory projects cover the basic security technologies and security architecture. The topologies suggested by Computer Emergency Response Team (CERT) and Zimmerman (Zimmerman, 2002) offer different security architecture levels such as simple, moderately complex, and complex. Execution of the laboratory projects requires the use of tools such as simulators and network management tools. Use of OSS/FS resources is recommended and they are provided in the security laboratory. The software is downloaded, installed, and tested before being recommended for use. A variety of tools from open sources (Top, 2005), (Free, 2005), (Howlett, 2005), (OpenLabs, 2005), (MRTG, 2005) can be used for investigating protocols, design scenarios, checking resistance to particular attacks, and formulating specific trace and state properties which capture more precisely the security related aspects of a system design. A wide range of Open Source tools for network management are described in (Kretchmar, 2004).

Laboratory Projects Part 3

This suite of laboratory projects are based on theoretical concepts introduced in the course INFORMATION SECURITY MANAGEMENT**.** Students are required to meet the prerequisites SECURITY ARCHITECTURE AND DESIGN and suite of laboratory projects Part 2. The laboratory projects cover the basic security technologies and techniques for security management including security policy violations and security auditing as summarized in Table 2. Currently intrusion detection systems (IDS) are an essential part of a defense strategy (Kayacik, 2005). SNORT is an open source software and it is the most used IDS which detects possible attacks or access violations while they are occurring (SNORT), (Rehman, 2003).

CONCLUSION

By performing a suite of laboratory projects using resources based on OSS/FS, students are challenged to look for alternative solutions and evaluate software to solve new problems. In addition, students learn to provide solutions for new situations that are imminent in the real world. By learning and developing tools for information security management as described in Laboratory Projects Part 3, students get skills in effective detection and prevention mechanisms and countermeasures for information security protection. By training students with technologies that

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Table 1. Laboratory Projects Part 1

LAB Projects	**Objectives**	**Resources – Use of Open Source**
LAB1, LAB2, LAB3 - Linux and Windows Operating Systems	Demonstrate access to services; scan for vulnerabilities, check open services, and shut down services as required.	Use open source software for testing passwords and vulnerabilities for open services.
LAB4, LAB5 - Host hardening	Demonstrate access to services, remote login, and access based on a logical address or name.	Use open source software for testing passwords and vulnerabilities for open services.
LAB6, LAB7 - Host defense with various security technologies	Demonstrate the security features of each category of the security software. Demonstrate access to services.	Use open source software for anti-virus, firewall, and host-based intrusion detection or system integrity checker.
LAB8 - Web Server Defense	Demonstrate access and use of services for the internal or external clients.	Use open source software for Web server defense and testing configurations and services for vulnerabilities as defined by Information Security policies.
LAB9 - Encryption and Certificates	Demonstrate the encryption and use of certificates.	Use a Certificate server downloaded from open source to create secure communication in both directions between internal and external clients.
LAB10, LAB11 – Email and Remote Access	Demonstrate the access and use of VPN services, Email services for both internal and external clients.	Use open source software (PGP) to create Email accounts, configure PGP options, export keys, send attachments, and create hidden file
LAB12, LAB13, LAB14, LAB15 - Implementing security for a small business using a firewall appliance and firewall software to protect the network for a small business.	Demonstrate the access and use of services as defined by Information security policies for both internal and external clients. Demonstrate the effectiveness and performance of the firewalls.	Using different security tools (existing laboratory resources, demonstration (trial) or open source).

Table 2. Laboratory Projects Part 3

LAB Projects	**Objectives**	**Resources – Use of Open Source**
LAB1, LAB2, LAB3 – Monitor different security technologies and Event Correlation for the network topology identified as moderately complex topology (LAB1 & LAB2) and complex topology (LAB3).	Security auditing and defining specific requirements for automated tools that are needed by a network administrator to be able to identify quickly the targets to take effective and proactive measures for protection.	Use open source software such as intrusion detection systems, honey pots, network monitoring and protocol analysis, and software vulnerabilities scans.
LAB4, LAB5 – Design and implement automated tools for network administrator.	Minimum objectives: Write scripts and programs to implement the specifications; demonstrate that the mechanism, interface, and tools work as designed. Identify the mechanism and interfaces to provide feedback to the network administrator.	Use open source to identify tools that can be enhanced or create new tools (shell scripts). Monitor alerts generated by different devices; identify false positive or negative alerts, reconnaissance alerts, and correlate events.

are vendor independent, there is better chance to become very attractive to prospective employers. Employers are looking for graduates that are proficient in many areas related to information security, including new technologies trends and issues. The framework for security laboratory projects based on use of Open Source Software/Free Software could have a positive impact for many educational institutions that are looking to introduce the Information Security education.

REFERENCES

Apple, (2005). Security in Mac OSX Safety by Design. http://images.apple.com/macosx/pdf/Mac_OS_X_Security_TB.pdf

Bishop, M., (2005). Introduction to Computer Security. Addison-Wesley, Boston, Massachusetts.

Brandon, D., (2005). Open Source: Application Level-Ready for Prime Time? Proceedings of 2004

International Management Association International Conference, May 2005, San Diego, California, pp. 805-807.

Breslau, L., Estrin, D., Floyd, S., Heidemann, J., Hemy, A., Hang, P., McCanne, S., Varadhan, K., Xu, Y., (2000). Advances in Network Simulation. IEEE Computer, May 2000, pp. 59-67.

Cartelli, A. (2004). Open Source Software and Information Management: The Case of BMB On Line.

Proceedings of 2004 International Management Association International Conference, May 2005, New Orleans, Louisiana, pp. 1023-1024.

CERT, http://www.cert.org

Cuellar, L.E. (2005). Open Source License Alternatives for Software Applications Is it a Solution to Stop

Software Piracy? Proceedings of 43rd ACM Southeast Conference, pp. 2-269-2-274, March, 2005, Kennesaw, Georgia.

Dhillon, H. & Hentea, M. (2005). Getting a Cybersecurity Program Started on a Low Budget. Proceedings of 43rd ACM Southeast Conference, March, 2005, Kennesaw, Georgia, pp. 1-294- 300.

Free Security Sources, http://www.yacc.co.uk/free.security/.

Gandel, P.B. & Wheeler, B. (2005). E-Content Of Birkenstocks and Wingtips: Open Source Licenses.

EDUCAUSE, January/February 2005, pp. 10-11.

Halstead-Nussloch, R. & Lu, Y. (2005). Building an Online Conference with Open-Source Components.

Proceedings of 43rd ACM Southeast Conference, March, 2005, Kennesaw, Georgia, pp. I-376-379.

Hentea, M. (2005). A Framework for Teaching Information Security with Laboratory Projects. Proceedings of the IFIP TC11 WG 11.8 Forth World Conference Information Security Education (WISE4), pp. 174-178, May 2005, Moscow, Russia.

Howlett, T. (2005). Open Source Security Tools Practical Applications for Security. Prentice Hall, Upper Saddle River, New Jersey.

Jin, L., Robey, D. & Boudreau, M. C., (2005). Beyond development: A Research Agenda for Investigating Open Source Software User Communities. Proceedings of 2005 International Management Association International Conference, May 2005, San Diego, California, pp. 642-645.

Kayacik, H.G., Zincir-Heywood, N.A., Heywood, M.I. (2005). Intrusion Detection Systems. Encyclopedia of Multimedia Technology and Networking. Editor: M. Pagani, Vol I, pp. 494-499, Idea Group Reference, Hershey, Pennsylvania.

Kretchmar, J.M. (2004). Open Source network Administration. Prentice Hall, Upper Saddle River, New Jersey.

Malick, S. & Subrahmanya, S.V. (2004). Use of Open Source Software for Information Technology Education. Proceedings of 2004 International Management Association International Conference, May 2005, New Orleans, Louisiana, pp. 1000-1003.

Monahan, B. (2004). From Security Protocols to Systems Security: Making a Case for Systems Security, MRTG. Multi Router Traffic Grapher. http://www.mrtg.org

Ns, http://www-mash.cs.berkeley.edu/ns

OpenLabs, http://www.openca.org/

OPNET, Simulation Software, http://www.opnet.com/products/home.html.

Rehman, R.U. (2003). INTRUSION DETECTION with SNORT. Prentice Hall, Upper Saddle River, NJ.

Shah, R.C. & Kesan, J.P. (2005). Nurturing the Software. Communications of the ACM, Vol. 48, No. 9, pp. 80-85.

Smith, E., Kritzinger, E., Oosthuizen, H.J., von Solms, S.H. (2005). Information Security Education: Bridging the Gap between Academic Institutions and Industry. Proceedings of the IFIP TC11 WG 11.8 Forth World Conference Information Security Education (WISE4), pp. 45-56., May 2005, Moscow, Russia.

SNORT, http://www.snort.org

St.Amant, K. & Still, B. (2005). Open Source Software and International Outsourcing. Encyclopedia of Multimedia Technology and Networking. Editor: M. Pagani, Vol. II, pp. 791-798, Idea Group Reference, Hershey, Pennsylvania.

Top 75 Security Tools, http://www.insecure.org/tools.html.

Vulnerability Assessment Scanner. (2001). Network Computing, January 21, 2001.

Wheeler, D.A. (2005). Why Open Source Software/Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers! http://www.dwheeler.com/oss_fs_why.html

Zimmerman, S.C., (2002), Secure Infrastructure Design. http://www.cert.org/archive/pdf/Secure_Infrastructure_Design.pdf

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/proceeding-paper/framework-teaching-information-security-laboratory/32765

Related Content

Olympics Big Data Prognostications
Arushi Jainand Vishal Bhatnagar (2016). *International Journal of Rough Sets and Data Analysis (pp. 32-45).*
www.irma-international.org/article/olympics-big-data-prognostications/163102

Regional Development Getting Smarter with ICT
Saleem Zoughbiand Sukaina Al-Nasrawi (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 6525-6533).*
www.irma-international.org/chapter/regional-development-getting-smarter-with-ict/113111

PolyGlot Persistence for Microservices-Based Applications
Harshul Singhal, Arpit Saxena, Nitesh Mittal, Chetna Dabasand Parmeet Kaur (2021). *International Journal of Information Technologies and Systems Approach (pp. 17-32).*
www.irma-international.org/article/polyglot-persistence-for-microservices-based-applications/272757

Generalize Key Requirements for Designing IT-Based System for Green with Considering Stakeholder Needs
Yu-Tso Chen (2013). *International Journal of Information Technologies and Systems Approach (pp. 78-97).*
www.irma-international.org/article/generalize-key-requirements-designing-based/75788

Defining an Iterative ISO/IEC 29110 Deployment Package for Game Developers
Jussi Kasurinenand Kari Smolander (2017). *International Journal of Information Technologies and Systems Approach (pp. 107-125).*
www.irma-international.org/article/defining-an-iterative-isoiec-29110-deployment-package-for-game-developers/169770