published as: J. Hu, D. Cordel, Christoph Meinel: New Media for Teaching Applied Cryptography and Network Security;
In Proceedings of the 1st European Conference on Technology Enhanced Learning (EC-TEL 2006);
Crete, Greece, October 2006, pp.488-493, ISBN 3-540-45777-1, Springer LNCS 4227.

New Media for Teaching Applied Cryptography and Network Security

Ji Hu[1], Dirk Cordel[1], and Christoph Meinel[1]

The Hasso-Plattner-Institute (HPI), University of Potsdam, Postfach 900460, 14440 Potsdam, Germany
{ji.hu,cordel,meinel}@hpi.uni-potsdam.de

Abstract. Considering that security education needs to train students to deal with security problems in real environments, we developed new media for teaching applied cryptography and network security. They permit students to gain real-life security experience from virtual laboratories on CD, DVD, or online. The application of those media is helpful to reduce investment and administration costs as well as effectively support security experiments which previously had to be done in conventional security laboratories.

1 Introduction

Teaching only theoretical facts has proved to be insufficient for today's IT security education because security teaching is focusing more on preparing the skillful workforce in response to increasing security challenges [Bishop, 2000]. In this context, we must meet the need of training students to apply security technologies for real environments. So far, computer helps practical security instruction in four ways:

Multimedia courseware is digitized lectures [Schillings and Meinel, 2002]. It provides no user interaction or real experiences; Demonstration software, e.g. [Esslinger, 2002], [Spillman, 2002] allows learners to play with cryptographic algorithms, but in very few cases, real tools or everyday environments are involved; Simulation systems let students accomplish security tasks in a very abstract and limited environment. This means that students have no chances to apply production tools [Irvine and Thompson, 2004], [Rowe and Schiavo, 1998]; Dedicated computer laboratories [Ragsdale et al., 2003] and [Vigna, 2003] are practical for security training because security exercises are performed with production software on real systems. However, they require expensive hardware/software investment and intensive efforts to create, configure, and maintain laboratory environments. Moreover most security exercises require privileged access to the OS, which introduces the risk of misuse and inconvenience of administration [Vigna, 2003]. For security reason, dedicated networks are isolated from production networks and not able to benefit the learners outside the campus.

The Tele-Lab IT-Security project at the HPI has developed new media to support learning/teaching applied cryptography and network security. In order to integrate hands-on experiences, Tele-Lab created virtual and lightweight laboratories on the CD, DVD, or online instead of constructing expensive traditional security laboratories. Students thus can gain real-life security experiences with CD/DVD or Internet connections without the limitation of time and place.

The following parts of the paper are organized as follows: Section 2 briefly introduces the Tele-Lab concept and architecture. Section 3 and Section 4 presents Tele-Lab CD/DVD and Tele-Lab server respectively. Then Section 5 describes application of Tele-Lab and shows how they can support daily teaching and learning. Finally, Section 6 concludes the paper.

2 The Tele-Lab Concept

Tele-Lab is intended to produce computer-aided tutoring systems that allow students to learn about IT security and also gain practical skills. Its contents cover many aspects of applied cryptography and network security such as encryption, authentication, email security, firewalls, intrusion detection, wireless security, etc. The originality of Tele-Lab is that it integrates real-life exercises and laboratory environments in e-learning/tutoring systems to help students understand how technologies are applied in reality. E.g. Tele-Lab not only explains and demonstrates encryption algorithms, but also offers students chances to apply cryptographic tools like PGP or OpenSSL to encrypt or digitally sign messages.

The concept of Tele-Lab is illustrated in Figure 1. Basically it consists of a Linux system and a tutoring system. The Linux system is equipped with various open-source security tools such as scanners and password crackers, and can be used as a virtual laboratory. The tutor is a local web server that presents teaching contents stored in a knowledge repository and manages exercises scripts. A user reads theoretical part by a web browser and finishes exercises by applying tools in Linux. User's results can be either text or data sent to the tutor or some changes on the operating system such as modifying configurations or opening/closing services. The tutor then evaluates the results by scripts. Hence, interactive and real-life exercises are realized.

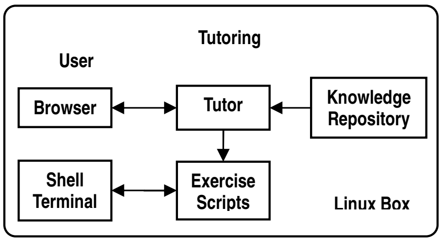


Fig. 1. The concept of Tele-Lab IT-Security

Tele-Lab replaces most administration work by managing configurations and exercises with scripts. But security exercises introduce risk of misuses because students are allowed to be a super user in many exercises, e.g. starting or closing services. Thus students might corrupt Tele-Lab by misusing their privileges, which results in administrative inconvenience and interruption of the learning process.

3 Tele-Lab CD: A Reliable and Portable Virtual Laboratory

In order to improve the reliability of the Tele-Lab and ease its administration, we developed Tele-Lab CD/DVD [Hu and Meinel, 2004]. It integrates the entire Tele-Lab on a Knoppix live-CD. This kind of CD has a special feature to detect a rich set of hardware and run a complete Linux on itself instead of installing it on a hard disk.

By implementing Tele-Lab on live CDs, we have a portable and reliable virtual laboratory. It can be distributed to students for the training at home or in the workplaces on general PCs. Tele-Lab CD will not affect hardware and software installations and runtime failures can be simply handled by re-booting.

4 Tele-Lab Server: Virtual Laboratories on the Internet

Tele-Lab CD/DVD has its limitation of usability: it only runs on those machines which the Live CD supports and can not provide network security exercises because of its performance and space limits. From the point of view of e-learning, it is desirable that students can work with Tele-Lab over the Internet. Therefore, we came up with the idea to develop an online learning and exercising platform, Tele-Lab IT-Security Server [Hu and Meinel, 2004]. Tele-Lab server differs from Tele-Lab CD by building virtual laboratories with virtual machines instead of Live CDs. Virtual machines (VMs) [Goldberg, 1974] are software copies of physical machines and can be connected to networks. This provides the possibilities to simulate real laboratory environments cheaply and for students to access them online easily.

The architecture of Tele-Lab server is shown in Figure 2. The user work environments are built with the User-Mode Linux virtual machines [Dike, 2001]. They behave normal applications running on a host computer and accessible from outside the host as any regular computer. Each VM is carefully installed and configured with security tools and user settings. Careful performance optimizations such as system resource allocations and separation among VMs are done for making VMs smaller and faster. A host can run multiple VM copies and their destruction would not result in any negative effects on the host. Therefore, it is possible to grant students super-user rights on a VM.

The user interface to VMs is realized by a remote desktop access service, VNC [Richardson et al., 1998]. VNC implements a remote frame buffer (RFB)

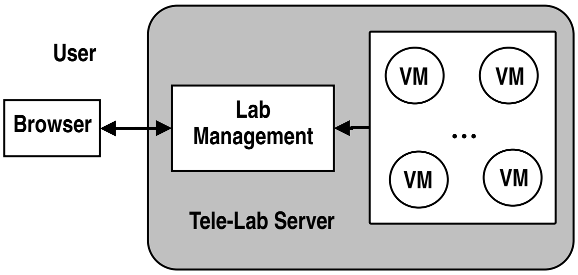


Fig. 2. Tele-Lab Server: a virtual machine based training system

protocol which can collect inputs from a remote client, encodes the desktop updates of the VM, and sends them back to the client. VNC also supports java-applet clients, and then the VNC clients can run inside a browser. Such a thin user interface permits students to access VMs via a standard browser without installing special client software.

Big concerns for running Tele-Lab online are its reliability and security. Firstly, VMs can be corrupted by users who have super-user rights. Second, it is also possible that VMs are converted to an attack station by their users for compromising production networks. Therefore, we developed VM management and security solutions to make Tele-Lab reliable and safe.

The status of VMs and user operations are monitored in real-time and defective VMs will be restored to default settings automatically. Security of Tele-Lab focuses on system and network level isolations which jail users inside the VM and prevent them from accessing production networks. The host OS is protected against intrusions from VM processes by separation between VMs and the host. We have a firewall between a VM and the production networks against network attacks from the VM. Further details about VM management and security can be found in [Hu et al., 2005].

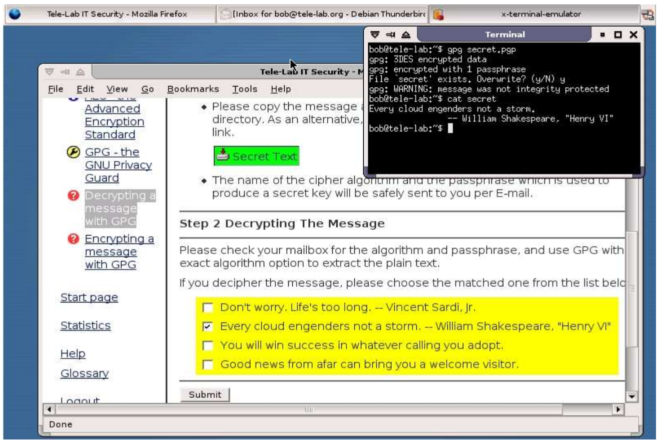
5 Application

Tele-Lab mainly supports learning/teaching cryptography and network security. It can also be adapted for other subjects and user groups. E.g. Tele-Lab can provide exercises for lectures, can be a complete e-learning program, or can be customized for industrial training. The feedback from the students who tried using Tele-Lab shows it was easy to follow theoretical parts and complete most exercises without help of a human instructor. If students are unfamiliar with Linux, some exercises about Linux security (e.g. the iptables firewall) would be a little bit difficult for them. However, other more general exercises can be handled without special Linux skills. E.g secure email exercises only require the skills to use browsers and email clients in a graphical environment. This indicates that the use of Linux as a laboratory platform might bring some difficulties but it is still an effective solution for IT students.

5.1 Example Chapter: Password-Based Authentication

This chapter is about how users are authenticated by passwords and how passwords are protected in Linux. In its exercise, privileged operations are involved. A user needs to crack a Linux passwd file with an open-source cracker, John-the-Ripper. The typical learning process includes following steps:

1. Concepts like password hashing (DES and MD5), "passwd/shadow" file, and advice on strong passwords are introduced.
2. Relevant password tools are presented. They include the "passwd" command, PAM (the Linux "Pluggable Authentication Modules"), and the John-the-Ripper password cracker.
3. In the exercise of password cracking, the work environment is prepared first. The system's password hashing mode is initialized to use DES algorithm.
4. A group of random passwords is generated and saved as a "passwd" file.
5. The user needs to download the "passwd" file and apply a root account for running the system level program, John-the-Ripper.
6. The user switches to the root user mode and runs John-the-Ripper to decode passwords. The user interfaces are shown in Figure 3.
7. After the plain passwords are found, the tutor examines the submission and saves completion records.


Tele-Lab IT Security - Mozilla Firefox
[Inbox for bob@tele-lab.org - Debian Thunderbird
x-terminal-emulator
Terminal
Tele-Lab IT Security - M
File
Edit
View
Go
Bookmarks
Tools
Help
Advanced Encryption Standard
GPG - the GNU Privacy Guard
Decrypting a message with GPG
Encrypting a message with GPG
Start page
Statistics
Help
Glossary
Logout
Secret Text
Submit
Done

```
bob@tele-lab:~$ gpg secret.pgp
gpg: 3DES encrypted data
gpg: encrypted with 1 passphrase
File `secret' exists. Overwrite? (y/N) y
gpg: WARNING: message was not integrity protected
bob@tele-lab:~$ cat secret
Every cloud engenders not a storm.
            -- William Shakespeare, "Henry VI"
bob@tele-lab:~$
```

- Please copy the message
directory. As an alternative,
link.
- The name of the cipher algo
produce a secret key will be safely sent to you per E-mail.

Step 2 Decrypting The Message

Please check your mailbox for the algorithm and passphrase, and use GPG with
exact algorithm option to extract the plain text.

If you decipher the message, please choose the matched one from the list belo

- ☐ Don't worry. Life's too long. -- Vincent Sardi, Jr.
- ☑ Every cloud engenders not a storm. -- William Shakespeare, "Henry VI"
- ☐ You will win success in whatever calling you adopt.
- ☐ Good news from afar can bring you a welcome visitor.

Fig. 3. Tele-Lab user interface

6 Conclusions

Tele-Lab IT-Security provides new media for teaching practical IT security. They allow students not only to learn security concepts and principles, but also to experiment security and gain hands-on experiences in a lightweight and safe laboratory environment. Tele-Lab is not to completely substitute the role of conventional security laboratories, e.g. it is hard to include those exercises which need complicated network environments; Security on Windows platforms has also not yet been addressed. Instead Tele-Lab is to provide more practical features and alternatives to traditional ways. In summary, Tele-Lab is a research attempt to fill the gap between e-learning and practical security training. This work has demonstrated the possibility to implement hands-on security laboratories on the Internet reliably, securely, and economically.

References

[Bishop, 2000] Bishop, M. (2000). Education in information security. IEEE Concurrency, 8(4):4–8.

[Dike, 2001] Dike, J. (2001). User-mode Linux. In Proceedings of the 5th Annual Linux Showcase & Conference, Oakland, California, USA.

[Esslinger, 2002] Esslinger, B. (2002). Cryptool - spielerischer einstieg in klassische und moderne kryptographie: Neue version - fundierte awareness in deutsch und englisch. Datenschutz und Datensicherheit, 26(10).

[Goldberg, 1974] Goldberg, R. P. (1974). Survey of virtual machine research. IEEE Computer, pages 34–45.

[Hu and Meinel, 2004] Hu, J. and Meinel, C. (2004). Tele-Lab IT-Security on CD: Portable, reliable and safe IT Security training. Computers & Security, Elsevier, 23(4):282–289.

[Hu et al., 2004] Hu, J., Meinel, Ch., and Schmitt, M. (2004). Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education. In Proceedings of ACM SIGCSE Norfolk, Virginia, USA 2004.

[Hu et al., 2005] Hu, J., Cordel, D., and Meinel, C. (2005). Virtual machine management for Tele-Lab IT-Security server. In Proceedings of IEEE ISCC 2005, pages 448–453.

[Irvine and Thompson, 2004] Irvine, C. E. and Thompson, M. F. (2004). Expressing an information security policy within a security simulation game. In Proceedings of the Sixth Workshop on Education in Computer Security (WECS6), pages 43–49, Monterey, USA.

[Ragsdale et al., 2003] Ragsdale, D., Lathrop, S., and Dodge, R. (2003). Enhancing information warfare education through the use of virtual and isolated networks. Journal of Information Warfare, 2(3):53–65.

[Richardson et al., 1998] Richardson, T., Stafford-Fraser, Q., Wood, K. R., and Hopper, A. (1998). Virtual network computing. IEEE Internet Computing, 2(1): 33–38.

[Rowe and Schiavo, 1998] Rowe, N. C. and Schiavo, S. (1998). An intelligent tutor for intrusion detection on computer systems. Computers and Education, 31:395–404.

[Schillings and Meinel, 2002] Schillings, V. and Meinel, C. (2002). Tele-TASK - teleteaching anywhere solution kit. In Proceedings of ACM SIGUCCS 2002, Providence, USA.

[Spillman, 2002] Spillman, R. (2002). CAP: A software tool for teaching classical cryptology. In Proceedings of the 6th National Colloquium on Information System Security Education, Redmond, Washington, USA.

[Vigna, 2003] Vigna, G. (2003). Teaching hands-on network security: Testbeds and live exercises. Journal of Information Warfare, 2(3):8–24.