Computer Security in E-Learning

Edgar R. Weippl
Vienna University of Technology, Austria

INTRODUCTION

Although the roots of e-learning date back to 19th century's correspondence-based learning, e-learning currently receives an unprecedented impetus by the fact that industry and universities alike strive to streamline the teaching process. Just-in-time (JIT) principles have already been adopted by many corporate training programs; some even advocate the term "just-enough" to consider the specific needs of individual learners in a corporate setting.

Considering the enormous costs involved in creating and maintaining courses, it is surprising that security and dependability are not yet considered an important issue by most people involved including teachers and students. Unlike traditional security research, which has largely been driven by military requirements to enforce secrecy, in e-learning it is not the information itself that has to be protected but the way it is presented. Moreover, the privacy of communication between teachers and students.

For a long time students and faculty had few concerns about security, mainly because users in academic areas tended not to be malicious. Today, however, campus IT-security is vital. Nearly all institutions install firewalls and anti-virus software to protect campus resources. Even the most common security safeguards have drawbacks that people often fail to see. In Stanford the residential computing office selected an anti-virus program. However, the program can be set to collect data that possibly violates students' privacy expectations; therefore many students declined using it (Herbert, 2004).

Whenever servers that store personal data are not well protected, they are a tempting target for hackers. Social security numbers and credit card information are valuable assets used in identity theft. Such attacks were successful, for instance, at the University of Colorado (Crecente, 2004). A similar incident happened at the University of Texas; the student who committed the crime was later indicted in hacking (Associated Press, 2004).

The etymological roots of *secure* can be found in *se* which means "without", or "apart from", and *cura*, that is, "to care for", or "to be concerned about" (Landwehr, 2001). Consequently, *secure* in our context means that in a secure teaching environment users need not be concerned about threats specific to e-learning platforms and to electronic communication in general. A secure learning platform should incorporate all aspects of security and dependability and make most technical details transparent to the teacher and student. However, rendering a system "totally secure" is too ambitious a goal since no system can ever be totally secure and still remain usable at the same time. The contribution of this chapter is to

- Define and identify relevant security and dependability issues.
- Provide an overview of assets, threats, risks, and counter measures that are relevant to e-learning.
- Point to publications that address the issues in greater detail.

BACKGROUND

While there a many definitions of the primary requirements of *security*, we will start with the classical *CIA requirements*. CIA is the acronym for confidentiality, integrity, and availability. All other requirements can be traced back to these three basic properties. Confidentiality is defined (Avizienis, Laprie, Randell, & Landwehr, 2004) as *the absence of unauthorized disclosure of information*, integrity as *the absence of improper system alterations* and availability as *readiness for correct service*.

Dependability is a broader concept that encompasses all primary aspects of security save confidentiality:

- Availability
- Reliability refers to the continuity of correct service
- Safety is defined as the absence of catastrophic consequences on the user(s) and the environment
- Integrity
- Maintainability is the ability to undergo modifications and repairs

For many universities e-learning systems have become production critical assets. It is therefore essential that all of the aforementioned generic requirements are evaluated during a process of risk assessment. The first step in such a process is to understand security and dependability as enabling technology. Only when systems work reliably will users trust and use them.

The obvious ultimate goal of an assessment is to implement cost-effective controls to avoid faults. Looking at all possible threats of a given application and subsequently mitigating the most important ones is a process that is called *threat modeling* (Swiderski & Snyder, 2004). The first step is to *decompose* the application and to determine how data is processed. This can best be done by creating data flow diagrams (Baskerville, 1993).

The second step is to *enumerate all threats*. There are eight dimensions along which faults can be categorized (Avizienis et al., 2004). Even though it is not required to categorize threats in this stage the eight dimensions are helpful to cover many different aspects and to avoid forgetting some.

1. **Phase of Creation:** Development faults vs. operational faults
2. **System Boundaries:** Internal faults vs. external faults
3. **Phenomenological Cause:** Natural faults vs. human-made faults
4. **Dimension:** Hardware faults vs. software faults
5. **Objective:** Malicious faults vs. non-malicious faults
6. **Intent:** Deliberate faults vs. non-deliberate faults
7. **Capability:** Accidental faults vs. incompetence faults
8. **Persistence:** Permanent faults vs. transient faults

The third step is to *rank the threats* according to the probability and potential damage. The forth and final step is planning and implementing *mitigation strategies* (Swiderski & Snyder, 2004).

RELEVANCE TO E-LEARNING

In this section we will first look at all requirements and highlight typical threats that are relevant in the context of e-learning. The final subsection highlights solutions and points to publications that address specific areas in greater detail.

Requirements

Availability

Attacks by insiders on servers delivering e-learning content are not as likely as on servers used for examinations. Students are in general interested in learning and will thus have little incentive to actively attack the system; non-malicious faults, however, might still occur. Obviously this does not mean that students will never attack an e-learning system used for studying, but examination systems are certainly more attractive targets. During learning, availability is not as important as, for instance, during online exams. A downtime of a few hours is acceptable for content servers but clearly not for exam servers.

For exams, the threat profile is different because students are likely to attack the system once they realize they might fail the exam. If they could crash the server their exams cannot be graded and they will have a second chance. Even if students cannot crash the server they might try to attack the availability of the local PC they use during the exam. Briefly unplugging it will cause a reboot and give them a good excuse for not being graded.

Reliability

When exams or assignments are graded automatically reliability is important; while multiple choice questions can be evaluated easily, reliability is more difficult to address the more sophisticated the evaluation algorithm is.

Keyword-based grading of free text answers will generally work well for technical exams that require precise answers but not for subjects with long and very free answers such as studies of literature.

Safety

In most cases there will be very little safety considerations required when introducing e-learning programs unless the subject taught is inherently critical. For instance, wrong instruction on how to operate certain machinery will in consequence create safety hazards once people operate the machinery.

Confidentiality

In many cases confidentiality is not a major requirement when creating e-learning content. The knowledge taught is generally widely available in text books. It is the way the content is presented and the effort of creating simulations and other interactive learning environments that are worth protecting.

For exams and assessments, confidentiality, however, is essential. Exam questions need to be kept secret until the exams commences; the correct answers need to be concealed until the exams are handed in.

Even if learning content contains few secrets, there are still elements that require protection against unauthorized read access. Discussion boards and forums are commonly used not only to discuss organizational issues