Chapter 6.2
Security and Privacy Management for Learning Management Systems

Wolfgang Hommel
Leibniz Supercomputing Centre, Germany

ABSTRACT

Once a prototype for a Learning Management System (LMS) has successfully been set up and tested, the demand for putting it into production use rises. However, seamlessly integrating an LMS into existing data center infrastructures is a challenging task whose complexity is often underestimated. In this chapter we take a risk-driven approach ("what could go wrong?") to discuss the real-world operation of a fully-featured LMS from the perspective of security and privacy management. First, the authors analyze their LMS-specific security goals and the related threats to LMS components. They then investigate how an LMS security policy should be established and which technical controls can be used for implementation, enforcement, and auditing by the LMS administrators as well as by the system and network administrators. Finally, the authors discuss the benefits of inter-organizational LMS usage when it is based on identity federation technologies, and the new security and privacy challenges it brings.

MOTIVATION

Projects to establish E-Learning typically start with a strong focus on content and suitable didactical methods for the delivery of the carefully crafted learning material. This obviously is a commendable approach because it prioritizes both the learners' and the instructors' requirements, and thus results in a system that addresses the users' needs. However, it also often leads to an evolutionary growth of the Learning Management System (LMS) infrastructure. For example, additional web servers are often not considered before a downtime caused by hardware failure leads to a first wave of user complaints. Once we have achieved hardware redundancy, we might figure

DOI: 10.4018/978-1-4666-0011-9.ch6.2

out that the new stand-by machine is not used during usage peaks, and so we rather need a load balancing solution – which, of course, must not only span the web servers, but also the backend, e.g. the streaming and the database servers. In a nutshell, building an LMS prototype, which lets us concentrate on the software and our E-Learning project goals, and operating a fully-featured LMS in a production environment are completely different tasks.

This chapter deals with two specific aspects that we need to keep in mind from the very beginning when we plan to put our LMS into production use and subsequently enter the operation phase: security and privacy. Security is at stake because an enhanced and feature-rich LMS is a complex distributed system and – as we will see – a lucrative target for various types of attackers. Privacy protection must not be neglected because various LMS functionalities, e.g. personalization and authorization based on information about the learner's study course and study progress, depend on sensitive personally identifiable information (PII).

Security and privacy have many facets, and the regulatory requirements – such as country- and state-specific data protection laws – as well as the measures that are necessary to achieve high user acceptance are, to a large degree, specific to each individual scenario. Thus, we cannot present an one-fits-all solution to LMS security and privacy here. Instead, we discuss successful best practices that provide guidance for the security and privacy aware implementation, deployment, and operation of real-world LMS infrastructures.

We will initially investigate which technical components an LMS is typically composed of. This is a prerequisite for the following discussion of LMS security risks, based on the attack surfaces of these components and the various LMS-specific threats, including a broad range of potential attackers, their motivation and sophistication, and their means. We will then see that security and privacy are twofold: On the one hand, there are measures required on the management level, such as specifying an LMS security policy. On the other hand, technical controls must be applied to prevent, detect, and react to attempted or successful attacks. We will discuss both types of measures under the assumption that the LMS is not a green field experiment, but shall rather be seamlessly integrated into an existing information and communication technology (ICT) infrastructure, e.g. the one provided by a university's computing centre or a company's IT department.

Furthermore, we discuss the upcoming inter-organizational usage of LMS infrastructures. Modern technologies, such as Federated Identity Management, allow us to selectively grant LMS access to external users, e.g. other universities' students, without requiring a manual or self-registration-based creation of local LMS accounts. We discuss the benefits of this technology for higher education institutions as well as for 3rd party LMS hosting services and learning content providers. After an overview of the technical aspects, we will discuss the new security and privacy challenges such scenarios introduce and show the tools that can be used to deal with them successfully. Finally, we will give an outlook to security and privacy topics LMS researchers and practitioners will have to address in the next few years.

SECURITY AND PRIVACY GOALS IN LMS INFRASTRUCTURES

If there was only one thing we should keep in mind about security and privacy, then it would be that neither of them is a feature that can easily be added to an already existing system at runtime. Instead, security and privacy must be integrated into the overall design from the very beginning in order to work properly and be efficient: Neither implementation nor configuration tricks can make up for a bad architectural design. Getting the design right requires that we know what we have to protect, and which threats we actually