Building Trust for Interactive E-Learning

Yuefei Xu
National Research Council Canada, Canada

Larry Korba
National Research Council Canada, Canada

INTRODUCTION

Learners, tutors and service providers are the basic players in an e-learning system. Similar to the situation in traditional campus education, "trust" composes the interaction baselines between each of these players. Although the establishment processes are different, the requirements and importance of "trust" are the same whether the situation is traditional education or remote e-learning.

"Trust" is one of the most important factors for the success of interactive e-learning applications. This chapter points out the primary trust challenges among learners, tutors and service providers. Then we introduce the trust mechanisms applied for interactive e-learning. The technical difference and application trends are discussed before the conclusion.

BACKGROUND

In interactive e-learning systems, learners interact with tutors via the support of service providers in a "virtual campus." Trust relationships are required between each of them. For instance, providers need to create trust relationships with learners and tutors. Because a user may come from anywhere on the Internet, one provider must make trust decisions, determining whether the user is eligible for the e-learning service and then what resources the user may access. Based on the created trust relationships between the provider and the user, appropriate authorization and monitoring are imposed on the user to facilitate interactive studying or teaching.

The learner also must trust in the provider and other partners as well, otherwise the learner will not use the e-learning system. Typical situations exemplifying the need for trust include when the learner: enters personal information on a Web page; makes online payments (secure payment); and participates or completes in an online test (fair testing, no cheating and accurate storage of results).

Furthermore, privacy also is an important factor that influences the creation of trust relationships and then interactive learning processes. Not only do people have different preferences for their privacy, service providers have certain obligations to meet requirements of current and new privacy acts. For any action involving a learner's personally identifiable information, the learner must be able to control what information is revealed to other parties, including service providers, tutors, classmates or outside third parties. For example, an institutional registrar can request a learner's full name, birth date and address for identification purposes, but no data regarding the learner's study behaviors and preferences; a tutor may have access to what courses a student has studied, and possibly some of the student's performance, but no other information—for instance, pertaining to the student's age or current career. A classmate may know with whom he is talking, but not the location of his partner.

It is clear to see that the trust-related decision making occurs throughout the whole interactive e-learning process. Just imagining the scenarios in traditional physical education, people can easily realize that "trust" will not only provide the base for interactive e-learning, but also increase a student's levels of motivation and aspiration to learn. The characteristic of fine-grained trust control will be a significant feature for the next generation of e-learning systems. In other words, "trust" will be one of the most crucial factors for the success of an interactive e-learning system.

MECHANISMS FOR BUILDING TRUST

Trust has been one of the emerging research topics in the field of information security. It absorbs many researchers, resulting in a series of published research papers in recent years (Mass, & Shehory, 2001). The most common trust mechanisms being researched and implemented are digital certificate-based approaches and policy-based trust management systems.

Digital Certificate-Based Trust Mechanisms

Digital certificate-based trust mechanisms are based on the belief that certificates represent a trusted party. The key concept behind these mechanisms is the digital certificate. A digital certificate is an electronic file containing data for establishing credentials for transactions. A Certification Authority (CA) issues a digital certificate to identify whether a public key truly belongs to the claimed owner. Two of most common approaches in use today are based on X.509/PKIX and Pretty Good Privacy (PGP) specifications.

X.509/PKIX was proposed by the IETF PKIX Working Group (Public-Key Infrastructure, 2004). This specification defines a framework for the provision of authentication services. X.509/PKIX is a hierarchically structured Public-Key Infrastructure (PKI), rooted in a Root Certificate Authority (RCA). In this hierarchical structure, trust begins at the root and is transferred hierarchically to all users in the network via CAs.

Phil Zimmermann, the creator of PGP, proposed PGP in 1991. PGP has become a well-known e-mail privacy application in the Internet community (An Open Specification for Pretty Good Privacy, 2004). It provides a way to enable users to digitally sign and encrypt information without the overhead of a PKI infrastructure. In PGP, anyone can decide whom to trust. Unlike X.509/PKIX certificates, which are issued from a formally setup and maintained CA, PGP implements a mechanism called a "Web of Trust," wherein multiple key-holders sign each certificate, attesting the validity of the certificate.

Policy-Based Trust Mechanisms

Policy-based trust management systems provide another solution for flexible and user-controlled mechanisms for building trust. These systems use standard frameworks or models that specify and interpret trust-related policies, credentials and entity relationships. Detailed rules and labels implement fine-grained information and service control. Here we briefly overview three policy-based trust management application systems: REFEREE (Chu, Feigenbaum, LaMacchia, Resnick, & Strauss, M., 1997), KeyNote (Blaze, Feigenbaum, Ioannidis, & Keromytis, 1999) and Policy Negotiation-Based Trust Model (Xu, & Korba, 2002).

Chu et al. (1997) suggested a trust management system called REFEREE (Rule-controlled Environment for Evaluation of Rules and Everything Else) for making access decisions relating to Web documents. REFEREE was developed by Yang-Hua Chu based on an earlier system, called PolicyMaker (Blaze, Feigenbaum, & Lacy, 1996). REFEREE uses PICS labels (Resnick, & Miller, 1996) to specify properties of an Internet resource. This system introduces the idea of "programmable credentials," which examine statements made by other credentials and fetch information from the network before making trust decisions.

Blaze et al. (1999) described a system called KeyNote to specify and interpret security policies, credentials and entity relationships. The five key components in this system are (a) 'Actions'—the operations with security consequences that are to be controlled by the system; (b) 'Principals'—the entities that can be authorized to perform actions; (c) 'Policies'—the specifications of actions that principals are authorized to perform; (d) 'Credentials'—the vehicles that allow principals to delegate authorization to other principals; (e) 'Compliance Checker'—a service used to determine how an action requested by principals should be handled, given a policy and a set of credentials.

Xu et al. (2002) described a Policy Negotiation-Based Trust Model for fine-grained security and privacy control on e-learning interactions. This model extended the trust model in comparison to the earlier models by considering security and privacy con-