Available online at www.sciencedirect.com
ScienceDirect
Computers & Education 48 (2007) 1–16
COMPUTERS & EDUCATION
www.elsevier.com/locate/compedu

A PKI approach for deploying modern secure distributed e-learning and m-learning environments

Georgios Kambourakis [a,*], Denise-Penelope N. Kontoni [b], Angelos Rouskas [a], Stefanos Gritzalis [a]

[a] *Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos, Greece*
[b] *Department of Civil Engineering, Technological Educational Institute of Patras, 1 M. Alexandrou St., Koukouli, Patras GR-26334, Greece*

Received 11 June 2004; accepted 13 October 2004

Abstract

While public key cryptography is continuously evolving and its installed base is growing significantly, recent research works examine its potential use in e-learning or m-learning environments. Public key infrastructure (PKI) and attribute certificates (ACs) can provide the appropriate framework to effectively support authentication and authorization services, offering mutual *trust* to both learners and service providers. Considering PKI requirements for online distance learning networks, this paper discusses the potential application of ACs in a proposed trust model. Typical e-learning trust interactions between e-learners and providers are presented, demonstrating that robust security mechanisms and effective trust control can be obtained and implemented. The application of ACs to support m-learning is also presented and evaluated through an experimental test-bed setup, using the general packet radio service network. The results showed that AC issuing is attainable in service times while simultaneously can deliver flexible and scalable solutions to both learners and e-learning providers.

Keywords: Architectures for educational technology system; Distance education and telelearning; E-learning; M-learning; Trust; Security; Public key infrastructure

* Corresponding author.
E-mail addresses: gkamb@aegean.gr (G. Kambourakis), kontoni@teipat.gr (Denise-Penelope N. Kontoni), arouskas@aegean.gr (A. Rouskas), sgritz@aegean.gr (S. Gritzalis).

0360-1315/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compedu.2004.10.017

1. Introduction

In recent years, distance learning systems (DLS) have become one of the most significant and promising platforms to fulfill the vision for wide-range, life-long training to a wide variety of audiences. In a distance learning scenario, learners are not required to attend classes on a regular basis. Nearly all contacts between them and the teaching organization are carried out by conventional or modern telecommunication infrastructure, even if some tutoring activities may take place in a face-to-face condition.

The term "m-learning" has lately emerged and is associated with the use of mobile technology in education. In this paper, this term is considered as *"The point at which mobile computing and e-learning intersect to produce an anytime, anywhere learning experience"* as quoted in (Harris, 2001).

Trust is an important factor in either traditional face-to-face education or in distance learning procedures and especially in interactive and distributed e-learning. Mutual trust between the learner and the e-learning provider is vital and has to be correctly established to provide the appropriate level of confidence and assurance to both sides. For instance, the learner needs to trust the provider and his procedures, restricting access only to that sensitive personal information authorized by the user. On the other hand, the e-learning provider has to deploy and support reliable authentication, authorization and accounting (AAA) mechanisms, which certify that the user accessing the provider's network is someone authorized for the particular service. The trust levels also substantially affect user's motivation or aspiration for learning. Students and teachers, who take part in an impersonal distributed e-learning or m-learning environment, have to enjoy respect, autonomy and reliance to become a trouble-free working party for their learning and teaching activities (Clark & Mayer, 2002; Horton, 2000).

Trust is a central research topic in information security research and it gains increasing attention over the years. At the same time, e-learning services are spreading fast and are gradually enjoying universal acceptance. Nevertheless, very few papers attempt to blend trust issues with e-learning or m-learning applications. The rapid increase of the number of users taking part in e-learning services, results in a many-to-many trust model. As a result, existing security schemes in current e-learning systems e.g. symmetric key techniques like passwords and pre-shared secrets/keys, are inadequate and there is an urgent demand to provide more flexible, configurable and scalable security mechanisms that can self-adjust as fast as e-learning or m-learning systems evolve.

A public key infrastructure (PKI) (Adams & Lloyd, 1999; Nash, Duane, Joseph, & Brink, 2001; PKIX WG, 2004) is an all-encompassing security infrastructure whose services are implemented and delivered using public-key concepts and techniques. Attribute certificates (ACs) (Farrell & Housley, 2002; Oppliger, 2002; Oppliger, Pernul, & Strauss, 2000), have been suggested by the Internet engineering task force (IETF) PKI Working Group as an alternative to and better than X.509 public key certificates (PKCs) (ITU-T, 1997), for carrying authorization information. Attribute authorities (AA) bind the characteristics of an entity (called attributes) to that entity by digitally signing the appropriate AC. Attributes can specify group membership, role, security clearance, or other authorization information associated with the AC holder. Therefore, ACs can be used for controlling access to system resources and employing role-based authorization and access controls policies accordingly (Oppliger et al., 2000). ACs are theoretically similar to privilege access certificates (PACs), as used in SESAME (Vandenwauver, Govaerts, & Vandew-