Multi-Agent Security Service Architecture for Mobile Learning

Mariana Hentea, Purdue University Calumet, Indiana

ABSTRACT

M-learning continues and extends the learning paradigms and styles derived from a classroom lecture-and-seminar model, now made accessible through Web-based delivery and mobile devices. In an environment, in which circumstances make using a laptop inappropriate, a handheld device offers a convenient alternative. Communicating with *anything* and *everything* via wireless can open new opportunities for individuals looking for easy electronic access, navigation, mobility to access the education information *anywhere* and *anytime*. However, managing security for m-learning users is one of the more challenging aspects.

The paper dis cusses a multi-agent high-level architecture for the security service. The proposed model is based on ontologies and a mediator for security service agents. Ensuring security of communication and privacy via a cooperative set of services is important for both consumer and m-learning environment. The proposed model for security service architecture is supporting the intelligent security management in the sense that can more accurately work at the human conceptual level.

Key words: security service, mobile learning, mobile computing, wireless, ontology.

MOBILE LEARNING OVERVIEW

Internet changed the way we communicate and conduct our daily life. A storm evolution for adding mobility to access Internet and information *anywhere* and *anytime* is taking place in wireless technology and the results are already visible. Wireless is not being just an adjunct but an integral part of and merges with the Internet. Implementing the wireless based technology infrastructure to support a high performance learning environment for in campus and distance education is a significant issue for universities seeking to broaden their audience. Communicating with *anything* and *everything* via wireless can open new opportunities for individuals looking for easy electronic access, navigation, mobility to access the education information *anywhere* and *anytime*. Communicating *with anything* and *everything* via wireless opens new business drivers for the universities to support global economy and individuals seeking opportunities for education.

The elements of distance education include policy, people, and technologies. The technologies used in distance education can be classified as the following:

- Communication technologies that include computer and network infrastructure (hardware and software), broadband, wireless, multimedia, distributed systems, and mobile systems.
- Intelligent technologies that include intelligent tutoring, artificial neural networks for behavior analysis, authentication mechanisms, soft computing, and visual computing.
- Educational technologies that include practical and new learning models, automatic assessment methods, effective and efficient authoring systems.

The development of new educational services, and advances in educational technology, these driving forces, while not independent of each other, each shapes the architecture and infrastructure evolution in a different way [1].

Experiments of using handheld computers such as Personal Digital Assistants (PDAs) in classroom demonstrate new opportunities in education [5] [7] [17]. Wireless networks and mobile computers are two Information and Communications Technology (ICT) that are impacting educational institutions worldwide [9]. The intersection of online learning and mobile computing is called mobile learning or m-learning [12]. This promises to offer frequent, integral access to applications that support learning *anywhere, anytime*. M-learning continues and extends the learning paradigms and styles derived from a classroom lecture-and-seminar model, now made accessible through Web-based delivery. In an environment, in which circumstances make using a laptop inappropriate, a handheld device offers a convenient alternative.

Future classrooms are likely to be organized around Wireless Internet Learning Devices (WILD) that include graphing calculators, Palm, Pocket-PC, cell phones, and other handhelds connected by wireless networks [6] [13] [15]. A

0-7803-8625-6/04/$20.00 ©IEEE

few of the advantages include mobility, beaming or sharing of the information and communications, the personalization of student work including the empowerment of each individual having a learning tool under his or her own control.

MOBILE COMPUTING

RIDEE is a distance educational supporting platform for performing real-time and interactive distance educational activities over a high-speed network [4]. RIDEE demonstrates that every one can join a distance education activity with its own information processing equipment such as personal computer, a PDA or a cellular phone. Users of m-learning applications based on handhelds recommend improvements such as better user interface, screen size, security and privacy, energy management, etc. [11].

The major issue to using the handhelds included inappropriate use (especially of beaming), technology management issues (particularly synchronization issues), usability issues (long text input) and equipment damage [7]. In addition, the mobile devices may thus lack certain services for reasons of efficiency or accidental omission [14]. Specifically, one issue is secure access and privacy. Managing privacy in the network is one of the more challenging aspects of wireless location privacy [8].

SECURITY SERVICE REQUIREMENTS

Before allowing a participant (lecturer, student, or presenter) to attend the seminar with their own computer or device, it is necessary to verify compliance to security such as access verification or authentication. The connection depends on the system and user's device and procedures to handle the connection setup, quality of communication, and wireless security assurance. Because wireless networks broadcast data on the open airways, wireless networks present unique challenges for authentication mechanisms not encountered on wired networks. Since wireless networks are different from wired networks with regard to authentication, the authentication methods should be designed specifically around the needs of wireless networks and users of the wireless application.

The authentication methods include public key certificate-based methods, the password methods, and the strong passwords. However, m-learning applications have specific needs such as the following:

a. Mutual authentication (authenticator must authenticate the user, but the user must be able to authenticate the authenticator as well).
a. Authenticates the user rather than the user's device. A simple secret that can easily be remembered by the user.
b. Quick and efficient with a minimal amount of computing resources
c. Low maintenance cost and easy to administer. For example, a method that requires the installation of a certificate on each user device, for example, is not easy to administer. Maintenance of certificate revocation lists can be a costly burden for the network administrators in a university with the continuous registration of students for distance learning classes or completion of the classes.
d. Convenient for users such as using a certificate stored on a device, though, burdensome to administrators, is convenient to users.

However, commercial entities are adept at concealing questionable requirements and practices with fine print in a service contract or click-wrap agreement.

SECURITY SERVICE BASED ON MULTI-AGENTS ARCHITECTURE

To support a scalable ubiquitous communications and computing system, the systems should support security features [16] that can be carried by agents:

a. Privacy conscious – give users maximum control over their incoming communication and the amount of information about their context that is revealed to others; construct privacy profiles to restrict delivery of the information (by location, content, time of day, or subscriber with some factors of mutuality to be factored)
b. Access control – authentication, explicit registration, obtaining a shared secret, or use of physical tokens such as swipe or smart cards; or second mechanism employing cross-domain authentication, authorization, and accounting.

One advantage of Web-based learning is its openness. Everyone on the Internet can participate in the learning and education process at any time they like. Traditional computer-aided instruction (CAI) systems based on client-server

architecture cannot cope with this requirement. A mediator-based architecture for Web-based education to build open multi-agent applications for eLearning is discussed in [2].

A mediator is an information-producing or serving entity in a large scale internetworked environment [3] acting as middle man to take as input, a request to find an agent that provides a security service, and returns as output, a list of such agents and their cooperation relationships. A mediator also stores the services offered by different agents in the existing environment, and when a new agent is introduced into the environment, it can register its capability to the mediator, using an agent service description language such as WSDL(Web Service Description Language) [19].

In addition, the Web Ontology Language (OWL) [20] defines the terms used to describe and represent an area of knowledge. Ontologies are critical for applications on the Web that need to search across or merge information from diverse communities. Security service information can be described using ontologies and security information can be exchanged via ontologies. Ontologies enable the semantics to be used by Web applications and intelligent agents. Using ontologies the security service management can be intelligent in the sense that can more accurately work at the human conceptual level. In m-learning environment, it is necessary to have a construct model for the automation of security service that supports discovery, marketing, and brokerage capabilities.

Figure 1 depicts the high-level architecture for the security service. The proposed architecture for security service model is based on a mediator for security service agents and OWL. Agents are developed over the Internet with heterogeneous architecture, and their functions vary from one to another. Due to the diversity of agents, the requests of services also vary. In most cases, we cannot expect that for a service request there is at least one agent to exactly provide that service, even though we suppose the service advertisement and request can fully express what the services are.

Mediating is a process that utilizes the knowledge on security service domain to introduce service providers and consumers. Mediating the security services is a high-level matching and brokerage, in terms of level of knowledge applied, and directions of information flow. Multiple matching strategies based on agent service ontology help agents finding appropriate service providers. The series of strategies consider various features of service providers, the nature of requirements, and more importantly the relationships among services.

For example, access mediation agents act as intelligent signaling firewalls. The enhanced security offered through access mediation mitigates the risks of inadvertent or malicious disturbances. Access mediation agents should be transparent. Access mediation agents should govern how the network can be used through policy-based enforcement. This type of enforcement should be interconnection specific. And each rule should determine how in-depth each message is examined. The level of detail must be configurable since each interconnection may require different levels of analysis depending on the types of traffic it carries.

Agents deal with the following: collection of security provider's information, security management, security compliance and analysis, consumer's profile, understand the m-learning environment, security service handling, and communication with the consumers. The agents may have different specific roles as follows:

- Marketing agent – supports security service advertisement
- Brokerage agent – supports billing and payment
- Ask agent – sends inquiries about m-learning security services, records the inquiries history
- Recommend agent – supports the dialog with the consumer and replies to the consumer
- Register agent – supports authentication and gets first-time access
- Verify agent – carries the management of security policy suitable for the consumer which is offered by the marketing agent (understands the m-learning environment).
- Collection of provider's information agent – gets the information of security services and details for handhelds, networks, changing this information into parameters in order to communicate it and make the analysis
- Understand the m-learning environment – makes various judgments and gives order to other agents
- Consumer's profile – collects information related to consumer's needs, environment, and location.

Consumers are the users (student, instructor, facilitator) of m-learning application.

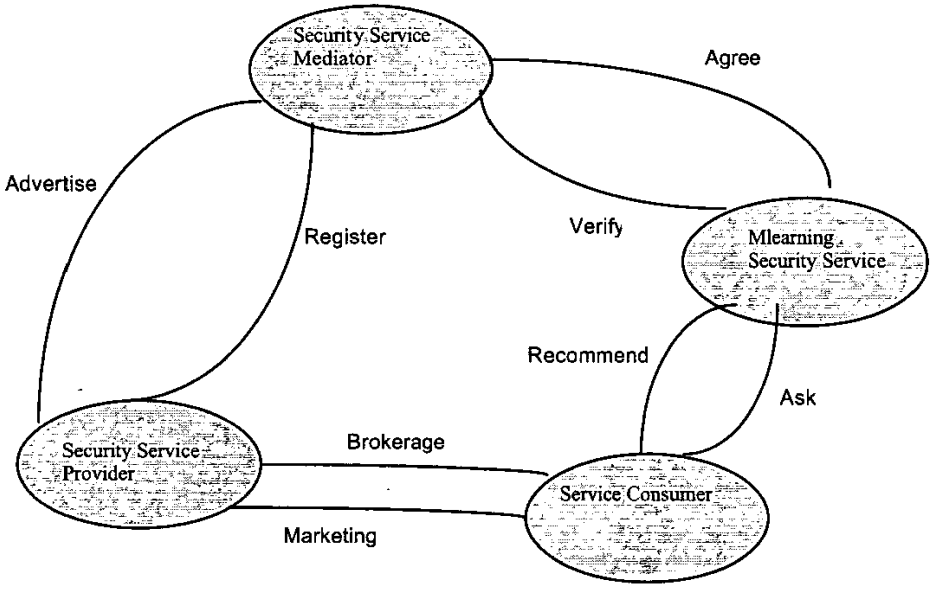

Figure 1 – Security Service Mediation

CONCLUSION

The introduction of wireless infrastructure promises improvements to the quality of distance education. Ensuring security of communication and privacy via a cooperative set of services is important for both consumer and m-learning environment. The proposed model for security service architecture is supporting the intelligent security management in the sense that can more accurately work at the human conceptual level. The question is whether providing security service would result in improved features and/or improved proficiency with technologies for m learning. However, more work is needed to refine the process and agents learning patterns to bring out more information for the future intelligent security management.

REFERENCES

1. Hentea, M, Shea, M.J., Pennington, L., "A Perspective on Fulfilling the Expectations of Distance Education", Fourth Conference on Information Technology Curricula (CITC IV), October 2003, Purdue University, West Lafayette, Indiana.
2. Lu, H., "Open Multi-Agent Systems for Collaborative Web-Based Learning", International Journal of Distance Education Technologies", Vol. 2, No.2, April-June 2004, pp. 36-45.
3. Dao, S., Perry, B., "Information Mediation in Cyberspace: Scalable Methods for Declarative Information Networks", Journal of Intelligent Information Systems, 6(23), 1996, pp. 131-150.
4. He, A., Zhang, G., Cheng, Z., "A Design of Real-time and Interactive Distance Education Environment", International Journal of Distance Education Technologies", Vol. 2, No.2, April-June 2004, pp. 1-12.

5. Brunswick, M.J., Hentea, M., "A Perspective on Wireless Networks for Education", ITRE 2003, August 2003, Newark, New Jersey.
6. Roschelle, J., Pea, R., "A walk on the WILD side: How wireless handhelds may change computer-supported collaborative learning", 2002, International Journal of Cognition and Technology, 1(1), pp. 145-168.
7. Wangeman, P., Lewis, N., Squires, D.A., "Portable Technology Comes of Age The Utilization of Handhelds in A Pilot Teacher Education Program", THE Journal, November 2003, Vol. 31, No.4, pp. 26-32.
8. Schilit, B., Hong, J., Gruteser, M., "Wireless Location Privacy Protection", IEEE Computer, Decemb er 2003, Volume 36, No. 12, pp. 135-137.
9. Davies, J. et al., "Implementing a Mobile Lab in a Faculty of Education", THE Journal, Octomber 2003, Vol. 31, No. 3, pp. 29-35.
10. Alexandria College
11. Myers, B.A., Beigl, M., "Handheld Computing", IEEE Computer, September 2003, Vol. 36, No.9, pp. 27-29.
12. Tatar, D., Roschelle, J., Penuel, W.R., "Handhelds Go to School: Lessons Learned", Myers, B.A., Beigl, M., "Handheld Computing", IEEE Computer, September 2003, Vol. 36, No.9, pp. 30-37.
13. Raghunath, M., Narrayanaswami, C., Pinhanez, C., "Fostering a Symbiotic Handheld Environment", IEEE Computer, September 2003, Vol. 36, No.9, pp. 56-65.
14. Medvidovic, N., Mikic-Rakic, M., Malek, S., "Software Architectural Support for Handheld Computing", IEEE Computer, September 2003, Vol. 36, No.9, pp. 66-73.
15. Barolli, L., Koyama, A., "A Distance Learning System for Delivering Appropriate Studying Materials and Stimulating Learner Volition", International Journal of Distance Education Technologies", Vol. 2, No.1, January-March 2004, pp. 1-17.
16. Schulzrine, H., Berger, S., "Ubiquitous Computing in Home Networks", IEEE Communications Magazine, November 2003, Vol. 41, No. 11, pp. 128-135.
17. Savage, P., "The Perfect Handheld: Dream On", IEEE Spectrum, January 2003, Vol. 40, No. 1, pp. 44-46.
18. http://www.wirelessdevnet.com/news/2003/169/news7.html
19. http://www.w3.org/TR/wsdl
20. http://www.w3.org/2001/sw/WebOnt/.