International Conference on Computer Supported Cooperative Work in Design

Portable Devices of Security and Privacy Preservation for e-Learning

Jianming Yong[1] Jiuyong Li[2] Hua Wang[3]
[1]*School of Information System, Faculty of Business*
University of Southern Queensland
Toowoomba QLD 4350,AUSTRALIA
Email:yongj@usq.edu.au
[2]*School of Computer and Information Science,*
University of South Australia, Mawson Lakes
Adelaide, Australia, 5095
Email: jiuyong.li@unisa.edu.au
[3]*Department of Mathematics and Computing,*
University of Southern Queensland,
Toowoomba, Australia 4350
Email: hua.wang@usq.edu.au

Abstract

This paper systematically addresses the security and pricacy concerns for e-learning systems. An effective architecture of e-learning system is proposed for a thorough overview on security and privacy issues related to current e-learning systems. This paper further examines the relationship among security & privacy policy, available security & privacy technolongy, and the degree of e-learning privacy & security. This paper significantly contributes to the knowledge of e-learning security & privacy research communities and will generate more research interests in this regard.

Keywords: E-learning, Security, Privacy Preservation, Security and Privacy Architecture

1. Introduction

E-learning has become a very important means to acquire required education. E-learning system has the capacity to allow all portable devices to access. With more and more people have portable devices, like personal data assistants (PDA), mobile phones, lap-top computers, pocket computers, etc. With the involvement of all types of portable devices, e-learning system will become a ubiquitous platform for the future education. At the same time, because all sorts of portable devices will be allowed to access e-learning system anytime and anywhere, one of biggest challenges is how to effectively mitigate the concerns on security and privacy of portable devices which are used by e-learning users to access e-learning systems. It is obvious that current mechanism of security and privacy for e-learning systems can not be effectively applied because of the universal access by these portable devices. So far there are extensive researches conducted on the security and privacy in general. But there is less specific research on the security and privacy issues for e-learning systems. This paper will address the security and privacy issues for current e-learning systems and further investigate the mechanism of security and privacy for the portable devices of e-learning systems.

This paper is organised as the follows. Section 2 discusses related work form both policy and technology perspectives. Section 3 illustrates a generalised e-learning architecture model. Section 4 further details the security and privacy issues on each layer. Section 5 presents a simplified modeling relationship among policy, technology, and the degree of e-learning security & privacy. Section 6 concludes the paper and initiates some further research perspectives.

2. Related work

The general concern of security and privacy for e-learning system is partially addressed in [1]. Some access control technologies [2, 3] can be used in the general e-learning systems. As the privacy is becoming one of major concerns for any open systems, some techniques of privacy preservation were proposed and designed to the research communities. Like in [4], the privacy preservation was discussed for the general data

mining domain. In [5], the challenge of security and privacy for open and dynamic environment was addressed from both policy and technology perspectives. In [6], the privacy of wireless location was addressed. Based on the current research, there are two general categories to address the security and privacy concerns: category 1 is about policy and management, like [5, 6, 9, 12]; category 2 is about technical solutions, like [7, 8, 10, 11, 13].

Based on category 1, it is essential to fully understand the standards, legislation, law, policy, and regulation, which have a decisive impact on the security and privacy. Normally the relationships among governments or their agents, organisations, individual users are explored to address the concerns of security and privacy and these researches are usually conducted by the discipline of information systems.

Based on category 2, it is import to find the technical solutions for the security and privacy. Like RBAC [2], it is a solution for system access control. Like generalization [14] and OLAP [15], they are effective approaches to preserve the privacy of sensitive data when mining on database systems. These researches are extensively conducted by the discipline of computer science and software engineering.

So far there is limited specific research on security and privacy of portable devices which are used in the ubiquitous e-learning systems. In order to fully demonstrate the security and privacy challenges over the portable devices, we show the architecture of e-learning systems with portable devices in the following section.

3. E-learning architecture with portable devices

As everyone can almost afford to have a portable devices, like mobile phone, PDAs, lap-top computer, palm computer, etc, it is essential for e-learning system to fully support the users who have their portable devices to effectively conduct the e-learning activities via their portable devices. With the interactive involvement of portable devices, e-learning systems become a kind of ubiquitous computing platform for all e-learning users. In order to explicitly show this ubiquitous e-learning platform, we need a generalised architecture for e-learning systems with a full support to portable devices to illustrate the components of e-learning. Figure 1 shows the architecture of e-learning systems with a full support to portable devices.

There are five layers: Layer 1: Core e-learning system, Layer 2: Intra e-learning system, Layer 3: Extra e-learning system, Layer 4: E-learning system extension, Layer 5: Portable devices.

Layer 1: Core e-learning system consists of the core computing platform, including hardware and software. At this layer, there are required high-performance servers to provide enough computing capacity to effectively run e-learning systems, like:

- WebCT[www.webct.com/],
- Blackboard[www.blackboard.com/us/index.Bb],
- eCollege[www.ecollege.com/index.learn],
- Sakai[www.sakaiproject.org/],
- Moodle[www.moodlerooms.com/].

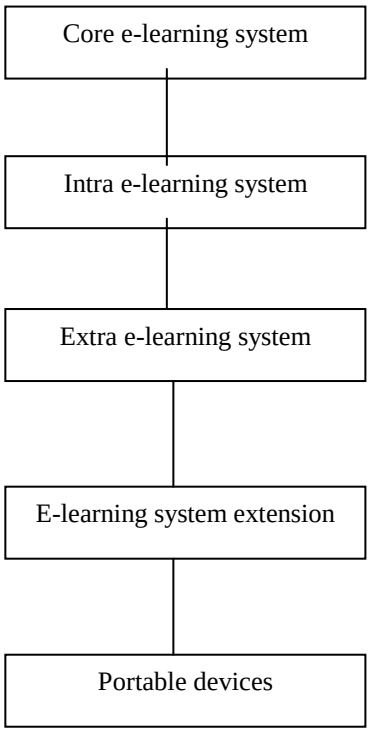

Figure 1 Architecture of e-learning system

Nearly all these e-learning systems are Web-based learning systems because the ubiquitous connection of the Internet is prevailing. E-learning users only need a web browser to access e-learning systems. Main development and implementation are carried out at the server sides. Main users in this layer are technical staff. The security and privacy issues for this layer will be further discussed in Section 4.

Layer 2: Intra e-learning system consists of all facilities for on-campus users like academic staff, administration staff. Academics use their office desk-top or lap-top computers to develop and manage their courses.

Administration people use their office computers to manage all related admin functions. Normally intra e-learning system is built on the scope of University Intranet. The security and privacy in this layer will further discussed in Section 4.

Layer 3: Extra e-learning system consists of facilities for external users, like partners, agents, cooperative organizations, etc. Normally this layer is operated under the scope of University Extranet. The further discuss on the security and privacy in this layer is on Section 4.

Layer 4: E-learning system extension is formed by public network infrastructure, like the Internet, PSTN, etc. This layer is supported by public service providers, like Internet Service Provider. This layer facilitates the universal connection by wired or wireless media so that all e-learning users can access the systems whenever and wherever they want to. Basically this layer is operated under the government regulations. The requirement of the security and privacy is guided by the law and regulations. There are no specific requirements for e-learning systems. The dataflow of e-learning systems is treated as the same as other traffic flows. Thus this layer is served under the common carriers' operations and does not have any impacts on the security and privacy of e-learning systems.

Layer 5: Portable devices include mobile phones, PDAs, palm or pocket computers, etc, for e-learning users to access e-learning systems for their learning or teaching activities. This layer provides the effective support to the mobile users via wired or wireless media. Quite often these portable devices depend on the wireless communications. This layer gives a ubiquitous access to e-learning systems via portable devices which extensively expand the availability accessibility of e-learning systems. With this extensive expansion of e-learning systems, the security and privacy of e-learning systems has become one of main concerns. The issues of security and privacy on this layer will be further discussed in Section 4.

Under this generalised architecture of e-learning systems, we understand how e-learning related activities are effective conducted via the public telecommunications infrastructure. As pointed out previously, the challenge of the security and privacy of e-learning systems are to be addressed in the followed section.

4. Security and privacy issues in e-learning

Based on the previous section, we can identity the issues of the security and privacy for e-learning systems from different layers respectively.

4.1 Security and privacy on Layer 1

As Layer 1 is core e-learning system, it is essential that the right policies and technologies for security and privacy are accurately implemented from here. Firstly, e-learning systems have to have the right security and privacy policies. Secondly, e-learning systems need right security and privacy technologies to be built in the e-learning systems. Figure 2 shows the steps to generate right security and privacy policies.

At the stage of environment requirement analysis, e-learning developers need knowing the legal requirements based on international and domestic laws and conventions. The developers must have a compliance with these laws and convention when designing their e-learning systems based on the consideration of security and privacy.

At the stage of organisation requirement analysis, e-learning developers must understand the organisational requirements as the final e-learning systems have to be delivered to the organisation, including knowing the formation of user groups, data/information sensitivity and classification, etc. Through this analysis, specific organizational requirements for security and privacy are built into the system consideration.

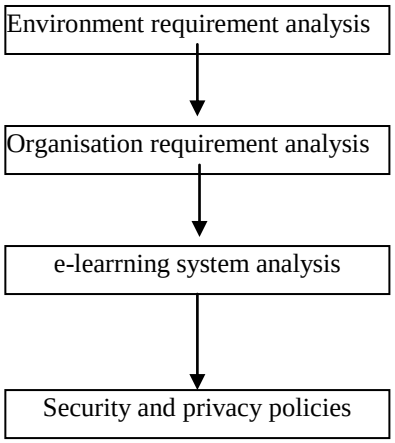

Figure 2 procedures of Security and privacy policies for e-learning systems

At the stage of e-learning system analysis, e-learning developers have to consider which e-learning platform is intended to be built for the organisation. The security and privacy requirements from intended e-learning platform need to be discussed carefully here.

At the final stage, through a thorough analysis of previous stages, the final security and privacy policies

are decided and delivered to the organisation which needs e-learning systems.

Based on delivered security and privacy policies, e-learning developers have to apply right security and privacy technologies into e-learning systems. The decision on security and privacy technologies directly impacts on Layer 2, Layer 3, Layer 4 and Layer 5. Also the security and privacy requirements form Layer 2-5 influence the selection of security and privacy technologies on Layer 1. Figure 3 shows the relationships between Layer 1 and Layer 2-5.

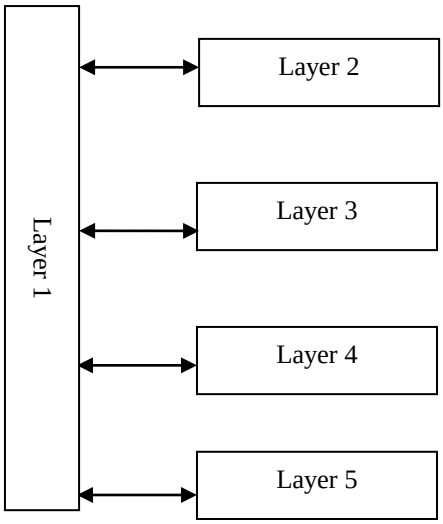

Figure 3 Relationships between Layer 1 and Layer 2-5

The privacy of this layer focuses on avoiding any exposure of concerned identities which can be explored by Layer 3-5. Like in Australia there is a request from Department of Education, Science and Training (DEST) for students' failure rate. E-learning system would send all students' grades without exposing any students' identities, especially those who do not have good grades. In this case, DEST belongs to a Layer 3 user. When core e-learning system receives any request for data, especially from upper management, it is essential to know whether privacy preservation is applied or not before data are sent out. We use the following repeatable process to justify the usage of privacy preservation technology for data request from Layer 3-5.

4.2 Security and privacy on Layer 2

As Layer 2 is much relevant to on-campus users, like academics, administration staff, management personnel and on-campus students which use universities' computing facilities. Based on different roles of these users, they are divided into different groups. Each group has its own rights to access prescribed resources. The security at this layer focuses on access control policies which are required by Layer 1. Figure 4 shows the procedures of implementation of access control for e-learning system.

While Core e-learning system

While data request

While privacy concern

While privacy preservation

Do selecting preserving techniques

Do data alteration

Until finalising privacy preservation

Until non privacy concern

Do Data transmission

Until satisfying data request

Until return to idle

Normally there is a limited privacy concern as e-learning systems are running within an organizational boundary. There is a trusted relationship between the neighbors [3]. The privacy at his layer only focuses on protecting users' identities and sensitive data across the university intranet.

4.3 Security and privacy on Layer 3

As Layer 3 supports external partners, it needs a prudent approach and robust facility to implement security and privacy policies here. Normally we need a robust firewall system to protect the internal system. A sound privacy technology is also needed to protect the privacy of e-learning systems. Further exploration on this regard will be conducted in the future.

4.4 Security and privacy on Layer 4

As Layer 4 is operated by the common carriers, e-learning systems do not have much more influence in the regard of security and privacy. Educational institutes normally have a contract with the service provider. In the contract, the service providers supply the security and privacy promises based on the relevant international law and conventions. Thus there is no need for any further discussion on security and privacy here.

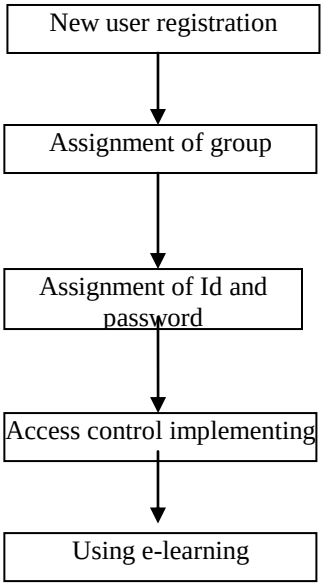

Figure 4 Procedures of e-learning access control

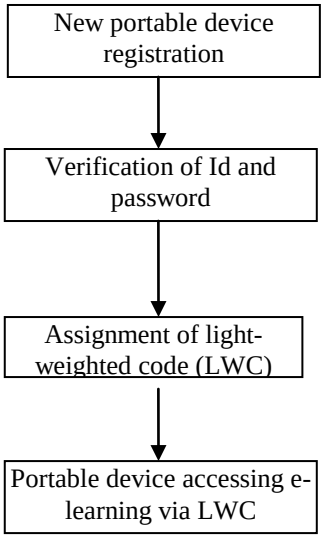

Figure 5 Procedure of access control for portable devices

4.5 Security and privacy on Layer 5

As Layer 5 provides the universal connection for portable device users to access e-learning systems, it is very import to understand the issues on security and privacy. The security in this layer focuses on access control which is decided by the security policy of layer 1. There needs a light-weighted access control technique for these portable devices because of the limitation of computing capacity and storage. Figure 5 shows the procedure of access control for portable devices.

In Figure 1, new portable device registration is charge of enrolment of portable device for e-learning system. Verification of Id and password is to authenticate the user who has a portable device is a legitimate e-learning user. Assignment of LWC is to send a short code to portable device so that this portable device can use LWC to access e-learning system if it is needed.

Here LWC is the key element for e-learning portable users and e-learning access control. A higher efficiency than normal user Id and password is a fundamental requirement to LWC. Through LWC, e-learning system can uniquely identify the real identity of the user of portable device. In the future we will further explore some effective approaches to generate LWC for portable devices.

The privacy issues lie in two aspects: portable device itself and core e-learning system. The privacy of core e-learning system is no difference with Layer 3 and 4. Normally a portable device stores some sensitive information, like contact details, personal information, etc. While this portable device is connected with e-learning systems via the service providers of common carriers, there is a risk to expose stored private information to e-learning systems and connected network users. It is very import not to compromise the privacy of sensitive information which is stored in the portable device while accessing and using e-learning systems. In order to effectively protect the privacy of portable device, e-learning system has a right solution at Layer 1. The portable device uses its LWC to download customized portable device terminal software, like a light-weighted browser (LWB) specifically designed for portable device. LWB strictly follows security and privacy policies which prohibit e-learning system to access any data stored in the portable device. Actually the portable device is virtually separated into two parts: one part keeps it original functions, like mobile telecommunications, geo-navigation, etc; the other part serves as an e-learning terminal.

5. Modeling the relationship between Security and privacy technology and policy

Generally speaking, the degree of e-learning security and privacy is decided by the two most important factors: policy and technology. Figure 6 shows the dynamic relationship among policy, technology and the degree of e-learning security and privacy.

From Figure 6, there are influences between policy and technology as well. Policy can impact on the security and privacy technology selection. Technology assists

security and privacy policy for the best practice. Further research on this regard is challenging. But it is out of the scope of this paper.

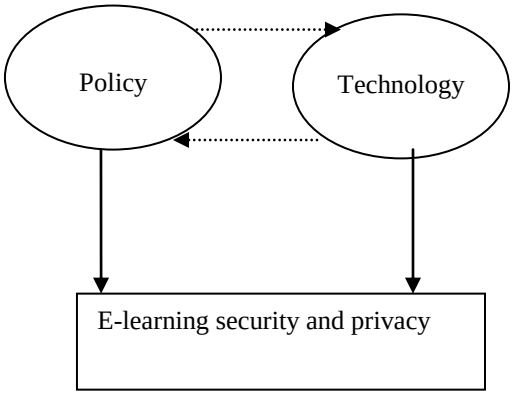

Figure 6 Relationship among policy, technology and security and privacy

Generally speaking, the degree of e-learning security and privacy is decided by the two most important factors: policy and technology. Figure 6 shows the dynamic relationship among policy, technology and the degree of e-learning security and privacy.

From Figure 6, there are influences between policy and technology as well. Policy can impact on the security and privacy technology selection. Technology assists security and privacy policy for the best practice. Further research on this regard is challenging. But it is out of the scope of this paper.

6. Conclusion remarks and future work

This paper has systematically discussed the e-learning security and privacy. A generalised architecture of e-learning systems is prescribed to illustrate the security and privacy issues. We thoroughly discussed the security and privacy for e-learning systems from layer 1 to layer 5, especially layer 1 and layer 5. This paper does not try to address too much technical details for e-learning systems on the security and privacy. Instead the paper focuses on the analysis of the influences from policy and available technology. As more and more e-learners are interested in using their portable devices to conduct their e-learning activities, the concerns on the security and privacy will generate more research and initiatives either on the technology perspective or on the management perspective.

References

1. Jianming Yong, Digital Identity Design and Privacy Preservation for e-learning, The 11th International Conference on Computer Supported Cooperative Design, Melbourne, Australia, pp858-863

2. Jianming Yong, Elisa Bertino, Mark Toleman, Dave Roberts, Extended RBAC with Role Attributes, The 10th Pacific Asia Conference on Information Systems, July 6-9, Kuala Lumpur ,Malaysia, pp457-469.

3. Jianming Yong, Neighbourhood-Trust Dependency Access Control for WFMS, The 10th International Conference on Computer Supported Cooperative Design, Nanjing, China, pp924-928.

4. Vassilelios S. Verykios, Elisa Bertino, Ogor Nai Fovino, Loredana Parasiliti Provenza, Yucel Saygin, Yannis Theodoridis, State-of-the-art in Privacy Preserving Data Mining, SIGMOD Record, Vol.33, No. 1, March 2004, pp50-57.

5. Lalana Kagal, Tiom Finin, Anupam Joshi, Sol Greenspan, Security and Privacy Challenges in Open and Dynamic Environments, Computer, Vol. 39, No. 6, June 2006, pp89-91.

6. Bill Schilit, Jason Hong, Marco Gruteser, Wireless Location Privacy Protection, Computer, Vol. 36, No. 12, December 2003, pp135-137.

7. Roberto J. Bayardo and Ramakrishnan Srikant, Technical Solutions for Protecting Privacy, Computer, Vol. 36, No. 9, September 2003, pp115-118.

8. Alfred Kobsa, Privacy-Enhanced Personalisation, Communications of the ACM, Vol. 50, No. 8, August 2007, pp24-33

9. Hal Berghel, Better-Than-Nothing Security Practices, Communications of the ACM, Vol. 50, No. 8, August 2007, pp15-18.

10. Tessa Lau, Oren Etzioni, Daniel S. Weld, Privacy Interfaces for Information Management, Communications of the ACM, Vol. 42, No. 10, October 1999, pp89-94.

11. Eugene Volokh, Personalisation and Privacy, Communications of the ACM, Vol. 43, No. 8, August 2000, pp84-88.

12. Annie I. Anton, Elisa Bertino, Ninghui Li, Ting Yu, A Roadmap for Comprehensive Online Privacy Policy Management, Communications of the ACM, Vol. 50, No. 7, July 2007, pp109-116.

13. Latanya Sweeney, Privacy-Enhanced Linking, SIGKDD Explorations, Vol. 7, No. 2, pp72-75.

14. Xiaokui Xiao, Yufei Tao, Personalised Privacy Preservation, SIGMOD 2006, June 27-29, Chicago, Illinois, USA, pp 229-240.

15. Rakesh Agrawal, Ramakrishnan Srikant, Dilys Thomas, Privacy Preserving OLAP, SIGMOD 2005, June 14-16, Baltimore, Maryland, USA, pp 251-262.