Journal of Universal Computer Science, vol. 17, no. 2 (2011), 296-310
submitted: 17/9/09, accepted: 7/12/10, appeared: 28/2/11 © J.UCS

Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes

Jianming Yong
(School of Information Systems, Faculty of Business
University of Southern Queensland
Toowoomba QLD 4350, Australia
yongj@usq.edu.au)

Abstract: This paper systematically discusses the security and privacy concerns for e-learning systems. A five-layer architecture of e-learning system is proposed. The security and privacy concerns are addressed respectively for five layers. This paper further examines the relationship among the security & privacy policy, the available security & privacy technology, and the degree of e-learning privacy & security. The digital identity attributes are introduced to e-learning portable devices to enhance the security and privacy of e-learning systems. This will provide significant contributions to the knowledge of e-learning security & privacy research communities and will generate more research interests.

Keywords: E-learning, Security, Privacy Preservation, Security and Privacy Architecture, Digital Identity
Categories: H.1.2, H.4.2, K.6.5, J.7

1 Introduction

E-learning in the recent years have become a very important means to acquire an education. It has the capacity to allow all portable devices to access useful data. Along with the recent increase in the ownership of portable devices, like personal data assistants (PDA), mobile phones, lap-top computers, pocket computers, etc. The involvement of all types of portable devices, e-learning system will become a ubiquitous platform for the future of education. However, due to the fact that 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 cannot be effectively applied due to its universally accessible nature. So far there are extensive researches conducted on the security and privacy in general. But there are only few specific researches 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 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 modelling relationship among policy,

technology, and the degree of e-learning security & privacy. Section 6 introduces the digital identity attributes for e-learning portable devices. Section 7 concludes the paper and initiates some further research perspectives.

2 Related Works

The general concern of security and privacy for e-learning system is partially addressed in [Yong 07, Aqqal et al 08, Geyer et al 07, Schrum 06]. Some access control technologies [Yong et al 07, Yong 06, Novak and Wust 04, Yang et al 08] can be used in general e-learning systems. As privacy is becoming one of the major concerns for any open systems, some techniques of privacy preservation were designed and proposed to the research communities. Like in [Verykio et al 04], the privacy preservation was discussed for the general data mining domain. In [Kagal et al 06, Bella 08, Chen et al 08], the challenge of security and privacy for open and dynamic environment was addressed from both policy and technology perspectives. In [Schilit et al 03], 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 [Kagal et al 06, Schilit et al 03, Berghel 07 and Anton et all 07]; category 2 is about technical solutions, like [Bayardo and Sirkant 03, Kobsa 07, Lau et al 99, Volokh 00 and Sweeney 05].

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

Based on category 2, it is import to find the technical solutions for security and privacy. Like RBAC [Yong et al 07], it is a solution for system access control. Like generalization [Xiao and Tao 06] and OLAP [Agrawal 05], 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

These days almost everyone can afford to have portable devices, such as mobile phones, PDAs, lap-top computers, Tablet PCs, etc. It is essential for e-learning system to fully support portable device users to effectively conduct the e-learning activities via their portable devices. With the interactive involvement of portable devices, e-learning systems are becoming 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, it is essential to have 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/].

Nearly all these e-learning systems are Web-based learning systems because the ubiquitous connection of the Internet is constantly evolving/advacning. 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 staff can use their office computers to manage all related admin functions. Normally intra e-learning system is built on the scope of a 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 a University Extranet. The further discussion on the security and privacy in this layer is can be found in Section 4.

Layer 4: E-learning system extension is formed by public network infrastructures, like the Internet, PSTN, etc. This layer is supported by public service providers, like Internet Service Providers. This layer facilitates the universal connection by wired or wireless media so that all e-learning users can access the systems whenever and wherever. Basically this layer is operated under government regulations. The requirement of the security and privacy is guided by laws 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 impact on the security and privacy of e-learning systems.

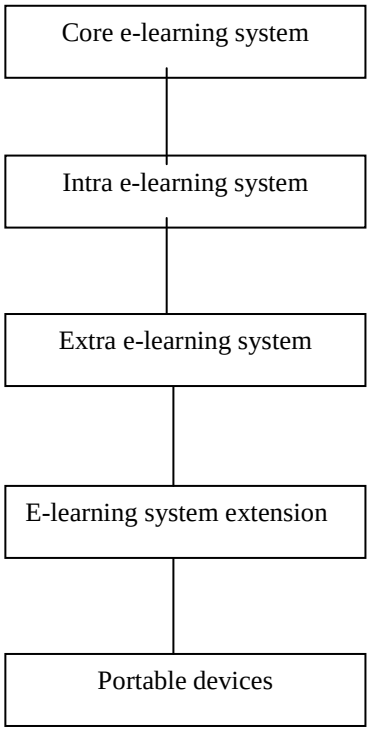

Figure 1: Architecture of e-learning system

Layer 5: Portable devices such as mobile phones, PDAs, palm or pocket computers, that allows users to access e-learning systems for their learning or teaching activities. This layer provides the effective support to mobile users via wired or wireless media. Quite often these portable devices depend on wireless communications. This layer gives a ubiquitous access to e-learning systems via portable devices which extensively expand the availability and 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 various e-learning activities are effectively conducted via the public telecommunications infrastructure. As pointed out previously, the challenges of the security and privacy of e-learning systems are to be addressed in the following section.

4 Security and Privacy Issues in E-learning

Based on the previous section, we can identify the issues with regards to 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 the right security and privacy technologies to build the e-learning systems. Figure 2 shows the steps to generate right security and privacy policies.

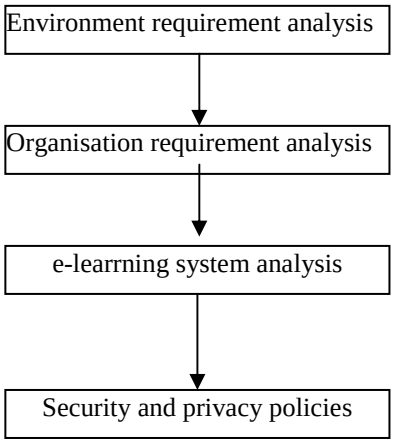

Figure 2: procedures of Security and privacy policies for e-learning systems

At the stage of environment requirement analysis, e-learning developers need know the legal requirements based on the international and domestic laws and conventions. The developers must have a full compliance with these laws and conventions when designing their e-learning systems with regards to 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 requirements.

At the stage of e-learning system analysis, e-learning developers have to consider which e-learning platform is intended to be built specifically 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 requires e-learning systems.

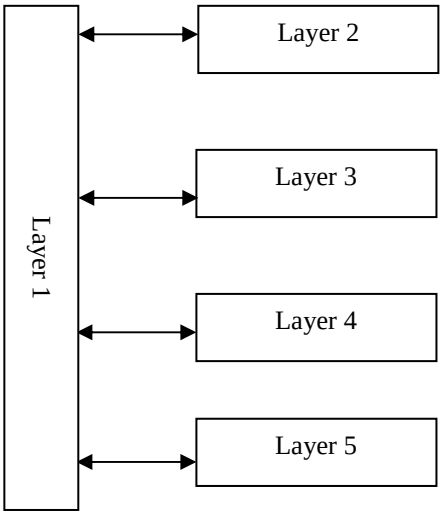

Figure 3: Relationships between Layer 1 and Layer 2-5

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

The privacy of Layer 1 focuses on avoiding any exposure of concerned identities which can be explored by Layer 2-5. Like in Australia there is a request from Department of Education, Science and Training (DEST) for students' failure rate.

E-learning system would send the grades of all the students 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, before the data are sent out, it is essential to know whether privacy preservation is applied or not. We use the following repeatable process to justify the usage of privacy preservation technology for data request from Layer 2-5.

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

4.2 Security and privacy on Layer 2

As Layer 2 has much relevance to on-campus users, like academics, administration staff, management personnel and on-campus students who 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 systems.

Normally there are limited privacy concerns as e-learning systems are running within an organizational boundary. There is a trusted relationship between the neighbors [Yong 06]. The privacy at his layer only focuses on protecting users' identities and sensitive data across the university intranet.

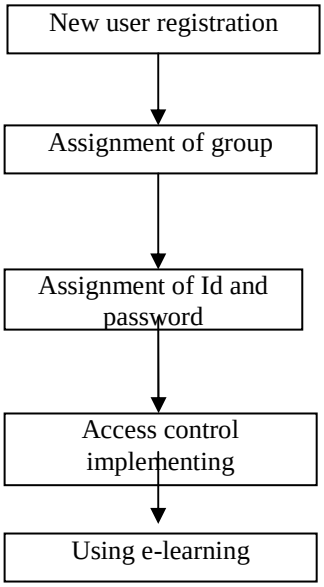

Figure 4: Procedures of e-learning access control

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.

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. It needs a light-weighted access control technique for these portable devices, due to the limitation of computing capacity and storage. Figure 5 shows the procedure of access control for portable devices.

In Figure 5, the new portable device registration is in charge of the enrolment of portable device for an e-learning system. The verification of Id and password is used to authenticate the user with a portable device. 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 when it needs to.

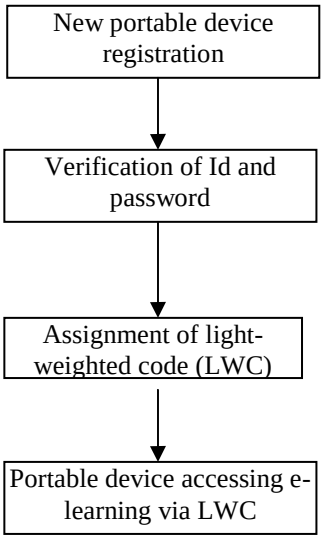

Figure 5: Procedure of access control for portable devices

Here LWC is the key element for e-learning portable users and e-learning access control. The fundamental requirement to LWC is to have more efficient user Id and password. Through LWC, e-learning system can uniquely identify the real identity of the portable device user. 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 different to Layers 3 and 4. Portable devices can stores sensitive information, like contact details, personal information, etc. While this portable device is connected with e-learning systems via service providers of common carriers, there is a risk of exposing stored private information to e-learning systems and connected network users. It is very import not to compromise the privacy of sensitive information stored within portable devices 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 the security and privacy policies which prohibit e-learning system to access any data stored in the portable device. The portable device is virtually separated into two parts: one part keeps the original functions, like mobile

telecommunications, geo-navigation, etc. While the other part serves as an e-learning terminal.

5 Modelling the Relationship Between Security & Privacy Technology and Policy

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

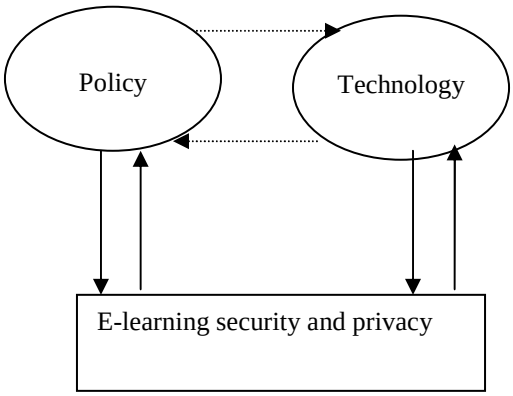

Figure 6: Relationship among policy, technology and security and privacy

Figure 6 shows that there are also influences between policy and technology. Policy can have an impact on the security and privacy technology selection. Technology plays a vital role in ensuring that security and privacy policies are performing at the optimum level.

5.1 The Policy of Security and Privacy for Mobile E-learning

Any e-learning system needs to have a clear policy framework to address the issue of security and privacy. The policy of security and privacy directly impacts on all components of mobile e-learning systems, including Contents (CT), User Management System (UMS), Assisted Tools (AT) and Mobile Supporting Module (MSM). The component of CT is developed by the lecturer/instructor. Normal IP (Intellectual Property) legislation has to be reflected in the security policy. UMS is in charge of managing all users, such as lecturer/instructor, student/learner, administrator or all system support. The security and privacy policy must clearly illustrate how to create, manage and revoke these users. AT is usually employed to enhance the contents delivery, such as images, animation, video, sound, simulation. MSM consists of all functions to support mobile devices to access e-learning system.

Figure 7 shows the correlation between security & privacy policy and e-learning system.

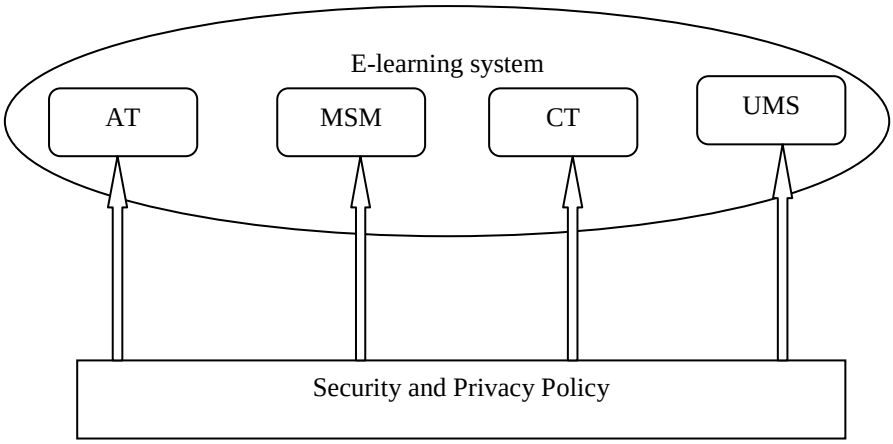

Figure 7: Correlation between security & privacy policy and e-learning

5.2 The Technology of Security and Privacy for Mobile E-learning

The technology is vital to secure mobile e-learning systems. The security and privacy over a traditional e-learning environment is well addressed. We will only focus on the concerns of security and privacy for MSM. MSM consists of an interface (ITF) to traditional e-learning platform, a mobile unit for lecturer/instructor (MUI), a mobile unit for student/learner (MUS), a mobile unit for administrator (MUA) and a mobile unit for technical support (MUT). The technology for security & privacy has to thoroughly analyse the requirements of all mobile units. Figure 8 demonstrates the processes of choosing the right technology of security & privacy for mobile e-learning systems.

Through the suitability processes, a set of security & privacy technologies are found for MSM. Further the cost benefit analysis against each found technology has to be conducted and a result table will be presented to the decision committee for the final selection.

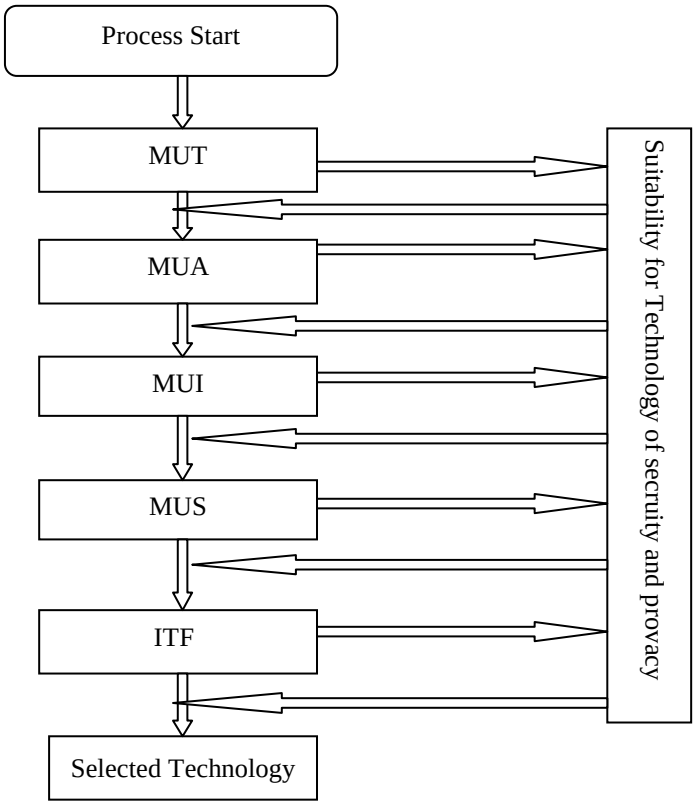

Figure 8: Processes of choosing technology for MSM security & privacy

6 Digital Identity Attributes for Portable Devices

Digital identity [Yong 2007, Yong and Bertino 2007] is addressed more for application domains, especially for e-learning systems. When the learners enrol into an e-learning system, they would be assigned their own digital identities for the e-learning system. A portable devices will be registered as one attribute associated with its owner's digital identity.

We denote a whole set of digital identities of all e-learning participants by *D.*

D={*d1, d2, d3, …, dn*} n is the maximum number of participants of an e-learning system. The *dx* represents an individual digital identity while 1<=*x*<=*n.*

When an e-learning system enrols a digital identity, the portable devices are assigned as the attributes of that digital identity. The formal expression of *dx* is shown as the follows

dx={ *a1, a2, a3, …, am*} m is the maximum number of attributes for any digital identity.

We denote a portable device as an attribute by *ap*. It is obvious that we have:

$$ap \in dx$$

Only the e-learning system registry is allowed to know the relationship *ap* and *dx.* All users who hold their portable devices will only be making transactions with e-learning systems via their unique *ap.* Based on e-learning system security and privacy policies, if you know *ap*, you cannot figure out *dx.* The privacy of *dx* will be saved by using its *ap*.

7 Conclusion Remarks and Future Work

This paper has systematically discussed e-learning security and privacy policies. A generalised architecture of e-learning systems is prescribed to illustrate 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. This paper introduces digital identity attributes for portable devices of e-learning systems. As digital identity is a new research area, we will expect more researches on digital identity for e-learning systems from a security and privacy perspective. 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.

Acknowledgements

This paper is partially supported by the Open Research Fund from the Key Laboratory for Computer Network and Information Integration (Southeast University), Ministry of Education, P. R. China.

References

[Agrawal 05] Rakesh Agrawal, Ramakrishnan Srikant, Dilys Thomas, Privacy Preserving OLAP, SIGMOD 2005, June 14-16, Baltimore, Maryland, USA, pp 251-262.

[Anton et al. 07] 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.

[Aqqal et al. 08] Aqqal, A., Rensing, C., Steinmetz, R., Elkamoun, N., Berraissoul,A.: Using taxonomies to support the macro design process for the production of Web Based Trainings, Journal of Universal Computer Science, 2008

[Bayardo and Srikant 03] Roberto J. Bayardo and Ramakrishnan Srikant, Technical Solutions for Protecting Privacy, Computer, Vol. 36, No. 9, September 2003, pp115-118.

[Bella 08] Bella G. "What is Correctness of Security Protocols?", Journal of Universal Computer Science, Vol. 14, num. 12, 2083—2107, 2008.

[Berghel 07] Hal Berghel, Better-Than-Nothing Security Practices, Communications of the ACM, Vol. 50, No. 8, August 2007, pp15-18.

[Chen et al. 2008] Chen L. et al, "Cryptography in Computer System Security", Journal of Universal Computer Science, Vol. 14, num. 3, 314--315, 2008.

[Geyer et al. 08] Geyer, W., Filho, R. S. S., Brownholtz, B. and Redmiles, D. F.: "The Trade-Offs of Blending Synchronous and Asynchronous Communication Services to Support Contextual Collaboration". In: Journal of Universal Computer Science, vol. 14, no. 1 (2008), 4-26.

[Kagal et al. 06] 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.

[Kobsa 07] Alfred Kobsa, Privacy-Enhanced Personalisation, Communications of the ACM, Vol. 50, No. 8, August 2007, pp24-33

[Lau et al. 99] Tessa Lau, Oren Etzioni, Daniel S. Weld, Privacy Interfaces for Information Management, Communications of the ACM, Vol.42, No. 10, October 1999, pp89-94.

[Novak and Wurst 04] Novak, J.; Wurst, M. Supporting Knowledge Creation and Sharing in Communities based on Mapping Implicit Knowledge. Journal of Universal Computer Science, vol. 10, 2004, no. 3, p235-251.

[Schilit et al. 03] Bill Schilit, Jason Hong, Marco Gruteser, Wireless Location Privacy Protection, Computer, Vol. 36, No. 12, December 2003, pp135-137.

[Sweeney 05] Latanya Sweeney, Privacy-Enhanced Linking, SIGKDD Explorations, Vol. 7, No. 2, pp72-75.

[Schrum 06] Schrum, L., Lamb, T.A.: Groupware for Collaborative Learning: a Research Perspective on Processes, Oppoities, and Obstacles, Journal of Universal Computer Science, vol. 2, no. 10 (1996), 717-731.

[Verykios et al. 04] 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.

[Volokh 00] Eugene Volokh, Personalisation and Privacy, Communications of the ACM, Vol. 43, No. 8, August 2000, pp84-88.

[Xiao and Tao, 06] Xiaokui Xiao, Yufei Tao, Personalised Privacy Preservation, SIGMOD 2006, June 27-29, Chicago, Illinois, USA, pp 229-240.

[Yang et al. 08]Yang G., Wong D.S. and Deng X. "Formal Security Definition and Efficient Construction for Roaming with a Privacy-Preserving Extension", Journal of Universal Computer Science, Vol. 14, num. 3, 441--462, 2008

[Yong 06] Jianming Yong, Neighbourhood-Trust Dependency Access Control for WFMS, The 10th International Conference on Computer Supported Cooperative Design, Nanjing, China, pp924-928.

[Yong 07] Jianming Yong, Digital Identity Design and Privacy Preservation for e-learning, The 11th International Conference on Computer Supported Cooperative Design, Melbourne, Australia, pp858-863

[Yong and Bertino 07] Jianming Yong and Elisa Bertino, Replacing lost or stolen E-passports, *IEEE Computer*, October 2007, Vol. 40 No. 10 pp. 89-91.

[Yong et al 07] Jianming Yong, Elisa Bertino, Mark Toleman and Dave Roberts, Extended RBAC with Role Attributes, The 10th Pacific Asia Conference on Information Systems, July 6-9 2007, Kuala Lumpur ,Malaysia, pp457-469.