Enhancing the Privacy of e-Learning Systems with Alias and Anonymity

Jianming Yong

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

Abstract. The privacy of e-learning systems has become a big concern. This paper proposes a new approach, which can effectively protect the privacy of e-learning users. We propose to use the alias and anonymity to implement the privacy preservation for e-learning systems. Through the approach, a unique alias represents the real e-learning user to communicate with each other or e-learning users use the anonymity to hide their information. This approach can be very simple and efficient to be implemented in the e-learning system by well designed meta-formats of digital identities of four types of e-learning users. The anonymity can be adopted by all e-learning users to keep their privacy.

1 Introduction

E-learning is defined as technology-based learning in which learning materials are delivered electronically to remote learners via a computer network [1], particularly the Internet. Based on [1], comparing to traditional classroom learning, the advantages of e-learning are learner-entered and self-paced, time and location flexibility, cost-effective for learners, potentially available to global audience, unlimited access to knowledge, and archival capability for knowledge reuse and sharing. The disadvantages are lack of immediate feedback in asynchronous e-learning, increased preparation time for the instructor, not comfortable to some people, and potentially more frustration, anxiety, and confusion. With the development of new technology, all the disadvantages could be overcome, like lack of immediate feedback will be solved by the adoption of wireless technology in e-learning. When a student needs an immediate feedback, his/her question will be sent to the instructor by a special wireless device and the instructor can reply the student's question immediately via the wireless device. It is obvious that e-learning will become a very important educational means for the learners. With more and more learners are acquiring their knowledge via e-learning systems which are usually connected by the Internet. When the Internet is mentioned, a natural question arises here, can we trust the Internet? In other word, do

we have the security confidence in e-learning? When Internet-based e-business is mentioned, more and less we pretty much concern the security. Very limited research has been conducted on the security of e-learning although extensive research has been done on the security and e-learning respectively. This paper is tried to address the security issue which e-learning system is facing. Through well designed meta-formats of digital identities, the privacy of e-learning users can be well preserved.

This paper is organised as: Section 2 discusses some general privacy preservation techniques by some researchers; Section 3 details the e-learning environment; Section 4 discusses the e-learning digital identities; Section 5 introduces digital identity design and privacy preservation for e-learning system; Section 6 illustrates the anonymity implementation mechanism. Section 7 addresses the further research yet to be done and concludes the paper.

2 Related Work

Since the Internet becomes the infrastructure of modern society, it not only brings a ubiquitous connectivity, but also brings an anonymous environment. When you communicate with someone via the Internet, you do not know whom you communicate with and the person who is communicating with you has no idea whom you really are. In the recent years, more and more research has been done on this concern. Digital identity management [2, 3, 4, 5, 6] has brought much more attention to the information security research communities.

In [2], a unique identifier is assigned to a user for a federation system. In order to protect the privacy of users' identities, a set of attributes are defined by the system. The attributes contain sensitive information which is only known by users themselves. Through the authentication of the attributes of users' identities, a federation system can alleviate the dependency on PKI for user authentication which is dominantly adopted by most systems. Because of the technical complexity, PKI has experienced more or less execution problems. Thus the identity attributes give an alternative way to secure the digital identities for the federation systems.

In [3], a biometric authentication mechanism is proposed for preserving the privacy of digital identity for federation system. So far because the biometric enrolment is conducted in-person, it makes the biometric authentication much more reliable. Because biometric authentication is based on zero knowledge proof and all biometric information is much accurate to the identified user. Many similar projects and research are still undergoing.

In [4], personal information is partitioned into different small sets. Each small set can not be linked and connected with any others. These small sets are represented by different pseudonyms. All operations and transactions are based on these pseudonyms so that the privacy of user identity can be preserved.

In [5], User-revocation manager is proposed to manage group signature scheme which is used to preserve the privacy of user identities. Actually the user-revocation manager knows the real of identities of involved users. This centralised user-revocation manager is the key element for the privacy preservation.

In [6], a proxy-based public key infrastructure and a mediated identity-based encryption are used to protect the privacy of the users in the mobile environment.

So far very limited research has been done to protect the digital identity of e-learning. How to effectively preserve the privacy and to manage the digital identities of the users of e-learning system becomes a challenge.

3 e-Learning Environment

In [8, 9], e-learning environment is detailed as the follows. E-learning is seen as a future worldwide application as it promotes life long learning by enabling learners to learn anytime, anywhere and at the learner's pace [10]. It is necessary to understand the role changes for all participants from the traditional teaching classroom to online universal virtual teaching venues. Traditional teaching classrooms involve lecturers/instructors, students/learners, and supporting personnel for administration purpose. E-learning classrooms have no meaning of traditional classrooms instead of various networked-computer platforms. All the activities are transacted by the universal network, usually the Internet. Likely the lecturers/instructors, students/learners, and administration personnel are needed to be involved. Because e-learning environment is heavily relying on IT technology, experts/technicians of IT support are definitely needed to facilitate all processes of e-learning. Thus, four types of identity are needed for an e-learning system. There are students' identities (SID), lecturers' /instructors' identities (LID), admin personnel's identities (AID) and technical experts' identities (TID).

4 Digital Identities in e-Learning

From the previous section, there are SID, LID, AID and TID needed for e-learning. When an e-learning system is delivered, the first digital identity needed is the system administrator, called root TID (r-TID). The system administrator will be in charge of assigning other TIDs for e-learning technical experts, called Sub TID (s-TID). R-TID and s-TIDs are in charge of managing the e-learning system from the perspective of technical support. R-TID or s-TID will assign AID and LID for admin personnel and lecturers/instructors respectively. AIDs are assigned the authority or delegation to allocate SID for individual students. LIDs are in charge of assigning the course identities (CID). The hierarchy of digital identity in e-learning is shown in Figure 1.

Privacy is lost in the proliferation of technology's omnipresent accessibility [7]. Because the five digital identities have been created in an e-learning system, how to effectively protect the privacy of the five digital identities and to seamlessly interact them each other has become one of main concerns. The following section will illustrate a new design approach to preserve the privacy of these digital identities in an e-learning system

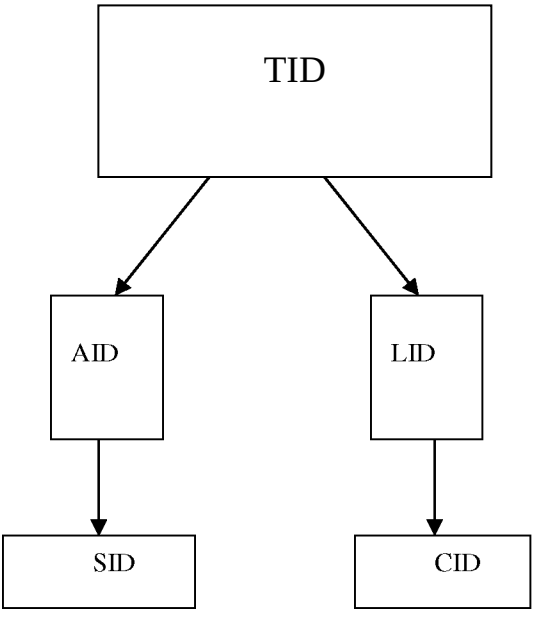

Fig. 1. Identity Hierarchy in an e-learning system

5 Digital Identity Design and Privacy Preservation for e-Learning Systems

As r-TID is configured by e-learning system developer, there is no chance to change the design of r-TID. All other digital identities can be designed to suit the needs of a specific e-learning system under r-TID's supervision. The following subsections will discuss more design details of s-TID, AID, LID, SID and CID.

5.1 Digital Identity Design

s-TIDs are assigned by r-TID for technical experts to manage the e-learning system. The meta-format of s-TID is described by XML as Figure 2.

AIDs are assigned by TID for admin staff to manage students' affairs. The meta-format of AID is described by XML as Figure 3.

LIDs are assigned by TID for lecturers/instructors to manage their courses and students' learning. The meta-format of LID is described by XML as Figure 4.

SIDs are assigned by AID for students to use their e-learning platform. The meta-format of SID is described by XML as Figure 5.

CIDs are assigned by LID for students to study their selected courses. The meta-format of CIS is described by XML as Figure 6.

5.2 Digital Identity Enrollment

Based on the meta-format of digital identity of e-learning, r-TID is in charge of enrolling s-TID. S-TID or r-TID will enrol the details of LID and AID. LID will enrol

the details of CID. AID will enrol the details of SID. After all digital identities are enrolled in the e-learning system, there is a strict process to verify all users' digital identities. Only the verified digital identities can use the e-learning system unless digital identities are revoked. Because of the space limitation of this paper, digital identity verification and revocation are not discussed in details here.

```
<?xml version^"1.0" encodings"ISO-8859-1" ?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name=”s-TID” > <xs:sequence> <xs:element
name=”staff ID” type=”xs:decimal”/> <xs:element
name=”resource” type=”xs:string”
           maxOccurs=”unbounded”/> <xs:element
  name=”alias” type=”xs:string” /> <xs:element
  name=”section” type=”xs:string” /> <xs:element
  name=”fullname” type=”xs:string” /> <xs:element
  name=”directsupervisor”,
         type=”xs:string” minOccurs=”0” />
<xs:element name=”subordinates” type=”xs:string”
           minOccurs=”0”> <xs:element name=”age”
  type=”ns:decimal” /> <xs:element name=”expertise”
  type=”xs:string”
         minOccurs=”0” /> <xs:element
name=”1oginname” type=”ns:string” />
 <xs:element name=”password” type=”ns:string” />
</xs:sequence> </xs:element>
```

Fig. 2. Meta-format of s-TID

```
<?xml version="1.0" encodings"ISO-8859-1" ?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name=”AID” > <xs:sequence> <xs:element
name=”staff ID” type=”xs:decimal”/> <xs:element
name=”alias” type=”xs:string” /> <xs:element
name=”section” type=”xs:string” /> <xs:element
name=”fullname” type=”xs:string” /> <xs:element
name=”directsupervisor”,
           type=”xs:string” minOccurs=”0” />
  <xs:element name=”subordinates”
         type=”xs:string” minOccurs=”0” />
<xs:element name=”age” type=”ns:decimal” />
<xs:element name=”1oginname” type=”ns:string”/>
<xs:element name=”password” type=”ns:string” />
</xs:sequence> </xs:element </xs:schema>
```

Fig. 3. Meta-format of AID

```
<?xml version^"1.0" encodings"ISO-8859-1" ?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name=”LID” > <xs:sequence> <xs:element
name=”staff ID” type=”xs:decimal”/> <xs:element
name=”alias” type=”xs:string” /> <xs:element
name=”section” type=”xs:string” /> <xs:element
name=”fullname” type=”xs:string” /> <xs:element
name=”directsupervisor”,
            type=”xs:string” minOccurs=”0” />
  <xs:element name=”age” type=”ns:decimal” />
  <xs:element name=”1oginname” type=”ns:string”/>
  <xs:element name=”password” type=”ns:string” />
  <xs:element name=”coursename” type=”ns:string”
           minOccurs=”0” /> <xs:element
  name=”research area” type=”xs:string”
        minOccurs=”0” <xs:element name=”contactdetails”
type=”xs:string” > <xs:element name=”email”
type=”xs:string” /> <xs:element name=”phone”
type=”xs:string” /> <xs element name=”office”
type=”xs:string” /> </xs:element </xs:sequence>
</xs:element </xs:schema>
```

Fig. 4. Meta-format of LID

```
<?xml version="1.0" encodings"ISO-8859-1" ?> <xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema"> <xs:element
name=”SID” > <xs:sequence> <xs:element name=”student ID”
type=”xs:decimal”/> <xs:element name=”alias”
type=”xs:string” /> <xs:element name=”degree”
type=”xs:string” /> <xs:element name=”fullname”
type=”xs:string” /> <xs:element name=”enrolment date”,
type=”xs:date format” /> <xs:element name=”age”
type=”ns:decimal” /> <xs:element name=”1oginname”
type=”ns:string”/> <xs:element name=”password”
type=”ns:string” /> <xs:element name=”courseenrolled”
type=”ns:string”
        minOccurs=”0” /> <xs:element
name=”contactdetails” type=”xs:string” > <xs:element
name=”email” type=”xs:string” /> <xs:element name=”phone”
type=”xs:string” /> <xs element name=”address”
type=”xs:string” /> </xs:element </xs:sequence>
</xs:element </xs:schema>
```

Fig. 5. Meta-format of SID

```
<?xml version^"1.0" encodings"ISO-8859-1" ?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name=”CID” > <xs:sequence>
  <xs:element name=”course ID” type=”xs:decimal”/>
  <xs:element name=”alias” type=”xs:string” />
  <xs:element name=”section” type=”xs:string” />
  <xs:element name=”fullname” type=”xs:string” />
  <xs:element name=”lecturer”,
            type=”xs:string” minOccurs=”0” />
  <xs:element name=”level” type=”ns:string” />
  <xs:element name=”prerequisite” type=”xs:string”
          minOccurs=”0”
  </xs:sequence>
</xs:element
</xs:schema>
```

Fig. 6. Meta-format of CID

5.3 Mechanism of Privacy Preservation of Digital Identity for e-Learning

From the meta-formats of s-TID, AID, SID, LID, all users are forced to have their aliases for their digital identities, except for CID. CID is controlled by LID. The students can get the information of CID via reasonable access controls. Thus there is no need of an alias for CID.

```
<xs:element name=”alias” type=”xs:string” />
```

When the e-learning system enrols these digital identities, an initial alias will be required. All users have to change their aliases when they first log into the e-learning system. All users' aliases theoretically are only known by the users themselves. If a user uses its alias to communicate with any other users, its real identity will not be aware by the others. For example, an AID can enrol a student digital identity. If this student uses its real digital identity to communicate with this AID, this AID will definitely know who the student is. But now if the student uses its alias to communicate with this AID, the AID will never know who the student is. Suppose the function f is used to define the transformation. The following equations will be needed for the e-learning system.

$$f\text{ (s-TID)=Alias (s-TID) } f\text{ (AID)=Alias (AID) } f\text{ (LID)=Alias (LID) } f\text{ (SID)=Alias (SID)}$$

Through this transformation, if all users concern their privacy, they can only use their transformed aliases to communicate with other users. By using the aliases, all users' sensitive information will not be exposed to the others. In case of tracing the real digital identity of a user from its alias, there is a strict security process to get a proper

authorisation to find the real digital identity of the alias. Like, if someone uses its alias to conduct a criminal activity via the e-learning system, this person can be identified through this security process.

6 *Anonymity and Implementation*

From the previous section, we have demonstrated how to use the alias for implementing privacy preservation for e-learning systems. It is obvious that the alias will be familiar by other users if the alias is used quite often. In some case, people do want to communicate with others without tracing their trails. For example, the students want to complain their instructor without any clues which will lead the instructor to trace their real identities. If the students have used their aliases for a while, the instructor will have a good chance to work out the real identities of the students based on their used aliases. Then the instructor may revenge the students by harshly marking their assessments and unfairly lowering students' performance. Under this scenario, the students would hesitate to use their alias to communicate with the instructor and most likely they want to communicate with the instructor anonymously to hide their real identities. From this perspective, anonymity can be effectively used in e-learning systems for the privacy preservation.

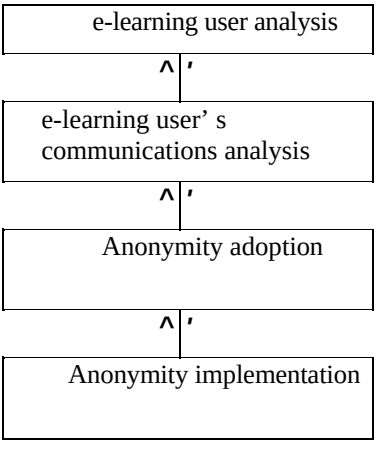

Fig. 7. Anonymity design process

6.1 Anonymity Design

There is a need for anonymity design for e-learning systems at the initial stage of system design based on the requirement of privacy preservation. Anonymity design will decide which type of communications needs the anonymity function and who can have the choice of anonymity function. In order to achieve the required anonymity function, the following process (Figure 7) will be needed.

E-learning user analysis will conclude who should have the anonymity function. E-learning user's communications analysis will decide which part of communications will need the anonymity among those who have the anonymity function. More details will be discussed in subsection 6.3. Anonymity adoption will have a detailed diagram which shows anonymity functions in the e-learning systems. Anonymity implementation will be discussed in the following sub-section.

6.2 Anonymity Implementation

After the stage of anonymity design, e-learning systems will need a mechanism to have anonymity implemented. Normally e-learning users will give three options to communicate with others (Figure 8). They can choose to use their real identities to communicate with the others if they feel comfortable. They can choose to use their aliases to communicate with the others if they feel not proper to use their real identities. They can choose to use anonymity to communicate with the other if they feel that any exposure of their identities or trails will result in compromising their roles or duties. After the e-learning users decide to use the anonymity to communicate with the others, e-learning systems will hide any information which could lead to trace their real identities, such as email address, age, postal address, postal code, race, nationality, blood type, height, user's computer MAC address, user's computer IP address, alias, etc. After all the identity-related information is hidden from the communications, the privacy of e-learning users can be effectively preserved.

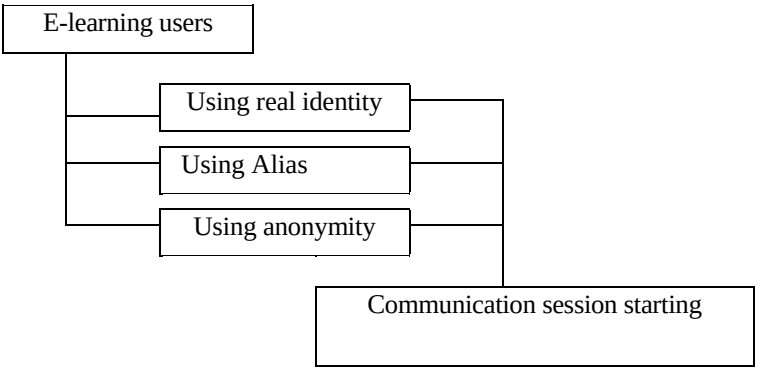

Fig. 8. Communication session selected by e-learning users

6.3 Anonymity Formulization

As mentioned in subsection 6.1, there is a need for a detailed analysis of anonymity mechanism. We further look at four types of users: students, lecturers /instructors, admin personnel and technical experts. We illustrate the analysis of intra-communications in the following table.

e-learning users		students			lecturers /instructors			admin personnel			technical experts		
students	Real	√	√	√	√	√	√	√	√	√	√	√	√
	Alias	√	√	√	√	√	√	√	√	√	√	√	√
	Anonym	√	√	√	√	√	√	√	√	√	√	√	√
lecturers /instructors	Real	√	√	√	√	√	√	√	√	√	√	√	√
	Alias	√	√	√	√	√	√	√	√	√	√	√	√
	Anonym	X	X	X	√	√	√	√	√	√	√	√	√
admin personnel	Real	√	√	√	√	√	√	√	√	√	√	√	√
	Alias	√	√	√	√	√	√	√	√	√	√	√	√
	Anonym	X	X	X	X	X	X	X	X	X	X	X	X
technical experts	Real	√	√	√	√	√	√	√	√	√	√	√	√
	Alias	√	√	√	√	√	√	√	√	√	√	√	√
	Anonym	X	X	X	X	X	X	X	X	X	X	X	X
√ - - allowed X- - not allowed													

7 Conclusion and Future Work

This.paper has mainly discussed the digital identity of e-learning. As more and more learners are moving to e-learning, the concern of lost digital identity becomes a big challenge. This paper has intentionally designed the meta-format of digital identities of e-learning users by their aliases or anonymity. Through the transformation of function f, all

users can use their unique aliases to communicate with each other with the help of conventional access controls so that the privacy of digital identity of e-learning users can be well preserved. By adopting the anonymity mechanism, the real identities of e-learning users can not be traced. Further research needs to be done on the digital identity verification and revocation. Effective alias function needs to be well defined. More systematic management of digital identity for e-learning needs to be further investigated. This paper is just a start to initiate more research on the security issues for e-learning

References

1. Zhang, D., Zhao, J.L., Zhou, L., Nunamaker Jr., J.F.: Can E-learning replace classroom learning? The communications of the ACM 47(5), 75–79 (2004)
2. Bhargav-Spantzel, A., Squicciarini, A.C., Bertino, E.: Establishing and protecting digital identity in federation systems. In: DIM 2005, Fairfax, Virginia, USA, pp. 11–19 (2005)
3. Bhargav-Spantzel, A., Squicciarini, A.C., Bertino, E.: Privacy Preserving mutli-factor authentication with biometrics. In: DIM 2006, Alexandria, Virginia, USA, pp. 63–71 (2006)
4. Borcea-Pfitzmann, K., Franz, E., Pfitzmann, A.: Usable presentation of secure pseudonyms. In: DIM 2005, Fairfax, Virginia, USA, pp. 70–76 (2005)
5. Isshiki, T., Mori, K., Sako, K.: Using group signatures for identity management and its implementation. In: DIM 2006, Alexandria, Virginia, USA, pp. 73–78 (2006)
6. Candebat, T., Dune, C.R., Gray, D.T.: Pseudonym management using mediated identity-based cryptography. In: DIM 2005, Fairfax, Virginia, USA, pp. 1–10 (2005)
7. Berghel, H.: Identity theft, social security numbers, and the web. The Communications of the ACM 43(2), 17–21 (2000)
8. Yong, J.: Internet-Based E-Learning Workflow Process. In: Shen, W.-m., Chao, K.-M., Lin, Z., Barthès, J.-P.A., James, A. (eds.) CSCWD 2005. LNCS, vol. 3865, pp. 516–524. Springer, Heidelberg (2006)
9. Yong, J., Yan, J., Huang, X.: WFMS-based Data Integration for e-learning. In: Proceedings of the 10th International Conference on Computer Supported Cooperative Design, Nanjing, China, pp. 1361–1367 (2006)
10. Iahad, N., Dafoulas, G.A., Kalaizakis, E., Macaulay, L.A.: Evaluation of online assessment: The role of feedback in learner-centered e-learning. In: The 37th Hawaii International Conference on System Science. IEEE, Los Alamitos (2004)