Project FLAME

Federated Local Access Management Environment

London School of Economics and Political Science

2007-2009

Social Study Report

Written by Isidora Kourti

Edited by Edgar Whitley, John Paschoud, Simon McLeish and Masha Garibyan

Project FLAME was funded by JISC
Executive Summary

This report presents the full results of the social study outcomes of the Federated Local Access Management Environment (FLAME) Project, which was undertaken by the London School of Economics and Political Science (LSE) Library between 2007 and 2009. Project FLAME engaged in a series of research and technical development activities to explore possible issues of Identity Management and practical responses to users’ attitudes when they access public and non-public online resources.

Issues of Delegated Authority Management (DAM), Attribute Release Policy (ARP) and Virtual Organisation Management (VOM) were explored in depth within the various activities described below. This report provides evidence of how lack of user awareness of the importance of internet security may lead to inappropriate release of attribute information and careless use of online resources. Given the complexity of the online world, this is unsurprising. One of the aims of the project was to bring to life some issues related to LSE and non-LSE technical infrastructures and LSE population’s attitudes towards their use of non-public online resources.

The research was conducted with the LSE population. Some important results were produced. The research findings have expanded existing knowledge of Identity Management and user attitudes towards internet security, and this evidence allows us to make recommendations for education institutions, technology developers and researchers.

Recommendations

R1 More research is needed to evaluate the most effective means of informing students about best practice with regards to their use of personal data. Moreover, as new technologies appear, these means might change (e.g. a Facebook campaign reminding everyone on the LSE network that they should change their password frequently using LSE for You, might be passé in a years time when a new site or service is the focus of attention) [para 64].

R2 LSE should do more to make students aware of the risks of disclosing their personal data. This advice should focus on the act of disclosure and an appreciation of the risks of passing data to different organisations [para 93].

R3 LSE should specifically highlight the sensitivity of LSE data and the consequences of disclosing this data inappropriately. For example, the consequences of being held responsible for an email sent ‘from your account’ if you share your logon name and password with someone else [para 94].

R4 LSE should do more to explain what data is held about students and why it is held [para 117].

R5 LSE should use this as an opportunity to review the data that is collected and held about students with a view to assessing whether it is really needed (data minimisation) [para 118].

R6 LSE should emphasize the role of the LSE identity credential and that access to academic resources is one of the privileges of student status [para 119].

R7 LSE should require students to change their passwords on an annual basis [para 120].
R8 LSE should actively encourage students to change their passwords on a more frequent basis. This will also require clear instructions on how this can be done [para 121].

R9 LSE should review its current policies and practices for the administrative management of identities and seek to streamline them. The review process should therefore document / update details of current practices. Staff induction should include details of any of these non-standard processes [para 122].

R10 LSE should review all systems and applications which are not integrated with central identity management system with a view of achieving full integration [para 123].

R11 If an institutionally provided system that allows more fine grained control over resources is going to be offered, then steps must be taken to ensure that the system is trusted by students (i.e. lecturers won’t routinely have access to the student spaces) [para 141].

R12 Students should be made aware of the risks of ‘natural consumer behaviour’ and given specific advice about password security [para 175].

R13 LSE should review the use of ‘remember my settings on this computer’ and switch them off by default where the consequences are potentially risky [para 176].

R14 LSE should ensure that public computers are particularly secure and ensure that the machines are checked for malware / spyware before the next user logs on [para 177].

R15 If LSE is not going to provide its own DAM services, it should provide lists of available services, highlighting those that require the minimal disclosure of personal data. These services must provide access to non-LSE users as well. LSE should also clearly state the implications of students signing up to these services using their personal details and clarify which personal details are particularly sensitive [para 178].

R16 If LSE is going to recommend commercial DAM services, it might focus on those that provide limited viewer rights for other users rather than full scale levels of access [para 179].

R17 Increased awareness of the risks of large scale disclosure of information needs to be instilled in users [para 180].

R18 If providing its own DAM / VOM services LSE needs to offer something over and above security of its services in order to motivate students use the LSE services over the alternative. The LSE also needs to further investigate issues of security related to the use of non-LSE resources [pa
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About FLAME</td>
<td>- 5 -</td>
</tr>
<tr>
<td>Background</td>
<td>- 6 -</td>
</tr>
<tr>
<td>Technical Strand</td>
<td>- 6 -</td>
</tr>
<tr>
<td>Social study</td>
<td>- 6 -</td>
</tr>
<tr>
<td>The LSE context</td>
<td>- 7 -</td>
</tr>
<tr>
<td>The institution</td>
<td>- 7 -</td>
</tr>
<tr>
<td>The LSE population</td>
<td>- 8 -</td>
</tr>
<tr>
<td>The LSE Library</td>
<td>- 8 -</td>
</tr>
<tr>
<td>The LSE IT Services</td>
<td>- 9 -</td>
</tr>
<tr>
<td>LSE Identity Management Practices</td>
<td>- 9 -</td>
</tr>
<tr>
<td>Aims of the social study</td>
<td>- 9 -</td>
</tr>
<tr>
<td>Objectives of the social study</td>
<td>- 9 -</td>
</tr>
<tr>
<td>Activities of the social study</td>
<td>- 10 -</td>
</tr>
<tr>
<td>Awareness campaign</td>
<td>- 10 -</td>
</tr>
<tr>
<td>Background</td>
<td>- 10 -</td>
</tr>
<tr>
<td>Observations</td>
<td>- 11 -</td>
</tr>
<tr>
<td>Implications</td>
<td>- 11 -</td>
</tr>
<tr>
<td>Recommendations</td>
<td>- 11 -</td>
</tr>
<tr>
<td>Experiment on disclosure of personal data</td>
<td>- 11 -</td>
</tr>
<tr>
<td>Background</td>
<td>- 11 -</td>
</tr>
<tr>
<td>Results</td>
<td>- 12 -</td>
</tr>
<tr>
<td>Implications</td>
<td>- 13 -</td>
</tr>
<tr>
<td>Recommendations</td>
<td>- 13 -</td>
</tr>
<tr>
<td>Survey of attitudes to personal data disclosure</td>
<td>- 14 -</td>
</tr>
</tbody>
</table>
Background.......................................................................................................................................... - 14 -
Approach ............................................................................................................................................. - 14 -
Results ................................................................................................................................................. - 14 -
Implications ......................................................................................................................................... - 16 -
Recommendations............................................................................................................................... - 16 -
Evaluation of ARP and VOM .................................................................................................................... - 17 -
Background .......................................................................................................................................... - 17 -
Results ................................................................................................................................................. - 17 -
Results: ARP ......................................................................................................................................... - 18 -
Implications ......................................................................................................................................... - 18 -
Recommendations............................................................................................................................... - 19 -
Trial systems built and evaluation of ARP, DAM and VOM ................................................................. - 19 -
Background .......................................................................................................................................... - 19 -
Approach ............................................................................................................................................. - 19 -
Results ................................................................................................................................................. - 19 -
Results: ARP ......................................................................................................................................... - 20 -
Results: DAM ....................................................................................................................................... - 21 -
Results: VOM ....................................................................................................................................... - 22 -
Implications ......................................................................................................................................... - 23 -
Recommendations............................................................................................................................... - 23 -
References .............................................................................................................................................. - 25 -
Websites .................................................................................................................................................. - 26 -

[This version of the Project FLAME Social Study Report does not include appendices. All published project material referenced can be accessed via: https://gabriel.lse.ac.uk/twiki/bin/view/Projects/Flame/FlameSocialStudyReport]
About FLAME

Background
1. The FLAME project arose out of previous work on Federated Access Management carried out by the Library Projects Team at LSE. The work indicated that the way forward was to let users have the ability to control the protection of their personal data and awareness of the need for discretion and control. This is particularly important since users assume more than one identity making effective identity management more complex (www.identity-project.org).

2. Following the publication of this previous work, the Joint Information Systems Committee (JISC) commissioned the LSE Library Projects Team to undertake a two component study of Identity Management in a HEI context. There was a technical component, developing institution wide prototype systems for Identity Management and access controls, and a social component that sought to understand existing user attitudes to the topic as well as evaluating the prototype technical systems. This document mainly reports on the social component.

3. The FLAME Project started in November 2007 and both the technical and social components were completed in March 2009.

Technical Strand
4. The technical strand of the project involved the development and testing of a number of technical systems. Three of these systems are of relevance for the social study and hence this report.

5. Delegated Authority Management (DAM): the ability for users with appropriate authority to define, via a central shared service, the authorisation of other users to access diverse sources of information, online services, and physical spaces, including the power to delegate such powers in controlled ways to other users;

6. Attribute Release Policy (ARP): the ability of the institution and each end user to effectively control what personal information about themselves is released to internal and external service providers; and

7. Virtual Organisation Management (VOM): the ability for LSE users to easily provide ‘guest’ access to colleagues based at other institutions (ideally but not necessarily institutions participating in the UK Access Management Federation).

8. Full details of the technical implementation of DAM, ARP and VOM, as well as the other systems from the technical strand are available from the companion technical report (https://gabriel.lse.ac.uk/twiki/bin/view/Projects/Flame/TechnicalReport). Target applications were chosen by the project team to showcase the use of the three technologies to end users; these were FlameSpace (www.flamespace.net), developed by the project team, and a Human Resources application, developed by WCN.

Social study
9. The social study was intended to complement the work of the Identity Project by undertaking large scale studies of typical user attitudes associated with the adoption of Federated Access Management (FAM) by an institution for cross–domain access to online resources. (Gluck et al., 1999). The study was, therefore, interested in the extent to which users (students and staff) value and manage their personal data in the both the LSE environment and in relation to external resources, the controls they are aware of and use, their understanding of what data is held by
service providers and the extent to which it is exchanged, and their evaluation of the systems (DAM, ARP, VOM) implemented by the technical strand.

10. Thus, whilst the Identity Project focused on interviews with identified ‘specialist’ individuals, the FLAME social study sought to obtain responses that were more representative of ‘average’ users (Bryman, 2008). Therefore, some of the differences between the results from the Identity Project and the FLAME social study arise from the differences in methodology. Other differences, however, are likely to arise from the change in technology usage (especially the proliferation of user–centric / web 2.0 technologies) (Gluck et al., 1999).

The LSE context

11. The social study took place at a single HE institution, namely the London School of Economics and Political Science (LSE). In many ways, LSE is a unique institution and the purpose of this section is to outline briefly the key features of the institutional context, including its history and focus, characteristics of the staff and student population, the LSE library - the largest provider of online services for staff and students (through access to online resources such as electronic journals), and LSE IT services (www.lse.ac.uk).

The institution

12. The London School of Economics and Political Science (LSE) is a world class education centre, renowned for its concentration of teaching and research across the full range of the social, political and economic sciences. Founded in 1895 by Beatrice and Sidney Webb, the aim of the School was the betterment of society.

13. Recently, LSE has been active in assessing the British government proposals to introduce compulsory identity cards, researching into the associated costs of the scheme, and shifting public and government opinion on the issue. The institution is also popular with politicians and MPs to launch new policy, legislation and manifesto pledges.

14. The LSE continues to have a major impact upon international society, especially with its close relationships and influence in politics, business and law. LSE has an outstanding reputation for academic excellence. LSE is an unusual university. Few university institutions in the world are as international. The study of social, economic and political problems covers not only the UK and European Union, but also countries of every continent. From its foundation LSE has aimed to be a laboratory of the social sciences, a place where ideas are developed, analysed, evaluated and disseminated around the globe.

15. The London School of Economics and Political Science has confirmed its position as a world-leading research university, with outstanding success in the 2008 Research Assessment Exercise.

16. LSE has the highest percentage of world-leading research of any university in the country, topping or coming close to the top of a number of rankings of research excellence. It is:

17. equal second in the UK when universities are ranked using a grade point average of their research strengths,

18. first when universities are ranked according to the percentage of their research receiving the top 4* (world-leading) grade, and

19. fourth when universities are ranked according to the percentage of their research receiving either 4* or 3* (internationally excellent) grades.
20. LSE submitted over 90 per cent of eligible staff for assessment.

21. LSE values the diversity of all its students, employees, governors, alumni and visitors. LSE believes in equal treatment based on merit and does not tolerate any form of discrimination. LSE seeks to ensure that people have equal access to studying and employment opportunities irrespective of their age, disability, race, nationality, ethnic or national origin, gender, religion, sexual orientation or personal circumstances.

**The LSE population**

22. The composition of LSE student body in the academic year 2008-2009 was 9148:

23. Undergraduate degree students: 4134 (45%)

24. Masters students: 3775 (41%)

25. Postgraduates PhD/MPhil/MRes students: 1142 (12%)

26. Visiting research students: 23 (0.3%)

27. Diploma students: 19 (0.2%)

28. Exchange students: 55 (0.6%). They come from 152 countries around the world: 36 per cent from the UK, 15 per cent from other European Union countries, 49 percent from other countries around the world, 48 per cent are women and 52 per cent are postgraduates.

29. Graduates find their way into senior positions in politics, the civil service, education, business and industry, and international organisations around the world.

30. LSE has over 1,900 full-time members of staff:

31. 44 per cent are from countries outside the UK, half of these from European Union countries, the remaining half from other nations around the world.

32. 97 per cent of academics are actively engaged in research.

33. LSE staff advise governments, serve on Royal Commissions, public bodies and government inquiries, and are seconded to national and international organisations.

34. LSE is in contact with around 80,000 alumni. The network extends around the world, with local alumni groups or contacts in over 60 countries, as well as special interest networks in areas such as law, environment and the media.

**The LSE Library**

35. The LSE Library is the largest in the world devoted exclusively to the social sciences. Founded in 1896, it is also known as the British Library of Political and Economic Science. Following a stunning multi-million pound building redevelopment, it offers a superb environment and an excellent resource for students.

36. It has some of the longest opening hours of any university library in Britain.

37. It collects material worldwide, in all major European languages, and is internationally recognised for its specialist research collection.

38. Over 95 per cent of its extensive stock is available on open access.

39. Over four million printed items, including 31,000 past and present journal titles, are accommodated on 50 kilometres of shelving – enough to stretch the length of the Channel Tunnel.
40. 1,600 study places including 480 networked PCs and 226 laptop drop-in points.

41. Around 8,000 e-journals are available online.

42. The Library is actively involved in self-financing and externally funded projects to help to develop the skills and technologies needed to support world class teaching, learning and research in the social sciences. A Projects Team based at the Library is also responsible for a variety of applied research projects, and library’s active participation in national and international consortia in these fields.

The LSE IT Services

43. IT Services provide centralised support for the teaching, research, learning and administrative needs of the LSE. The department covers audio-visual (AV) and telecommunications services across the LSE as well as IT, and has three main service sections:


45. Management Information Systems: Programme Office, MIS Development and Database Services


47. User support work alone required a lot of attention. The teams took and dealt with well over 43,000 calls in the year. That kind of service requires a major commitment from staff. They ensure that LSE can continue to provide the very best that IT has to offer the academic world.

LSE Identity Management Practices

48. Each institution has its own particular model of information services, which is the product of local, historical, cultural and economic factors. LSE operates a centralised ID management and record system through LSE Central, including the various names and addresses and other information about staff and students. Students Record System (SITS) stores information about students concerning their progress, exam results and class attendance. Management Information System (MIS) maintains the collection of databases and the LSE website. LSE uses Shibboleth technology in order to provide access to students to LSE and non-LSE online resources. LSE provides every student with a single username and password in order to access these resources.

Should this also mention the Enterprise Directory?

Aims of the social study

49. The aim of the social study was to explore how and to what extent end users will demand and participate in using user-based controls, including measurement of end user awareness and concern about issues such as sharing of their personal information.

Objectives of the social study

50. Thus, the social study conducted a substantial programme of internal publicity and awareness-raising with end users of all types (students, staff, researchers, administrators and individuals with various ‘non-member’ relationships with LSE), explored their attitudes and current practices for controlling their personal data and actively sought to present users with practical opportunities (via the key target applications) to exercise their own control over DAM and ARP services. Data on user
attitudes and other feedback was collected from these end users by methods including short face–
to–face and online surveys, more detailed interviewing and focus groups (Bernard, 2000).

Activities of the social study

51. The activities on the social study began with a background literature review to understand the
kinds of factors and contexts that relate to the degree of user awareness concerning the use of the
vast public medium of the Web, institutional efforts to increase students’ awareness and
institutions’ identity management processes (Leeuw et al., 2008, Todorov, 2007, Acquisti, et al.,
2007).

52. In addition, the relevant literature about research methods was also reviewed to inform the design

53. Four distinct activities were undertaken in the social study, three of which provided results that
were suitable for direct evaluation (see www.angel.ac.uk/FlameSocialStudyReport for the Social
Study activities). The first activity was an LSE–wide user awareness campaign. The aim of the
campaign was to increase awareness amongst LSE students and staff about the best use of the
internet and the most appropriate management of their personal information. Posters, leaflets,
gadgets, presentations to students and publicity through local means of communication were used.
Examples of some of the outputs from this activity are given in Appendix 1. The awareness
campaign was not explicitly evaluated.

Awareness campaign

Background

54. Although users were quite aware of the sensitivity of their credentials, they appeared to detach it
from the potential practical implications if their credentials were compromised. The campaign
aimed to reinforce the importance of reasonable digital identity self-management (Todorov, 2007).

55. The awareness campaign aimed to prepare the ground for potential LSE end users of FAM services
to be able to take the benefits. In order to do so end users ought to understand the importance of
privacy and security issues (Andrade et al. 2001).

Approach

56. The campaign was based on high visibility and interaction with users. The crucial period of the
campaign was during the first week of the academic year 2008/2009, especially during the
Freshers’ Fair.

57. In preparation of the awareness campaign the following gadgets were ordered:

58. 8,000 pens, 8,000 button badges and 8,000 coasters with the FLAME logo

59. 8,000 awareness leaflets and 80 A1-size posters

60. 5,000 of each: pens, button badges, leaflets, were distributed to the new student by Student Union
in freshers’ packs. 5,000 coasters were delivered to two bars on the campus and in students’
canteen. In addition around 1,500 gadgets were distributed directly amongst students when
conducting face-to-face conversations and interviews (completing questionnaires) with students at
the stands during students’ Freshers’ Fair. To encourage students’ interest sweets were offered
and 600 leaflets with prize draw £20 vouchers were distributed through the Student Union office.
A message informing all student and staff about the campaign was placed in the pop-up window that appears after performing LSE login between 28 October 2008 and 2 November 2008.

Observations

Whilst it was clear that most students understood the basic issues concerning the importance of proper, secure identity management, they were not showing any interest in developing their knowledge further. They were quite passive in their approach. This gave an impression of being a result of learning from experience rather than an effect of any systematic process. A lot of users were not aware of wide ranging implications of compromising their digital identity credentials.

Implications

Despite extensive work on disseminating the FLAME message, the effects of the campaign were quite limited. This might have been because of the unclear ‘path’ of implications (e.g. there might be high awareness of FLAME as something that was happening, without follow through as to what it actually meant), or because the information about what FLAME was trying to do was not delivered at the time of need for students (Freshers week is when students are busy sorting out their administration with LSE, making new friends, adjusting to living in London etc. Learning best practice in password usage was a low priority) [I1]

Recommendations

More research is needed to evaluate the most effective means of informing students about best practice with regards to their use of personal data. Moreover, as new technologies appear, these means might change (e.g. a Facebook campaign reminding everyone on the LSE network that they should change their password frequently using LSE for You, might be passé in a years time when a new site or service is the focus of attention) [R1].

Experiment on disclosure of personal data

Background

One commonly held belief is that many users are willing to disclose sensitive, personal information in exchange for small rewards (Andrade et al., 2001). To test this, an experiment on the disclosure of personal data was held at LSE (Adams et al, 1997).

Approach

The research team got ethics approval from IT Services. The IT information desk was notified so as to know how to respond if there were any complaints from students.

The team notified and explained all the details of the experiment to the LSE Students Union. They gave us a stand at the Freshers’ Fair and we proceeded with the experiment after having their approval (Petković et al., 2007).

The research team set up the stall as part of the Freshers’ Fair (October 2008) to target undergraduates, masters and research students who came to register with societies (random sample) (Bernard, 2000).

Students who approached the stall were encouraged to provide details about themselves based on a set of questions (Appendix 2 gives the questions that were asked). If they answered the first set, they received a piece of confectionary (a chocolate bar) and were
encouraged to answer the second and third sets for more rewards. Each set of questions asked about increasingly sensitive personal information, such as age, term address, LSE username, mobile phone number, non-LSE email address (first card), date of birth, LSE logon password, bank, partner’s name, number of partners (second card), LSE library number, mother’s maiden name, credit card number, Facebook password and bank sort-code (third card).

Results

70. 361 students participated in the experiment. 34 participants did not give valid answers or refused to submit their set of answers and they were excluded from the analysis of the data. Therefore, the actual sample size was 327 students. At the end of the experiment an attempt was made to contact all of the participants to provide explanations about the conduct of the experiment and inform them about the results. They were also sent an email from IT services about the need to not disclose their passwords and to regularly change their passwords.

71. Undergraduate, masters and research students participated in the experiment. From those students 327 answered the first set of questions, 176 answered the first and the second set of questions and 92 answered all three sets of questions.

72. In exchange for the confectionary, the research team managed to collect some interesting personal data about the participants. Most of the participants released their LSE username, term address, mobile phone number, non-LSE email address, date of birth and LSE library card number. Some participants also released their LSE logon password, Facebook password, credit card number and sort code. More specifically,

73. for round one questions:

74. 91% of the participants gave a valid LSE username while there were no blank answers.

75. 90% of the participants released what appeared to be a valid term address and only 1% did not give an answer.

76. 67% of the participants released a valid mobile phone number. 15% did not answer this question.

77. 60% of the participants gave a valid non-LSE email address and 3% did not answer this question.

78. For round two questions:

79. 73% of the participants released their date of birth while there were no any blank answers. [As we had their age from the first set of questions we were able to do a quick check on this data]

80. 14% of the participants gave their LSE password. There were no blank answers.

81. For round three questions:

82. 63% of the participants gave a valid LSE Library number and only 10% did not answer this question.

83. 40% of the participants released their Facebook password. 23% did not answer this question.

84. 30% of the participants gave a valid credit card number while 46% did not answer this question.

85. 34% of the population gave a valid sort-code while 36% did not give an answer.

86. The validity of the student responses was assessed using different approaches, including using Google maps to check for a valid address, making phone calls to mobile numbers provided, sending emails to the email addresses that students provided, checking library records for valid library card
numbers etc. Answers given for LSE usernames and passwords were checked by submitting them as a batch query using a secure LDAP access available to the project team for testing, ensuring that any clear-text records of passwords were handled securely by the team and destroyed after the check. Moreover, the research team was taking field notes during the experiment that were included at the back of the cards (Crano et al., 2002). For example, some students admitted that they were lying. The research team made a note at the back of those cards and these cards were excluded from the analysis of the data. Some students were discussing the task with their friends who were giving them instructions to lie as they completed it. Those cards/questions were marked and also excluded from the analysis (in total 34 cards were excluded from the first category, 24 from the second and 18 from the third). A table that summarises the results of the experiment can be viewed at www.angel.ac.uk/FlameSocialStudyReport.

87. An important issue about the release of attribute information emerged as participants released their personal data to people who have not revealed their identity. Apart from some general information about the organisation they were working for, the research team did not answer any specific questions about the reason why they were asking for students’ personal information.

88. In addition, when participants provided their personal information they had no way of ensuring the security of that information (and were provided no information about this, although, of course, the project team were scrupulous in ensuring that the personal data was kept secure and, once the participants had been notified about the experiments, was destroyed).

89. Some photographs of the experiment are available in Appendix 3.

Implications

90. While some students refused to participate in the study, or deliberately gave inaccurate data, many students divulged sensitive information. This clearly demonstrates a lack of appreciation of the risks associated with this behaviour, both in terms of the act of disclosure and to whom they might be disclosing the data [I2].

91. Of particular concern was the fact that LSE data (LSE password, library card number) was more likely to be disclosed than traditionally sensitive data (date of birth, credit card number etc.). This suggests that awareness of the sensitivity of the LSE personal credentials is particularly low [I3].

92. As the use of Federated Access spreads, the benefit of a single set of organisational identity credentials for single sign-on across many resources implies that these credentials are more powerful and should therefore be more carefully guarded than in the past [I4].

Recommendations

93. LSE should do more to make students aware of the risks of disclosing their personal data. This advice should focus on the act of disclosure and an appreciation of the risks of passing data to different organisations [R2].

94. LSE should specifically highlight the sensitivity of LSE data and the consequences of disclosing this data inappropriately. For example, the consequences of being held responsible for an email sent ‘from your account’ if you share your logon name and password with someone else [R3].
Survey of attitudes to personal data disclosure

Background

95. The research team wanted to learn more about how LSE members felt about the way their identity was managed by LSE and about the way they manage their identity. In order to collect data on these issues, a face to face and an online questionnaire were launched in October 2008 (Peterson, 2000).

Approach

96. In parallel with the data disclosure experiment a survey of attitudes to personal data disclosure was undertaken. First, during the same Freshers’ Fair, a separate FLAME stand was set up in a different location to the experiment. In addition to being part of the general awareness campaign for FLAME [distributing leaflets, gadgets (pens, pins and coasters), cards and posters] individuals visiting the stall were also invited to complete a questionnaire about their attitudes to personal data disclosure (see Appendix 4 for a copy of the questionnaire).

97. The Bristol Online Survey (BOS, www.survey.bris.ac.uk), a service that allows developing, deploying, and analysing surveys via the Web, was used for the online version of the questionnaire, and also by the project team to record responses collected from the printed questionnaire (see www.angel.ac.uk/FlameSocialStudyReport for combined results of face to face and online questionnaire). The online questionnaire included exactly the same questions as the face to face questionnaire. The online questionnaire was available from October 23rd 2008 to November 2nd 2008. In order to collect as many responses as possible, a brief was included in the LSE Student Union weekly email and in the Briefing (the LSE online Newsletter). We also offered as a prize 20 Vouchers (£20 on books).

98. The data from the questionnaires were analysed quantitatively. Using a multi-level approach, the analysis of the data aimed to elucidate the role of factors such as context, background, public and non-public resources in relation to awareness about the risks when accessing online resources (Crano et al., 2002). This was followed by further analysis of the data focusing on the institution’s Identity Management processes and users’ satisfaction with these (Ngo et al., 2005).

Results

99. The final target group of our study was 351 LSE students and 61 staff. From the 82 questionnaires that were submitted online, 21 were completed by staff and 61 by students. From the 330 questionnaires that were completed face to face, 40 were submitted by staff and 290 by students.

100. The original intention had been to achieve a balanced sample of both students and staff. This goal was not fully realized, and the sample consisted of more students than staff. However, this does not have a significant affect on the validity of the results, since the LSE students body is 9148 and the academic and administrative body is 1900 (Bryman, 2008). The inclusion of three categories of students (undergraduates, masters and research students) and staff from various departments provided an alternative perspective on a range of issues (Cohen, 2000).

101. In total, we received 412 completed questionnaires. This gathered perceptions, views and reported experiences concerning users’ attitudes to online resources, users’ awareness to the risks when accessing online resources, user’s opinions about the way their personal information identity is managed by LSE.
Some interesting results were collected with the questionnaires. The majority of the participants were satisfied with the services the LSE provides. Most of the participants agreed on the personal information (name, date of birth, address, contact number, nationality, family status), the financial information (bank details, account number, accommodation and school fees, annual income of family, loans), the library information (books issued, fines, internet usage, access to library, journals used) and study information (exam results, marks, attendance, timetable, courses) that the LSE holds about them.

Nonetheless, participants could not identify the purposes for which the LSE holds this information. A variety of answers was collected: communication, registration, enrolment, administration, marketing, operation, reference. However, the most common answer was that ‘The School needs to know’.

The majority of the participants claimed that they use LSE credentials to access: computers, wireless, email, journal, internet services, library services, career services, Moodle (institutional VLE), LSE For You (the LSE web portal), sign up for classes and print-purchasing. Participants supported that they use their LSE ID card in order to: access the library and other LSE premises, borrow books, to enter in clubs and to have discounts. Apart from the use of their LSE credentials, the majority of the students also recognised the importance of not letting other students use their LSE username and password. The same results emerged for the use of an LSE ID card, as most of the participants have never lent their LSE ID card to other people.

Results: Identity Management and LSE users

During the process of registration students claimed that they had to present a photo ID and their acceptance letter or other relevant academic documents. The majority of the students claimed that they had to identify themselves only once and that they found the registration process efficient. Returning second and third year students found the process of re-registration had improved compared to previous years.

As mentioned above, the majority of the participants do not let other people use their LSE username, password and ID card. However, some participants did present some examples where they lent their LSE account, LSE library card and debit card to their friends. Participants clearly do not realise the risks related to these actions as they claimed that they do not think that it is bad to let their friends use their accounts, library and debit cards.

None of the participants has ever been a victim of identity theft. However, they have not taken any action in order to prevent their LSE credentials from being stolen, i.e. most of the participants have never changed their LSE password and some of them did not even know that this is possible. Some participants were quite surprised (and dissatisfied) with LSE because it does not have a policy that forces them to change their password after a specific time as it usually happens at most HEIs.

Results: Identity Management and LSE administration

At the LSE, administrators create unique naming policies for each of their systems and utilize this naming convention to assign a unique identifier to users of their systems (individual accounts). Administrators aim to assign accounts with uniformity across all LSE systems. For systems which cannot use the defined uniform naming convention there arises an opportunity for identity management to transcend across the systems and provide a solution.

Although the administration does its job very well, multiple teams are involved in the user administration activities. This may result in increasing overheads in the administration of identities.
Moreover, the teams spend a lot of time performing routine administration tasks that can be automated. It takes a lot of time to provide access to external users, such as visiting students and fellows, while their functions or roles may limit their ability to access services available to internal users. More confusion takes place when students de-register for one term and later return, as it takes time to restore access rights to resources. Former staff and students may have restricted access to services as alumni.

110. Issues of Identity Management and security risks relate to accounts created with unauthorised system access rights. Changes to the staff cause confusion and delays in Identity Management processes. Security risks occur when frustrated or overburdened administrative staff may take shortcuts. As it is mentioned above, terminations may not be done as soon as required or permissions granted may be in excess of what is really needed or may limit users’ ability to access resources that they need.

111. On the other hand, security issues were raised, since most of the participants have never changed their LSE username and password, while some of them are happy to give their credentials to friends in order to access LSE resources. Moreover, when they allow access to non LSE members, issues of security concerning the access and the inappropriate use of resources (articles, journals, books, library spaces) apply. In addition to the security risks, this attitude makes the work of the administrative staff much more difficult.

Implications

112. It is apparent that there is little real awareness of what data is held by the LSE or why it is held [I5].

113. Whilst students are aware of the role of the LSE identity as a credential for accessing services, they have less awareness of their responsibility to keep it secure (compare these results with the ‘experiment’ that was conducted at the same time) [I6].

114. Many students are familiar with systems that require them to change their passwords regularly. The fact that LSE does not require this and does not emphasise this practice may well reduce confidence in the LSE as a trusted environment for storing personal data [I7].

115. There is clearly an overhead associated with the administrative management of identities at LSE and the potential for more automation of these tasks [I8].

116. Whilst many of the LSE systems use a single LSE username / password to provide access to services, this is not always the case. Some end-user systems (such as Moodle) implement single sign-on in ad-hoc ways (e.g. using direct LDAP connections instead of Federated Access) which reduces the administrative and security benefits of having a single identity & access management infrastructure. Having isolated systems that operate outside of the central system causes potential problems of revoking access controls / having multiple passwords etc [I9].

Recommendations

117. LSE should do more to explain what data is held about students and why it is held [R4].

118. LSE should use this as an opportunity to review the data that is collected and held about students with a view to assessing whether it is really needed (data minimisation) [R5].

119. LSE should emphasize the role of the LSE identity credential and that access to academic resources is one of the privileges of student status [R6].

120. LSE should require students to change their passwords on an annual basis [R7].
121. LSE should actively encourage students to change their passwords on a more frequent basis. This will also require clear instructions on how this can be done [R8].

122. LSE should review its current policies and practices for the administrative management of identities and seek to streamline them. The review process should therefore document / update details of current practices. Staff induction should include details of any of these non-standard processes [R9].

123. LSE should review all systems and applications which are not integrated with central identity management system with a view of achieving full integration [R10].

Evaluation of ARP and VOM

Background

124. In order to collect data about LSE user experiences and practices with online services, ARP and VOM we conducted some group discussions with LSE students (Puchta et al., 2004, Dai et al., 2005).

Approach

125. Participants were selected from those who had indicated that they would be willing to participate in follow-up work on the questionnaire.

126. From 26 students who had offered to attend the focus groups, 18 showed up: 3 research students, 5 masters students and 10 undergraduate students.

127. Although 4 focus groups were organised only 3 took place since one was cancelled due to a fire alarm. The cancelled focus group was not rescheduled as the majority of the participants managed to participate in one of the other focus groups.

128. The focus groups were conducted the second and the third week of May Nov?? 2008. All the group discussions were recorded and they lasted up to one hour (Bernard, 2000).

129. An introductory video was used in order to explain the aims of the project and of the study, and the structure of the focus group. The focus group guidelines are included in Appendix 5.

Results

130. None of the participants has ever been a victim of identity theft. However, some of the participants gave examples of their friends using their LSE account, LSE library card and debit card. An important issue was that participants presented those examples as part of their daily life, commenting that they could not see any problem with sharing their credentials, library card and debit card with their friends.

131. When participants receive phone calls asking to release personal data they hesitate to provide any information unless they are sure who they are dealing with. Usually they ask for more information and they prefer to call back the organisation that the caller claims to be from. However, it is quite interesting that some participants would not mind giving information like name, date of birth and address that they characterise as basic information to release.

132. All of the participants agreed that they were careful with their online transactions. However, they admitted that most of the time they proceed with a transaction if it was necessary in order to get what they want. Most of the participants trust websites that are well known (e.g. Amazon, e-Bay). If the website looks amateurish, they will cancel the transaction. Furthermore, participants access a
website if it contains information they need without taking into account the security of the website. If there are some issues of security they will just refresh the webpage and try again.

133. When participants use non-LSE resources they don’t usually change their privacy settings in order to restrict access to viewers of their material because they do not think it is necessary. Some of the participants didn’t even know that some online services provide this option.

134. In line with the survey, many students claimed in the interviews that they have never changed their LSE password. In addition, most of the participants did not know that they could change their passwords. It seems that users’ common approach is to use different versions of the same password while they choose not to have more than 4 passwords.

Results: ARP

135. All of the participants put material online for others to share. Most of them use Facebook as the main online service to share pictures, videos, notes, personal information (i.e. hobbies, favourite movies). The participants admitted that they like to share information without considering too much who has access to that information. This links to the fact that most of the participants didn’t know about or haven’t turned on their privacy settings in Facebook. They claimed that since they put their information online they do not mind to share it with those who can get access to their page. Only two of the participants try to limit the information they release online.

136. All the participants agreed that it is necessary to release personal data in order to get access to online services. What is quite interesting is that they do not wonder why third parties are asking for their personal information. Participants saw it as a simple fact of their daily life without having any thought about the use of their data by the third parties to whom they have released it. As a result, participants claimed that they wouldn’t hesitate to release their true name, email address, date of birth and mobile number.

137. An important issue that emerged from the groups is that students do not make any effort to limit the information they put online. The fact that they release their personal information to non-LSE services is an encouragement rather than a discouragement. Participants do trust public online services, and they prefer to share their personal data and material using non-LSE services because they know that their lecturers will not have access to this data. Moreover, they suggested that public services provide a place to share not only academic material but also personal material.

Results: VOM

138. Most of the participants seemed to realise the difficulty of managing the material they put online and suggested that the best way to control it was by decreasing the amount of information they put online. Most of the participants have experiences of managing their space using Facebook. The majority of the participants choose to give access to all those who are in the ‘LSE’ Facebook network without exceptions. They do know that all people on the ‘LSE’ Facebook network will be able to access their data, however, it does not seem to be an issue. They claimed that since they put their personal or academic information there, it means that they are actually happy to share it with others.

Implications

139. It is apparent that users do share materials and that these materials are both work and private. However, they don’t really ‘control’ access other than in very broad terms. There was a feeling that they would prefer more fine-grained control [10].
A particular concern for an institutionally based DAM is whether academics (personal tutors etc.) would normally be able to have access to students’ materials. In this sense, externally hosted services are considered ‘safer’ [111].

Recommendations

If an institutionally provided system is going to be offered that allows more fine grained control over resources then steps must be taken to ensure that the system is trusted (i.e. lecturers won’t routinely have access to the student spaces) [R11].

Trial systems built and evaluation of ARP, DAM and VOM

Background

In order to try the new applications that the technical team launched to encourage users to try out DAM, ARP and VOM, some interviews were conducted (Kvale, 2007). Further to this aim was the collection of data about users’ attitudes to DAM, VOM and ARP (Leeuw et al., 2008).

Approach

Participants were selected from those who had participated in the focus groups, seemed to be familiar with the concepts behind DAM, VOM and ARP concepts and indicated that they would be willing to participate in follow-up interviews.

16 interviews were conducted (12 with LSE students and 4 with administrative staff) during the last week of January 2009. All the interviews were recorded and they lasted up to one and a half hours (Kvale, 2007).

The participants experimented with two applications: FlameSpace (www.FlameSpace.net) and Google Docs (www.docs.google.com). Google Docs is a well known service developed by Google, while FlameSpace is a WIKI-based service developed by the project team. Both enable users to share data with selected other individuals and were chosen as exemplars of real world use of VOM, ARP and DAM.

They were asked to comment on those applications while they answered questions about VOM, ARP and DAM. The interview guidelines are included in Appendix 6.

Results

Important issues of security arose from the collected data. The participants were asked about the non-LSE resources that they most frequently access. Most of the participants access their non-LSE email, Facebook and Google many times per day while most of them access YouTube, Yahoo and Wikipedia at least one time per day. In order to access these services, participants usually give their real personal details without even reading the terms and conditions of the service. Participants are happy to give their name, email address, date of birth, gender, address, university and program of study. A small number of the participants claimed that they are happy to give any kind of information they are asked for in order to gain access to public resources they wish to use.

When participants try to access a website and the browser identifies a problem with the website’s security certificate (e.g. the certificate is out of date or not associated with the particular site) they choose to access or refresh the website. If the problems persist, they rarely leave the site particularly if they really want to access the information that is included there. It seems that the
most important factor for their decision is the type of information included on the website rather than the security of the website.

149. Of particular interest was the claim made by a number of students that they were more likely to visit potentially unsafe sites if they were accessing them from LSE computers rather than their own. That way, if there were any problems with the site (such as the installation of malware), it would be a problem for IT services. It is important to mention here that most of the participants are careful with their online transactions. They only trust websites that are well known and if the website looks amateurish, they cancel the transaction. However, some of them decide to proceed with a transaction even when they are not sure about the security of the website in order to get what they want. Most of the participants have done this in the past and are happy to do it again. The issue is linked to Identity Management and users’ awareness considerations as well.

150. Participants were aware of the risks of reusing the same or similar passwords. Other security issues arose concerning the storage of their credentials as most of the participants admit that they store their passwords on their computer, on paper, in their notes, in their diary or on their personal notice board. The storage of their credentials may cause further confusion and problems, as usually users forget their passwords and the place where they have stored them. Most importantly users are not aware of the risks related to the storage of their passwords and they are not willing to change their attitude.

151. Most of the participants said that they usually choose the option ‘Remember me on this computer’ and save their username and password in order to get quicker access to most of the services that require identification.

Results: ARP

152. Interesting results came from our discussions concerning users’ attribute release policies for non-LSE resources. All of the participants agreed that it is necessary to release personal data in order to get access to online resources. Participants stated they are willing to release their name, email address, date of birth, gender, address, university and program of study in order to access those services they wish to use. Nevertheless, some participants claimed that they would release any kind of personal data in order to get access to some online resources.

153. Users are quite careful when they have to release personal data by phone. The majority of the participants claimed that they do not release personal information by phone unless they are sure who they are dealing with. The most common approach to these phone calls is to ask for more information about the person who is calling or call back the organisation that the caller claims to call from. However, although the minority, some of our subjects were happy to provide the information they had been asked to without trying to identify who is calling.

154. As the data showed, most of the time participants do not read the terms and conditions before they agree to sign up for an online service. However, they tend to give their real details when they sign up. Moreover, when users sign up for an online service they do not usually read the instructions in order to prevent the release of their personal data. For example, when users were asked if they have turned on their privacy settings to restrict access to their Facebook account, most of them claimed that they have not while some of the participants’ admitted that did not know that there is this option. Based on these results, it can be argued that LSE users are not aware of the risks related to the release of their personal data and they are not aware of the policies or tips that will help them protect their personal information as well.
155. Issues of security arose from the collected data. Users are happy to release the information they have been asked for in order to have access to the online services they wish to use. It seems quite common and harmless to provide information like: name, address, email address, date of birth, university and program of study. In addition to not really understanding the risks of releasing their personal data and they often have a naïve understanding of what personal information is safe to be released and what is not.

156. By exposing their personal information to online services like Facebook they put this data at risk. However, it seemed that the reasons for not exposing their data by restricting access to their account are more personal and not related to the risks of releasing their personal data. For example, from those participants who claimed that they have turned on their privacy settings, most of them supported that they have done it in order to prevent other people from looking at their photos and their wall postings.

157. The results also confirmed that the users do not look at the terms of the agreement before they agree to sign up for an online service. This proved that the users are not aware of their rights and responsibilities, and the terms and conditions under which they may use the websites they access. It seemed that the agreement to the terms and the release of personal data are common processes in order to gain access to online resources. This data raised serious issues of security and the need to increase users’ awareness concerning their attribute release policies.

158. Issues of security arose from the collected data. Users are happy to release the information they have been asked to in order to have access to the online services they wish to. Although in most of the cases they hesitate to release any kind of information, it seems quite common and harmless to provide information like: name, address, email address, date of birth, university and program of study. An explanation could be that participants do not really understand the risks of releasing their personal data and even some times they have a naïve understanding of what personal information is safe to be released and what is not. – this whole para repeats what 155 says Both LSE and the sector as a whole should consider this in order to take action and educate users about the management of their personal data.

159. As users usually do not look at the terms and conditions before they agree to sign up for an online service they are not aware of their rights and responsibilities and those of the service provider. – repeats what 154 says

Results: DAM

160. All of the participants put material online for others to share. They usually share pictures, notes, files, documents, videos and personal information and regularly use Facebook for this purpose. Users choose to give access to their accounts and their material to LSE members, family and friends. Since users tend to share a lot of material, they want to have the ability to give others access to non-public resources.

161. The majority of the participants would like to be able to share material with viewers who they personally invite. It appeared that the participants are aware of the risks and the dangers of giving to other users the ability to edit, delete, edit and write effectively the same, at least in an electronic context or manage ‘their’ material. They admitted that only in cases where they have to collaborate with others (e.g. for a project or a group exercise) would they give other users the ability to write, edit and delete. However, even in these cases they would hesitate to share the management role. Participants also recognised that it is very important to understand the meaning (‘power’) of each role before they give it to the users of their space. They also agreed that usually
the instructions are not straightforward and do not help them to identify the appropriate access that they wish to give to others.

162. Furthermore, participants were not aware of the risks of giving view level access to their material to others, as the majority of the participants supported that they share pictures, notes, files, documents, videos and personal information. From the participants’ answers, it was concluded that they are happy to share any kind of material they are able to share with an online service. On the other hand, they do discriminate between users known to them (even if very vaguely, such as other members of the institution) and the public in general. This indicated that the users realise that they should not share their material with anyone apart from people they know. Follow up research is needed to obtain some meaningful results concerning the detailed rationale behind users’ decisions about the level of access that they provide to their material.

Results: VOM

163. The majority of the participants claimed that it is hard to control information once it has been released online while some of them admitted that they should limit the information they put online more than they do as this is the best way to keep it under control. Users choose to allow LSE members, family and staff to access their H-space and non-LSE online resources. It appeared from the data that Facebook is the principal space where LSE members can control who has access to their personal files. Other popular options are Google and Yahoo.

164. Most of the participants expressed the need for a service that will allow them to share their data and collaborate in a simply and secure way with people inside and outside LSE. Nevertheless, it seems that they prefer a non-LSE service instead of a service provided by LSE. The participants were asked to use and then decide whether they prefer to collaborate with people inside and outside LSE with Google Docs or with FlameSpace. The majority of the participants chose Google Docs. The main reason was that they find that Google Docs is a more familiar and well established service than FlameSpace. Although they were asked about issues of security, they believed that Google Docs is as safe as an equivalent application provided by LSE. Even when the differences of the login process were introduced, they still supported that they find Google Docs as safe as FlameSpace in terms of the release of their personal data. There were also a few cases where the participants claimed that FlameSpace appears less safe than Google Docs.

165. Participants found the ability to collaborate with LSE and non-LSE users very important. They claimed that current LSE services do not provide this option and that leads them to use non-LSE services in order to collaborate and share material with people outside LSE (Facebook, Google, Yahoo and MySpace). It emerged that the most important issues of security are related to the use of non-LSE resources in order to facilitate the collaboration between LSE and non-LSE members. These services are not controlled by the LSE and yet students do trust them. They think that these services are as secure as LSE services. In addition, they believed that non-LSE services are more user-friendly and simpler.

166. Users also indicated that any new LSE application that will facilitate the collaboration and information sharing would need to do so between LSE and non-LSE users. Students also suggested that this LSE service should be a space not only for academic purposes but also for personal uses (to chat with their friends, post videos, photos, documents etc.).
Implications

167. It is important to acknowledge “natural consumer behaviour” on the part of the students. They are often more interested in the outputs than the potential risks of visiting sites, they often use the same password for multiple services, take advantage of ‘remember me on this computer’ options and save passwords in insecure locations [I12].

168. If they are aware of the risks of particular sites, they will often experiment with those sites on institutional rather than personal computers, as someone else will have to fix any resulting problems [I13].

169. Because of the desire to use commercial DAM services students often need to reveal excessive amounts of personal data. This data is rarely required to provide the service, but rather is collected for marketing purposes [I14].

170. In most cases of DAM, users only need to provide viewer access rights. On those occasions when work related collaboration is required, then a limited range of more advanced rights are required [I15].

171. Because most users’ only offer viewer rights, when VOM services are used they are less concerned about the precise membership of the group that is given viewer rights [I16].

172. Use of sites like Facebook means that it is normal behaviour to make many different resources available (even with viewer only restrictions) without thinking through the long term implications of this release [I17].

173. The results from the use of DAM / VOM highlight the importance of sharing materials beyond the institution (e.g. family and friends) and this is a necessary feature of any DAM/VOM alternative proposed [I18].

174. When considering external DAM / VOM services, students felt that they were ‘as secure’ as the LSE alternative and easier to use [I19].

Recommendations

175. Students should be made aware of the risks of ‘natural consumer behaviour’ and given specific advice about password security [R12].

176. LSE should review the use of ‘remember my settings on this computer’ and consider disabling them by default where the consequences are potentially risky [R13].

177. LSE should ensure that public computers are particularly secure and ensure that the machines are checked for malware / spyware before the next user logs on [R14].

178. If LSE is not going to provide its own DAM services, it should provide lists of available services highlighting those that require the minimal disclosure of personal data. These services must provide access to non-LSE users as well (I.17). LSE should also clearly state the implications of students signing up to these services using their personal details and which personal details are particularly sensitive [R15].

179. If LSE is going to recommend commercial DAM services, it might focus on those that provide limited viewer rights for other users rather than full scale levels of access [R16].

180. Increased awareness of the risks of large scale disclosure of information needs to be instilled in users [R17].
181. If providing its own DAM / VOM services LSE needs to offer something over and above security of its services in order to motivate students to use the LSE services over the alternatives. The LSE also needs to further investigate issues of security related to the use of non-LSE resources [R18].
References


Websites
www.angel.ac.uk/
www.angel.ac.uk/ShibbolethAtLSE/index.html
www.athensams.net/
www.dlib.org/dlib/february98/arms/02arms.html
www.identity-project.org
www.internet2.edu/pubs/200703-IS-MW.pdf
www.jisc.ac.uk
www.nextgov.com/the_basics/tb_20080327_1273.php
www.ukfederation.org.uk/
www.2ab.com/pdf/AccessManagement.pdf