Development of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education

Nigel Beacham
Computing Science
University of Aberdeen
Email: n.beacham@abdn.ac.uk

Bob Duncan
Business School
University of Aberdeen
Email: bobduncan@abdn.ac.uk

***Abstract*—The use of IT based systems in mainstream education brings a particular focus to bear on security. When these systems involve the use of cloud, the challenge increases exponentially. There are a great many benefits to be gained from cloud use, and therefore, we argue that developing a suitable approach to provide a secure cloud based learning environment, which would be used to facilitate use for inclusive practice in mainstream education would be a worthwhile goal. We demonstrate how to develop such an approach, which we believe could provide a more effective approach than traditional technology based approaches.**

Keywords–Inclusive education; security; privacy;cloud system.

I. Introduction

Educational systems are complex socio-technical systems and we need to consider what makes this so. Introducing educational services through the cloud can open pupils and staff to further exploitation, which we need to investigate [1][2]. We must bear in mind that the use of technical solutions alone can never succeed. Any solution must be addressed from a social engineering perspective, which considers the political, personal and social aspects. This paper addresses this important issue from this different perspective in order to address both the special needs of all involved, the special security and privacy issues raised by using a cloud based solution, and the other security and privacy factors, which must be taken into account.

Proper security and privacy for any web based system is challenging. When cloud systems are used, these challenges become considerably more difficult to address successfully. Thus, in Section II, we discuss the motivation for this work. In Section III, we discuss the educational needs and requirements, which must be satisfied in order to deliver the aims and goals of the work. In Section IV, we outline the security requirements needed to deliver the goals and aims of this work, and in Section V, we explain how achieving these security requirements will meet the security goals of the project. We discuss our conclusions and future work in Section VI.

II. Motivation

Virtual Learning Environments (VLE)s tend to be perceived as providing tools for specific individuals and not as tools for everybody [3]. They tend to be used for what is suggested as inclusion; to facilitate a pupil's ability to participate in learning [4]. We argue that such tools allow the pupils to access learning materials and/or curriculum, and in doing so, can allow pupils to sometimes integrate within the classroom [5]. To be seen as fully inclusive, they should be made available for everybody, including teachers, parents, support staff and other agencies, if appropriate. Instead of the emphasis being on the use of VLEs to allow individuals to participate, there needs to be a greater emphasis on the way all those in the class use VLEs to allow all to participate. Consequently, at present, little is understood about the way VLEs can be made available and used for everybody. Looking at current practices using VLEs, they tend to be used by pupils in schools under the control of teachers, despite teachers tending not to use VLEs themselves as part of their teaching practice. With a huge variety of VLEs available, teachers often lack confidence, awareness and knowledge of VLEs, particularly in how best to use them in the classroom [6]. Naturally, it can take teachers extra time and effort to consider how to use VLEs within the classroom for those pupils who are deemed as requiring such support. VLEs tend to be made available only to those children within their school who require them, and only to those areas the educational system deems require their use [7].

Even when VLEs are made available to a pupil outwith the school, they are often reported as failing to work appropriately and many VLEs are only available for use within a particular class. There are also numerous reports of many materials in VLEs residing on the shelf, often unused. Where VLEs have been used effectively in schools, it is unclear how useful they were, the impact they had on the children's learning, whether it is used in terms of integration or inclusion, and whether the tools were available from home and outside the school. Whether VLEs are made available or not, it can leave pupils excluded in class and also at home. New ways of observing and analysing the way VLEs are used need to be explored and better understood [8]. Whilst many children see technology as just part of life, some pupils see the computer and the use of VLEs as essential in all aspects of their learning. This is particularly evident from those pupils with disabilities, who have access to VLEs through assistive technologies and computers at home that support their needs, as opposed to those available in school. For other pupils, some may not wish to use VLEs as part of a differentiated task but as part of 'normal' class work. Furthermore, savvy teachers and pupils consider the limitations of some VLEs as being restrictive, especially when similar open source tools are free.

The impact of technology on learning is much more difficult to determine than first thought. Factors inside and outside school can impact on the use of VLEs for learning. For

example, barriers within schools can prevent the use of open source tools, while outside school, they are widely and freely available to all [9]. We believe that a cloud based approach can fulfil many of the practical requirements that must be addressed. Principal among these is the adaptable approach, with rapid scalability, and the ability to tailor resource usage to the demands of teaching in order to optimise operating costs. The use of cloud facilities also removes the barriers associated with rolling out large scale computing projects using traditional distributed hardware and software. This means the system could quickly and easily be scaled out to service not just a single school, but many schools within a region, or indeed across a country. We cover many of these technical points in later sections. Thus, our discussions throughout this paper are based on the premise that we will use a cloud based approach. We are acutely aware that pupils can be open to exploitation and grooming within VLEs, not just at school, but also in home and community environments. We are aware that pupils, teachers and administrative and support staff must be made ready for the step change in approach needed to ensure a high level of cloud-based security as the main mechanism by which we can ensure security and privacy inside the VLE. The lessons learned from this robust approach to security and privacy in this VLE can provide pupils with the foundation for a key skill in protecting the secure development of their personal on-line future. In the next section, we address the educational needs and requirements, which must be delivered in order to develop a successful system.

III. The Educational Needs and Requirements

It is likely that teachers may lack preparedness in understanding the proper use of tools and techniques to monitor and retain a secure and safe VLE, a vital part of ensuring the successful running of a safe and secure environment, so this must form part of the preparation for the use of such a system [9]. We must also consider current VLE limitations in the context of Transformability theory.

Transformability theory is a framework for transforming learning capacity [10]. It provides a way of conceptualising learning capacity and how to improve it through the teaching practices used by teachers and schools [11][12][13]. Underpinning the theory are the three principles: co-agency; everybody; and trust. Co-agency relates to teachers, pupils, parents and support services being a joint enterprise. Everybody relates to teachers, pupils, parents and support services being responsible and committed to all pupils in a learning community. Trust relates to building close trusting relationships between teachers, pupils, parents and support services. This theory not only provides a lens within which to research, reflect and inform the ways Assistive Technology (AT) and Information and Communications Technology (ICT) are generally used to enable meaningful participation in learning, but can guide teachers on what to do, and not to do, in their practice with cloud-based VLEs to improve security.

In educational terms, AT focuses on providing access to materials and the curriculum [4]. Research on the development and use of AT tends to centre on investigating how tools improve access. This is only one of a number of aspects, which need to be addressed to improve the capacity to learn. Other aspects include the role AT plays in enhancing collaboration, achievement, acceptance and recognition of learner diversity, and furthermore how effective using a particular AT is to facilitate collaboration, achievement and acceptance and recognition of diversity. It is these aspects, which tend to be ignored, and as many teachers will know, make an important difference in improving learning capacity. An inclusive pedagogical approach draws attention to these additional aspects. Theories such as transformability help inform teachers not only to use AT to improve access to the materials and the curriculum but also to address the other crucial aspects of learning capacity [14][15].

Thus, we need a theoretical framework to extend inclusive education practices to security – in effect using a transformability theory approach. By this means, we can ensure that not just technical staff are aware of preparedness in cloud-based security, but everybody in the learning ecosystem does too. This co-agency approach between pupils, parents, teachers, administrators and technical staff is vitally important and is required to keep pupils and staff safe, not just for the duration of their learning, but as a solid foundation to ensure their lifelong online protection. This will also help us to satisfy the need to develop closer trust within learning communities as a whole, and to ensure everybody perceives and benefits from being recognised, accepted and included [16].

IV. Security Requirements to be Addressed

The well recognised security requirements of any enterprise are confidentiality, integrity and availability (CIA). Duncan and Whittington [17], suggest that we should also add the goals of sustainability, resilience and ethics. The traditional approach to satisfy the CIA requirements, are access control, plus encryption, for confidentiality; transaction monitoring, possibly with encryption, for integrity; and redundancy for availability. Long term sustainability comes from providing a system that works, achieving the goals set for it, providing value for money, and does so in a reliable fashion. Resilience comes from providing a system that is resilient to unexpected shock; and a business continuity mechanism or policy, can assist with this task. Ethical behaviour on the part of all the actors in a cloud ecosystem can be delivered where all parties are properly accountable, and through their individual ethical behaviour, demonstrate they will not try to gain personal advantage at the expense of others within the ecosystem.

These goals are generally well understood by enterprises, and are often approached using technical solutions. However, in any business environment, the business architecture comprises a combination of people, process and technology [18], not by technology alone. The people of any business are generally recognised as being the weakest link, and whether it is a FTSE100 world class enterprise, a government organisation, a small firm, or an educational body, the fact remains that the people in the organisation present the largest threat. When we talk about people in the context of this paper, we refer to the description for everybody in Section II, above. To this, we must add all the agents involved in the cloud ecosystem, and of course, the attack community. The bad guys have long recognised that the weakest part of any IT system is actually the users of that system, which is why they have long been developing and polishing the very successful practice of social engineering. Thus, proper user training must be undertaken.

Since cloud computing is enabled by use of the internet, then web based applications present some of the most successful attack vectors for the bad guys. While web vulnerabilities are well understood, we can see from data collected by the Open Web Application Security Project (OWASP) [19], who

publish a top ten list of web security vulnerabilities every three years, that these attacks continue to be perpetrated successfully year on year. OWASP provide the most comprehensive list of the most dangerous vulnerabilities and a number of very good mitigation suggestions. The last three OWASP lists for 2007, 2010 and 2013 are provided in TABLE I, below. These lists are

TABLE I. OWASP TOP TEN WEB VULNERABILITIES — 2013 - 2007 [19]

2013	2010	2007	Threat
A1	A1	A2	Injection Attacks
A2	A3	A7	Broken Authentication and Session Management
A3	A2	A1	Cross Site Scripting (XSS)
A4	A4	A4	Insecure Direct Object References
A5	A6	-	Security Misconfiguration
A6	-	-	Sensitive Data Exposure
A7	-	-	Missing Function Level Access Control
A8	A5	A5	Cross Site Request Forgery (CSRF)
A9	-	-	Using Components with Known Vulnerabilities
A10	-	-	Unvalidated Redirects and Forwards

based on the result of analysis of successful security breaches across the globe, and highlight the most easily breached areas in web based systems. It illustrates the worst ten web vulnerabilities in computing systems globally. While these vulnerabilities are relatively easy to address, it is concerning that they continue to recur year after year. Thus, these should all be addressed. There are likely to be additional potential vulnerabilities, which also must be considered, not necessarily only technical issues such as we have illustrated above. Duncan and Whittington [17], identified ten key management issues, which also must be addressed. Often these are not properly thought through by management.

The ten key management security issues identified are: The definition of security goals; Compliance with standards; Audit issues; Management approach; Technical complexity of cloud; Lack of responsibility and accountability; Measurement and monitoring; Management attitude to security; Security culture in the company; and the threat environment. Further details on each of these key areas of potential weakness are provided in [17]. As quickly as security researchers come up with solutions to new vulnerabilities, the bad guys, in turn, come up with successful attacks against these fixes. This continual "arms race", means that it is also essential to ensure a proper monitoring system forms part of the design framework. Also, since cloud provides easy scalability of resources to track the demand curve, it will also be necessary to have a system that can track the addition of new instances, the shutting down of instances no longer required, and the extraction of suitable audit trail and system logging data for forensic examination purposes in the event of a breach. These security requirements we propose go much further than conventional technical approaches in use until now. It is clear from recent annual security breach reports such as [20][21][22], which clearly demonstrate the security and privacy problems still faced today. The same attacks continue to be successful year on year. Looking at this five year summary of Verizon reports shown in TABLE II below, we can see the result of failing to use a complete solution to the security problem:

It is clear that a more complete solution must be used, and we have outlined the essential components of such a system. While a cloud service provider might well have an incredibly secure and effective technical cloud solution, it will be useless where cloud users are compromised by a successful social engineering attack.

TABLE II. VERIZON TOP 5 SECURITY BREACHES — 2010-2014 (1=HIGHEST) [23][24][25][26][20]

Threat	2010	2011	2012	2013	2014
Hacking	2	1	1	1	1
Malware	3	2	2	2	2
Misuse by company employees	1	4	5	5	5
Physical theft or unauth. access	5	3	4	3	4
Social Engineering	4	5	3	4	3

V. HOW THIS MEETS SECURITY GOALS

There are many challenges, which must be met by cloud based systems, meaning a far more rigorous approach is needed. A fundamental requirement is the use of a proper monitoring system [27]. Without one, it will be almost impossible to tell that a system has been breached. With no proper audit trail and sufficient forensic evidence, it will be extremely difficult to understand precisely which data has been accessed, modified, ex-filtrated or deleted. The popular approach to cloud cyber security generally centres around technical solutions. For the reasons stated in Section IV, this will always prove inadequate in the face of adversaries with ever improving skill levels and attack tool sets. Thus, our proposed framework must incorporate some addition components. Cloud can necessarily create and destroy instances at will, in order to scale up, or down, as demand dictates, so it will be necessary to have some level of control and monitoring system to log each new instance as it is created, or deleted, and should constantly monitor the instance throughout its life-cycle, to ensure it continues to function as expected, and has not been compromised by an attack.

The controller function should be created in a separate server from the running instances. The data logs and any audit trail should be stored in another separate secure server running immutable database software to guard against attack. Neither of these systems should run any other software, and should not be exposed to public access on the internet. Each should run behind a strong firewall, and should be protected by intrusion detection software. In addition, the main system should also run behind a secure cloud firewall, and should also run intrusion detection software. Access should be delivered via multi-step authentication, to protect against common password attack strategies. There are three ways to do multi-step authentication:

1) Something the user knows (e.g., a password, partial password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern), or security question);
2) Something the user has (e.g., wrist band, ID card, security token, mobile phone with built-in hardware token, software token, or mobile phone holding a software token);
3) Something the user is or does (e.g., fingerprint, retinal pattern, signature, face, or voice identifier).

The minimum use of at least two of the categories with three or more questions to be successfully answered before access is granted, provides an extremely secure level of access control, without the use of passwords. We have outlined how there are many more threats than just those that can be solved by technical means alone. These additional threats are very effective, yet relatively simple to guard against. The approach we have outlined here is not technically difficult to achieve,

nor expensive to implement, yet these steps, taken in concert with conventional technical solutions, can prove invaluable in the fight against attack. This section considers the above security threats from the perspective of transformability theory and its three underlying principles. Transformability theory has as its underlying philosophy 'Learning without Limits'. Based on this premise, we suggest that security threats should be faced in a similar fashion — 'Security without Barriers'. From a social perspective the more barriers are erected, the less secure communities will be. Thus, it is important to develop a culture of ethical hacking between agencies. A culture that ensures everybody is involved and included so they acquire the knowledge and skills to keep them safe from, and prepared for, cyber security threats. Core to this is the need to develop trust within the community so focus can be targeted outside, in the knowledge that inside, the community is soundly built.

Threats caused by e.g., pupils targeting their peers by sending SMSs, emails and tweets, etc., need to be confronted and addressed immediately and openly within the learning environment. The perpetrator, their parents and (where necessary) other agencies need all to be aware. This may not reduce the stress on the targeted pupil but does identify and expose the perpetrator and their behaviour. Such an approach requires everybody's participation, trust and involvement. Action needs to focus on improving respect and acceptance with the outcome of changing behaviour. Physical threat or unauthorised access can be reduced when working with and through others. So, working on activities requiring the synchronisation of two or more agents can reduce the likelihood a third party will obtain unauthorised access. We encourage more use of computer-supported collaborative learning (CSCL)[28][29], approaches and tools. Social engineering threats ultimately tend to target entire communities rather than individuals within.

VI. Conclusion

This paper has outlined the problems faced when considering the use of a cloud based technology solution in mainstream education, and in particular where the learning environment is to be used for inclusive practice. We argue for a more inclusive approach to ethical hacking; providing an environment that encourages security without barriers; all of which can be used for communities as well as a society built on trust. Transformability theory provides a framework, which introduces a positive mind-set that together, communities such as those within education, can address security threats within both educational systems and any socio-technical system. It provides a common language from a social engineering perspective to discuss and deal with threats; and provides a way to measure and monitor environments for threats in the future. Such an approach, whilst still in its infancy, will be developed and piloted and provide useful knowledge in the implementation of cloud-based security.

As we move towards virtual and augmented collaborative learning environments such as Second Life, inclusive pedagogies must have more dynamic security. Many real-world social skills are replicated in these virtual and augmented worlds [30]. It is therefore important that inclusive pedagogies are adaptable for physical and virtual learning environments, including considering the role AT can play in enabling meaningful participation in learning within such multi-dimensional environments. To date, few ATs can be integrated effectively within groupware systems in mainstream education.

References

[1] S. K. Beach, "Usable cybersecurity: Human factors in cybersecurity education curricula, " Natl. Cybersecurity Inst. J., 2014, p. 5.

[2] N. Sultan, "Cloud computing for education: A new dawn?" Int. J. Inf. Manage., vol. 30, no. 2, 2010, pp. 109–116.

[3] G. Attwell et al., "Personal learning environments-the future of eLearning?" Elearning Pap., vol. 2, no. 1, 2007, pp. 1–8.

[4] L. Florian and J. Hegarty, ICT and special educational needs: a tool for inclusion. McGraw-Hill Education (UK), 2004.

[5] N. Beacham and K. McIntosh, "Student teachers' attitudes and beliefs towards using ICT within inclusive education and practice," J. Res. Spec. Educ. Needs, vol. 14, no. 3, 2014, pp. 180–191.

[6] N. Sclater, "eLearning in the cloud," Int. J. Virtual Pers. Learn. Environ., vol. 1, no. 1, 2012, pp. 10–19.

[7] S. Hubackova, "Pedagogical foundation of eLearning," Procedia-Social Behav. Sci., vol. 131, 2014, pp. 24–28.

[8] E. Wiebe and D. Sharek, "eLearning," in Why Engagem. Matters. Springer, 2016, pp. 53–79.

[9] N. Beacham, "Developing NQTs e-pedagogies for inclusion," Institution University of Aberdeen, May 2011.

[10] S. Hart, A. Dixon, M. Drummond, and D. McIntyre, "Learning without limits," in Sage Handb. Spec. Educ., 1st ed. Open University Press, 2008, ch. 38, pp. 499–514.

[11] L. Florian and J. Spratt, "Enacting inclusion: A framework for interrogating inclusive practice," Eur. J. Spec. Needs Educ., vol. 28, no. 2, 2013, pp. 119–135.

[12] L. Florian, K. Young, and M. Rouse, "Preparing teachers for inclusive and diverse educational environments: Studying curricular reform in an initial teacher education course," Int. J. Incl. Educ., vol. 14, no. 7, 2010, pp. 709–722.

[13] C. Forlin and D. Chambers, "Teacher preparation for inclusive education: Increasing knowledge but raising concerns," Asia-Pacific J. Teach. Educ., vol. 39, no. 1, 2011, pp. 17–32.

[14] S. Riddell, "Social justice, equality and inclusion in Scottish education," Discourse Stud. Cult. Polit. Educ., vol. 30, no. 3, 2009, pp. 283–296.

[15] T. Mortimore, "Dyslexia in higher education: Creating a fully inclusive institution," J. Res. Spec. Educ. Needs, vol. 13, no. 1, 2013, pp. 38–47.

[16] M. Ainscow and A. Sandill, "Developing inclusive education systems: The role of organisational cultures and leadership," Int. J. Incl. Educ., vol. 14, no. 4, 2010, pp. 401–416.

[17] B. Duncan and M. Whittington, "Enhancing cloud security and privacy: The power and the weakness of the audit trail," in Cloud Comput. 2016 7th Int. Conf. Cloud Comput. GRIDs, Virtualization. Rome: IEEE, 2016, pp. 125–130.

[18] PWC, "UK information security breaches survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com Last accessed: Jan 2017

[19] OWASP, "OWASP top ten vulnerabilities 2013," 2013. [Online]. Available: https://www.owasp.org/ Last accessed: Jan 2017

[20] Verizon, "2014 Data breach investigations report," Tech. Rep. 1, 2014. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf Last accessed: Jan 2017

[21] PWC, "2014 Information security breaches survey: Technical report," Tech. Rep., 2014.

[22] Trustwave, "Trustwave global security report," Tech. Rep., 2013. [Online]. Available: https://www2.trustwave.com/2013GSR.html Last accessed: Jan 2017

[23] W. Baker et al., "Data breach investigations report," Tech. Rep., 2010.

[24] Verizon, "2011 Data breach investigation report: A study conducted by the Verizon RISK team in cooperation with others," Verizon/USSS, Tech. Rep., 2011.

[25] Verizon, N. High, T. Crime, I. Reporting, and I. S. Service, "2012 Data breach investigations report," Verizon, Tech. Rep., 2012.

[26] Verizon, "Verizon2013," Tech. Rep., 2013.

[27] B. Duncan and M. Whittington, "The importance of proper measurement for a cloud security assurance model," in 2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci., Vancouver, 2015, pp. 1–6.

[28] Wikipedia, "Computer supported collaborative learning," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Computer-supported_collaborative_learning Last accessed: Jan 2017

[29] S. Järvelä and A. F. Hadwin, "New frontiers: Regulating learning in CSCL," Educ. Psychol., vol. 48, no. 1, 2013, pp. 25–39.

[30] A. Dix, J. Finlay, G. Abowd, and R. Beale, "Evaluation techniques," Hum. Comput. Interact., 2004.