A Multi-factor Authentication Method for Security of Online Examinations

Abrar Ullah[1(✉)], Hannan Xiao[2], and Trevor Barker[2]

[1] School of Computing and Management, Cardiff Metropolitan University, Cardiff, UK
aaaullah@cardiffmet.ac.uk
[2] School of Computer Science, University of Hertfordshire, Hatfield, UK
{H.xiao,T.l.barker}@herts.ac.uk

Abstract. Security of online examinations is the key to success of remote online learning. However, it faces many conventional and non-conventional security threats. Impersonation and abetting are rising non-conventional security threats, when a student invites a third party to impersonate or abet in a remote exam. This work proposed dynamic profile questions authentication to identify that the person taking an online test is the same who completed the course work. This is combined with remote proctoring to prevent students from taking help from a third party during exam. This research simulated impersonation and abetting attacks in remote online course and laboratory based control simulation to analyse the impact of dynamic profile questions and proctoring. The study also evaluated effectiveness of the proposed method. The findings indicate that dynamic profile questions are highly effective. The security analysis shows that impersonation attack was not successful.

Keywords: Security · Authentication · Online examination

1 Introduction

Security is an important non-functional requirement for design and implementation of web-based applications. According to Schechter [1], it is a process of securing computer hardware, software, and networks against misuse and harm. A harm or misuse is a loss of desired system properties including confidentially, integrity and availability. The application of computer security has a wider scope, including hardware, software and network security. The focus of this research is application-level security, which falls into the information security context. Online summative assessment faces a number conventional and non-conventional security threats. The conventional threats include common web application threats. These are prevented and mitigated using the same approaches adopted for many web applications. However, the non-conventional threats are beyond the scope of many conventional security methods. These threats include collusion and impersonation during online assessments. This research proposes the use of dynamic profile questions and remote proctoring to prevent against impersonation and abetting in a remote online examination. This paper reports an empirical

A.-S. K. Pathan et al. (Eds.): SGIoT 2018, LNICST 256, pp. 131–138, 2019.
https://doi.org/10.1007/978-3-030-05928-6_13

study using an online course and laboratory based session where participants simulated an impersonation and abetting attack in presence of a live proctor.

2 Background

Security is protection of assets. According to Ullah [2], asset is anything that has value for an organisation. Tajuddin [3] states that information security is protection of valuable "information". According to ISO/IEC 27002 [4], it is the protection of information from a wide range of threats that ensures business continuity and minimises business risks. The concept of business can be applied in any commercial or non-commercial context, such as online learning. The focus and research context of this work relates to summative assessment or remote online examinations. The growth in the use of online learning in higher education has been documented and reported in many studies [5–9]. It has attracted significant research focus on developing and delivering secure, efficient and effective learning environments. However, there have been many concerns about the security of online learning environments. With increasing demand, there are equally increasing concerns for the integrity of the summative assessment also known as online examinations [10].

The work is part of an ongoing research on security and usability of authentication by challenge questions. The authors conducted multiple empirical studies to analyse usability and security threats of text-based, image-based and dynamic profile questions to mitigate impersonation and abetting attacks [11, 12]. In these attacks, a student invites a third party to impersonate or abet in an online examination scenario. In the previous studies, the author proposed and evaluated a text-based challenge questions approach [13]. However, these questions were reported with usability and security issues [14]. In a similar vein, the use of image-based questions revealed improved usability [15], however, these questions were not sufficient to mitigate impersonation and abetting. In order to address the security issues, the authors proposed dynamic profile questions [7]. These questions are created in the background when a student performs learning activities. Individual student profile is built during the learning process. To access an online assessment, the student is presented with a subset of questions randomly extracted from his/her profile. In a recent study, the authors conducted a focus group study [6] with online programme tutors who recommended the use of dynamic profile questions [7], remote proctoring [16], and a secure browser to mitigate impersonation and abetting attacks.

The focus group study presented in an earlier study indicates that the use of dynamic profile questions with a secure browser and proctoring (ProctorU) [16] can positively influence collusion attacks. As described above, the dynamic profile questions are created non-intrusively and non-distractingly in the background when a student performs learning activities [7]. Using this method, a student's profile is built and consolidated in the background during the learning process. Students are not aware of which questions will be asked for authentication. This attempts to verify that the person who is taking the online test is the same individual who completed the coursework. The use of a secure browser and proctoring monitors an online examination, and attempts to ensure that a student is not taking help from the Internet or an abettor sitting close by or

remotely. However, a student may still circumvent the system and share access credentials with an impersonator before the test session. Furthermore, usability attributes such as effectiveness is also important for secure implementation of authentication methods. The effectiveness is an important attribute defined by the International Organisation for Standards (ISO) which contributes to the usability [17]. In the context of this study, effectiveness means that students were able to answer dynamic profile questions correctly with a low error rate. This study will investigate the following:

- The effectiveness of dynamic profile questions in a proctored examination.
- Whether a student can share information about learning activities and experience with a third party impersonator using email, instant messaging, phone, or face-to-face meeting before an online test session, and how successful the impersonator is in answering the dynamic profile questions.

3 Research Methodology

This study was conducted using a real online course followed by a controlled laboratory-based simulation session. The usability test and risk-based security assessment methods were adopted to evaluate the usability and security of dynamic profile questions. The usability test method is a usability inspection, which tends to focus on the interaction between humans and computers [18]. Using this method, the representative users – i.e. students – work on typical system tasks on an online course and examination, which implements dynamic profile questions in a proctored test. In this study, the system tasks were simulated in a laboratory-based environment. The usability evaluation scale was used to translate the effectiveness analysis. This scale describes the usability of products in the 90 s as exceptional, 80 s as good, 70 s as acceptable, and anything below 70 indicates usability issues that are cause for concern [19].

The risk-based security assessment approach provides rapid quantification of security level risks associated with processes [20]. This method focuses on the test of features and functions of artefacts based on the risk of their failure using abuse case scenarios [21]. An abuse case scenario was simulated to investigate impersonation attacks, when dynamic profile questions are implemented for authentication of students in a proctored examination.

This study was conducted in a remote online learning environment and face-to-face sessions involving on-campus students. It was organised into two phases described below i.e. Phase I – online course and Phase II – abuse case simulation.

3.1 Phase I – Online Course and Student Pairing

In Phase I of the study, an online course was conducted to provide learning opportunities for students and facilitate the collusion abuse case scenario. The structure of Phase-I is described below.

- **PHP & MySQL Course Design:** A 'PHP and MySQL' online course was organised with three weekly modules, which included lessons, forum discussions, assignments, quizzes, grades and student reflection at the end of each week. The course was set up and deployed in the MOODLE Learning Management System (LMS) on a remote web server accessible on the Internet. Students were required to invest 10 h weekly learning effort for 15 days in a span of three weeks.
- **Participants Recruitment:** On-campus students from the School of Computer Science, University of Hertfordshire, were recruited to participate in the study and the online course. The course was advertised on the StudyNet. To motivate students the course was offered free of charge. Participants were selected on the basis that they knew each other already. They were also required to have basic programming knowledge in order to enrol. A total of 12 students were enrolled and completed the three-week course. There were 7 (58%) male and 5 (42%) female participants. They were also enrolled in BSc/MSc programmes which were helpful in setting up face-to-face meetings to present the study structure and research objectives, and perform the abuse case scenario in a laboratory.
- **Presentation and Students Registration:** Participants were required to attend a face-to-face 15 min presentation on the course structure and research objectives, before registration. They were also provided detailed information on an impersonation abuse case scenario. After the presentation, all participants signed the consent forms mandated by the University ethics regulations.
- **Pairing up of Participants for Impersonation:** In order to perform the impersonation, each participant was paired up with a fellow student (classmate), where both participants confirmed that they were familiar already. All participants consented to share learning experience and activities with their pairs. They were informed about the format of an impersonation abuse case scenario, which was conducted towards the end of the course.
- **Online Course Work:** The instructor-led course was conducted over a period of three weeks. Participants were required to submit their weekly assignments in order to access their weekly quizzes. Each assignment was based on the weekly course content, which ensured participants' engagement. It was mandatory for each participant to take their weekly quizzes and provide a 'reflection feedback' towards the end of each week.
- **Creating Dynamic Profile Questions:** Dynamic profile questions were created manually during the course for each individual student and stored in a Microsoft Word file in a secure location. These questions were created on a daily basis for each participant after access to course content including lessons, assignment submission, assignment grades, quiz completion, feedback and reflection, and forum discussion. This helped with creating and consolidating a profile for each participant. A total of 28 dynamic profile questions were created for each participant. Dynamic profile questions created during the coursework were not shown to any participant during the online course until the abuse case scenario described in the following section.

3.2 Phase II – Impersonation Abuse Case Scenario

This phase was performed towards the end of three week online course described in Phase I above. This study simulated the following impersonation abuse case scenario:

1. Participants were paired up before registration as described above in Phase I.
2. Dynamic profile questions for each participant were manually created and stored in their respective profiles. These questions were extracted from student activities on a daily basis, as described above in Phase I.
3. Participants were asked to share their learning experience, learning activities, and cues with their pairs during the course. They were allowed to share this information using any communication means, e.g. email, phone, WhatsApp, Skype, face-to-face meeting, Facebook, Facetime, SMS, printed paper, etc. They were required to memorise the shared information for simulating impersonation in a proctored examination.
4. At the end of week three, participants attended a laboratory-based simulation session.
5. Participants were informed about the format of simulating the laboratory-based proctored session. They were required to answer the questionnaire from memory and were not allowed to use an electronic or printed copy of the information shared by their pairs for impersonation. Also, they were not allowed to communicate or share information when answering the two questionnaires in the following order:
   (a) **Questionnaire 1 (Effectiveness)**: Participants were asked to answer paper-based Questionnaire 1 with a total of 10 dynamic profile questions randomly extracted from their own profiles created during the course work in Phase I.
   (b) **Questionnaire 2 (Impersonation)**: After answering Questionnaire 1, the participants were asked to answer a paper-based Questionnaire 2 with a total of 5 dynamic profile questions randomly extracted from their pair's profile to simulate impersonation.

4 Results

This section aims to evaluate the usability of dynamic profile questions in the presence of a live proctor. At the end of week three, 12 participants answered 120 dynamic profile questions which were created during the course. Results of the abuse case scenario is also analysed to determine the outcome of an impersonation attack.

4.1 Effectiveness

The effectiveness is considered to be the degree of accuracy of participants' responses. It is an important usability factor which indicates a degree of completeness with which users achieve a specified task in a certain context [22]. In the context of this study, it means that participants were able to provide correct answers to their dynamic profile questions correctly with a low error rate. It was analysed on the data collected from participants' answers on paper-based questionnaire 1 in a laboratory-based session.

Table 1 column 2 shows the mean of correct answers to dynamic profile questions in order to analyse effectiveness. The findings show 114 (95%) correct answers, which indicates positive outcome.

Table 1. Usability and security analysis

	Effectiveness	Impersonation
1	10 (100%)	2 (20%)
2	10 (100%)	1 (10%)
3	9 (90%)	3 (30%)
4	9 (90%)	3 (30%)
5	10 (100%)	2 (20%)
6	9 (90%)	1 (10%)
7	10 (100%)	2 (20%)
8	9 (90%)	2 (20%)
9	9 (90%)	3 (30%)
10	9 (90%)	2 (20%)
11	10 (100%)	2 (20%)
12	10 (100%)	3 (30%)
Total	114 (95%)	26 (22%)

According to the usability scale and letter grades (70%–79% acceptable, 80%–89% good, more than 90% exceptional) described by [17], 95% correct answers is an exceptional effectiveness.

4.2 Impersonation in Presence of Live Proctoring

The abuse case scenario was performed to decide if dynamic profile questions can mitigate impersonation in a proctored exam. In a laboratory-based session, participants answered paper-based Questionnaire 2 consisting of five dynamic profile questions on behalf of their pairs. They memorised the shared information during pairing and answered the questionnaire from memory. These questions implemented five multiple choice options and the probability of a correct answer to a random guessing would be 1/5th or 20%. In the impersonation abuse case scenario, participants answered 26 (22%) of the questions correctly on behalf of their pairs. These questions were not shown to any participant during the online course and presented at the final stage of the study to evaluate their ability to circumvent the dynamic profile question approach and impersonate students in the presence of a live proctor. The findings in Table 1 column 3 show that the sharing of information associated with individuals' learning experience led to correct answers just above 1/5th of the total questions.

To determine the significance of difference in the means of correct answers to dynamic profile questions by a student and a third party impersonator, a one-way ANOVA was performed on the data shown in Table 1 columns 2 and 3, which shows a significant difference $F = 596$; $p = 0.00$ ($p < 0.01$); eta-squared $\square 2 = 0.97$..

An ANOVA test on a small sample size may not produce significant values due to insufficient power. However, findings of the test here yielded significant value.

In a practical situation, this may fail the authentication and alert the proctor or invigilator. This shows that students were able to answer their own challenge questions presented in the previous section; however, collusion between students and impersonators was not successful.

5 Conclusion

This study examined the use of dynamic profile questions in a proctored examination. Participants shared information using mobile phones, emails, chat, and face-to-face meetings at their own convenience before an online examination in pairs. They memorised the shared information and answered the questionnaire on dynamic profile questions on behalf of their pairs in the presence of a proctor. The results showed that dynamic profile questions decreases impersonation attacks when implemented with live proctoring. Participants' sharing helped the impersonators to provide 26 (22%) correct answers in the impersonation attack, which is just above 20%, which is the percentage of correct answers by chance. There was a significant difference ($p < 0.01$) in the correct answers between a student (114: 95%) and an impersonator (26: 22%). This indicates that, dynamic profile questions extracted from course content and submissions makes sharing harder for students and could be implemented for secure authentication. However, future work is warranted on a larger sample size.

References

1. Schechter, S.E.: Computer Security Strength & Risk: A Quantitative Approach. Harvard University Cambridge, Massachusetts, Massachusetts (2004)
2. Ullah, A.: Security and Usability of Authentication by Challenge Questions in Online Examination. University of Hertfordshire, Hatfield (2017)
3. Tajuddin, S., Olphert, W., Doherty, N.: Relationship between stakeholders' information value perception and information security behaviour. In: International Conference on Integrated Information (IC-ININFO 2014): Proceedings of the 4th International Conference on Integrated Information 2015. AIP Publishing (2015)
4. Sahibudin, S., Sharifi, M., Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In: Modeling & Simulation, 2008 AICMS 2008 Second Asia International Conference on 2008. IEEE (2008)
5. Buzzetto-More, N.: Student perceptions of various e-learning components Interdisciplinary. J. E-Learn. Learn. Objects **4**(1), 113–135 (2008)
6. Ullah, A., Barker, T., Xiao, H.: A focus group study: usability and security of challenge question authentication in online examinations. In: International Conference on Information Technology and Applications (ICITA). Academic Alliance International, Sydney Australia (2017)
7. Ullah, A., Xiao, H., Barker, T.: A dynamic profile questions approach to mitigate impersonation in online examinations. J. Grid Comput. (Knowl. Discov.), 1–15 (2018)

8. Allen, I.E., Seaman, J.: Online Nation Five Years of Growth in Online learning Needham. Sloan Consortium, Mass (2007)
9. Koohang, A., Riley, L., Smith, T., Schreurs, J.: E-learning and constructivism: from theory to application Interdisciplinary. J. E-Learn. Learn. Objects **5**(1), 91–109 (2009)
10. Watson, G., Sottile, J.: Cheating in the digital age: do students cheat more in online courses? Online J. Distance Learn. Adm. **13**(1), n1 (2010)
11. Ullah, A., Xiao, H., Barker, T.: A dynamic profile questions approach to mitigate impersonation in online examinations. J. Grid Comput. 1–15 (2018)
12. Ullah, A., Xiao, H., Barker, T.: A study into the usability and security implications of text and image based challenge questions in the context of online examination. Educ. Inf. Technol. 1–27 (2018)
13. Ullah, A., Xiao, H., Lilley, M.: Profile based student authentication in online examination. In: International Conference on Information Society 2012. IEEE, London (2012)
14. Ullah, A., Xiao, H., Barker, T., Lilley, M.: Evaluating security and usability of profile based challenge questions authentication in online examinations. J. Internet Serv. Appl. **5**(1), 2 (2014)
15. Ullah, A., Xiao, H., Barker, T., Lilley, M.: Graphical and text based challenge questions for secure and usable authentication in online examinations. In: The 9th International Conference for Internet Technology and Secured Transactions (ICITST) 2014. IEEE, London (2014)
16. Mahmood, N.: Remote Proctoring Software Means Students Can Now Take Exams From Home. Technological News Portal; 2010 [cited 2011 13/07/2011]. http://thetechjournal.com/science/remote-proctoring-software-means-students-can-now-take-exams-from-home.xhtml
17. Iso9241-11. Ergonomic Requirements for Office Work with Visual Dispaly Terminals, Part 11: Guidance on Usability. ISO 9241-11. Geneva1998)
18. Corry, M.D., Frick, T.W., Hansen, L.: User-centered design and usability testing of a web site: an illustrative case study. Educ. Technol. Res. Dev. **45**(4), 65–76 (1997)
19. Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: adding an adjective rating scale. J. Usability Stud. **4**(3), 114–123 (2009)
20. Ni, M., Mccalley, J.D., Vittal, V., Tayyib, T.: Online risk-based security assessment. IEEE Trans. Power Syst. **18**(1), 258–265 (2003)
21. Mcgraw, G.: Software security & privacy. IEEE **2**(2), 80–83 (2004)
22. Seffah, A., Kececi, N., Donyaee, M.: QUIM: a framework for quantifying usability metrics in software quality models. In: Quality Software, 2001 Proceedings Second Asia-Pacific Conference on 2001. IEEE (2001)