J Grid Computing
https://doi.org/10.1007/s10723-018-9442-6

# A Dynamic Profile Questions Approach to Mitigate Impersonation in Online Examinations

**Abrar Ullah · Hannan Xiao · Trevor Barker**

Received: 29 January 2018 / Accepted: 9 May 2018


**Abstract** Online examinations are an integral component of many online learning environments, which face many security challenges. Collusion is seen as a major security threat to such examinations, when a student invites a third party to impersonate or abet in a test. This work aims to strengthen the authentication of students via the use of dynamic profile questions. The study reported in this paper involved 31 online participants from five countries over a five-week period. The results of usability and security analysis are reported. The dynamic profile questions were more usable than both the text-based and image-based questions ($p < 0.01$). An impersonation abuse scenario was simulated using email and mobile phone. The impersonation attack via email was not successful, however, students were able to share answers to dynamic profile questions with a third party impersonator in real time, which resulted in 93% correct answers. The sharing of information via phone took place in real time during an online test and the response time of an impersonator was significantly different ($p < 0.01$) than a student. The study also revealed that a response time factor may be implemented to identify and report impersonation attacks.

**Keywords** Authentication · Security · Usability · Online examinations

## 1 Introduction

In typical online learning environments, students are assessed from remote locations, which raise the security concerns of stakeholders about the integrity of online examinations [1]. Cheating is one of the major threats due to vulnerable authentication approaches and the degree of difficulty to verify the identity of remote users. Face-to-face invigilation can be expensive and logistically challenging in dispersed geographical locations. However, many educational institutions prefer supervised examinations to the use of high stake online examinations largely because of the difficulty in the authentication of a remote user with no face-to-face interaction [2].

Student cheats in online examinations using a number of methods. The work presented in this paper investigates collusion attacks i.e. impersonation, when a student invites a third party to take the test on his/her behalf. The student shares their access credentials via two methods: email, and instant messaging using

Abrar Ullah (✉)
Llandaff Campus, Cardiff Metropolitan University,
Cardiff, CF5 2YB, UK
e-mail: aaaullah@cardiffmet.ac.uk

Hannan Xiao · Trevor Barker
College Lane Campus, University of Hertfordshire,
Hatfield, AL10 9AB, UK
e-mail: h.xiao@herts.ac.uk

Trevor Barker
e-mail: t.1.barker@herts.ac.uk

Published online: 31 May 2018

mobile phone. Collusion is a challenging threat which is difficult to detect and report after the completion of an online examination.

This paper presents the findings of an empirical study conducted in a real online course with remote international participants. The work focuses on research that aims to strengthen the authentication of examinees via the use of a challenge questions approach [3]. The traditional text-based challenge questions approach requires students to register their answers before authentication.

This allows students to store, memorize, and share these questions with a third party to perform an impersonation attack. To discourage students from sharing their credentials, this study proposes dynamic profile questions, which are created in the background when a student per-forms learning activities. This study will investigate the following:

1. The effectiveness of the proposed dynamic profile question approach.
2. Whether a student could share dynamic profile questions with a third party impersonator using asynchronous and real-time communication methods (i.e. email and mobile phone) and successfully perform impersonation.

The paper is organized into multiple sections starting with introduction to highlight the overview and objectives. Section 2 provides a literature review, discussion on security threats and justification for the research work presented in this paper. Section 3 outlines detail of research methodology. Usability and security findings are discussed in Sections 4 and 5.

## 2 Background and Related Work

The threat level of collusion in online examinations is different from other online applications such as banking where implicit collusion is unlikely to happen [4]. Students are motivated by varying reasons to collude in online examinations. Evans and Craig [5] identified different reasons to collude including desire for better grades, fear of failure, pressure from parents to do well, unclear instructional objectives and being graded on a curve.

A collusion attack is an organized form of cheating which involves collaboration between a student and a third party to solve examination problems. It is a consensual and pre-planned cheating attack by a student. It has an ongoing issue reported in a number of recent studies [6–8]. Collusion can be classified in the following categories based on its occurrence in different scenarios [9]

### 2.1 Impersonation

In an impersonation attack, a student shares his or her access credentials with a third party who takes the online test. It is difficult to detect impersonation once an online test is completed [10]. These attacks are pre-planned and consensual, involving legitimate students with valid access credentials. Moini and Madni [2] state that impersonation and illegal sharing or disclosure of authentication secrets is challenging to defend against in a remote online setting. They identified that students invite third parties to take their online tests for extra benefit. Such attacks are evolving with the advent of new communication technology. A number of scenarios are presented below to describe the potential impersonation attacks [9]

#### *2.1.1 Credential Sharing with a Third Party via Email (Asynchronously)*

The conventional login-identifier and password is a widely used approach for the authentication of students in online tests. This method may provide adequate security in many online applications. However, it is vulnerable to attacks when students invite third parties to take their examinations. A student is able to share his or her access credentials prior to the test via email, phone and instant message. Rowe [11] states that individuals share credentials with collaborators, who take the online test on behalf of the intended test taker.

#### *2.1.2 Credential Sharing with a Third Party via Phone (Real Time)*

The mobile phone has become an increasingly used communication technology and an essential personal accessory. McGee [12] identified that students may use smartphones for information exchange during online examinations. Howell et al. [13] reported that students exchange answers to questions using their phones and take photographs of exams and transmit them to others. Paullet et al. [14] identified phone use as a new method of cheating. They argue that the use of browser-locking techniques may become irrelevant

if a student has access to a smartphone during their exam. There are two possible scenarios where a smart phone may be used to cheat in an online test, i.e. sharing answers to questions, and sharing access credentials for impersonation.

#### *2.1.3 Credential Sharing with a Third Party via Instant Messaging (IM)*

Instant Messaging (IM) is another potential method to communicate during an online examination session. The growth of IM services is a global phenomenon, which is rapidly changing the way people interact. IM applications are easily available on mobile phones, tablets and computers for little or no cost. Ease of access makes it a potential tool for cheating in online examinations. Examples of instant messaging applications include Skype, Viber, WhatsApp, and Phone [15]. The prevalence and free availability of these applications means they are gradually replacing short messaging service (SMS) communication [16]. As of 2016, chat service WhatsApp has reached 1 billion registered users [17]. Technology has been a useful tool for advanced learning; however, it may also be used by people in promoting their personal objectives, including cheating. McGee [12] state that technology is the most commonly used strategy to cheat in online examinations. Research studies reported that students with access to phones and computers use instant messages during online examinations [18, 19].

#### *2.1.4 Remote Desktop Sharing*

Using remote desktop sharing applications, a remote user can access and control a desktop with permission to all programs [20]. By combining remote desktop sharing and an online examination session, a student may login and invite a third party to impersonate him in an online test. Desktop sharing is reported as one of the ten most inventive cheating attempts in eCampus News [21]. Heussner [22] state that it could be tempting to accept help from a friend or helper remotely using technology including remote desktop sharing. This enables a third party in the next room, or even in a different city, country and time zone, to impersonate a test taker. This type of attack is pre-planned and the student and attacker agree a time to perform the test.

The security measures such as "secure browser" [23] can mitigate the use of instant messaging (on personal computer), Internet browser access, and remote desktop sharing during an examination session [24]. However, students may still circumvent the security and share their credentials with a third party using email and mobile phone.

### 2.2 Authentication Approaches

The conventional authentication approaches fall into three categories based on "what you know" e.g. password and secret information "what you have?" e.g. a smart card and "what you are" e.g. biometrics [25]. These methods are driven by knowledge, objects and human characteristics. The existing methods satisfy identity and authentication to ensure that the correct student has access to an online test. However, based on the literature review and evaluation of potential threats above, it has been identified that an authenticated student is sometimes not the expected student, or an expected student may start a test but does not complete it. Hence, the existing mechanisms are not sufficient to ensure that the correct student takes the online test.

Table 1 shows an overview of the existing methods in the context of impersonation threats. In the majority of features, students may be able to share access credentials with an impersonator. For example, students reveal their passwords to third parties for impersonation [26]. Apampa et al. [6] state that an impersonator could produce correct login details on behalf of a student, which raises the question "is the student really who he/she claims to be?" Authentication methods provide a different level of security assurances, reliability and deterrence to impersonation threats. According to guidelines the proposed method needs to [27]:

- support, not prevent or disrupt, learning (usable)
- be integrated in the learning process (secure)
- be simple and flexible to deploy (usable)
- be secure, non-invasive and not diminish privacy (secure and usable)
- be low-cost (feasible).

Knowledge Based Authentication (KBA) is the simplest technique to fulfill the security requirements. This is an easy to use method, and expected to provide secure authentication in online examinations. This is a low-cost, accessible, widely acceptable and preferred authentication method [28]. However, a review of KBA methods suggests impersonation attacks are

**Table 1** Authentication approaches and impersonation

| Authentication methods | Impersonation |
|---|---|
| Knowledge-based Authentication (KBA) | |
| Login identifier and password | Can be shared with a third party |
| Personal challenge questions | Can be shared with a third party |
| Object-based Authentication (OBA) | |
| Smartcard, or magnetic card | Can be shared with a third party |
| Biometrics | |
| Fingerprint recognition | Cannot be shared with a third party |
| Face recognition | Cannot be shared with a third party |
| Signature recognition | Cannot be shared with a third party |
| Web video recording | Cannot be shared with a third party |
| Human invigilation | |
| Face-to-face invigilation | Cannot impersonate with identity verification |
| Remote monitoring (Web cam) | Cannot impersonate with identity verification |

inevitable. Using both challenge questions based on personal information, and login-identifier and password, students may be able to share credentials with third party impersonators using phone, IMs, remote desktop and email.

Object Based Authentication (OBA) method utilizes physical objects such as smart cards and magnetic strip cards [29]. This method is widely used in the banking, transport and hospitality sectors with a purpose-built infrastructure. Implementation of these features requires special purpose input devices and infrastructure, which incurs additional costs and human resources. Smart cards can be shared in person or by post with impersonators before online tests, meaning the method is fallible, and vulnerable to impersonation attacks. Furthermore, implementation of the OBA method may be challenging to implement in dispersed geographical locations with students needing to access online learning and examinations from their homes and offices.

Biometric features such as fingerprint and face recognition methods are suggested to enhance security in online examinations [30]. Thus, it is anticipated that only the correct student can authenticate, due to unique physical attributes associated with individuals. Ko and Cheng [31] proposed the use of video recording of an online examination session, which may countermeasure impersonation attacks. These features are reported to be more reliable than KBA and OBA. However, some studies identified issues with the use of biometrics. Balie and Jortber [32] state that biometrics require proprietary software, special purpose hardware and broadband Internet to transmit the required input. Unlike KBA, biometric features are associated with an individual's physical or behavioral characteristics, which cannot be updated if compromised. For example, some studies indicated that an individual's fingerprint can be lifted from the surfaces of objects without one's knowledge and used for replay attacks [2, 33]. False Reject Rate (FRR) and False Accept Rate (FAR) are widely known issues with these features: Ratha et al. [34] stated that fingerprint matching faces two common and competing errors, these being FRR and FAR. The same issues were reported in other biometric features, including face recognition. In a recent study, Sahoo and Choubisa [35] identified that the video recording feature may enhance security, but it will require post-assessment monitoring of exam sessions for all students, which incurs additional resources and demands extra effort [31]. This discussion implies that biometrics is more reliable in terms of identification; however, they are unreasonably intrusive, expensive and may cause difficulties in wider implementation where students are situated in dispersed geographical locations.

A human invigilator is an example of a secondary authentication method which can be used to ensure the presence of the correct student. This includes face-to-face proctoring and remote monitoring via a web cam. Face-to-face proctoring requires test centers and human invigilators in all locations (different cities worldwide) where students are enrolled on an online course. In addition, each test center requires a review by academic staff to ensure proctor quality

and compliance with the institution's test center standards [32]. Student authentication that relies upon a human invigilator will require extra human resources, costs and allocated test centers. Remote monitoring via webcam may be a feasible alternative to physical invigilation. A dedicated proctor is assigned to authenticate identity and monitor an online test [36]. Students can access their tests from the home or office without needing to go to an allocated test center. This approach may be cost-efficient compared to face-to-face invigilation, but there is a cost attached to remote proctoring [36]. This approach requires one-to-one monitoring and, therefore, would be expensive and challenging in testing a large number of students in dispersed geographical locations.

The above discussion suggests a need for an authentication approach which is accessible, usable, cost effective, and prevents collusion attacks in online examinations.

### 2.3 Previous Research

In the previous work, the authors conducted multiple studies to analyze usability and security of text-based and image-based challenge questions in an online examination context [37–41]. The overall findings of the earlier studies reported varying results. The following usability and security issues were identified.

- The conventional text-based questions with clarity, relevance and ambiguity issues were less usable. This influenced efficiency and effectiveness during the authentication process.
- In a guessing attack, questions in some areas were reported with security vulnerabilities as specific questions were successfully guessed.
- The usability of image-based questions was better than the text-based questions due to memorability of pictures and use of multiple-choice questions [42].
- One key issue with pre-defined text-based and image-based questions was the ability of a student to store, memorize and share them with an impersonator.
- A study [43] by authors identified that an increase in the number of questions shared, increased the success of an impersonation attack. Also, an increase in the profile (database) size decreased the success of an impersonation attack.

In response to impersonation attacks identified in the previous section and the issues identified above associated with the use of text-based and image-based challenge questions, this research study proposes dynamic profile questions.

### 2.4 Dynamic Profile Questions

In an earlier study, Babic et al. (2009) proposed a theoretical approach for activity-based security questions, which programmatically generates a security profile based on an individual's network and search activities for authentication of users in web applications. In another study, Jortberg and Baile (2009) implemented challenge questions from a US consumer database for identification of online students in online examinations. However, the database was limited to the US consumers' market and does not hold information about prospective students from across the world. The authors developed and researched text-based, image-based and activity-based questions as discussed above in the previous research section. Findings of these studies were encouraging. However, there were security challenges with these approaches which led to the creation of dynamic profile questions.

Figure 1 shows an overview of dynamic profile questions approach, which is an adaptable method. A profile is created dynamically based on a student's learning activities. Questions are created non-intrusively and non-distractingly in the background during the learning process. These questions are extracted from a student's learning activities, content submissions, grades, lessons, and forum posts in order to build and consolidate a profile. In order to access an online examination, the student is required to answer a subset of questions randomly presented from his or her profile.

This study implemented multiple choice questions using a combination of distractors and correct answers. A total of 18 dynamic profile questions were utilized in this study which is discussed later in the results section.

## 3 Research Methodology

The study was conducted in a real online learning course. A usability test method was adopted to evaluate the effectiveness of dynamic profile questions. It is a usability inspection method, which tends to

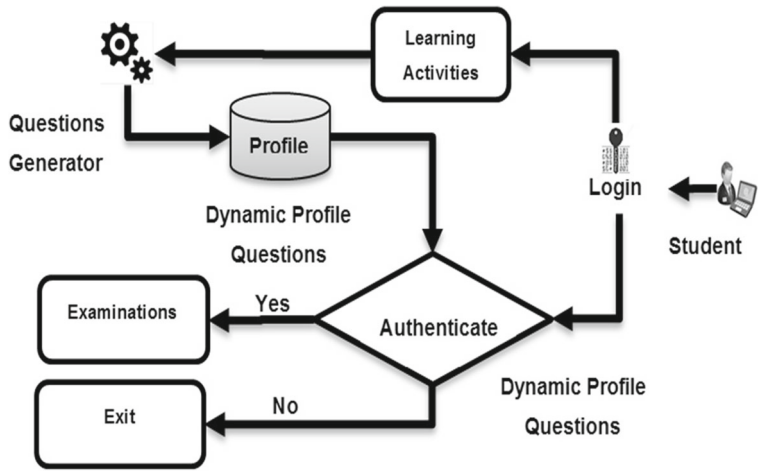


**Fig. 1** An overview of profile based authentication using dynamic profile questions

focus on the interaction between humans and computers [44]. Using this method, the representative users, i.e. students, interact with online learning and examinations using dynamic profile question authentication.

Multiple abuse case scenarios were simulated to test impersonation attacks. A risk-based security assessment method was adopted to perform the impersonation abuse case scenarios. This approach focuses on the test of features and functions of artifacts based on the risk of their failure using abuse case scenarios [45]. Abuse case scenarios were simulated to analyze impersonation attacks when students and impersonators communicated asynchronously (via email) and in real time (via a mobile phone) to share access credentials (dynamic profile questions). The study was conducted in multiple phases, which are described in the following sections.

- **Designing PHP & MySQL Course**: Online course design plays an important role in setting up learning goals and assessment for students. The dynamic profile question approach utilized a student's learning interactions during the course work to create and consolidate a profile; therefore, the course design was highly relevant. A remote "PHP and MySQL" online course was organized in five weekly modules, which included lessons, forum submissions, assignments and students' reflections 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. The course content was released on a daily basis to maximize participants' engagement and learning interactions. A total of five weekly quizzes were set up for summative assessment. The participants were recommended to invest 10 hours weekly learning effort over a span of five weeks.
- **Participant Recruitment**: In order to recruit and motivate participants, the course was offered free of charge and advertised on the University of Hertfordshire online portal (StudyNet). A total of 31 students were enrolled onto the course; however, only 21 completed the five-week course. Of the 21 students, the majority 17(80%) were students from United Kingdom and 1(5%) each were from Slovakia, Kenya, Malta, and Trinidad and Tobago. They were already enrolled in different programs at the University of Hertfordshire as distance learners. This was helpful for the participants' engagement due to their existing knowledge of using a remote online learning environment. In order to motivate students to perform the security abuse case scenarios a free advanced PHP course was offered on completion of the five week course. Due to specialized programming context, the course targeted computer science students. The participation was voluntary and performed with real students in order to create a real learning context. This led to a smaller sample size.
- **Registration**: The students were required to email a short introduction before registration. Guidance notes on the registration process and an enrolment key were emailed to all participants. It was a standard MOODLE sign up process, which was essential to create login credentials to access the learning material. Upon successful registration, the participants received a confirmation email to

access the course. The course was only available to registered users.

- **Online Coursework:** An instructor-led course was taught over a period of five weeks. To collect pertinent data for the evaluation of usability and security, authentication results were stored in the database. The participants were required to submit their assignments in order to access their quizzes. Each assignment was associated with each week's course content. The participants were required to complete a quiz at the end of each week. The course content of the following weeks were conditionally released to those who completed their quizzes – e.g. week 2 content was released to participants who completed the week 1 quiz.
- **Creating Dynamic Profile Questions**: In order to conduct the experiment in a controlled environment, dynamic profile questions were created manually for each individual student and uploaded to the database in their profiles via the user interface in MOODLE. As shown in "Appendix – Dynamic profile questions", these questions were created on a daily basis for each participant after access to course content and lessons, assignment submissions, assignment grades, quiz completions, feedback and reflection, and forum discussions.

## 3.1 Simulating Abuse Case Scenarios

The following collusion abuse case scenario was simulated toward the end of week five in order to evaluate impersonation attacks using email and phone:

***Threat Scenario****- A student is registered on a PHP & MySQL programming course, which is delivered in an online learning environment. The course uses dynamic profile questions for the authentication of students in summative assessments, which are accessible on a secure browser with no access to unwanted software e.g. Internet browser, chat sessions, etc. The student is due to write his/her final semester online test. He or she wants to boost his/her grades and recruits a third party impersonator to help him/her to take his test. However, to satisfy the authentication, the student needs to share his/her dynamic profile questions and answers (access credentials) with the impersonator. The impersonator would use the shared information to answer the randomly presented dynamic profile challenge questions during authentication in order to access the online test.*

Given the above scenario, this study simulated two types of collusion attacks: i) a student shares dynamic profile questions with a third party impersonator through email (asynchronously) before an online examination session; and ii) a student shares dynamic profile questions with a third party impersonator in real time through the mobile phone during an online examination session. Before simulating the abuse case scenarios:

- Two impersonators were recruited to attempt to impersonate students in an online examination session.
- Each impersonator was assigned a group of 10 students to simulate the abuse cases in allocated time slots.
- Skype accounts and email addresses for each impersonator were shared with his/her allocated students.
- Each impersonator was required to access a simulation quiz (online examination) created on the course on behalf of each allocated student in the scheduled time slot.
- Each impersonator was required to answer all 18 dynamic profile questions associated with each of his/her allocated students in order to complete the simulation.

### *3.1.1 Credential Sharing with an Impersonator via Email (Asynchronously)*

Email attack was simulated as described below:

1) Students were asked to share their dynamic profile questions via email.
2) Students emailed their dynamic profile questions and login details to their allocated impersonator.
3) The impersonator accessed the online course using the allocated student's login details.
4) In order to access the online quiz on behalf of a student, the impersonator was randomly presented with three dynamic profile questions.
5) The impersonator answered the dynamic profile questions using the shared information. The impersonator was required to search and locate the correct answer from the shared information and to guess answers to questions if they were not shared. The authentication results were stored in the database for analysis.
6) Steps 4 to 5 were repeated until all of the 18 dynamic profile questions were answered by the impersonator.

*3.1.2 Credential Sharing With an Impersonator via Phone (in Real-time)*

A student may share answers to his dynamic profile questions with a third party impersonator in real time during an online examination session using a smart phone. The participants were emailed the guidance notes. The impersonator was taking the test on a PC computer and communicated with the student using Skype messenger installed on a smart phone. The attack was simulated as described below:

1) At a scheduled time, an impersonator and a student started a chat session on the phone using the Skype instant messaging service.
2) A student shared his login details with the impersonator who accessed the online course on a PC using the shared login details.
3) In order to access the simulation online quiz, the impersonator was randomly presented with three dynamic profile questions on behalf of the student.
4) The impersonator shared these questions and multiple choice options with the student on a mobile phone using Skype in real time to collect the correct answers.
5) The student identified and shared a correct answer on Skype. The impersonator answered the questions and the authentication results were stored in the database for analysis.
6) Steps 4 to 5 were repeated until all of the 18 dynamic profile questions were answered by the impersonator.

## 4 Usability Results

This section presents the usability analysis of dynamic profile questions in the context of online learning and examinations. A total of 21 participants answered 378 questions for authentication in five weekly quizzes. The response time to questions was not recorded as they were created non-intrusively, non-distractingly in the background. This method shows an increased efficiency compared to pre-defined text-based and image-based questions which require students to register their answers. The effectiveness analysis is presented in the following section.

### 4.1 Effectiveness of Dynamic Profile Questions

The effectiveness is considered to be the degree of accuracy of the participants' responses. In the context of this study, it means that participants were able to submit correct answers to dynamic profile questions effectively with a low error rate. This was analyzed from the data collected from the participants' answers to dynamic profile questions during weekly quizzes. Table 2 shows the analysis of dynamic profile questions and the mean correct and incorrect answers. The results show that a large number of answers were correct. Out of 378 questions answered by 21 participants, 376 (99.5 %) were correct, which shows satisfactory effectiveness.

As shown in Table 2, the dynamic profile questions were based on the introduction and objectives, assignment submissions, forum discussions, assignment content, student reflection and grades. Each question was presented with five multiple choice options i.e. four distraction and a correct answer. For example:

**Table 2** Usability analysis: Effectiveness of dynamic profile questions

| Questions | | Correct | Incorrect |
|---|---|---|---|
| 1 | Course objectives 1 | 21(100%) | 0(0%) |
| 2 | Course objectives 2 | 21(100%) | 0(0%) |
| 3 | Course objectives 3 | 21(100%) | 0(0%) |
| 4 | Assignment 1 | 21(100%) | 0(0%) |
| 5 | Assignment 2 | 21(100%) | 0(0%) |
| 6 | Assignment 3 | 21(100%) | 0(0%) |
| 7 | Assignment 4 | 21(100%) | 0(0%) |
| 8 | Assignment 5 | 23 20(95.2%) | 1(4.8%) |
| 9 | Forum Post 1 | 21(100%) | 0(0%) |
| 10 | Forum Post 2 | 21(100%) | 0(0%) |
| 11 | Forum Post 3 | 21(100%) | 0(0%) |
| 12 | Assignment content 1 | 20(95.2%) | 1(4.8%) |
| 13 | Assignment content 2 | 21(100%) | 0(0%) |
| 14 | Assignment content 3 | 21(100%) | 0(0%) |
| 15 | Assignment content 4 | 21(100%) | 0(0%) |
| 16 | Student Reflection | 21(100%) | 0(0%) |
| 17 | Grades 1 | 21(100%) | 0(0%) |
| 18 | Grades 2 | 21(100%) | 0(0%) |
| Total | | 376(99.5%) | 2(0.5%) |

Which one of the following statements below was written by you as a course objective?

1. Distraction statement
2. Distraction statement
3. Distraction statement
4. Correct Answer
5. None of the above

The participants were required to recognize the correct answer among the multiple choice options in order to authenticate. The multiple choice options provided cues to the participants in order to identify their answers, which resulted in 99.5% correct answers. As presented in our previous study [42], the percent of correct answers to pre-defined text-based and image-based questions were 66% and 85% respectively. The current results for dynamic profile questions suggest a further increase. This is likely to be a result of using multiple choice options and creating questions associated with the students' learning activities.

According to the usability scale described by [46], 70%-79% usability is acceptable, 80%-89% good, and more than 90% exceptional. Therefore, 99.5% correct answers to dynamic profile questions is an exceptional effectiveness.

## 5 Security Results

This section reports the security analysis of dynamic profile questions to evaluate impersonation attacks when students and impersonators communicate through email and mobile phone. The analysis was performed on the data collected from simulation abuse case scenarios. In total, 21 participants performed email and phone collusion attacks with two impersonators. The findings of impersonation using email resulted in 29 (8%) correct answers. The findings of impersonation using a mobile phone (Skype) resulted in 351 (93%) correct answers. A detailed discussion on the findings of the abuse case scenarios is presented below:

### 5.1 Impersonation Using Asynchronous Sharing via Email

The security analysis of an impersonation attack in this section is based on the number of correct answers received when third party impersonators answered dynamic profile questions on behalf of allocated students and the information was shared asynchronously through email. Table 3 "Email Impersonation" shows the list of participants and the mean of correct and incorrect answers submitted by an impersonator. The email attack was performed before the phone attack to evaluate participants' ability to recall and share their dynamic profile questions, which would help a third party to impersonate them in an online examination.

Dynamic profile questions implemented five multiple choice options and the probability of a correct answer by chance would be 1/5th or 20%. In the abuse case scenario, the impersonators answered 29 (8%) challenge questions correctly. This was largely based on information shared via email and guessing by the impersonators.

Of the 21 participants, only 7 were able to share at least one correct question and answer with a third party impersonator. In order to test the significance of any differences in the means of correct answers between students (during authentication) and third party impersonators in an email abuse case scenario on

**Table 3** Security analysis: Impersonation via phone

| Question no. | Content type | Authentication | |
|---|---|---|---|
| | | Correct | Incorrect |
| 1 | Course objectives 1 | 20(95%) | 1(5%) |
| 2 | Course objectives 2 | 20(95%) | 1(5%) |
| 3 | Course objectives 3 | 21(100%) | 0(0%) |
| 4 | Assignment 1 | 20(95%) | 1(5%) |
| 5 | Assignment 2 | 20(95%) | 1(5%) |
| 6 | Assignment 3 | 20(95%) | 1(5%) |
| 7 | Assignment 4 | 21(100%) | 0(0%) |
| 8 | Assignment 5 | 19(90%) | 2(10%) |
| 9 | Forum Post 1 | 18(86%) | 3(14%) |
| 10 | Forum Post 2 | 20(95%) | 1(5%) |
| 11 | Forum Post 3 | 21(100%) | 0(0%) |
| 12 | Assignment content 1 | 17(81%) | 4(19%) |
| 13 | Assignment content 2 | 18(86%) | 3(14%) |
| 14 | Assignment content 3 | 20(95%) | 1(5%) |
| 15 | Assignment content 4 | 19(90%) | 2(10%) |
| 16 | Student Reflection | 18(86%) | 3(14%) |
| 17 | Grades 1 (Assignment) | 21(100%) | 0(0%) |
| 18 | Grades 2 (Quiz) | 18(86%) | 3(14%) |
| Total | | 351(93%) | 27(7%) |

the data shown in Table 2 "Email Impersonation" and Table 3, a paired-sample t-test was performed. There was a significant difference in the correct answers by students (M = 99.5, SD = 2.4) and impersonators in email abuse case attack (M = 7.8, SD = 14.9) conditions t (20) = 28.41, p < 0.01. This suggests that students were significantly less likely to share their dynamic profile questions with a third party impersonator via email; however, they recognized their correct answers when presented with multiple choice options during weekly quizzes reported in the effectiveness analysis above.

### 5.2 Impersonation Using Real-time Sharing via Phone

The security analysis of an impersonation attack in this section is based on the number of correct answers received when third party impersonators answered dynamic profile questions on behalf of allocated students and the information was shared in real time through a mobile phone. Table 3 "Phone Impersonation" shows the analysis of the dynamic profile questions and the mean correct and incorrect answers.

The findings revealed that a third party impersonator answered 351 (93%) questions correctly. This suggests that students were able to share correct answers to their dynamic profile questions on the mobile phone in real time. In order to test the significance of any difference between correct answers submitted by students (during authentication) in weekly quizzes and third party impersonators using mobile phone, a paired-sample t-test was performed on the data shown in Tables 2 and 4. There was a significant difference in the correct answers by students (M=99.47, SD=2.4) and impersonators by phone (M=92.8, SD=10) conditions t (20) = 3.49, p = 0.002. However, the mean of correct answers by phone (M=92.8) indicates a high percentage of the total answers. This identified a vulnerability of the dynamic profile questions. A student can circumvent this approach if an online examination process is not monitored or the response to questions during authentication is not timed.

### 5.3 Security Performance and Response-time Factor

Traditional online examinations are often required to be completed in an allocated time. Students are expected to authenticate and complete their online tests on or before the allocated time. In a practical situation, when a third party impersonator communicates with a student to share answers to dynamic profile questions using a mobile phone or email, the response time may change. It is anticipated that the response time of a genuine student and an impersonator may be different when answering these questions.

In order to test the significance of any differences in the mean response time to dynamic profile questions between a genuine student and a third party impersonator, a paired-sample t-test was performed on the data shown in Tables 2 and 4. There was a significant difference in the scores for the response time of a genuine student during authentication (M=39.69, SD=104.07) and a third party during impersonation by phone (M=290.47, SD=90.39) conditions t (377) = -35.55, p < 0.01.

The impersonation abuse case scenario via phone was simulated using Skype instant messaging. It is anticipated that verbal communication via phone may

**Table 4** Security Analysis: Impersonation via Email/Phone

| Participants | Email impersonation | | Phone impersonation | |
|---|---|---|---|---|
| | Correct | Incorrect | Correct | Incorrect |
| 1 | 9(50%) | 9(50%) | 18(100%) | 0(0%) |
| 2 | 0(0%) | 18(100%) | 12(67%) | 6(33%) |
| 3 | 0(0%) | 18(100%) | 13(72%) | 5(28%) |
| 4 | 1(6%) | 17(94%) | 18(100%) | 0(0%) |
| 5 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 6 | 1(6%) | 17(94%) | 14(78%) | 4(22%) |
| 7 | 0(0%) | 18(100%) | 16(89%) | 2(11%) |
| 8 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 9 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 10 | 5(28%) | 13(72%) | 16(89%) | 2(11%) |
| 11 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 12 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 13 | 0(0%) | 18(100%) | 17(94%) | 1(6%) |
| 14 | 0(0%) | 18(100%) | 16(89%) | 2(11%) |
| 15 | 5(28%) | 13(72%) | 16(89%) | 2(11%) |
| 16 | 1(6%) | 17(94%) | 18(100%) | 0(0%) |
| 17 | 0(0%) | 18(100%) | 17(94%) | 1(6%) |
| 18 | 0(0%) | 18(100%) | 16(89%) | 2(11%) |
| 19 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 20 | 0(0%) | 18(100%) | 18(100%) | 0(0%) |
| 21 | 7(39%) | 11(61%) | 18(100%) | 0(0%) |
| Total | 29 (8%) | 349 (92%) | 351 (93%) | 27 (7%) |

**Which one of the following PHP code belongs to your assignment 2?**

1. 
```
$i = array("Orange","Plum","Banana","Mango");

foreach ($i as $value) {
        echo $value."<br />";
}
```

2. 
```
echo "Table of 2 is <br/>";

for($i=1;$i<=10;$i++)
{
        echo $i."*2=".$i*2;
        echo"<br/>";
}
```

3. 
```
$i=array("Orange","Plum","Banana","Mango");

  for ($x=0; $x <count($i) ; $x++) {
    echo $i[$x]."<br />";
  }
```

4. 
```
$table = $_POST['tableof'];

for ($x=0; $x <=10 ; $x++) {
    echo '{$x} x {$table} =’. $x*$table ."<br />";
}
```

5. None of the above

**Fig. 2** Example of dynamic profile questions

be quicker than texting. However, reading a question with 5 multiple choice options may still require extra time for an impersonator, compared to a genuine student who could choose a correct answer in a shorter time. Furthermore, dependent upon the question design, some questions may be challenging to describe verbally as shown in Fig. 2.

In order to test the significance of any trend in the response time on the data presented in Tables 2 and 4, a one-way ANOVA was performed with linear contrasts. A trend was found for response time by students and a third party impersonator $F(1,754) = 1250.96$, $p < 0.01$. A Pearson correlation was performed on the data presented in Tables 2 and 4 to test the direction of the trend in response time by a student and a third party $r = 0.79$, $n = 756$, $p < 0.01$. This indicates an increasing trend. The above findings show that the response time of a genuine student is shorter than that of a third party impersonator.

## 6 Conclusion

The study reported in this paper implemented dynamic profile questions in a real online course. These questions were created non-intrusively and non-distractingly in the background during a student's learning period. This increased the efficiency compared to text-based and image-based questions. The findings revealed a significantly increased effectiveness, i.e. 99.5% correct answers. These questions are usable and influence impersonation when a student and impersonator communicate asynchronously via email. The security analysis revealed that dynamic profile questions may not influence impersonation attacks when a student and an impersonator use a smart phone to communicate in real time during the exam session. However, there was a significant difference ($p < 0.01$) in response time between a genuine student and a third party impersonator. This may be implemented as an additional factor on which to base reports of impersonation attacks. The response time factor can influence students from sharing access credentials with impersonators in real time to perform collusion attacks.

**Acknowledgments** A special thank you to those who contributed to this paper: Paul Kirk Business Manager and Jay Beavan, MARS Programmer, School of Postgraduate Medical and Dental Education, Cardiff University for their help and support with the study.

## Appendix: Dynamic Profile Questions

Q.1 which one of the following statement below were written by you?

- I am currently in second year of Economics Degree
- I have a degree in Chemistry from Trinity College Dublin, Ireland and pursued a part-time research MSc in Computational Chemistry with Trinity College. 3 publications.
- I used SQL during the second year of my course a few years ago, along with Java (JDBC)
- Currently I'm enrolled at the MSc Computer Science course, previously I studied BSC (Hons) in Computers and Electronics at the Northampton University.
- None of the above

Q.2 which one of the following statement below were written by you as a course objective

- I have over seven year experience in the IT sector, I'm currently working as database administrator/programmer
- I am doing this course as part of my CPD required in my workplace
- I would like to pursue this course in order to learn more for my field of work and have more knowledge for advancement.
- I want to do this course because i can work as a freelancer after doing php as i have seen so many projects in Freelancer, Odesk and Elance and i already have some experience of Sql.
- None of the above

Q.3 which of the following statement were written in your introduction email?

- For networking I need to know some of scripting languages and so I want to learn php.
- I work in a non-IT related field- I am a cook.
- Have already got the basics in HND for PHP and MySQL but thought this would be a good opportunity to refresh memory and expand on this
- Recently my employer have introduced software products and web pages written in PHP and using MySQL databases so it will be highly beneficial for my career to familiarize myself with this technologies.
- None of the above

Q.4 which one of the following discussion posts were made by you?

- I just completed the week 1 quiz and all the contents of week 1. I can't access to week 2, Am I too late for it, or is there any specific reason for it?
- When I run the page that should execute Hello World. I'm getting an error saying the URL was not found on the server
- I've tried the following: Test after starting of Apache (and MySQL), go to the address http://localhost/ or http://127.0.0.1/ in your browser and examine all of the XAMPP examples and tools. but all I get is a HTTP 404 not found page
- Did you save the example1.php in your xampp folder correctly? (i.e. make a new folder called myproject in the htdocs folder)
- None of the above

Q.5 which one of the following discussion posts were made by you?

- I have now completed week 1 assignment. Can I have access to week 1 quiz?
- I have managed to install XAMPP but I cannot connect to MySQL module. I have tried to uninstall and reinstall but nothing is working. I had installed MYSQL database previously.
- Thanks Mr Abrar but I do not think that is going to be necessary. I have managed to install XAMPP on another computer.
- Hi Evens, It works for me but it is not is English. AND. Many thanks Chelsea, not a great start but you cracked it.
- None of the above

Q.6 which one of the following discussion posts were made by you?

- I found this too. Googling it, as I understand it what is happening is when the script first runs the $i variable is not initialized, effectively resulting in a null being passed in to the switch statement
- You have stated that the second example is the same as the first one. So how come you have used quotation marks for the second example?
- Normally port 443 is used for secure host and accessible using https
- You nailed it. Perfect. Actually if the port is used by another service, apache won't start as the port is already taken.
- None of the above

Q.7 your score for the week 1 quiz was:

- Within the 60%-69% range
- Within the 80%-100% range
- Within the 40% -59% Range
- Within the 70%-79% range
- Less than 40%

Q.8 which one of the following assignments have you submitted in week 1?

- Write a PHP program to assign your name to $myname and qualification to $qualification variables and display the output on page with on two separate lines.
- List examples of logical operators and provide evidence with php programs?
- Write a php function to compute standard deviation of data array?
- Write a php program to connect to database using PDO and retrieve data using select statement?
- None of the above

Q.9 which one of the following assignments have you submitted in week 1?

- Write a php program to demonstrate difference between static, private and public class?
- Write a PHP program to assign any two numbers to two variables and display their sum on screen.
- Write a php program for traffic lights control
- Write a php program to submit data using form $_POST and insert into MySQL database?
- None of the above

Q.10 which one of the following assignments have you submitted in week 1?

- Write a PHP program to assign any number to a variable and display the value using pre-decrement operator (–). Check PHP operators for help.
- Write a PHP program to compute factorial of a number n?
- Write a PHP program to demonstrate post decrement
- Write a PHP program to compare pre-increment with post-increment
- None of the above

Q.11 which one of the following PHP code belongs to your assignment?

- while ($minNum < $maxNum){
- echo "Perform addition: $a + $b = ".$addition."";
- foreach($data s $dataitem)
- $sum = $numberone + $numbertwo;
- None of the above

Q.12 which one of the following PHP code belongs to your assignment?

- $a= ++$a;
- $sum(a+b);
- $addition = $a + $b;
- addFunction(10,10);
- None of the above

Q.13 your score for the assignment 1 was:

- Within the 40% -69% Range
- Within the 70%-79% range
- Within the 80%-89% range
- Within the 90%-100% range
- None of the above

Q.14 which one of the following reflection posts were made by you?

- I have learnt to create php classes and objects

- I have learnt to create my first PHP page and coding, assign variables and the different arithmetic operations.
- I have learnt to create database connection to backend using PHP in week 6
- I have learnt email function using php, which is very relevant to my ongoing project
- None of the above

Q.15 which one of the following assignments have you submitted in week 2?

- Write a PHP program to develop gradebook using array
- Write a PHP program to display your favorite fruit from the given choices: Mango, Orange, Apple, Plum, Cherry, pineapple, kewi using PHP Switch statement.
- Write a PHP program to display odd number for array list
- Write a PHP program to sort an array list
- None of the above

Q.16 which one of the following assignments have you submitted in week 2?

- Write a PHP program using an indexed array to store name of cars: Honda, BMW, Toyota, Ford, Audi and Fiat and print them all on screen line by line.
- Develop a bubble sort program using PHP
- Develop push and pop functions of stack using PHP program
- Write a php program to connect to database using PDO and retrieve data using select statement?
- None of the above

Q.17 which one of the following PHP code belongs to your assignment 2?

- print_largest($array);
- While(NOT $thelargetnumber)
- function getLarget($array =array());
- $cars[0]=”Honda”;
- None of the above

Q.18 which one of the following PHP code belongs to your assignment 2?

- echo $cars[0].” ”.$cars[1].” ”.$cars[2].” ”.$cars[3].” ”.$cars[4].” ”.$cars[5];
- foreach($numbers in $numbersArray())
- echo $find_favorite_fruite($fruitArray);
- Do While ($num[0] < $num[1])
- None of the above

## References


1. Watson, G., Sottile, J.: Cheating in the Digital Age: Do Students Cheat More in Online Courses? Online J. Dist. Learn. Adm. **13**(1), n1 (2010)
2. Moini, A., Madni, A.M.: Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. IEEE Syst. J. **3**(4), 469–76 (2009)
3. Ullah, A., Xiao, H., Lilley, M.: Profile Based Student Authentication in Online Examination. In: International Conference on Information Society 2012. IEEE, London (2012)
4. Rabkin, A.: Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In: SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security 2008, p. 23. ACM, New York (2008)
5. Evans, E.D., Craig, D.: Teacher and student perceptions of academic cheating in middle and senior high schools. J. Educ. Res. **84**(1), 44–53 (1990)
6. Apampa, K.M., Wills, G., Argles, D.: User security issues in summative e-assessment security. Int. J. Digit. Soc. (IJDS) **1**(2), 1–13 (2010)
7. Ayodele, T., Shoniregun, C., Akmayeva, G.: Towards E-Learning Security: A Machine Learning Approach. In: International Conference on Information Society (i-Society) 2011, IEEE (2011)
8. Sonhera, N., Kritzinger, E., Loock, M.: A Proposed Cyber Threat Incident Handling Framework for Schools in South Africa. In: Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference, ACM (2012)
9. Ullah, A., Xiao, H., Barker, T.: A Classification of Threats to Remote Online Examinations. In: International Conference and Workshop on Computing and Communication (IEMCON) 2016, IEEE (2016)
10. Kerka, S., Wonacott, M.E.: Assessing Learners Online. Practitioner File, Washington (2000)
11. Rowe N. C.: Cheating in online student assessment: Beyond plagiarism. Online Journal of Distance Learning Administration **VII** N2 (2004)
12. Mcgee, P.: Supporting Academic Honesty in Online Courses. J. Educ. Online **10**(1), n1 (2013)
13. Howell, S., Sorenson, D., Tippets, H.: The news about cheating for distance educators. Faculty Focus Specialty Report [serial on the Internet]. 2010: Available from: http://www.facultyfocus.com/wp-content/uploads/images/promoting-academic-integrity-in-online-edu1.pdf
14. Paullet, K., Chawdhry, A.A., Douglas, D.M., Pinchot, J.: Assessing Faculty perceptions and techniques to combat academic dishonesty in online courses. In: Proceedings of the EDSIG Conference (2015)
15. Church, K., De Oliveira, R.: What’s up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. In: Proceedings of the 15th international

conference on Human-computer interaction with mobile devices and services 2013, ACM (2013)
16. Oghuma, A.P., Chang, Y., Libaque-Saenz, C.F., Park, M.-C., Rho, J.J.: Benefit-confirmation model for post-adoption behavior of mobile instant messaging applications: A comparative analysis of KakaoTalk and Joyn in Korea. Telecommun. Policy **39**(8), 658–77 (2015)
17. Mccarthy, N.: Whatsapp Reaches One Billion Users. New Jersey: Forbes LLC; 2016 [cited 2016 03/02/2016]; Available from: http://www.forbes.com/sites/niallmccarthy/2016/02/02/whatsapp-reaches-one-billion-users-infographic/#14158bb0520b
18. Dee, T.S., Jacob, B.A.: Rational ignorance in education: A field experiment in student plagiarism. J. Human Resour. **47**(2), 397–434 (2012)
19. Rogers, C.F.: Faculty perceptions about e-cheating during online testing. J. Comput. Sci. Coll. **22**(2), 206–12 (2006)
20. Manion, T.R., Kim, R.Y., Patiejunas, K.: inventors; Google Patents, assignee. Remote desktop access2014
21. Barbour, A.: The 10 most inventive cheating attempts on online exams (2014)
22. Heussner, K.M.: 5 ways online education can keep its students honest. GIGAM Research [serial on the Internet]. 2012: Available from: https://gigaom.com/2012/11/17/5-ways-online-education-can-keep-its-students-honest/
23. Respondus. Respondus Assessment Tools for Learning Systems. Redmond, WA2016 [01/04/2016]; Available from: https://www.respondus.com/products/lockdown-browser/
24. Kitahara, R., Westfall, F., Mankelwicz, J.: New, multi-faceted hybrid approaches to ensuring academic integrity. J. Acad. Bus. Ethics **3**(1), 1–12 (2011)
25. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. **37**(11), 2245–55 (2004)
26. Weippl, E.R.: Security in e-learning eLearn. Magazine **2005**(3), 3 (2005)
27. Jortberg, M.A.: Methods to verify the identity of distance learning students. Acxiom; 2009 [cited 2011 01/04/2011]; Available from: http://u.cs.biu.ac.il/ariel/download/de666/resources/dependable_distributed_testing/verify_students.pdf
28. Hafiz, M.D., Abdullah, A.H., Ithnin, N., Mammi, H.K.: Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. In: 2008 AICMS 08 Second Asia International Conference on Modeling & Simulation, IEEE (2008)
29. Deo, V., Seidensticker, R.B., Simon, D.R.: inventors; Google Patents, assignee. Authentication system and method for smart card transactions. US1998
30. Agulla, E.G., Rifón, L.A., Castro, J.L.A., Mateo, C.G.: Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments. In: Eighth IEEE International Conference on Advanced Learning Technologies, IEEE (2008)
31. Ko, C.C., Cheng, C.D.: Secure Internet examination system based on video monitoring. Internet Res. **14**(1), 48–61 (2004)
32. Bailie, J.L., Jortberg, M.A.: Online learner authentication: Verifying the identity of online users. Bull.-Board Postings **547**, 17 (2009)
33. Derakhshani, R., Schuckers, S.a.C., Hornak, L.A., O'gorman, L.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recogn. **36**(2), 383–96 (2003)
34. Ratha, N.K., Bolle, R.M., Pandit, V.D., Vaish, V.: Robust Fingerprint Authentication Using Local Structural Similarity. In: 2000 Fifth IEEE Workshop on Applications of Computer Vision, IEEE (2000)
35. Sahoo, S.K., Choubisa, T.: Multimodal Biometric Person Authentication: A Review IETE. Techn. Rev. **29**(1), 54 (2012)
36. Mahmood, N.: Remote Proctoring Software Means Students Can Now Take Exams From Home. Technological News Portal; 2010 [cited 2011 13/07/2011]; Available from: http://thetechjournal.com/science/remote-proctoring-software-means-students-can-now-take-exams-from-home.xhtml
37. 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)
38. Ullah, A., Xiao, H., Lilley, M., Barker, T.: Usability of Profile Based Student Authentication and Traffic Light System in Online Examination. In: The 7Th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, London (2012)
39. Ullah, A., Xiao, H., Lilley, M., Barker, T.: Using Challenge Questions for Student Authentication in Online Examination. Int. J. Infonomics (IJI) **5**(3/4), 9 (2012)
40. Ullah, A.: Security and Usability of Authentication by Challenge Questions in Online Examination (2017)
41. 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); Sydney Australia: Academic Alliance International (2017)
42. 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). IEEE, London (2014)
43. 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 unpublished (2017)
44. 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)
45. Mcgraw, G.: Software security Security & Privacy. IEEE **2**(2), 80–3 (2004)
46. Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: Adding an adjective rating scale. J. Usability Stud. **4**(3), 114–23 (2009)