DOI:
https://doi.org/10.1109/IEMCON.2016.7746085

A Classification of Threats to Remote Online Examinations

Abrar Ullah, Hannan Xiao, Trevor Barker
School of Computer Science, University of Hertfordshire, Hatfield, UK
{a.ullah3, h.xiao, t.1.barker}@herts.ac.uk

Abstract— **Summative online examinations is a high stake process which faces many security threats. The lack of face-to-face interaction, monitoring or invigilation motivates many threats, which includes intrusion by hackers and collusion by students. This paper is based on a survey of literature to present a threat classification using security abuse case scenarios. Collusion is one of the challenging threats, when a student invites a third party collaborator to impersonate or aid a student to take an online test. While mitigation of all types of threats is important, the risk of collusion is increasingly challenging because it is difficult to detect such attacks.**

Keywords—Online examination, collusion, impersonation, threats, security

I. Introduction

A threat is the potential for misuse or abuse that will cause harm or exploit assets [1]. In security taxonomy, threats which exploit vulnerabilities of assets are interruption, interception, modification and fabrication [2]. An online examination is considered a critical asset in the context of online learning. It is delivered in a remote web based environment which is open to a wide number of security threats [3]. In an attempt to protect secure assets, it is essential to understand and identify the nature of all threats. Miguel et al., [4] state that security threats in online examinations can be approached in two stages i.e. threats are analysed, and then, recommendations are introduced and discussed in order to cope with the detected threats.

This paper is based on a literature review to present a classification of threats to online examinations.

II. Background

Online examinations faces a number of security threats. However, many authors agree that cheating motivates and contributes to a large number of them. It is widely reported by researchers in all forms of education [5, 6]. Research has taken place on cheating dating back to the 1930s [7]. More work was published on this subject in 1960s and 1970s [8, 9]. Bowers [6] reported the involvement of 75% of students from 99 colleges and universities in the US in cheating activities. Thirty years later McCabe and Pavela [10] repeated the study and reported involvement of 70% of the students in cheating. It is considered a challenging issue for online courses and examinations. McGee [11] states that cheating is a priority for all environments, however it is a particular concern for courses offered in a remote online learning environment.

For example, numerous studies [12, 13, 14] have reported that online learning offers more opportunities for cheating than traditional face-to-face examinations. Chiesel [p-339 ,15] reported that 64% of university professors perceived cheating in online examinations to be easier. In another study King [16] reported that 73.6% of students perceived that cheating in online examinations is easier compared to traditional face-to-face exams. Pillsbury and Harmon [17, 18] in their studies indicated that unethical conduct has intensified in online learning platforms due to more opportunities for cheating as a result of use of technology and the Internet. The lack of physical interaction or monitoring during learning and examinations is a security risk which increases opportunities for cheating.

Some researchers indicate that there was no difference in cheating due to the use of examination environments [19, 20]. McNabb surveyed faculty members regarding their perception of cheating in online and face-to-face examinations. The majority of faculty members did not believe that there was a difference in cheating between the two environments. Spaulding [20] presented a similar literature survey reporting no difference in cheating between different environments. McGee [11] argues that much of the research about cheating is based on self-reports or students' perceptions of academic dishonesty. Spaulding [20] state that it is difficult to capture comprehensive rates of cheating in either environment

Students often cheat in online examinations to qualify or enhance their grades. This motivates a number of unique security threats which may be classified into multiple categories including non-intrusion and intrusion. Non-intrusion threats are further classified into collusion and non-collusion threats. Collusion attacks happen when students invite third party impersonators or abettors for help with online examinations. Intrusion attacks are performed by cyber attackers, criminals and hackers. In general, these threats are open-ended and wide-spread due to access of learning and examinations on the Internet and weak authentication mechanism. Figure 1 shows a threats classification tree, which is described below:

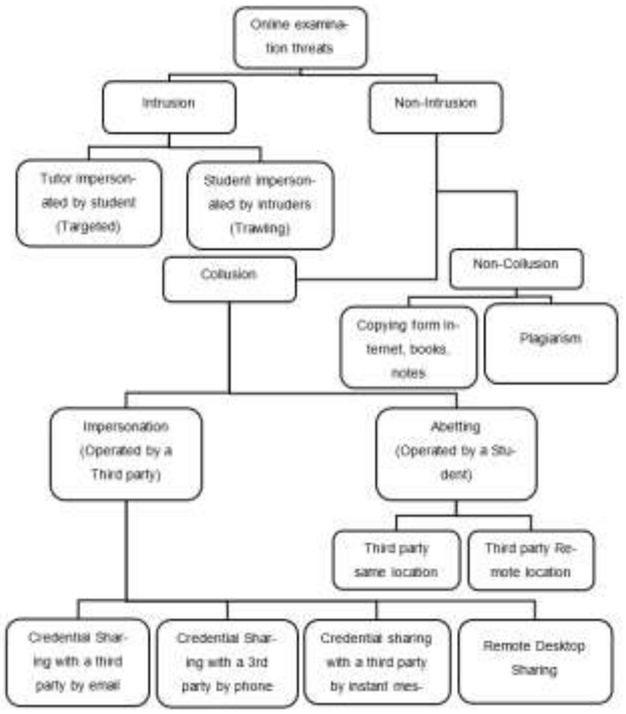
Online examination threats
Intrusion
Non-Intrusion
Tutor impersonated by student (Targeted)
Student impersonated by intruders (Trawling)
Collusion
Non-Collusion
Copying form internet, books, notes
Plagiarism
Impersonation (Operated by a Third party)
Abetting (Operated by a Student)
Third party same location
Third party Remote location
Credential Sharing with a third party by email
Credential Sharing with a 3rd party by phone
Credential sharing with a third party by instant mes-
Remote Desktop Sharing

Figure 1 Threats Classification

III. INTRUSION

Unlike an online bank with deposit transfer capabilities, a university with an online program is normally not a target for an attacker to break in and steal an online course. However, there are still concerns for intrusion into online examinations [21]. Intrusion attacks are carried out with malicious intentions and classified as i) targeted and ii) trawling attacks [22]. In a targeted attack, the attacker possesses information about a user of the targeted account. As an example, a student attacking account of an online tutor, would be interested to collect information about the tutor to penetrate his account using different attack methods. By contrast, a trawling attack is performed without any prior information about a user. Intrusion attacks may come from fellow students, friends and cyber criminals. Different types of intrusion attacks are described below.

A. Student Impersonated by Intruders (Trawling)

In this type of attack, an attacker impersonates a student in an online examination without his or her knowledge [23]. This type of attack is deliberate and may come from cybercriminals to reveal information about an online course. Hugerat et al. [24] state that these attacks are carried out to exploit information in an online course and examinations without causing any harm to the online learning system. Although, the attacker may not destroy data in an online course, however, this causes distrust and affect credibility of an online system. Ramim and Levy [25] conducted a case study on the Knowledgeville University, which experienced cyberattack in 2002, that resulted in shutting down the server hosting e-learning courses, in the middle of the semester. This put a halt to academic work of students' and faculty members' on the courses. These attacks may come from fellow students, insiders, hackers, and individuals who sells exam secrets on the Internet to potential students undertaking an online course.

With the advent of technologies, students are adopting new methods of cheating [11]. For example, Krsak [26] reported a method of cheating, where a student starts an online test in order to retrieve all questions. The student stores the exam questions, aborts the test in order to search for answers and then re-attempt the test. Students or attackers may share or sell exam questions to students on the same course or the Internet. For example, a professor in Indiana State University found her test questions for sale on E-bay [27]. Research studies have reported a new method of cheating known as braindump, which is a service that maintains a bank of questions and answers stolen from many online exams [27, 28, 29]. Hackers may attack online examinations to access questions to sell or share them with online users and potential buyers such as braindump services e.g. Cramster, Koofers, Study Blue and Course Hero [11].

B. Tutor Impersonated by Intruder/Student (Targetted)

Rowe [30] has shown that students may be able to log in as online tutors to reveal correct answers to exam questions. He identified that many online tests are protected by short passwords. For example, Blackboard allows passwords as few as eight characters to protect online assessment, such passwords may be relatively simple to circumvent using systematic "cracker" software. Rowe explained that even, if the password guessing fails, student can still use "social engineering" methods that have been successfully used to scam people into revealing their passwords. For example, "emergency" calls from alleged programming staff or "please change your password temporarily for system testing" requests [31]. Since few online tutors are security experts, they can potentially fall for many of these scams. Students and hackers may use a number of methods to gain access to an online examination. For example, password protection can be circumvented using key logger, Sniffing, clickjacking, dictionary attack, token theft, user surveillance, malware and brute force login attacks [32]. For example, sniffers could be used to decipher message packets of a local-area network used by fellow students or the instructor and thereby read their answers or passwords. In another example, Rowe [30] states that student could use spyware to sneak a look at activities of the person preparing electronic files for the assessment.

IV. NON-INTRUSION

These type of attacks may come from a legitimate student individually or in collusion with a third party. There are a number of reasons that influences cheating behaviour of students in general. Evans and Craig [33] identified numerous common reasons including desire for better grades, fear of failure, pressure from parents to do well, unclear instructional objectives, and being graded on a curve. Chiesel [p.329 ,15] identified more reasons i.e. everyone else is doing it, it helps me get better grades, a good job, or admitted to graduate school, no fear of being caught, and no fear of punishment if caught. Other studies provided similar reasons including pressure to succeed, to gain high grades, getting away with something, lack of organizational skills, and fear of failing a course [34]. Other reasons that students report include a desire to help others, procrastination, need to pass, course difficulty, it doesn't matter if I cheat, or cheating is easy [35]. Irrespective of the factors that motivate students, there is a common consensus that collusion and plagiarisms are major threats to online examinations.

Non-intrusion is classified into two categories: collusion and non-collusion. These threats are also identified in the code of practice for the Assurance of Academic Quality and Standards in Higher Education (QAA) for the UK. The QAA identified plagiarism, collusion, impersonation, and use of inadmissible material as academic misconduct in online examinations [36]. Such attacks can be carried out in several ways, which are described below.

A. Non-Collusion

A non-collusion attack is a form of cheating which is different from collusion as it does not involve a third party collaborator. Such attacks happen when a student breaks exam regulations about what can be used to complete course assignments or exams [11]. Students in an online environment feel "distant" from others and are more likely to engage in deceptive behaviours [30]. This view is incomplete as regardless of the learning environment, non-collusion threats may be a cause for concern in different modes of assessment. In both face-to-face and online learning, students may write their assignments, dissertations and course work in their own time. Bunn, Caudill and Gropper [37] identified non-collusion as planned cheating which involves copying from books, notes, and plagiarizing. This is classified into the following categories.

1) Copying From the Internet, Books,and Notes

While writing assignments and online tests, students can search for answers from the Internet, books, and notes. In online learning, planned cheating is more common due to the nature of online environment [38]. In their work, Underwood and Szabo [39] reported students using concealed notes to cheat on tests, exchanging work with other students, and using the Internet.

These threats depend upon the type of assessment and examination. In many remote assessments tutors may not be particularly concerned about students using a book or other source of information. These tests are designed carefully and may need to be completed in an allocated time, which may discourage students from accessing books or the Internet.

2) Plagiarism

Plagiarism is copying someone else's ideas and material from any source and claiming it as your own work [40]. The growth of the Internet makes it appealing to copy, paste and take one's writing without having the need to put extra effort. It has been defined in many ways, including theft, deception, and misunderstanding [41].

The use of technology and the Internet has increased a student's ability to plagiarize written assignments [42]. Plagiarism has been reported in both online and face-to-face courses. However, with the increasing availability of information online, it is more prevalent in online courses [43]. Turnitin [44] is a widely used originality software to determine the origin of written work. It is used by more than 3,000 institutions in the U.S alone with 55 million documents submitted for plagiarism checking. However, plagiarism still poses a threat to online examinations.

B. Collusion

A collusion attack is a form of organized cheating which involves collaboration between a student and a third party to solve examination problems. It is an ongoing issue, which has been reported in a number of recent studies [2, 45, 46]. The threat level of collusion in online examinations can be different from other online applications such as banking where implicit collusion is unlikely to happen as the stakes are different [47]. Collusion involves legitimate students and may be challenging to circumvent. However, it can be made harder for an attacker to reach their goal. Schechter [48] argues that for a collusion attack, the number of adversaries is likely to be smaller than for a non-collusion attack. In another study, Laubscher et al. [45] suggest that collusion is one of the major security threats to remote assessments and proposed remote proctoring to detect impersonation. Howell et al., [29] reported online services such as *Wetakeyourclass*, *Boostmygrades* and *UnemployedProfesssors* in which students pay a fee for someone to take their online classes and exams. It is anticipated that students would be sharing their credentials with these websites to take their online tests. As shown in Figure 1, collusion is classified into two broad categories Impersonation and Abetting as described below.

1) Impersonation

In impersonation attacks, an online examination is taken by a third party impersonator. A student shares access credentials or provides access to an impersonator to his/her online test. It is difficult to identify or detect impersonation, once a test is completed [46]. These attacks are pre-planned and consensual, involving legitimate students with valid access credentials. Moini and Madni [49] state that impersonation and illegal sharing or disclosure of authentication secrets is challenging to defend in a remote online setting. They identified that students invite third parties to take their tests for extra benefit. Such attacks are evolving with the advent of new communication technologies. A number of scenarios are presented below to describe the potential impersonation attacks.

a) Credential Sharing via Email (Non Real-time)

The conventional login-identifier and password is a widely used approach for the authentication of students in online examinations. This method may provide adequate security in many web-based applications, however, it is vulnerable to attacks when students invite third parties to take their exams. A student is able to share access credentials prior to the test via email, phone, and instant message. Email is a widely used communication method and students may share information with potential impersonators via this method.

b) Credential Sharing via Phone (Real-time)

Mobile phone has become an increasingly used communication technology and dependable personal accessory. McGee [11] identified that students may use smartphones for information exchange during online examinations. Howell et al. [29] reported that students exchange answers to exam questions with their phones. They also take photographs of exams and transmit them to others using their phones. Paullet et al. [28] identified the phone as a new method of cheating. They argue that the use of browser locking techniques may become irrelevant if a student has access to smartphones during their exams. There are two possible scenarios where a smart phone could be used to cheat in an online test i.e. sharing answers to questions, and sharing access credentials for impersonation. Although, it can be argued that access credentials could be shared before an online test, however, if a challenge questions method [21] or a random PIN code is implemented where questions or PIN code are generated randomly, this cannot be shared before an online test. Thus, smartphones are convenient to share access credentials with a third party impersonator in real-time. In a recent study, Paullet et al. [50] identified the use of mobile phones as a rising concern, which is a challenging issue.

c) Credential Sharing via Instant Messaging (IM)

The Instant Messaging (IM) is another potential method to communicate in real-time during an online examination session. The growth of IM services is a global phenomenon, which is rapidly changing the way people communicate. Many IM applications are easily available on mobile phones, tablets and computers for no cost on the Internet. Ease of access and communication makes it a potential tool for cheating. Examples of IM applications include Skype, Viber, Whatsapp, Phone, SMS [51]. Technology has been a useful tool for advanced learning, however, it can also be used for cheating. McGee [11] states that technology is the most commonly used strategy to cheat in online examinations. Students with access to phones and computers use instant messages during online examinations [52]. A student and a third party impersonator can exchange access credentials using IMs to access an online examination.

d) Remote Desktop Sharing

Using remote desktop sharing applications, a remote user can access a desktop with permission to all programs on a PC [53]. By combining remote desktop sharing and an online examination session, a student can login and invite a third party impersonator to impersonate in an online test. Desktop sharing is reported as one of the 10 most inventive cheating attempts in eCampus News [54]. Heussner [55] state that it could be tempting to take help from a friend or helper remotely using technology including remote desktop sharing. This enables a third party in the next room or a different city, country and time zone to impersonate a test taker. This type of attack is pre-panned and a student and the attacker takes the test on an agreed time.

Secure browser is one possible solution to mitigate remote desktop sharing. For example a safe exam browser is an application to prevent running of undesirable applications during an online examination session [56]. Similarly, Respondus Lockdown Browser [57] is another secure browser application for online examinations.

2) Abetting

In abetting attacks, a legitimate student takes an online examination, however, he or she takes help from a third party [40, 58]. This is described as “panic cheating”, when a student is struggling to answer a question during a test. Stuber-McEwen et al. [58] state that aiding and abetting is a common practice in both online and classroom cheating. Regardless of whether students were online or “on-ground” classes, aiding and abetting with exams were the most frequently reported form of cheating [40]. Dietz-Ulher and Hurn state that panic cheating occurs during a test when the student finds himself at a loss for an answer. Abetting is classified in the following two categories.

a) Third Party Same Location

A fellow student or a third party collaborator sitting next to a student can help him or her in an online test [30]. In absence of a live invigilation or remote monitoring, it may be difficult to deter the presence of helpers and abettors during an online examination. McGee [11] identified that in a test taking situation, a student and a third party can be physically located in the same place. Rowe [30] state the issue of authentication has been widely researched to ensure that a genuine student is present, however, not that he or she is alone, which requires different methods. Presence of a third party with the test taker is a challenging issue.

b) Third Party Remote Location

Students may get help from third party collaborators based in a remote location during their online exams [11, 29, 52]. Students use their phones for getting help with exam questions, and take photographs of questions to transmit them to others [29]. As discussed above, a student may use smartphone, instant messaging, and emails to get help from third parties remotely. Paullet et al. [28] identified that phone has been increasingly used for cheating in online examinations. This view is helpful to establish that students can use all possible means in a panic situation when they need help in exams.

V. CONCLUSION

In this paper threats to online examinations are reviewed in general and collusion in more detail. Collusion threats are motivated by vulnerabilities in identity and the authentication model. These threats are classified into impersonation and abetting. Impersonation happens, when a student willingly colludes and shares access credentials with a third party to perpetrate impersonation. Abetting happens when a student takes an online examination assisted by a third party based in the same location or remotely. It is challenging to track collusion attacks when an online test is completed. However, it is important to mitigate such attacks in order to increase confidence of stake holders and enhance the credibility of online assessment.

REFERENCES

[1] Haley C. B., Laney R. C., Nuseibeh B., editors. "Deriving security requirements from crosscutting threat descriptions". Proceedings of the 3rd international conference on Aspect-oriented software development; 2004: ACM.

[2] Apampa K. M., Wills G., Argles D. "User security issues in summative e-assessment security." International Journal of Digital Society (IJDS). 2010;1(2):1-13.

[3] Kritzinger E. Information Security in an E-learning Environment. Education for the 21st Century—Impact of ICT and Digital Resources: Springer; 2006. p. 345-9.

[4] Miguel J., Caballé S., Xhafa F., Prieto J. "A massive data processing approach for effective trustworthiness in online learning groups." Concurrency and Computation: Practice and Experience. 2015;27(8):1988-2003.

[5] Aggarwal R., Bates I., Davies G., Khan I. "A study of academic dishonesty among students at two pharmacy schools." Pharmaceutical journal. 2002;269(7219):529-33.

[6] Bowers W. J. "Student dishonesty and its control in college." 1964.

[7] Strang R. Behavior and Background of Studentsin College and Secondary Schools. New York: Harper and Brothers; 1937.

[8] Wrightsman Jr L. S. "Cheating—A research area in need of resuscitation." Peabody Journal of Education. 1959;37(3):145-9.

[9] Bushway A., Nash W. R. "School cheating behavior." Review of Educational Research. 1977:623-32.

[10] Mccabe D. L., Pavela G. "Ten Principles of Academic Integrity for Faculty." The Journal of College and University Law. 1997;24:117-8.

[11] Mcgee P. "Supporting Academic Honesty in Online Courses." Journal of Educators Online. 2013;10(1):n1.

[12] Colwell J. L., Jenks C. F., editors. "Student Ethics in Online Courses". 35th Annual Conference Frontiers in Education (FIE '05) 2005; IN, USA: IEEE.

[13] Wielicki T., editor. "Integrity of online testing in e-learning: Empirical study". Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06); 2006: IEEE.

[14] Jung I. Y., Yeom H. Y. "Enhanced security for online exams using group cryptography." IEEE Transactions on Education. 2009;52(3):340-9.

[15] Chiesel N. "Pragmatic methods to reduce dishonesty in web-based courses." A Orellana. 2009:327-99.

[16] King C. G., Guyette Jr R. W., Piotrowski C. "Online Exams and Cheating: An Empirical Analysis of Business Students' Views." Journal of Educators Online. 2009;6(1):n1.

[17] Pillsbury C. "Reflections of academic misconduct: An investigating officer's experiences and ethics supplements." Journal of American Academy of Business. 2004;5(1/2):446-54.

[18] Harmon O. R., Lambrinos J., Buffolino J. "Assessment design and cheating risk in online instruction." Online Journal of Distance Learning Administration. 2010;13(3).

[19] Mcnabb L., Olmstead A. "Communities of integrity in online courses: Faculty member beliefs and strategies." Journal of Online Learning and Teaching. 2009;5(2):208-23.

[20] Spaulding M. "Perceptions of academic honesty in online vs. face-to-face classrooms." Journal of interactive online learning. 2009;8(3):183-98.

[21] Bailie J. L., Jortberg M. A. "Online learner authentication: Verifying the identity of online users." Bulletin-board postings. 2009;547:17.

[22] Bonneau J., Just M., Matthews G. What's in a Name? Financial Cryptography and Data Security: Springer; 2010. p. 98-113.

[23] Kumar S., Gankotiya A. K., Dutta K., editors. "A comparative study of moodle with other e-learning systems". Electronics Computer Technology (ICECT), 2011 3rd International Conference on; 2011: IEEE.

[24] Hugerat M., Odeh S., Saker S., Agbaria A. "Vulnerabilities and Attacks on Information Systems in E-learning Environments in Higher Education." 2013.

[25] Ramim M., Levy Y. "Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university." Journal of Cases on Information Technology (JCIT). 2006;8(4):24-34.

[26] Krsak A., editor. "Curbing academic dishonesty in online courses". TCC Worldwide Online Conference; 2007.

[27] Hill C. "Student Authentication:What Are Your Duties Under the HEA Reauthorization." Madison, Wisconsin, US: Magna Publications, Inc Retrieved December. 2010;18:10-1.

[28] Paullet K., Chawdhry A. A., Douglas D. M., Pinchot J., editors. "Assessing Faculty Perceptions and Techniques to Combat Academic Dishonesty in Online Courses". Proceedings of the EDSIG Conference; 2015.

[29] 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.

[30] Rowe N. C. "Cheating in online student assessment: Beyond plagiarism." Online Journal of Distance Learning Administration. 2004;7(2).

[31] Mitnick K. The art of deception. New York: CyberAge books; 2002.

[32] Christodorescu M., Jha S., Seshia S. A., Song D., Bryant R. E., editors. "Semantics-aware malware detection". Security and Privacy, 2005 IEEE Symposium on; 2005: IEEE.

[33] Evans E. D., Craig D. "Teacher and student perceptions of academic cheating in middle and senior high schools." The Journal of Educational Research. 1990;84(1):44-53.

[34] Heyneman S. "The corruption of ethics in higher education." International Higher Education. 2015(62).

[35] Owunwanne D., Rustagi N., Dada R. "Students' perceptions of cheating and plagiarism in higher institutions." Journal of College Teaching & Learning (TLC). 2010;7(11).

[36] Agency Q. A. Code of practice for the assurance of academic quality and standards in higher education. Assessment of students (Second edition)2006.

[37] Bunn D. N., Caudill S. B., Gropper D. M. "Crime in the classroom: An economic analysis of undergraduate student cheating behavior." The Journal of Economic Education. 1992;23(3):197-207.

[38] Grijalva T. C. Academic honesty and online courses: Department of Economics, Weber State University; 2006.

[39] Underwood J., Szabo A. "Academic offences and e‐learning: individual propensities in cheating." British Journal of Educational Technology. 2003;34(4):467-77.

[40] Dietz-Uhler B., Hurn J., editors. "Academic dishonesty in online courses". 44th Annual Conference June 12-16, 2011; 2011.

[41] Sutherland-Smith W. "Retribution, deterrence and reform: the dilemmas of plagiarism management in universities." Journal of Higher Education Policy and Management. 2010;32(1):5-16.

[42] Scanlon P. M. "Student online plagiarism: how do we respond?" College Teaching. 2003;51(4):161-5.

[43] Gilmore J., Strickland D., Timmerman B., Maher M., Feldon D. "Weeds in the flower garden: An exploration of plagiarism in graduate students' research proposals and its connection to enculturation, ESL, and contextual factors." International Journal for Educational Integrity. 2010;6(1).

[44] Turnitin. Turnitin effectiveness in U.S Colleges and Universities2014: Available from: https://spahp.creighton.edu/sites/spahp.creighton.edu/files/Turnitin_Effectiveness_HE.pdf.

[45] Laubscher R., Olivier M. S., Venter H. S., Eloff J. H. P., Rabe D. J., editors. "The role of key loggers in computer-based assessment forensics". Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries; 2005: South African Institute for Computer Scientists and Information Technologists.

[46] Kerka S., Wonacott M. E. "Assessing Learners Online. Practitioner File." 2000.

[47] Rabkin A., editor. "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; 23, New York, NY, USA: ACM.

[48] Schechter S. E. "Toward econometric models of the security risk from remote attack." IEEE security & privacy. 2005(1):40-4.

[49] Moini A., Madni A. M. "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective." IEEE Systems Journal. 2009;3(4):469-76.

[50] Paullet K., Douglas D. M., Chawdhry A. "Verifying user identities in distance learning courses: Do we know who is sitting and submitting behind the screen?" Issues in Information Systems. 2014;15(1).

[51] Church K., De Oliveira R., editors. "What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS". Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services; 2013: ACM.

[52] Dee T. S., Jacob B. A. Rational ignorance in education: A field experiment in student plagiarism: National Bureau of Economic Research2010.

[53] Manion T. R., Kim R. Y., Patiejunas K. Remote desktop access. Google Patents; 2014.

[54] Barbour A. The 10 most inventive cheating attempts on online exams. Technology news for Today's Higher-Ed Leader; 2014 [30/12/2015]; Available from: http://www.ecampusnews.com/top-news/exams-online-cheating-400/.

[55] 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/.

[56] Frank A. J., editor. "Dependable distributed testing: Can the online proctor be reliably computerized?". e-Business (ICE-B), Proceedings of the 2010 International Conference on; 2010: IEEE.

[57] Respondus. Respondus Assessment Tools for Learning Systems. Redmond, WA2016 [01/04/2016]; Available from:

https://www.respondus.com/products/lockdown-browser/.

[58] Stuber-Mcewen D., Wiseley P., Hoggatt S. "Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom." Online Journal of Distance Learning Administration. 2009;12(3).