Journal of International Technology and Information Management

Volume 29 | Issue 1 Article 3

2020

Cybersecurity of Online Proctoring Systems

Ludwig Slusky
California State University, Los Angeles, lslusky@calstatela.edu

Cybersecurity of Online Proctoring Systems

Ludwig Slusky

California State University, Los Angeles

ABSTRACT

The online proctored examinations are adopted exceedingly in all forms of academic education and professional training. AI with Machine Learning technology take the leading role in supporting authentication, authorization, and operational control of proctored online examination. The paper discusses how administrative, physical, and technical controls can help mitigate related cybersecurity vulnerabilities of online proctoring systems (OPS). The paper considers two classes of OPS: fully automated AI-enabled systems and hybrid systems (automated AI-enabled with an expert live proctor in control). Based on the review of 20 online proctoring systems, the paper discusses methods and techniques of multi-factor authentication and authorizations, including the use of challenge-response, biometrics (face and voice recognition), and blockchain technology. The discussion of operational controls includes the use of lockdown browsers, webcam detection of behavioral signs of fraud, endpoint security, VPN and VM, screen-sharing and keyboard listening programs, technical controls to mitigate the absence of spatial (physical area) controls, compliance with regulations (GDPR), etc. Other topics discussed include confidentiality of the exam content, logging of control data, video and sound recording for auditing, limitations of endpoint-based security protection and detection techniques of behavior-based cheating and the effect of new intrusive technology on students' privacy.
In conclusion, the paper lists advanced features of online proctoring systems.

Keywords: Distance education, online learning, proctoring, academic integrity, authentication, authorization, information security, operational security, exam, AI, lockdown browser, face recognition, voice recognition, control, security safeguards

ISSN: 1941-6679-On-line Copy

INTRODUCTION

The security of eLearning technologies and online examinations draws the attention of educators actively involved in online teaching. According to some estimates (Jose, n.d.), the global eLearning market surpassed $100 billion mark. Lately, as the coronavirus pandemic forced colleges and schools to replace classroom education by online education, the use of eLearning technologies expanded exponentially. Due to the current circumstances caused by COVID-19, several providers of online assessment systems (e.g., ProctorExam, n.d., Proctorio, n.d.) offered accommodating procedures for easing the transition to online assessments in colleges and organizations for the duration of the crisis. With this sharp increase in the transition to online education, the cybersecurity vulnerabilities of online educational technologies became more noticeable and caused greater concerns, including privacy and integrity issues. Among various eLearning activities (presentations, lab exercises, exams, quizzes, discussions, etc.), remotely administered online exams are much more susceptible to fraud than in traditional face-to-face (F2F) modality.

The published data assessing the annualized cheating expectancy rate is sketchy, but the researchers' findings illustrate the severity of the problem. According to McCorkle (2018), 76 percent of faculty believe it is true that "undergraduate students do not have a sufficient understanding of what plagiarism is." Proctortrack (n.d.) raises this estimate to 86% of students in Higher-Ed admitting cheating.

Information technology, advanced with new tools, is widely used to enhance online learning; however, often, it does not adequately address the security problems of online education and testing. All forms of learning, from online courses to traditional F2F courses and professional training, exceedingly adopt online proctored examinations. Researchers anticipate that in the future, most of the exams (academic and professional, on campuses and at home) will be proctored using innovative technologies, such as Artificial Intelligence (AI). These innovative techniques can help alleviate privacy and security concerns. The security of online learning involves the management of the learners' profiles, authentication, authorization of access to exams and learning resources, examination process. It includes user behavior monitoring, which may trigger flags of fraud attempts. It also controls confidentiality, integrity, and availability of data at rest (in databases) and in transit (in networks), and can control enforcement of Digital Rights Management (DRM), etc.

ISSN: 1941-6679-On-line Copy

The security controls used for online learning are quite different from the security methods used in traditional classes. For example, in F2F settings, operational security relies on visual observation in the physical environment of a classroom. But, in online exams, the emphasis of such reliance is shifted to technical controls (e.g., webcam, software), which is the focus of this research.

CONCEPTS AND METHODS

The purpose of cybersecurity of online proctoring systems (OPS) is to help prevent cybersecurity attacks that lead to fraud, breaches of the assessment data confidentiality and the assessment results integrity, disruptions of OPS operations, breaches of accounting and non-repudiation of the assessment activities and results, and theft of personally identifiable information. It achieves its objectives to detect and/or prevent cybersecurity attacks by encompassing administrative, technical, and physical controls applied to (information) assets security, computer and network security, access control (to authorized and not-authorized assets), and security operations (including physical security control of the exam space).

The article investigates capabilities of a set of existing OPS, the controls and advanced technologies they use - to assist a reader in identifying potential vulnerabilities and selection of the appropriate methods and tools for secure OPS operations suitable for a specific online class offering.

eLearning platforms are subjected to typical vulnerabilities that characterize information systems. They include XSS (Cross Site Scripting), SQL code injection in the web page, virus and warms, trojan files, password cracking, and others (Ciobanu & Ciobanu, 2012). Accordingly, a trustworthy model for OPS is based on the fundamental security concepts of CIA triad (confidentiality, integrity, availability) and other security concepts, such as identification, authentication, authorization, accounting, control, non-repudiation, and auditing of online examination processes. These concepts can be implemented using administrative, technical, and physical controls.

This paper reviews the implementation of these concepts and security features in 20 proctoring systems: B Virtual, Eklavvya, Examity, Examus, Honorlock, Kryterion, Labster simulations, Loyalist Exam Services, Mettl Proctor Plus, MyLab + ProctorU Auto, Online Proctoring for Remote Examination (OP4RE), PBAF, onVUE, ProctorExam, Proctortrack, ProctorU, PSI, Respondus, Tegrity, and Xproctor. Their cybersecurity capabilities of these systems range from low

ISSN: 1941-6679-On-line Copy

scalability experimental (e.g., PBAF) to high scalability advanced (e.g., Respondus) levels. This study considers eight categories of methods and technologies employed by proctoring systems:

- Access control devices and methods
- AI and Machine Learning
- Biometrics
- Blockchain technology
- Regulatory compliance
- Endpoint security
- Video and audio monitoring
- VPN, Virtual Machines, and Virtual Labs

Cybersecurity capabilities come with costs (acquisition, maintenance, operations, skills). Some of them deal with risks that may have a low probability for specific exams, so an instructor should weigh the benefits and costs of the discussed controls. As online proctoring systems achieved some preeminence, several associations had been formed to share experience in online proctoring (eAA, n.d., ATP, n.d.), but this effort did not go far enough.
This research applies the basic principles of cybersecurity (confidentiality, integrity, availability, accountability, administrative/technical/physical controls, etc.), used for management information systems (MIS), to OPS. For example, penetration of access control and data (content) "leakage" are attacks on confidentiality. Fraud and plagiarism are attacks on integrity. Denial of service attacks against OPS are attacks on availability. Premature erasure of examination logs and exam video recordings is an attack on accountability.

"Leakage" of the exam content is one of the fundamental threats that instructors are facing. For example, even if a text cannot be copied and pasted, screen scanners (grabbers) can capture its image for storing as PDF files. The PDF file can be further converted, using an optical character recognition (OCR) software, into an editable text ready for copying. However, security features can prevent it by disabling screen scanners. Data leakage can occur via other means as well, such as access to the content of prior exams, a proxy impersonating the user, use of stolen identity, breach of the integrity of the students' records, etc. There are other types of content theft, such as "Brain Dumping" (e.g., recollecting the exam content from human memory) or the use of hidden cameras to copy exam content, that is also difficult to prevent.

Additional vulnerabilities may arise through the integration of online proctoring with other products. For example, an OPS implementation can be invasive if it is

ISSN: 1941-6679-On-line Copy

set up on a standalone platform or a generalized Learning Management System (LMS) platform. LMS is designed for administration, documentation, content delivery, practicing, examination, tracking activities, and reporting on learning processes in academic and corporate training environments. The LMS may contain some sensitive or proprietary information (e.g., learners' profiles, proprietary learning content) that also needs to be protected. Additionally, to expand functionality, the contemporary LMS are interlinked with other third-party software tools, such as cloud-based lab assignments (for example, short videos, hacking simulations, short essays, quizzes), plagiarism control, etc. Removing or lessening the impact of these vulnerabilities requires security capabilities and additional controls for identification, prevention, detection, investigation, mitigation, response, and documentation of security incidents.

Using the pool of the selected OPS, we evaluated their features and the technical controls for advanced online proctoring practices. Specifically, this review focuses on access control capabilities (identification, authentication, and authorization) and operational controls. Attempts to penetrate authentication in access controls have emerged as one of the most prevalent forms of cyber-attacks. According to the National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST 800–53), the authentication process can be performed at the following three levels (Grassi, Garcia, Fento, 2017):

- Basic level of authentication - controlled with single-factor or multifactor authentication
- Higher level of authentication - controlled with two distinct authentication factors and cryptographic techniques
- Very high level of authentication – controlled with cryptographic techniques and hardware-based authenticator that has the "impersonation resistance" feature (i.e., authenticator that cannot be "fooled" by a proxy impersonating the applicant)

Multi-factor authentication (MFA) is typically based on a combination of two or three factors selected from knowledge (e.g., password), possession (credentials based on items that the user has), and biometrics (static or dynamic). Two frequently used methods for MFA and fraud prevention are a password and a Knowledge-Based Authentication with the pre-determined (fixed) challenge-response authentication questions, which, however, may be repeated in the subsequent authentication attempts. A general model of authorization system is shown in Figure 1. Authorization is performed by a server to determine the user's privileges to access system resources and to perform specific actions on the system objects. Authorization uses user assertion, user credentials (attributes), policy rules,

ISSN: 1941-6679-On-line Copy

and resource attributes. An authentication assertion indicates that the user has been authenticated using a defined method at a specified time.

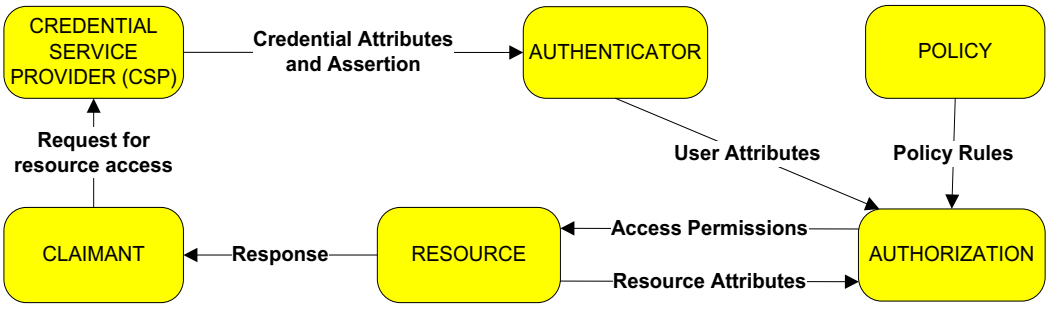

Figure 1. Model of authorization

The applicant (Claimant) requests Credential Attributes from the Credential Service Provider (CSP). The credential attributes and CSP assertion are directed further to *Authenticator*. Authorization server verifies user attributes, provided by Authenticator, against resource permissions (attributes) and policy rules to determine the applicable resource access authorizations. As a result, Claimant receives a response with authorized permissions to access Resource. Access Control permissions can be granted to individuals and roles (using a Role-Based Access Control system). Reliance on only one-factor authentication (password, challenge-response, biometrics, etc.) is not enough. Thus, additional MFA factors (typically two or three factors used together) need to be considered, such as challenge-response, biometrics, etc.

A general diagram of an online proctoring system and an exam room (see Figure 2) outlines users (test-taker, proctor, and unauthorized collaborator), unauthorized information resources, wireless communication, computing devices, and data storage.
A general diagram of an online proctoring system and an exam room (see Figure 2) outlines users (test-taker, proctor, and unauthorized collaborator), unauthorized information resources, wireless communication, computing devices, and data storage.

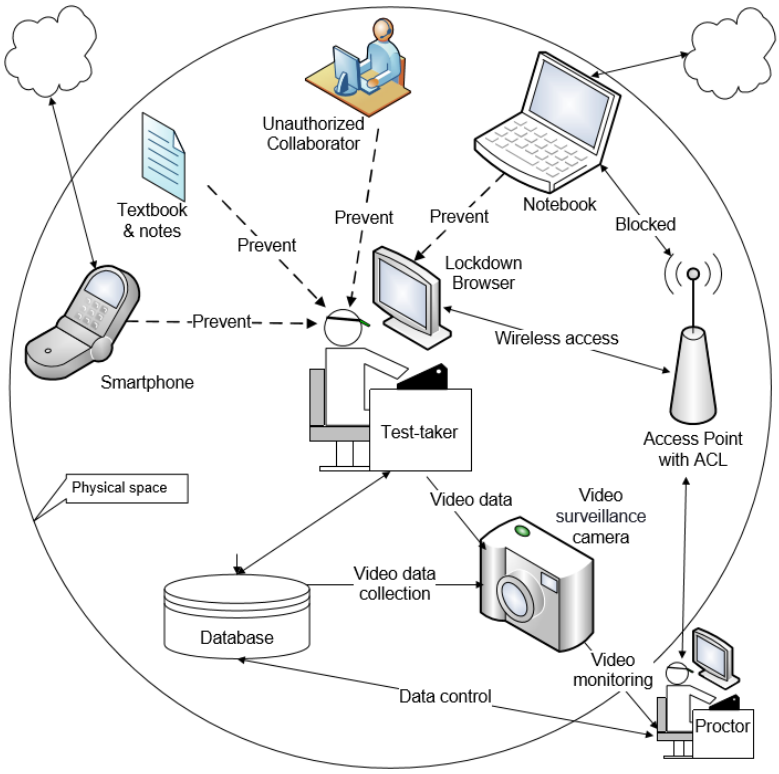

Figure 2. Online proctoring system

We will now focus on the access controls to authorized resources and detection of use of unauthorized resources via behavior monitoring.

ACCESS CONTROL AND BEHAVIOR MONITORING

Access control using static, repeated passwords is a traditional method to authenticate a user. Its limitations are well known. The improvements, such as a one-time password, may be feasible for large-scale OPS. Developers of small-scale OPS often consider challenge-response methods of authentication. Thus, Ullah, Xiao, Barker, & Lilley (2014, 2017) developed a Profile Based Authentication Framework (PBAF) where a student builds his/her profile of personal information (academic, private, contact, data about other optional and dated subjects). Then the information contained in the profile is used in challenge-response authentication for online examination. One of the weaknesses of PBAF is that its algorithm may require the 100% accuracy match of questions and answers based on the string-to-

string comparison. Another example is Experian identity authentication, which integrates the Knowledge IQ system based on interactive challenge-response questions, and the fraud detection and prevention Precise ID® platform (Experian, n.d.; Experian Product Sheet, n.d.). The Precise ID® platform allows real-time identification based on a combination of multiple data sources specific to the user.

A more innovative approach, suitable only for high-security OPS, is available with *blockchain* technology, which can provide user identification, authentication, and authorization using public-key cryptography (Cresitello-Dittmar, 2016). Essentially, with the blockchain technology, there is no need for a traditional password to authenticate devices and users. When a user joins blockchain, his public/private keys pair is generated and stored together with the blockchain address: the private key - on the user's device, and the public key, along with the blockchain address, on the blockchain. This method assures a high level of security: the data reside in a blockchain, and identity authentication is performed using the private key. Another significant benefit of blockchain infrastructure is the ability to provide security decentralization and avoid single points of failure, which are typical in centralized systems.

Consider differences in access control between F2F and online exam proctoring. The traditional methods for one-time (at the beginning of the exam) authentication used in F2F exams are not adequate for a secure OPS. In OPS, a test-taker may need to be re-authenticated continuously or periodically throughout the examination to detect a proxy impersonation. Another difference is the control of behavioral indicators. In F2F exams, the proctor observes student's behavior visually, but the computer activities remain largely non-monitored.

The popular and effective method to monitor and record the behavioral activities is via a webcam. A screen-sharing software and a keyboard listener program can also be installed to control the user actions on the computer. Such dual monitoring distinguishes two significant types of fraud: the unauthorized behavioral activities (faked identity, use of multiple computers, books), and unauthorized computer activities. Monitoring of the behavioral activities can occur synchronously (real-time preventive safeguard) or asynchronously (after-exam recordings' review as a detective safeguard).

Two popular systems – Xproctor and ProctorU – include the capability to control these two types of fraud. Xproctor (n.d.) authenticates students and performs continual tracking of the claimant's participation via facial recognition, behavior video-streaming, sound, and photographic methods. Xproctor supports configuration with an LMS (Canvas, Blackboard, Moodle, Desire2Learn), and,

ISSN: 1941-6679-On-line Copy

when installed on the user's computer (Windows or Mac OS), it offers an unlimited number of photo captures, screenshots per exam, and length of video captures.

ProctorU (n.d.) offers an automated AI-based OPS that can be used as a standalone product or in integration with Pearson's MyLab product portfolio. It comes as a fully automated solution that uses multifactor identity verification (with continuous biometric authentication), video recording, and AI-powered behavior analysis. The purpose of the AI component in ProctorU is to "strengthen the accuracy of proctoring in identifying details such as shadows, whispers or low sound levels, reflections, etc." The machine learning (ML) algorithms collect the following digitized data:

- Numerous human behavior patterns are recorded by webcam scanning of movements labeled as "data points" (such as movements of eyes, head, hands, etc.).
- Patterns symptomatic of fraud are defined and deployed as security "events" in the algorithm.
- The ML algorithm is trained with actual data to recognize these "events."
- Human examiners retrace the data to verify that the event occurred.
- If the sum or severity of the detected events exceeds the defined threshold, it would indicate a likely breach of integrity within the designed margin of type I and type II cybersecurity errors (i.e., the risk of false-positive and false-negative errors).

One-factor authentication (like a password) proved to be highly vulnerable to the attacks. Replacing one-factor authentication with MFA (e.g., in combination with biometrics) became a common feature of contemporary OPS. For multi-factor authentication, it's essential to combine factors from different categories, such as passwords, challenge-response tokens (also used as a credential recovery technique), IP addresses, smart cards, face recognition, voice recognition, knuckle scans, fingerprints, etc. All of them have some inherent vulnerabilities. For example, a dictionary attack can reveal a password. Smart cards can be lost. The biometric factors (fingerprints, iris patterns, facial scans, etc.) are not entirely accurate and subject to False Acceptance / False Rejection Rate errors. It is also essential to have MFAs where one factor compensate for the weaknesses of the other.

Furthermore, biometric authentication systems may require expensive equipment (e.g., for iris patterns), prolong throughput time (time to process and identify individual subjects), enlarged data storage (corpus) for storing images (e.g., up to 250KB per fingerprint), and other. There is also a risk of corruption of images

ISSN: 1941-6679-On-line Copy

during collection and mislabeling. Another limitation – for medical reasons, not all biometric methods are acceptable for some individuals. The integration of behavioral biometrics, voice recognition, and keys security (using, for example, blockchain) into multifactor authentication will significantly strengthen identity management and authentication across applications.

Another significant difference between F2F and online proctoring is that the F2F examinations rely mostly on administrative and physical controls, while online proctoring depends mainly on technical controls. The presence of a live proctor (even acting remotely), who can actively intervene in the examination process, provides an additional layer of administrative controls. But at the same time, it may complicate the process.

There are other points of view, as well. For example, Moneo et al. (2015) proposed a trustworthy model for secure learning assessments based on hybrid (live and auto) proctoring. He argues that security is mainly an organizational and management issue, not much dependent on the logical (technical) controls such as the virtual environment for assignments/exams and security monitoring.

Although security breaches of online examinations are not overwhelming, they are still significant, and online proctoring with security controls proved in practice its effectiveness. For example, ProctorU ("Harnessing the Power of AI," n.d.) reported that out of 1.5M exams proctored during 12 months, more than 10% required active intervention, about 0.5% had breaches of integrity, and 1.1M unpermitted resources were removed before examinations.

ADMINISTRATIVE, TECHNICAL, PHYSICAL CONTROLS

Administrative Controls

The online proctoring systems use three categories of controls to meet security objectives – administrative, technical, physical. Administrative controls include plagiarism policies, examination procedures, practices, rules, etc. Penalties for non-compliance with legal regulations can be high. A college providing online education needs to show a proof for accreditation agencies that its online courses meet academic integrity requirements (Cluskey, 2011). Among them, there are compliance requirements of the General Data Protection Regulation (GDPR), the Service Organization Control (SOC 2), and the U.S. Privacy Shields.

ISSN: 1941-6679-On-line Copy

GDPR directive protects the privacy and personal data of residents of the European Union; it is now adopted in the USA as well. Compliance with GDPR is now required in administrative controls that involve gathering of behavior data and biometric data. Thus, Proctortrack (n.d.), one of the most versatile OPS, offers data gathering functionality compliant with GDPR.

Another regulatory compliance, SOC 2 requires that control reports, certified by a public accountant (CPA), address specifically the critical system security principles: confidentiality, processing integrity, data integrity, availability, and auditing (Threat Stack, n.d.). The SOC 2 regulation controls that the system can monitor malicious activities, generate alerts of anomaly events, create a detailed audit trail, investigate the root cause of an attack, and take corrective action before data is compromised.

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed to define principles and provide a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States. For example, the Online Proctoring for Remote Examination (OP4RE, n.d.) project is compliant with the EU-wide regulations to protect privacy in online examinations and to assure security and reliability of the examination process. Another example is the PSI Bridge (2018) platform, which uses a proprietary lockdown browser and self-authentication to ensure proper compliance with student privacy while minimizing security risks. The platform is highly secure without being invasive - no access to a student's computer is needed to verify the exam integrity. The platform infrastructure includes a cloud-based Software as a Service (SaaS) integrated with an LMS. Any regulatory compliance requirement applied to a student needs to be somewhat verifiable. Thus, the exam session is recorded, and a proctor can review later in the LMS server: the exam logs, flagged violations, and annotated video. In another example of regulatory compliance, Honorlock (n.d.) Remote Proctor for universities – also on-demand SaaS cloud-based system - meets complex of regulations: the SOC 2 requirements, compliance GDPR and with the U.S. Privacy Shield.

ISSN: 1941-6679-On-line Copy

Enforcing DMCA copyright protection is not a frequently available feature in online proctoring systems. Honorlock (n.d.) distinguished itself by implementing it as the "Search and Destroy" application, which searches for unauthorized copies of the exam on the third-party websites and then files DMCA copyright requests to remove the discovered unauthorized copies of the exam.

Campuses highlight the attention to administrative controls in fighting students' cheating. Thus, Proctorio (n.d.), an automated online proctor (from Columbia University) protects end-to-end integrity, and in addition to technical controls (webcams and microphones to monitor students' activities) emphasizes an honor statement that students must sign before an examination. This statement enforces academic integrity policy and the consequences for violations (a practice adopted in many colleges). Similarly, "PennState College Academic Integrity" (n.d.) requires students to certify before an online exam (with a computer click) a statement that "all work on this assessment is entirely my own and does not violate ….Academic Integrity policy."

Automated online proctoring includes some methods that students may consider as being too invasive (e.g., behavior video recording and profiling), thus bringing confidentiality and integrity controls in conflict with privacy needs (Milone, Cortese, Balestrieri, & Pittenger, 2017). Such conflicts are not unique to online proctoring. Administrative controls can help to mitigate these conflicts. For example, a security policy should define a short data retention period and guaranteed purge of collected data after that, thus preventing the sharing and use of the collected data for any other purpose except for the specific online exam.

Physical Controls

Physical controls are not well suited for online proctoring. Still, some measures can be taken to remediate the lack of them with technical control methods. The primary objective is to establish a spatial control, i.e., the ability to monitor objects located in physical area close to a test-taker, understand the vulnerabilities that these objects may bring to the confidentiality and integrity of the exam, and the relationships between them and the student. For example, in ProctorExam (n.d.) system, spatial controls are augmented with an innovative 360° monitoring, which includes a combination of webcam, screen-sharing capability, and a smartphone camera to create a 360° view around the user. Besides, the system uses facial recognition to detects attempts to receive outside help and use unauthorized sources (devices, course materials).

ISSN: 1941-6679-On-line Copy

Proctorio OPS (from Columbia University) validates placement and proper direction of a webcam, provides video recording of the room near the test-taking location, and audio recording of unusual sounds, talking, or sudden changes in noise level.

Similarly, the AI module of ProctorU can itemize the objects which are available to the exam participant at the time of examination and determine positions of these objects in the actual area surrounding the test-taker. However, the ProctorU automated proctoring is not highly secure and can be deceived. For examinations requiring higher security, ProctorU offers a hybrid solution augmenting automated proctoring with professionally trained live proctors, which can intervene and interrupt the test. ProctorU supports easy integration with all major LMS and some leading exam authoring and delivery platforms (e.g., Cirrus).

Technical Controls

Technical security controls are essential for exam confidentiality and integrity. They are applied to computers, networks, data sources, software, and physical space. Technical controls of online exam proctoring can be classified as static and dynamic. (Dimeo, 2017)

Static controls do not undergo any significant changes and remain approximately the same throughout an examination, such as user biometric profile, data encryption, secure browser. Dynamic controls are related to the processes and change significantly throughout the examination, e.g., capturing live images, logging of detailed data for a variety of activities.

Among static controls, the most advanced are virtualization and isolation of the exam process and related applications from other unauthorized methods and applications that a user might run on his/her computer. For example, the Safe Exam Browser (SEB, n.d.) is a client software (kiosk application and a browser part) to work with an LMS platform. *Kiosk mode* allows to lock down a Windows device for a specific task; it prevents tabbing out of the application and browsing other applications. SEB locks down the examination computer and its browser to permit communication only with the LMS and an exam software running on a server. When activated on a student's computer, SEB will allow exam attempts using only one browser. It will disable other unauthorized shortcuts keys (such as Win, Ctrl+Alt+Del, Alt+F4, F1, Ctrl+P, Printscreen), copy/paste, switching to other applications and surfing of other web sites. SEB can be combined with Virtual Desktop Infrastructure (VDI) to use third party applications in exams. (See details of the ongoing development in https://sourceforge.net/projects/seb/)

ISSN: 1941-6679-On-line Copy

Compatibility and integration of OPS with LMS is necessary. Examity (n.d.) and Respondus (n.d.) OPS is well suited for this purpose. Respondus offers two tools: Respondus LockDown Browser and Respondus Monitor. Respondus LockDown Browser keeps open only one browser and disables access to the rest of the endpoint (user computer) environment. As a native application, it is superior to a browser plugin (Idb-vs-plugins, n.d.). Respondus Monitor, built upon the capabilities of LockDown Browser®, can monitor student's behavior by using a webcam and performs video analytics to detect behavioral events that can signal cheating during online exams.

Recording of an exam session is a basic functionality of any proctoring system. The recorded sessions can be used for both synchronous (real-time monitoring) and asynchronous (after exam detecting review) proctoring. Also, video-streaming, image, and sound capturing functions can be added as well. For example, Talview software (Jose, n.d.) supports synchronous and asynchronous use of recorded audio-video streaming and screen snapshots capturing user's computer activities.

The purpose of gathering data about the test-takers behavior and activities on the computer is to detect and log security events (indicating a possible fraud) that are triggered if the test-taker deviated from the standard online procedure. The events in the log file are identified and noted with "flags." The data gathered during the exam (including video-streaming, image, audio, and student's desktop screenshots) are recorded and can be used for safekeeping and exam validation.

In OPS, technical controls are implemented in two areas: endpoint-based (computer-based) security protection and behavior-based cheating detection. Controls for both include a combination of various methods and techniques.
A computer security policy defines the level of computer security for different groups (or roles) of users, where the users of the computer administrator group can exercise the highest level of control. The idea of hardening the endpoint security is to prevent an authorized user (a test-taker) from using unauthorized computer resources, software, and keyboard functions that may inhibit the integrity of the online exam. In part, that can be accomplished through security policy, for example, by reducing the user rights to the least privileges level in accessing only specific functions or applications through role-based access control. Security policy can also stipulate the principle of Need to Know, which limits access to resources (data, programs) based on the task to accomplish and time frame.

ISSN: 1941-6679-On-line Copy

For example, Avecto Defendpoint (Innnovera, n.d.), an accredited partner of McAfee ePolicy Orchestrator, combines privilege management and application control technology, which grants access privileges to (blacklisted/whitelisted) applications. Its Endpoint Privilege Manager removes local administrator privileges on a computer. Instead, it allows "to grant privileges to individual applications, tasks and scripts, never to users." So, all users run as standard users, and elevation of privileges to the admin level can be done only on-demand, which hardens security.

Special keys, keyboard shortcuts, function keys, and hotkeys can be blocked by programming these keys (with Java, Python code, C#). The functions invoked by function keys can vary among applications and, therefore, they can be added or modified in a web application (The ETI Introduction to Computers Tutorial, n.d. WebNots, 2018). A keyboard listener program, running in the background, can be programmed to record the keyboard actions. It can, for example, trigger a key event each time when a student uses the keyboard to access unauthorized resources outside of the exam task.

There are several well-developed technical controls focused on encryption and hash functions to secure data at rest (on a hard disk) and in transition (over networks) – for example, digital certificates, digital signatures, cryptographic applications, secure protocols (e.g., SSL), and others.

As other information resources on campuses, online proctoring systems can be a target of hacking attacks. To minimize the effect of these attacks, organizations implement detection, prevention, and remediation controls. Like for any cyber secure-protected system, the effectiveness of the controls should be tested for the required cybersecurity assurance level. Thus, Mettl's (Mercer Mettl, n.d.; Mettl, n.d.) diagnostic tool can automatically run the complete system diagnostics check for an online proctoring platform. For a proctored exam, Mettl (n.d.) specifies required and prohibited equipment, exam rules, check system compatibility, the needed browser extension, and the detailed test procedure. The OP4RE Consortium recommends a penetration test to check whether students could penetrate the OP4RE Proctor Exam platform; it can do it by using a Grey Box Infrastructure Penetration Test and a WebApp Penetration Test (OP4R, n.d.; Fouad 2015; Vidalis, 2019).

It is also essential to keep in mind that with time the students are getting more sophisticated with their technical (and basic hacking) skills. It is important, therefore, for an instructor to assess students' level of MMO (Means, motive, and opportunity) and commensurate it with the appropriate controls.

ISSN: 1941-6679-On-line Copy

It could appropriate for an instructor to ask the campus Information Technology Service department to do technical investigation (e.g., penetration testing, replacing computer image, etc.) of the exam server or other specific computers if the instructor suspects a fraud.

ADVANCED TECHNOLOGIES

Online proctoring systems can be grouped into three classes: discretional live-proctor systems, automated (AI-enabled) systems, and hybrid (automated with a live proctor) systems. A good example of the last two classes is ProctorU, which offers (among others) two options:

- *Automated* option with multi-factor authentication, end-to-end video recording, and AI-enabled behavior flagging is suitable for lower to middle-security exams.
- *Hybrid* option with live proctors, AI-enabled behavior analysis, professionally qualified proctors is ideal for professional tests, certifications.

In both options, the AI component helps to control the integrity of examination by identifying unique behavioral signals (e.g., low audible voices, slight lighting variations, movements). These signals may trigger live proctor's actions on the screen or prompt communication with a student via the monitor or through the webcam.

With advanced IT tools added to online proctoring, the use of new intrusive technologies elevates students' concerns for privacy. The students' perception that it is like "big brother invading their computers" and the faculty reservations that online exams test more the students' ability to memorize and less to analyze, deter efforts for implementation of new technologies (Dimeo, 2017). Protection of privacy and compliance with relevant regulations must be enforced through technical control procedures, and privacy concerns of students and faculty must also be alleviated with administrative controls.

VPN, VM, VLAB

Another but limited solution for securing access control is a VPN. Thus, Sonicwall enables restricted and secure VPN access and firewall solutions for higher education.

ISSN: 1941-6679-On-line Copy

VPN client installed on the user's computer can be configured to permit internet access only to the specific website(s) and for the designated application(s). Furthermore, if the campus IT staff administers the student's computer and a student does not have administrator privileges, then the IT staff can enable port-based blocking, i.e., close specific ports on this computer to restrict some types of communication. Besides, a VPN-enabled application can close all network ports on the user's computer except for the port required by the exam application.

Virtual machines (VM) offer the highest level of protection for running applications isolated from the rest of the computer environment. Virtual Labs (VLab) are frequently used for fully interactive simulations, whether it is for presentations, practices, or examinations. VLabs provide time-flexible access, real-time feedback from the completed assignments, use of advanced technology at a lower cost. Typically, the virtual labs are cloud-based (for example, using Microsoft Azure Virtual Cloud Hosting). In some security-sensitive areas of training – cybersecurity, ethical hacking, or courseware for penetration testing – VLabs are indispensable. Three examples of such systems are Virtual Hacking Labs (VHL, n.d.), Virtual Security Cloud Labs (JBL, n.d.), and HERA Lab (eLearnSecurity, n.d.).
In physical and life sciences (academic, clinical, forensic, government, biology, and chemistry), virtual labs, such as Virtual Science Lab (Labster, n.d.), go even further by offering virtual reality and fully interactive simulations for multiple services.

Webcam

Webcam can be used for authentication and physical space monitoring within a proximity to the user. It is capable of accurate face recognition based on the shape and movements of mouth, eyes, and nose using image capturing. But as with any video security check, face recognition is not easy to use, and it can be prone to a high false rejection rate. Webcam authentication has a restriction that will affect the usability or accuracy of imaging. For example, it does not permit a profile view, objects that will obscure a view (e.g., sunglasses, hat), low lighting, etc. These restrictions may be difficult to control, and the user may use them to avoid or obstruct video monitoring during examination. Despite its deficiencies, webcam offers video scanning functionality that cannot be effectively replaced by other devices. The webcam records the user's position, and a proctor, who monitors the user's behavior, can, if needed, remotely freeze the examination screen, place a security flag, or send a message (or a voice command) to prompt the user to re-adjust the webcam.

Remote control of other objects in the physical space outside of the webcam's scope of view presents more significant difficulties and is frequently neglected in online examinations. For example, can an instructor be confident that a participating

ISSN: 1941-6679-On-line Copy

student does not use an unauthorized computing device sitting nearby or that a student does not have access to an unauthorized source of information in a printed/written form? Or, can another collaborating person pass exam answers undetected to the test-taker? A webcam is a stationary device with a relatively narrow scope of observation. Still, using it for spatial control, when a student takes an exam at home) is suitable and recommended.

Security breaches of online exams are difficult to assess. Not surprisingly, the results from formally administered OPS equipped with video-streaming devices differ significantly from a regular exam with no surveillance involved. Of course, as with any monitoring of students in classrooms, a student must be informed that he/she is or will be under surveillance during the examination. Thus, online proctoring with webcam should not be performed without the student's knowledge of it.

However, there are other technical tools and administrative controls that can help, albeit indirectly, mitigating weaknesses or absence of direct spatial control. For example, as an administrative preventive measure, limiting time allowed for the exam can help to deter the test-taker from time-consuming search of information on the Web. Disabling and limiting online access functionality can help. For example, local area network isolation can be implemented using network segmentation. In wireless networks, the Access Control List (ACL) of the Wireless Access Point (WAP) can filter connecting computing devices based on their MAC address. Only computers designated for the exam will be able to connect and run exam application all other endpoints will be blocked. However, the devices that can connect to the Internet independently via an Internet provider will not be blocked (e.g., smartphones), and to detect them, a proctor will have to rely on the visual space controls (e.g., a webcam).

Web Searching and Web Browser

Students frequently use "Web-searching" attack during examination. Lockdown Browser application can block all browsers in the user's computer except for one browser used by the exam application, so it will prevent the student from using other windows. Blocking websites and web applications can be performed by using the web browser settings (e.g., Chrome). Lockdown of a web browser may not be the ultimate solution to prevent "web-searching."

For example, a student can use a second computer (or a smartphone) just for web browsing. A test-taker can easily position another computer or a smartphone out of view of the webcam, which will not detect nor prevent the use of this secondary computing device. The obvious (although far from perfect) administrative safeguard against it is a reduction of time allowed for completing the exam. But

ISSN: 1941-6679-On-line Copy

doing it beyond a certain threshold can be contrary to the exam requirements. The difficulty of controlling the exam-taker isolated from unauthorized sources of information in the exam's physical space is the most significant vulnerability of online proctoring.

AI & ML

The use of AI and other new technologies for assessments of students' learning accelerates rapidly. The purpose of AI is to search for cues to potential violations of exam confidentiality and integrity. AI-enabled biometric authentication (e.g., 2-factor or higher, facial or voice recognition) is just one example. AI is beneficial in a variety of hard to manage functions of online proctoring. As already mentioned, examples of that include mobile ID biometric verification (fingerprint, face, and voice), detection of potential violations, and capturing behavior signals of potential fraud via screenshots, audio files, and video. AI can also help in grading the exam results, for example marking essays (i.e., non-structured answers to questions), which is a very labor-intensive and costly part of examinations at all levels of education. Nevon (n.d.) developed an AI system that checks structured (multiple choice) and unstructured (brief, with no pre-defined answers) questions. For the latter, this AI system analyzes the degree of relevance of each given answer with the stored correct answer and assigns the correctness mark. In another example, Assess By Computer (ABC), an AI-based software developed by Assessment21 at Manchester University, can assess and record with grading marks responses to complex, essay type of questions (Sandle, 2017; Gibson, 2017). There are AI-enabled systems that bridge online lecturing and online examination. For example, Examus (n.d.) offers the capability of obtaining student's behavioral characteristics during online lectures and provides them to proctoring services for online exams.

Complete scope of implementation of AI in online proctoring will support all aspects of operational security. It may include methods for fraud detection using behavioral signs, face (or voice) recognition for authentication, computerized adaptive testing for knowledge testing. The latter includes dynamic questions selection, selecting exploratory questions, forming logically chained and branched questions to explore the test-takers' abilities and knowledge fully.

The role of AI concepts and ML applications for secure authentication and behavior analysis in online proctoring increased significantly. But they are vulnerable to external manipulation and must be secured too. Therefore, access and use of these tools need to be protected with technical controls typically used against application attacks (such as back door, escalation of privilege, SQL injection, and others). AI and ML define the future of online proctoring. As the use of AI applications, adopted in online proctoring for secure authentication and analysis, increase, the

ISSN: 1941-6679-On-line Copy

number and frequency of the automated online exams will also increase significantly. AI concepts and ML applications, adopted in online proctoring for secure authentication and analysis, must be secured as they are also vulnerable to external manipulation. Access and use of these tools need to be protected with technical controls typically used against application attacks (such as back door, escalation of privilege, SQL injection, and others).

CONCLUSION

Table 2 summarizes important features of online proctoring systems. Not all of them are integrated into every proctoring system. The author suggests classification of these features as mandatory (M), recommended (R), and optional (O). Advance features, which typically implemented in AI-supported automated proctoring, are classified as optional. For convenience, the features are grouped into eleven categories: access control, compliance, control, cryptography, detection, interaction, platform, proctoring, recognition, recording, test content.

Table 1 Features of online proctoring systems

Cat	Features	Description
M	Access control: Authentication	Password, profile-based challenge-response, webcam video, picture ID card, multifactor biometrics (fingerprint, facial recognition, voice recognition, palm reader, keystroke analytics, etc.)
M	Access control: Authorization	Discretionary, mandatory, and role-based access methods
M	Access control: Availability	Uninterrupted operational availability of a hosting service and data (exams and logs) retaining policy and procedures
M	Access control: Identification	The first step of access control, followed by authentication and authorization
R	Access control: Non-repudiation	Non-deniability (proof) that a test-taker took certain actions
M	Compliance: Academic Integrity policy	Policy rules to determine the applicable resource access authorizations and the consequences for violations

ISSN: 1941-6679-On-line Copy

M	Compliance: Digital Rights Management	Compliance with DMCA Digital Millennium Copyright Act (DMCA) law (1998)
M	Compliance: GDPR	Mandatory if personally identifying information (PII) or sensitive personal information (SPI) are collected
R	Compliance: SOC 2	Security audit compliance requirement
O	Control: AI-assisted	Artificial Intelligence concepts implemented via ML algorithms to support authentication and analysis of collected data
O	Control: Blockchain	Method for authentication and authorization using public-key cryptography
R	Controls: keystrokes	Blocked keystrokes - disabling blacklisted keystrokes
R	Controls: blocked ports	Blocked ports - prevention of unauthorized network applications
R	Controls: blocked scanners	Blocked screen scanners - prevention of test-takers from taking screenshots
M	Controls: CIA	Confidentiality, integrity, availability are the pillars of cybersecurity concepts for proctoring system
R	Controls: defense-in-depth	Cybersecurity concept implemented via layers of administrative, technical, physical controls
M	Controls: Exam time restriction	Deterring search through unauthorized sources (e.g., book, web)
M	Controls: Lockdown browser	Preventing from use of other browsers
R	Controls: Lockdown resources	Protecting authorized resources from coping (e.g., screen capturing)
R	Cryptography	Use of cryptographic systems for confidentiality
R	Detection: proxy imposter	Detection of an imposter as a proxy test-taker typically, with webcam
R	Detection: second monitor	Can be detected automatically
R	Detection: sound	Playing sound from a remote (test-taker's) computer
M	Interaction: Chat or email	Activate proctor's intervention or support during a test

ISSN: 1941-6679-On-line Copy

R	Interaction: Screen sharing	Activate proctor's pop-ups on the test-taker's screen
R	Platform: Cloud-based hosting	Cloud Security As A Service provides better flexibility, automatic updates, but has its data breaches too.
O	Platform: Cloud-based virtual labs	Offer the highest level of secured, isolated online environment for fully interactive simulation
R	Platform: LMS compatible	LMS as a platform for learning and testing with 3-rd party providers
O	Proctoring method: automated	Synchronous AI-supported, automated active proctoring, includes interactions with test-takers as needed
R	Proctoring method: live	Synchronous, active during examination proctoring, includes interactions with test-takers as needed via audio, video, screen sharing, screenshots
R	Proctoring method: past exam	Asynchronous, passive after examination proctoring with no interactions with test-takers during examination
R	Recognition: face	Based on the shape and movements of eyes, nose, mouth using photo and image capturing with a webcam
R	Recognition: voice	Becoming more popular for authentication
R	Recording: audio	The system records audio at the test-taker's site
O	Recording: audit logs with flagged security events	The system logs the test-taker's behavior cues (voice, movements, etc.) and activities on the computer. The ML algorithm is trained with actual data to recognize security "events" in the log and classify them with flags.
O	Recording: behavioral biometrics	Low audible voices, lighting variations, body movements, keystrokes
M	Recording: logs/records	Logging of test-taker's actions for accounting and auditing events are classified by flag and timestamp
R	Recording: photo	Photo capture (in addition to video and screenshots captures) by proctor
R	Recording: screenshots	Allow proctor to take screenshots of the test-taker's screen (in addition to photo and video capturing).

O	Recording: spatial control monitoring	Monitoring the immediate area that surrounds a test-taker
M	Recording: video	Proctor's access and versatile use of test-taker's webcam for still and dynamic video recording.
R	Test content: Randomization via diffusion	Randomization of exam questions via diffusion - random order of questions and random order of answers (choices) per question in each exam instance per student
R	Test content: Randomization via substitution	Random alteration of each exam question (from a corresponding pool of alternate questions) for each exam taker.

Note: Cat – Category (M-mandatory, R-recommended, O-optional)

Modern online proctoring systems (e.g., Proctortrack) assemble advanced features as follows:

- AI-enhanced live proctoring
- Continuous scans of hardware and peripherals to detect virtual machines and other restricted devices
- Disabled blacklisted keystrokes and applications
- Facial recognition and detection of attempts to receive outside help or to use unauthorized sources (devices, course materials)
- Flagging attempts to search the web for answers.
- Live proctor intervention
- Lockdown browser
- Multifactor Biometric Authentication such as face scan, knuckle scan

Online examinations, advanced with new IT tools and methods, are increasingly used for academic education and professional training. With that, security issues associated with it are multiplying and cause legitimate concern. Sensitive biometric data (in addition to examination data) can be collected and stored for verification and future auditing and purged at the end of its life cycle. Collecting biometric data may need the authorization of the Research with Human Subjects (IRB) Board. If online proctoring procedures are not defined to include security objectives and legal requirements, the proctoring organization or a proctor may face legal complaints and charges.

Personal data collected during OPS operations need to be identified, classified, and labeled according to its sensitivity level for storage. Accordingly, the proper

security procedures and controls need to be implemented for Personally Identifiable Information (PII) to maintain its confidentiality, integrity, and availability, whether these data is at rest on a hard disk or in transition over networks.

The features discussed above are essential for online proctoring systems. But, not all of them may be applicable for smaller classes, so an instructor is advised to do a prior evaluation of their suitability. An instructor should also consider the effect of the security features implemented in an online class, empowered with automated online proctoring, on the student's perception of this class.

COVID-19 boost to online learning may not necessarily lead to positive results if the instructors skip careful planning, training, and collaboration with the IT departments. Without that, the educational technology, its skillful use, and understanding of the security implications will remain the "Gordian knot" for successful transition on a large scale to secure and reliable online proctored assessments of learning.

REFERENCES

ATP. (n.d.). The Association of Test Publishers. Retrieved from https://www.testpublishers.org/

Ciobanu, C. & Ciobanu, N. (2012). E-learning security vulnerabilities. WCES – 2012. Procedia: Social and Behavioral Sciences. 46 (2012) 2297 – 2301. Elsevier. SciVerse ScienceDirect. https://reader.elsevier.com/reader/sd/pii/S187704281201603 5?token=65BEB1B0413463901DECE2217F422EA4938EDC00C7EA7A327B2B63D15847843E57637D20E6439939DCA2609435449075

Cluskey, G.R., Ehlen, C.R. & Raiborn. M. (2011). Thwarting online exam cheating without proctor supervision. Journal of Academic and Business Ethics. Retrieved from https://gato-docs.its.txstate.edu/jcr:0bfb0d86-e1df-41f6-a78c-52249218dc9a/Integrity%20of%20online%20exams.pdf

Cresitello-Dittmar, B. (2016). Application of the blockchain for authentication and verification of identity. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

Dimeo, J. (2017). Online Exam Proctoring Catches Cheaters, Raises Concerns. Inside Digital Learning. Retrieved from

https://www.insidehighered.com/digital-learning/article/2017/05/10/online-exam-proctoring-catches-cheaters-raises-concerns

eAA. (n.d.) e-Assessment Association. Retrieved from https://www.e-assessment.com/remote-proctoring-sig/

eLearnSecurity. (n.d.). Hera Lab. Retrieved from https://www.elearnsecurity.com/virtual-labs/hera/

Examity. (n.d.). Learning validation: online proctoring, on your terms. Retrieved from https://examity.com/

Examus. (n.d.) Examus proctoring service. Retrieved from https://appsource.microsoft.com/en-us/product/web-apps/examus.examusproctoring

Expedian. (n.d). Knowledge-based authentication and scoring. Experian product sheet. Retrieved from https://www.experian.com/decision-analytics/knowledge-iq.html

Experian Product Sheet. (n.d.). Precise ID® A risk-based fraud detection and prevention platform. Retrieved from https://www.experian.com/assets/decision-analytics/product-sheets/precise-id-overview-product-sheet.pdf

Fouad, Y., Lodder, A., Hrudey, J, Draaijer S. (2015) A Lawful basis for online proctoring. Vrije Universiteit Amsterdam. Research Poster Presentation Design. Retrieved from www.PosterPresentations.com

Gibson, M. (2017). 'Many' ways to create artificial intelligence. Just ask the UK's AI businesses. Retrieved from https://www.theregister.co.uk/2017/07/13/british_ai_smbs/

Grassi, P.A., Garcia, M.E., Fento, J.L. (2017). Digital Identity Guidelines. NIST Special Publication 800-63. Revision 3. Retrieved from https://doi.org/10.6028/NIST.SP.800-63-3

Honorlock. (n.d.). Exclusive features. Retrieved from https://honorlock.com/exclusive/

  ISSN: 1941-6679-On-line Copy

Idb-vs-plugins. (n.d.). Lockdown browser vs. locked browser plugin. Retrieved from https://web.respondus.com/wp-content/uploads/2019/07/ldb-vs-plugins.pdf

Innnovera. (n.d.). Avecto Defendpoint. Retrieved from https://www.innoverabt.com/en/vendors/avecto/avecto-defendpoint/

JBL. (n.d.). Virtual Security Cloud Labs. Jones and Bartlett Learning (JBL). Retrieved from http://www.issaseries.com/applied-labs/

Jose, S. (n.d.). Online proctoring is trending: here is all you should know about it. Talview. Retrieved from https://blog.talview.com/a-complete-guide-to-online-remote-proctoring

Labster. (n.d.) Labster simulations. Retrieved from https://www.labster.com/simulations/

McCorkle, R. (2018). Dispelling the concerns around utilizing remote proctoring systems. EDSCOOP. Retrieved from https://edscoop.com/dispelling-concerns-of-utilizing-remote-proctoring-systems/

Mercer Mettl. (n.d.). Mettl ProctorPlus: how it works? Mercer Mettl. Retrieved from https://mettl.com/en/online-remote-proctoring/how-it-works/

Mettl, (n.d.). METTL® User Guide Bcmtms™ Exam. Retrieved from https://www.nbmtm.org/wp-content/uploads/2019/01/Mettl-User-Guide-for-BCMTMS-Exam.pdf

Milone, A.S., Cortese, A.M., Balestrieri, R.L., Pittenger, A.L. (2017). The impact of proctored online exams on the educational experience. Currents in Pharmacy Teaching and Learning. Volume 9, Issue 1, 2017, Pages 108-114, ISSN 1877-1297

Moneo, J.M., Caballé, S., Xhafa, F., Prieto-Blazquez, J. (2015). Security in online web learning assessment: providing an effective trustworthiness approach to support e-learning teams. Research Gate. Retrieved from https://www.researchgate.net/publication/273277604_Security_in_online_web_learning_assessment

  ISSN: 1941-6679-On-line Copy

Nevon. (n.d.). Online examination system with AI. Nevon Projects. Retrieved from https://nevonprojects.com/online-examination-system-with-ai/

OP4RE. (n.d.). Online proctoring for remote examination (OP4RE). Retrieved from https://www.onlineproctoring.eu/en/home/

PennState College Academic Integrity. (n.d.). Strategies for preventing academic integrity issues. Retrieved from https://facdev.e-education.psu.edu/teach/preventingissues

ProctorExam. (n.d.). ProctorExam. Retrieved from https://proctorexam.com/

Proctoru. (n.d.). Harnessing the power of artificial intelligence to improve online proctoring. Retrieved from https://www.proctoru.com/harnessing-the-power-of-artificial-intelligence

Proctorio. (n.d.). A comprehensive learning integrity platform. Retrieved from https://proctorio.com/

PSI. (2018). PSI services introduces new platform to unite remote proctoring methods with industry leading security. Retrieved from https://www.psionline.com/blog/psi-services-introduces-new-platform-to-unite-remote-proctoring-methods-with-industry-leading-security/

Respondus. (n.d.). Lockdown browser. Retrieved from http://www.respondus.com/

Sandle, T. (2017) Artificial intelligence used to mark exam essays. Digital Journal. Retrieved from http://www.digitaljournal.com/tech-and-science/technology/artificial-intelligence-used-to-mark-exam-essays/article/499072

SEB. (n.d.). Safe exam browser. Retrieved from https://safeexambrowser.org/about_overview_en.html

Sonicwall. (n.d.). Higher education: deploy massively scalable protection for entire university systems. Retrieved from https://www.sonicwall.com/solutions/industry/higher-education/

The ETI Introduction to Computers Tutorial. (n.d.). Special keys, keyboard shortcuts, function keys and hotkeys. Retrieved from

  ISSN: 1941-6679-On-line Copy

https://www.issco.unige.ch/en/research/tutoriel-informatique/EN/special_keys_keyboard_shortcuts_function_keys_and__hotkeys.html

Threat Stack. (n.d.). 4 things you need to know about SOC 2 compliance. Threat Stack. Retrieved from https://www.threatstack.com/blog/not-soc-2-compliant-4-reasons-your-customers-wont-work-with-you

Ullah, A., Xiao, H., Barker, T., Lilley, M. (2014). Evaluating security and usability of profile based challenge questions authentication in online examinations. Journal of Internet Services and Applications 2014, 5:2. Retrieved from http://www.jisajournal.com/content/5/1/2

Ullah, A., Xiao, H., Barker, T., Lilley, M. (2017). Graphical and text based challenge questions for secure and usable authentication in online examinations. IEEE. The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014). 8-10 Dec. 2014. Electronic ISBN: 978-1-908320-39-1. London, UK

VHL. (n.d.). Virtual hacking labs (VHL). Retrieved from https://www.virtualhackinglabs.com/

Vidalis, S. (2019). Penetration tests on ProctorExam platform. OP4RE: IO2 - Penetration Test. Version: 20180405:02. February 12, 2019. University of Hertfordshire College Lane Hatfield Hertfordshire AL10 9AB Retrieved from https://www.onlineproctoring.eu/en/dissemination/dissemination-dissemination/penetration-tests-on-proctorexam-platform/

WebNots. (2018). How to set keyboard shortcuts for applications in windows 10? Retrieved from https://www.webnots.com/how-to-set-keyboard-shortcuts-for-applications-in-windows-10/

Xproctor. (n.d.). Xproctor: The solution to online education. Retrieved from http://xproctor.com/

  ISSN: 1941-6679-On-line Copy