DEPENDABLE DISTRIBUTED TESTING
Can the Online Proctor be Reliably Computerized?

Ariel J. Frank
Department of Computer Science, Bar-Ilan University, Ramat-Gan, Israel

Keywords: Lockdown Software, Dependable Distributed Testing, Distributed Education, Identity Verification, Online Proctoring, Secure Online Testing, Test Cheating, Test Integrity, Testing Management System.

Abstract: Distributed Education (DE) enables education, both teaching and learning, anytime, anywhere, using any media or modality, at any pace. Assessment, especially testing, is a major component in the overall evaluation of an educational program. However, there still is an important component missing from most DE programs to enable its full realization in a distributed environment: dependable distributed testing (DDT). The paper presents a comprehensive risk analysis of dependable distributed testing that classifies seven (types of) risks, introduces the resultant DoDoT (Dependable observable Distributed online Testing) reference model, and examines its coverage by three commercial systems. However, these systems are not yet in use in most DE frameworks and do not have yet full DoDoT coverage. The vision of the DoDoT reference model is the continued pursuit and adaptation of new, innovative technologies and methods to make dependable distributed testing increasingly more computerized, reliable, affordable and prevalent.

1 INTRODUCTION

The incessant evolution of the Web has also accelerated the adaptation of Distributed Education (DE), a generalization of Distance Learning, which is in wide use nowadays for educational aims (Allen & Seaman, 2010). DE enables education, both teaching and learning, anytime, anywhere, using any media or modality, at any pace.

There are many important topics in education in general and in distributed education in particular (Simonson, Smaldino, Albright & Zvacek, 2009). We concentrate here on the topic of assessment – of learners by teachers – a major component in the overall evaluation of an educational program. Assessment, be it summative or formative, is a process dealing with control, measurement and the systematic documenting of learners' achievements so as to be able to examine to what extent have the learners advanced towards predefined educational goals. Learners' assessment can be achieved using some combination of tools, such as assignments, papers, projects, quizzes, open and closed tests, forums, group work, etc.

The focus here is on the classic assessment tool – the test (exam, quiz), taken by a testee (examinee, test taker), usually a student, pupil, or trainee, learning in an organization associated with higher education, high schools, or business, respectively. But how can testing security be provided to assure testing integrity? Obviously, there are people who will cheat or defraud if the stakes are high enough and the deterrence too low (Bailie & Jortberg, 2009; King, Guyette & Piotrowski, 2009; McCabe, Trevino & Butterfield, 2001; VS1, n.d.).

Tests can be paper-based or computer-based. Modern educational frameworks (e-learning) provide for computer-administered testing (e-testing). However, notwithstanding the significant growth of DE and its recent ubiquity, there still is an important component missing from most DE programs to enable its full realization in a distributed environment: dependable distributed testing (DDT) (Bailie & Jortberg, 2009; Graf, 2002; Guess, 2008). The term "dependable" here means that distance testing is available to all testees in a secure, reliable manner that maintains testing integrity. The focus here is only on the technical aspects of DDT.

The contribution of this paper is in the comprehensive risk analysis of DDT, in the resultant DoDoT (Dependable observable Distributed online Testing) reference model and in examining its coverage by three commercial systems. The rest of the paper is structured as follows. The following section discusses some relevant aspects of dependable testing. In Section 3, seven (types of)

Frank A. (2010).
DEPENDABLE DISTRIBUTED TESTING - Can the Online Proctor be Reliably Computerized?.
In *Proceedings of the International Conference on e-Business*, pages 22-31
DOI: 10.5220/0002985500220031

risks in DDT are analyzed. In Section 4 the resultant DoDoT reference model is introduced and its coverage by three commercial systems is examined in Section 5. We conclude the paper with Section 6.

2 DEPENDABLE TESTING

Before delving into the risk analysis of DDT, the following subsections review some relevant aspects of dependable testing: accreditation of DE programs, in-person proctoring, and testing integrity.

2.1 DE Program Accreditation

Are DE programs as reputable as regular educational programs? Or more formally, are DE programs regulated and accredited as non-DE programs are? Specifically, accreditation requires that an organization offering an educational program must positively prove by some documentation that an enrolled person is the same learner who does the work leading to graduation (Acxiom, n.d.; VS2, n.d.).

Admittedly, there is a trend in DE not to rely on high-stakes testing for learners' assessment (Foster, 2008). This trend advocates worry that they will be forced to use a particular assessment process that could turn out be too expensive or that would overemphasize tests. Their driving idea is that DE teachers should rely more for assessment on written assignments, threaded discussions, blogs, wikis, e-portfolios, online quizzes, open tests and capstone projects. The assumption is that teachers can become familiar with their learners' working and writing styles in order to spot cheating and fraudulent work, and in time be able to individually assess them.

However, educational organizations requiring high-stakes assessment probably need to depend on testing (Heubert & Hauser, 1999). The lack of dependable testing might turn out to be a major obstacle in complying with required accreditation. Having such “validated testing” could garner more respect for DE programs and raise their credibility with regulators. However, even if distance testing is provided, it is recommended that learners should not be forced to take an online test. In the same way that usually there is a choice if to take an educational program on-ground or online, so should there be a choice for test taking.

2.2 In-person Proctored Tests

Dependable testing is usually realized by human oversight, in the form of proctors who administer the test. Dependable test delivery, with in-person proctors, can be realized using one of three options (Questionmark, n.d.):

1. On-site testing
2. Off-site testing centers
3. One-on-one proctoring.

On-site testing necessitates the physical arrival of all proctors and testees (and usually their teachers) to the organization at the same time. With computer-administered testing, each testee works on a computer that is organizationally preloaded with the test and other tools authorized for use. This is a major undertaking by all involved, though it does provide dependable testing.

Off-site testing centers necessitate the physical arrival of proctors and testees to the closest testing center at similar times (time zone adjusted). This requires travel of staff and faculty to proctor tests taken at off-site public facilities or at third-party testing centers. With computer-administered testing, the organizational logistics required to support multiple testing centers in parallel is a complex effort. It can turn out to be a cumbersome operation, though it also provides dependable testing.

One-on-one proctoring necessitates the recruitment of an in-room proctor to supervise a certain testee at a pre-designated place and time. That is, the testee usually has to make all arrangements for selecting a certified proctor (former teacher, work colleague, librarian, etc.), which will physically oversee the taking of a secured test delivered on time to the testee computer. Overall, this is a burdensome option with a lower testing dependability, since there is higher opportunity for collusion between a not-so-reputable testee and a not-so-reputable proctor.

As aforementioned, each of these in-person proctoring options requires much planning and execution, involving relevant DE administrators, proctors, learners, and teachers, and the appropriate computer-administered testing infrastructure, to solve what can turn out to be “a logistical nightmare”. Any of these options, above and over the, often repeated, efforts and costs, can also lead to growing frustration among the distance learners since these options contradict the core principles of DE and its full realization.

2.3 Test Integrity

The prevalent assumption is that traditional proctors and secure logins suffice to ensure honest computer-administered testing (Carter, 2009). However, any (testing) security system can be circumvented if the will is there and the capabilities exist. In-person proctored tests are also not foolproof. Proctors never

do anything but keep honest testees or uncreative ones honest. How does one make sure that no one cheats in an auditorium attended by a large number of testees? Or as another example, consider a testee with a hidden pinhole camera on a shirt button that broadcasts the screen content to an accomplice who uses a cellphone to advise the testee that wears a miniature wireless earphone concealed by long hair. What should be possible is to inhibit testing integrity risks, not fully prevent them (Graf, 2002; Weippl, 2005).

3 ANALYSIS OF DDT RISKS

Assuming no in-person proctors in DE frameworks makes dependable distributed testing even tougher to realize, but does not turn it into "mission impossible". The fact that (at least) three commercial DDT systems are in use is an indication of a need for such DE systems (Section 5). As part of a literature survey (see References) and extensive research leading to the proposed DoDoT reference model (Section 4), we conducted a comprehensive risk analysis of the cheating and fraud options attemptable during tests. Following, we analyze seven (types of) risks that were identified and classified: testing mismanagement, impersonator, PC misuse, forbidden stuff, accomplice, test leakage, and "electronic warfare".

3.1 Testing Mismanagement

Dependable distributed testing requires varied services and tools for test creation, test data management and archiving, test scheduling, test delivery, test grading, test reporting and test security. The potential for testing mismanagement is huge. Fortunately, the following coupled DE systems can handle this risk.

DE frameworks are usually based on a Learning (Content) Management System (LMS/LCMS) – a software application, usually web-based, for the administration, documentation, tracking, and reporting of e-learning programs, classroom and online events, and educational content (Ellis, 2009). The companion system, Testing Management System (TMS), has similar functionalities but specializes on the testing domain. A TMS can be integrated into an LMS or be interconnected with existing one.

The TMS simplifies the entire test management process while adhering to privacy policies. It should provide testing security for the entire lifecycle of a test. Teachers can post tests from anywhere and learners can take them anywhere with computerized test delivery and full documentation of the testing process. The TMS provides teachers with complete control over and access to the test items, test results and other test information. It can track testees' progress throughout the test sessions, reducing the tension and administrative burdens normally associated with the test season. A TMS can also be used to manage other assessments including unproctored practice tests, quizzes and take-home tests, but this is not the emphasis here.

To support DDT, a TMS should be rigorously secured by use of leading-edge test security and communication technologies or even be run on a secure network. For example, it should use data encryption technologies for test information, secure protocols, firewall protection, etc.

In terms of distributed systems, such a TMS is a "dependable system" where the dependability concept covers important requirements such as availability, reliability, safety, maintainability, integrity, security and fault tolerance (Kopetz & Verissimo, 1993). In a similar sense, the term used here – "dependable distributed testing" – is a generalization of the often used term of "secure online testing".

As aforementioned, there are many components to a testing management system. The focus here is on the test delivery aspects of a TMS. Commercial TMSs include: Perception Secure (Questionmark, n.d.), Respondus (Respondus, n.d.). Section 5 reviews three commercial DDT systems that are TMS based: ProctorU (Pupilcity, n.d.), Online Proctoring (KryterionOLP, n.d.), Remote Proctor (Securexam, n.d.).

3.2 Impersonator

A serious DDT risk is an impersonator testee. How to verify that a learner, signed up for a DE program, is the same one taking the test if the testee is far away? The identity check required when taking a test can be realized by testee verification (Acxiom, n.d.; Bailie & Jortberg, 2009; Schaefer, Barta & Pavone, 2009; Weippl, 2005). Baseline verification of testee identity in computer-administered testing can be achieved by authenticating the username and password during testee login.

The problem though is how secure are usernames and passwords? Learners employing someone else to take their test instead of them would willingly share their username and password with the impersonator, regardless of any rules or regulations. Similarly, we cannot rely on common information about testees (e.g., identification number, mailing address) or even something supposedly only testees know but

that is a "shared secret" with the TMS (e.g., mother's maiden name, favorite color). The problem is that "what you know" is easily sharable. We also cannot rely on some artefact the testees have (e.g., driver's license, smartcard, wearable RFID tag), i.e., on "what you have". Note that we should also not rely on the location of the testees (e.g., IP address, GPS tracking device), i.e., "where you are", so as not to limit the testees in where they take the test.

So how can impersonation be prevented in DE environments? One solution is to achieve testee verification using biometric enrollment and authentication processes (i.e., "what you are"). There are several biometric verification technologies that could be considered (Prabhakar, Pankanti & Jain, 2003). Some are already in use in DE frameworks: fingerprint verification (Securexam, n.d.), face verification (Kryterion, n.d.; Securexam, n.d.), signature verification (StudentPen, n.d.). As part of the authentication process, there is a need to decide when (at start, periodic or random) and how to authenticate the testee and what are the consequences of failure to authenticate. (These processes are also important to assure non-repudiation of test taking.)

Some researchers have coined the term "behaviometrics" for behavioral biometrics such as typing rhythms patterns or mouse movements (i.e., "what you do"), where this analysis can be done continuously without interrupting or interfering with user activities. For example, Webassessor (Kryterion, n.d.) uses keystroke analysis for recognizing unique typing styles. It measures the pattern of keystroke rhythms of a user and develops a unique biometric template of the user's typing pattern for future authentication.

Another testee verification option is use of the challenge questions methodology to inquire on personal history that only the testee can answer for (i.e., "what only you know"). For example, Acxiom Student Identity (Acxiom, n.d.; Bailie & Jortberg, 2009) poses in real-time a few targeted questions that challenge the testee and scores the answers. Challenge questions can be based on third-party data retrieved from large-scale public or private databases, while maintaining privacy policies. Strategies can be used to determine which challenge questions to ask, how many questions, passing thresholds, and red flags on fraud indicators. For example, challenge questions could be asked at sign-on, periodically or also at random. Unlike biometric and behaviometric authentication, the challenge questions methodology does not require pre-test enrollment.

3.3 PC Misuse

Nowadays, most learners have their own personal computer (PC) or can easily gain access to one for testing purposes. We assume the testee uses a well-equipped PC. For purposes like voice verification, environment sounding, or audio chat, the PC requires a microphone. In addition, speakers need be connected to the PC unless the testee wears headphones. For purposes like face verification, environment watching, or video chat, the PC requires a (preferably sound-equipped) webcam. Moreover, for DE purposes, PCs need broadband connections to access the Internet from anywhere, anytime. We do not relate here to mobile learning (m-learning) and its varied devices and connections.

With computer-administered open tests, the testee can access local files, use PC applications or browse the Web. Web browsers are usually designed to be as open and flexible as possible. The focus here though is on high-stakes closed tests. Consequently, when delivering such tests, there is need for more security than is available on a regular PC or that a common Web browser provides (Questionmark, n.d.).

However, with no in-person proctors, how can the entire test session be secured to ensure the testing integrity? For example, the testee could have installed some software on the PC before the test for the express purpose of defeating the test security. Or as another example, there is always a temptation to Google for help. The solution is to use PC lockdown software to secure the testing environment and its test contents. However, how can the lockdown software be securely activated on the PC to ensure its continued reliable operation? The solution is to securely access and activate the PC lockdown software via the TMS and keep them interoperating.

With lockdown software running on the PC, it can be ensured that the test is only delivered via the organization's TMS, after successful biometric enrollment and authentication processes. PC lockdown software includes varied tools that enable lockdown of the desktop, operating system, and Web browser. The idea is to flexibly restrict or completely disable testees' access to the compromising functionalities of these resources. Besides access to the test questions and use of authorized files or tools (e.g., word processing, spreadsheet analysis), the lockdown software secures the testing PC by preventing print, capture, copy, or access to other locally stored or Web accessible files and programs.

PC Lockdown software usually disables (if not restricts) the following functionalities:

- Cut/copy/paste of data to/from the testing environment

- Screen capture/printing functions
- Control/function keys/shortcuts
- Task/application start/access/switch
- Right-click menu options
- Menu options or icons activation
- Setting of PC date/time
- Pop-up windows
- Messaging, screen sharing, network monitoring.

In addition, browser lockdown usually disables (if not restricts) the following functionalities:

- Search/surf the Web
- Browser menu and toolbar options with possible exception for Back/Forward/Refresh/Stop
- HTML source code viewing
- Cache/store of pages in history/search listings.

Moreover, PC lockdown software can provide for the following requirements:

- Automatically start at sign-on page of the organization's TMS.
- Testees cannot commence a test until they are provided with a special password by the TMS.
- The test questions are displayed in a full-screen mode that cannot be minimized.
- Following test completion, all test-related files are automatically submitted back to the TMS.
- Clearing of any cookies, caches, and temporary files at test session end.

When a test is launched, the testee is locked up into the testing environment (i.e., cannot suspend or exit it) until the test is submitted back. The testing environment should be able to withstand (un)intentional actions or breakdowns, shutdowns or restarts, and network disconnections, and be able to recover the testing environment and contents. With advanced technologies such as "software as a service", Web services, virtualization and cloud computing, such robust testing environments can be nowadays supported.

As another option, "Remote Desktop" software can be used to observe the testee screen and even control the PC if deemed necessary by an online proctor. It can also be used to assist the testee and provide technical support if need be. The testee must have given previous authority for remote access to the online proctor.

Commercial PC lockdown software include: Simpliciti (Simpliciti, n.d.), KioWare Lite (KioWare, n.d.), Perception Secure (Questionmark, n.d.), Respondus (Respondus, n.d.). There is also an open-source Safe Exam Browser (SEB, n.d.).

3.4 Forbidden Stuff

In regular closed tests, the testee puts away all forbidden stuff such as notes, reference sources, textbooks, computers, cellphones and other devices (King et al., 2009). But how can this restriction be enforced in the absence of in-person proctors?

The solution is online monitoring to proctor the testing environment to detect anything forbidden. Online monitoring, using real-time audio and video (A/V), can hear and watch the testees and their surrounding environment, while they enroll, authenticate and take the test on their PC. It can be carried out by (live or random) online proctor observation or by (continuous) test session recording that consists of A/V, biometrics and other testing event data that is sent to the TMS. Online proctors can observe the testee using one-on-one videoconferencing technologies. Test session recording uses streaming technologies where the A/V stream can also be viewed by an online proctor. Computerized processes can detect aberrances and use red flags to real-time alert the online proctor or indicate need for post-test analysis.

However, with a common webcam, there is a problem detecting forbidden material displayed at the room back or hidden behind or below the PC. We provide a solution for this in the next subsection.

3.5 Accomplice

Another serious DDT risk is a testee accomplice (Eplion & Keefe, 2007). How can an accomplice be prevented from aiding the testee? There is a need to disallow the same accomplice means used in a regular test such as exchange of notes, use of cellphones, rendezvous at the toilets, etc. The distance testee should be required to disconnect all phones, not leave the room, not let another person enter the room, etc.

Online monitoring can also be used to detect an accomplice via a sound-equipped webcam. However, a regular webcam isn't enough to ensure testing integrity. For example, a video projector in back of the room or a hidden (pinhole) camera in front can project the screen content to an in-room accomplice standing behind the PC. The accomplice can in return signal the testee (say for multiple choice questions), use sign language, or write answers onto a raised (hand-held) whiteboard.

Asking the testee to physically pan the webcam around the PC to check on the surroundings is an awkward process, especially if it has to be repeated during the test itself. A better solution is to use a 360^{o} webcam. For example, the Securexam Remote Proctor (SRP) unit (SecureExam, n.d.) encloses a 360^{o} webcam. The unit features a mirrored sphere suspended above a small pedestal. The sphere reflects a deep 360^{o} view around the testee, which

the webcam picks up. A 360° webcam can be used to detect an accomplice, as well as use of forbidden stuff, also behind and below the PC, and red flag online monitoring that something might be awry. It is hard to cheat without some suspicious sound or motion being made by the testee or the accomplice.

Another countermeasure is to detect and obstruct any (hidden pinhole) camera by use of an inexpensive, simple laser pointer – not damaging to humans – to zap (blind) the camera, thereby generating a camera capture resistant environment (Naimark, 2002). Similarly, a long video cable or hidden camera can transmit the screen content to an off-site accomplice who uses a cellphone to advise the testee who wears a miniature wireless earphone. The countermeasure is the use of cellular detectors and jammers (Wollenhaupt, 2005).

Advanced recognition technologies could also be put to use. For example, if the testee decides to play music to relax while taking the test, voice/sound recognition can disregard it. As another example, image/object recognition can prevent a false alarm if a pet suddenly wanders around the room or jumps on the testee lap.

3.6 Test Leakage

An acute DDT risk is test leakage, especially for same time tests (Eplion & Keefe, 2007). Although testees can (try to) memorize (some of) the closed test's content, at least they should not be able to compromise it at test time. The use of a secure TMS and PC lockdown software prevents many of the options for test leakage. Restrictions enforced for the accomplice risk also apply. Options to prevent test leakage via an accomplice have also been covered.

However, in regular closed tests, scrawling is a natural test activity that is allowed in the test book ("blue book" in USA). Similarly, scrawling in computer-administered testing can be allowed in a digital notebook ("private workspace") that is part of the secured testing environment. Forbidden writing to paper can be detected by online monitoring. However, indirect recording of test questions by a testee that seemingly just reads the questions aloud is hard to detect (if the recording device is hidden), so such systematic reading aloud should be disallowed.

To hinder the leakage of a test, its questions and answers, one or more of the following or similar methods, collectively named here "Schemed questioning", could be considered:

- Use of test banks with random selection of questions.
- Scrambling the order of questions and answers (for multiple choice questions).
- Presenting just one question at a time.
- Setting time allotments for question answering (timed test delivery).

3.7 "Electronic Warfare"

The concern here is with the physical protection of the PC hardware and devices. How can the PC and especially its devices such as the camera, microphone and biometric devices be protected from tampering? There is a need to detect lost A/V signals or loss of feed quality. As another problem, the webcam real-time A/V stream could be substituted by a pre-recorded one.

The detection of this can be done by online monitoring. However, to discourage more advanced "electronic warfare", i.e., disabling or circumventing the capability of these devices, a separate hardware proctoring unit that physically encloses the devices can be used. To be easy to use, the unit should be portable and pluggable, say via USB. The proctoring unit has to be of course first acquired by the learner before any testing activity. To ensure the testing integrity, as part of an enrollment process, the unit should be remotely registered to both the testee and the PC used for test taking. The proctoring unit itself should be physically tamperproof, and secured by the TMS and PC software lockdown so as to red flag any mishandling of the unit.

4 DoDoT REFERENCE MODEL

Based on the above DDT risk analysis, we introduce the resultant DoDoT/RM (Dependable observable Distributed online Testing Reference Model). (Dodot stands for aunts in Hebrew – it is slang for the traditional elderly female proctors.) DoDoT/RM suggests an array of specific methods that can answer the seven risks (see mapping in Table 1), so as to enable the reliable computerization of online proctoring in DDT systems. The paper's author is unaware of any published similar attempt to define a dependable distributed testing reference model.

The premises of DoDoT/RM are as follows. To assure DDT, each and every one the seven (types of) risks should be covered. Moreover, not just one, but at least two of the proposed methods should be used for risk mitigation. The idea is to make cheating and fraud significantly hard – too expensive for the testee to make it worthwhile taking the risks. For example, for testee verification it is recommended to

use two-factor authentication, where two different factors (out of biometrics, behaviometrics and challenge questions) are used in conjunction to deliver a higher level of authentication. Similarly, both online proctor observation and test session recording can be used for more reliable monitoring. However, since most of the suggested methods can concurrently answer several risks, just a minimal covering set of methods should be chosen.

The monitoring of the test session should be online, not just offline, since the test environment should be real-time observable and the testee be made aware of it. However, online monitoring does not necessarily require that a human proctor continuously observe the testee. Since a human proctor is an expensive resource, live observation could be done at test launch, randomly, or if real-time computerized red flags were raised. It also does not have to be achieved via a one-on-one videoconference. The A/V stream of the test session recording received at the TMS can be observed by an online proctor. Note also that there is no, or less, need to repeat authentication processes if there is test session recording that can be post-test analyzed.

However, how many proctors can be employed concurrently? And of those, how many are capable to diligently watch and listen to hours of testees A/V during or after the test taking with the possibility in mind that testees might cheat at some point? Considering the human limitations in continuous monitoring, the premise of DoDoT/RM is that computerized processes are preferable in this regard to human ones. Most, if not all, of the online proctor observations can be replaced by computerized processes (possibly adaptive AI agents) that can deter and detect aberrant events and red flag them as real-time alerts for the online proctor or as signals indicating a need for post-test analysis.

The online proctor could then monitor a testee just a few times during a test to observe if what is being done matches the sounds and actions on the testee PC. If there are red flags, the test session recording can be later analyzed, preferably again by computerized processes, which provides in addition the recorded proof of any wrongdoing.

To inhibit the risks of accomplice and test leakage, it is recommended to use technologies for hidden devices obstruction such as camera zapping and cellphone jammers. For sophisticated computerized monitoring and post-test analysis, use can be made of advanced recognition technologies such as voice/sound and image/object recognition. Post-test analysis of multiple tests can be used to detect aberrant trends, for example, by data mining.

As aforementioned (Section 3.5), use of a common webcam is not enough – only a 360^{o} webcam provides continuous view of the entire testee surroundings. Moreover, having separate PC devices such as 360^{o} webcam, biometric devices, camera zappers and cellphone jammers is problematic (Section 3.7). Use of a separate proctoring unit to enclose all the devices is required.

A cost-effectiveness analysis of DoDoT/RM still needs to be carried out. However, it is assumed that a covering set of its methods, and specifically the separate proctoring unit, can be realized in a cost effective way (subsidized by the organization or priced at few hundred dollars overall per testee). For such and further technical considerations refer to (Acxiom, n.d.; Bailie & Jortberg, 2009; Foster, 2008; Jortberg, 2009). Clearly, when choosing such a covering set, other relevant aspects such as social, legal, ethical, economical, and psychological ones need also be considered (Schaefer, 2009).

5 COMMERCIAL DDT SYSTEMS

For a feasibility check of DoDoT/RM we examine its coverage by three commercial DDT systems (Bailie & Jortberg, 2009; Foster, 2008): Pupilcity ProctorU, Kryterion Online Proctoring, Securexam Remote Proctor. Due to paper space constraints, the review focus here is on their outstanding techniques and services (more detailed information is on their websites). Note also that no caught cheating rates are made public by these companies. For each system, we mark in Table 1 the methods that are in use by a checkmark and those not in use by a dimmed x. Subsection 5.4 compares these working DDT systems regarding their DoDoT/RM coverage.

5.1 Pupilcity ProctorU

ProctorU (Pupilcity, n.d.) allows learners to securely take tests online by using videoconferencing to connect one-on-one with live, certified proctors and follow their instructions. ProctorU was originally developed for internal use at Andrew Jackson University (AJU) and was later spun off into a separate company, Pupilcity (Morgan, 2008). ProctorU uses the Acxiom Identify-X technology for a real-time online identity verification service that uses the challenge questions methodology (Acxiom, n.d.). This technology was piloted and put to test several times at National American University (ANU) (Bailie & Jortberg, 2009). ProctorU is affiliated with 20 educational institutions.

Table 1: DDT risks and methods.

Risks	Methods that can answer the seven risks	Pupilcity ProctorU	Kryterion OLP	Software Secure SRP
Testing Mismanagement	• Testing Management System	✓	✓	✓
	• Secure communication	✓	✓	✓
Impersonator	• Biometric authentication	×	✓	✓
	• Behaviometric authentication	×	✓	×
	• Challenge questions	✓	×	×
	• Online proctor observation	✓	✓	✓
	• Test session recording	×	✓	✓
PC Misuse	• PC Lockdown Software	×	✓	✓
	• Remote Desktop Software	✓	×	×
	• Aberrance computerized red flags	×	✓	✓
Forbidden Stuff	• Online proctor observation	✓	✓	✓
	• Test session recording	×	✓	✓
	• Aberrance computerized red flags	×	✓	✓
Accomplice	• Online proctor observation	✓	✓	✓
	• Test session recording	×	✓	✓
	• Use of 360° webcam	×	×	✓
	• Hidden devices obstruction	×	×	×
	• Advanced recognition technologies	×	×	×
Test Leakage	• PC Lockdown Software	×	✓	✓
	• Online proctor observation	✓	✓	✓
	• Test session recording	×	✓	✓
	• Use of 360° webcam	×	×	✓
	• Aberrance computerized red flags	×	✓	✓
	• "Schemed questioning"	×	✓	×
"Electronic Warfare"	• Detect lost A/V signal & feed quality	✓	✓	✓
	• Separate proctoring unit	×	×	✓

Each testee first needs to individually schedule a test at ProctorU's Online Proctoring Center. There are four steps in taking the test:

1. Connect – ProctorU automatically connects the testee to the online proctor.
2. Observe – proctor connects to testee's screen.
3. Prove identity – proctor watches the testee as he/she authenticates identity.
4. Monitor – proctor observes testee taking test.

ProctorU uses the TokBox video chat and Remote Desktop software. The online proctor watches the testee via a webcam as he types away at the keyboard, observes the screen, and listens for other sounds in the testing environment. Aberrant actions can be manually documented in the form of screen captures and camera shots that are sent to the TMS. ProctorU does not make use of the other methods suggested by DoDoT/RM.

5.2 Kryterion Online Proctoring

Webassessor (Kryterion, n.d.) is a secured online testing platform that provides a wide variety of testing technologies and services. Kryterion introduced Webassessor's Online Proctoring (OLP) system (KryterionOLP, n.d.) in 2007. A series of OLP pilots was carried out in conjunction with World Campus, the online arm of the Pennsylvania State University system (Shearer, Lehman, Hamaty & Mattoon, 2009).

It uses the Akamai secure network to provide robust testing delivery. OLP uses the Sentinel Secure technologies to lockdown the PC and conduct face verification and keystroke analysis for testee enrollment and authentication. The testing environment is continuously monitored and a testing session recording is generated. OLP utilizes varied security technologies and processes to deter and detect aberrance during the testing session and alerts online proctors when suspicious activities occur.

Kryterion employs certified, online proctors, called KCOPS, who can remotely observe and listen to as many as 50 testees at a time. They monitor a live video feed of each testee in real-time. Previous testing activity of testees is available to KCOPS for detecting aberrant behavior. Testee's aberrant behaviors or response time patterns (e.g., answering a question too fast or too slow) alert the KCOPS. OLP uses Real Time Data Forensics (RTDF) technology to red flag unusual events.

The KCOPS communicate with testees just via drop down menu options. KCOPS can send messages to the testee as necessary and take actions such as pausing, suspending or stopping the test based on testee behaviors and actions. For "Schemed questioning", testees receive questions one at a time after scrambling the order of test questions.

5.3 Securexam Remote Proctor

Software Secure (SoftwareSecure, n.d.) provides a suite of tools for secure online testing. The Securexam Remote Proctor (SRP) (SecureExam, n.d.) was an initiative of Troy University, which was commercially developed by Software Secure. It has been extensively experimented with and is long in use at Troy University (Powers, 2006; Guess, 2008). It was used for a pilot at a Small Southern Regional University (Bedford, Gregg & Clinton, 2009). SRP is affiliated with 15 educational institutions.

PlanetSSI is their web-based TMS. PC lockdown software is comprised of the Securexam Student and Securexam Browser. SRP uses biometric fingerprint verification and face verification, real-time A/V monitoring and recording of the testing session.

The SRP device is a separate proctoring unit that connects to the testee's PC as a USB plug-in. It includes a groove for scanning fingerprints, and a built-in 360^{o} webcam. SRP interconnects with Securexam Browser and Securexam Student. SRP verifies the testee's identity through the use of finger-scan and face verification. Testees are recorded during tests and the recorded stream can be observed online. In addition, computerized filters can detect any suspicious changes in sound or motion, and red flag them for post-test analysis.

5.4 Discussion

Pupilcity ProctorU is a technically simple DDT approach since it mainly depends on online proctor observation and uses challenge questions for testee verification (Table 1). Consequently, it has only partial coverage of DoDoT/RM. ProctorU is more oriented to individual test taking than to same time testing. It does not have two-factor authentication since there is no biometric/ and behaviometric authentication; it relies solely on challenge questions. It does not use PC lockdown software, do test session recording or provide aberrance computerized red flags. It also does not have a separate proctoring unit having a 360^{o} webcam.

Kryterion Online Proctoring is a technically rich DDT approach with good coverage of DoDoT/RM (Table 1). OLP has two-factor authentication: biometric (face verification) and behaviometrics (keystroke analysis). It is noteworthy that this chosen two-factor authentication scheme requires no biometric device. OLP supports both online proctor observation and test session recording so any required balance between them can be realized. It has a varied set of computerized processes to real-time red flag aberrant actions and behaviors. However, it does not make use of a separate proctoring unit having a 360^{o} webcam.

SRP has excellent coverage of DoDoT/RM since it also uses a separate proctoring unit with a 360^{o} webcam (Table 1). However, it has only two-factor biometric authentication: face and fingerprint verification. It is noteworthy that SRP emphasizes test session recording while relying less on online proctor observation. It uses computerized processes to red flag suspicious activities by recording A/V clips for post-test analysis and aberrance proof.

Note that these systems could use more advanced recognition technologies for sophisticated computerization of processes to red flag aberrances. They could also utilize hidden devices obstruction (Section 4) to inhibit the associated risks. In any case, a DDT system with full or fuller coverage of DoDoT/RM has yet to be developed and deployed.

6 CONCLUSIONS

To increase the testing integrity of DE programs, there is growing need to deliver DDT anytime, anywhere. Wide deployment of DDT systems to achieve testing integrity has long been overdue. The introduced DoDoT/RM is based on a comprehensive DDT risk analysis. The fact that three commercial DDT systems are in use is an indication for their need. Nowadays, due to technological advances and improved methods, DDT systems can securely deliver high-stakes tests worldwide. These DDT systems utilize varied test security methods to deter and detect cheating and fraud by testees.

However, DDT systems are not yet in use in most DE frameworks. Moreover, these systems do not yet provide full DoDoT/RM coverage to enable reliable computerization of the online proctor – more experimentation and comprehensive field use is still needed. The vision of DoDoT/RM is the continued pursuit and adaptation of new, innovative technologies and methods to make dependable distributed testing increasingly more computerized, reliable, affordable and prevalent.

ACKNOWLEDGEMENTS

Thanks to Tomer Patron for research contributions.

REFERENCES

Acxiom (n.d.). *Identity Verification to Support Academic Integrity,* Acxiom White Papers. http://www.acxiom.com/StudentIdentity

Allen, I. E. & Seaman, J. (2010). *Learning on Demand: Online Education in the United States, 2009*. Newburyport, MA: The Sloan Consortium. http://www.sloanconsortium.org/publications/survey/pdf/learningondemand.pdf

Bailie, J. L. & Jortberg, M. A. (2009). Online Learner Authentication: Verifying the Identity of Online Users. *MERLOT JOLT*, 5(2), 197-207. http://jolt.merlot.org/vol5no2/bailie_0609.pdf

Bedford, W., Gregg, J. & Clinton, S. (2009). Implementing Technology to Prevent Online Cheating: A Case Study at a Small Southern Regional University (SSRU). *MERLOT JOLT*, 5(2), 230-238. http://jolt.merlot.org/vol5no2/gregg_0609.pdf

Carter, D. (2009, July 10). ED OKs Proctors, Secure Logins for Online Tests. *eSchool News*. http://www.eschoolnews.com/2009/07/10/ed-oks-proctors-secure-logins-for-online-tests-2

Ellis, R. K. (2009). Field Guide to Learning Management Systems. *ASTD Learning Circuits*. http://www.astd.org/NR/rdonlyres/12ECDB99-3B91-403E-9B15-7E597444645D/23395/LMS_fieldguide_20091.pdf

Eplion, D. M. & Keefe, T. J. (2007). Practical Tips for

Preventing Cheating on Online Exams. *Faculty Focus*. http://www.magnapubs.com/issues/magnapubs_ff/4_4/news/600136-1.html.

Foster, A. L. (2008, July 25). New Systems Keep a Close

Eye on Online Students at Home. *The Chronicle of Higher Education, Information Technology*, 54(46). http://chronicle.com/article/New-Systems-Keep-a-Close-Eye/22559

Graf, F. (2002). Providing Security for eLearning. *Computers & Graphics*, 26(2), 355-365.doi:10.1016/S0097-8493(02)00062-6

Guess, A. (2008, October 8). From Blue Books to Secure Laptops. *Inside Higher Ed*. Retrieved Feb 3, 2010, http://www.insidehighered.com/news/2008/10/08/tests

Heubert, J. P. & Hauser, R. M. (Eds.). (1999). *High Stakes: Testing for Tracking, Promotion, and Graduation*. National Research Council, Washington, DC: The National Academies Press. http://www.nap.edu/openbook.php?record_id=6336

Jortberg, M. A. (2009). Student Authentication Solution Comparison. *Online Student Identity blog*. http://mikejortberg.blogspot.com/2009/06/student authentication-solution.html

King, C. G., Guyette, R.W. & Piotrowski, C. (2009). Online Exams and Cheating: An Empirical Analysis of Business Students' Views, *The Journal of Educators Online*, 6(1). Retrieved February 3, 2010, http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf

KioWare (n.d.). *KioWare Browser Lockdown Software*. www.kioware.com/default.aspx?source=kmshowcase

Kopetz, H. & Verissimo, P. (1993). Real Time and Dependability Concepts*,* In Mullender, S. (Ed.), *Distributed Systems*, Addison-Wesley, 411-446.

Kryterion (n.d.). *Webassessor*. www.kryteriononline.com KryterionOLP (n.d.). *Kryterion Online Proctoring*. http://www.kryteriononline.com/delivery_options

McCabe, D. L., Trevino., L. K. & Butterfield. K. D. (2001). Cheating in Academic Institutions: A Decade of Research. *Ethics & Behavior*, 11(3), 219-232. http://www.swarthmore.edu/NatSci/cpurrin1/plagiarism/docs/McCabe_et_al.pdf

Morgan, J. (2008). *Online Proctoring Perfected, Spun off by Tech-savvy University.* Retrieved February 3, 2010, www.webwire.com/ViewPressRel.asp?aId=80502

Naimark, M. (2002). *How to ZAP a Camera: Using Lasers to Temporarily Neutralize Camera Sensors*. http://www.naimark.net/projects/zap/howto.html

Powers, E. (2006, June 2). Proctor 2.0. *Inside Higher Ed*. www.insidehighered.com/news/2006/06/02/proctor

Prabhakar, S., Pankanti, S. & Jain A. K. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy*, 1(2), 33-42. doi:10.1109/MSECP.2003.1193209

Pupilcity (n.d.). *Pupilcity ProctorU*. www.proctoru.com

Questionmark (n.d.). *Questionmark Perception Secure*. http://www.questionmark.com/us/perception/

Respondus (n.d). *LockdownBroswer*. www.respondus.com

Schaefer, T., Barta, M. & Pavone, T. (2009). Student Identity Verification and the Higher Education Opportunity Act: A Faculty Perspective. *Intl. J. of Instructional Tech. and Distance Learning*, 6(8), 51-58. http://itdl.org/Journal/Aug_09/article05.htm

SEB (n.d.). *SEB,* www.safeexambrowser.org/

Securexam (n.d.). *Securexam Remote Proctor*. http://www.remoteproctor.com/SERP

Shearer, R., Lehman, E., Hamaty, P. & Mattoon, N. (2009). Online Proctored Exams at a Distance: How can you Help Assure Academic Integrity?. *UCEA 94th Annual Conference*, Boston, Massachusetts.

Simonson, M. R., Smaldino, S. E., Albright, M. & Zvacek, S. (2009). *Teaching and Learning at a Distance: Foundations of Distance Education*. Allyn and Bacon.

Simpliciti (n.d.). *Lockdown Solutions*. www.simpliciti.biz

SoftwareSecure (n.d.). www.softwaresecure.com

StudentPen (n.d.). *Bio-Pen*. http://www.studentpen.com

VS1 (n.d.). *Integrity in Education Online*. http://www.virtualstudent.com/?page_id=19

VS2 (n.d.). *Accreditation in Online Degree Programs.* http://www.virtualstudent.com/?page_id=9

Weippl, E. R. (2005). *Security in E-Learning*. Advances in Information Security, Springer, Vol. 16.

Wollenhaupt, G. (2005). How Cell Phone Jammers Work, www.howstuffworks.com/cell-phone-jammer.htm