Study
Report
2002-07

Training on the Web: Identifying and Authenticating Learners

Christina K. Curnow
Caliber Associates

Michael W. Freeman
Computer Sciences Corporation

Robert A. Wisher and James Belanich
U.S. Army Research Institute

United States Army Research Institute for the Behavioral and Social Sciences

June 2002

Approved for public release; distribution is unlimited.

20020821 030

U.S. Army Research Institute
for the Behavioral and Social Sciences

A Directorate of the U.S. Total Army Personnel Command

ZITA M. SIMUTIS
Acting Director

Research accomplished under contract
for the Department of the Army

Caliber Associates

Technical Review by

Allan Pettie
Danny Hubbard
G.A. Redding

NOTICES

DISTRIBUTION: Primary distribution of this Study Report has been made by ARI. Please address correspondence concerning distribution of reports to: U.S. Army Research Institute for the Behavioral and Social Sciences, Attn: TAPC-ARI-PO, 5001 Eisenhower Ave., Alexandria, VA 22333-5600.

FINAL DISPOSITION: This Study Report may be destroyed when it is no longer needed. Please do not return it to the U.S. Army Research for the Behavioral and Social Sciences.

NOTE: The findings in this Study Report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

REPORT DOCUMENTATION PAGE

1. REPORT DATE (dd-mm-yy) June 2002	2. REPORT TYPE Final	3. DATES COVERED (from. . . to) April 2001-March 2002
4. TITLE AND SUBTITLE Training on the Web: Identifying and authenticating learners		5a. CONTRACT OR GRANT NUMBER DASW01-98-D-0049
		5b. PROGRAM ELEMENT NUMBER 665803
6. AUTHOR(S) Christina K. Curnow (Caliber Associates), Michael W. Freeman (Computer Sciences Corporation), Robert A. Wisher, and James Belanich (U.S. Army Research Institute)		5c. PROJECT NUMBER D730
		5d. TASK NUMBER 259
		5e. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Caliber Associates 10530 Rosehaven Street, Suite 400 Fairfax, VA 22030		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Institute for the Behavioral and Social Sciences ATTN: TAPC-ARI-II 5001 Eisenhower Avenue Alexandria, VA 22333-5600		10. MONITOR ACRONYM ARI
		11. MONITOR REPORT NUMBER Study Report 2002-07

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Contracting Officer's Representative: Robert A. Wisher

14. ABSTRACT *(Maximum 200 words)*:

Soldiers who receive training in the workplace, at their residences, or at other sites outside the traditional classroom increasingly rely upon asynchronous distributed learning systems. This accentuates the need to identify various forms of training compromise, such as obtaining questions beforehand or enlisting a proxy for test taking in non-proctored, web-based learning environments. A one-day workshop, summarized in this report, was conducted to identify practical solutions to training compromise on the Web or military intranets. Experts from government, academia, and industry generated solutions in the areas of test security, biometrics (including fingerprint identification, face recognition, iris scanning, and hand writing recognition), legal issues, public key infrastructure, instructional design, and test design. Following the workshop, an Army advisory group prioritized the solutions into a final list of recommendations, included here as a starting point for addressing and preventing training compromise.

15. SUBJECT TERMS

Training, Education, Distributed Learning, Cheating, Testing, Online Instruction, Security, Compromise, Biometrics

SECURITY CLASSIFICATION OF			19. LIMITATION OF ABSTRACT	20. NUMBER OF PAGES	21. RESPONSIBLE PERSON (Name and Telephone Number)
16. REPORT Unclassified	17. ABSTRACT Unclassified	18. THIS PAGE Unclassified	Unlimited	37	Robert A. Wisher 703/617-5540

Study Report 2002-07

Training on the Web: Identifying and Authenticating Learners

Christina K. Curnow
Caliber Associates

Michael W. Freeman
Computer Sciences Corporation

Robert A. Wisher and James Belanich
U.S. Army Research Institute

Advanced Training Methods Research Unit
Franklin L. Moses, Chief

U.S. Army Research Institute for the Behavioral and Social Sciences
5001 Eisenhower Avenue, Alexandria, Virginia 22333-5600

June 2002

Army Project Number
2O465803D730

Personnel and Training
Analysis Activities

Approved for public release; distribution is unlimited.

FOREWORD

The U.S. Army Training and Doctrine Command's (TRADOC's) goals include increasing training opportunities for all soldiers, improving the quality of instruction, increasing access to training, and reducing the time soldiers spend away from their unit. There is an interest on the part of the Army to consider distributed learning as at least part of the solution towards advancing these goals. In these environments, soldiers who receive training in the workplace, at their residences, or other sites outside the traditional classroom, increasingly will rely on the use of the Web or military intranets.

This study originated from a request by the Army Training Support Center, who recognized that an increased reliance upon distributed learning systems accentuates the need to identify various forms of training compromise, such as obtaining questions beforehand or enlisting a proxy for test taking in non-proctored, web-based learning environments. There is no definitive evidence that such training compromise is currently a problem in the Army, but greater use of distributed learning in the future coupled with reported trends of high levels of cheating among high school students, the Army's prime enlistment pool, is reason for concern.

The study examined potential solutions, such as proctored test environments and biometric measures, recommended by a group of experts during a workshop hosted by Carnegie Mellon University. The results of this study were presented to the sponsors from the Army Training Support Center and representatives from TRADOC Headquarters on 21 February 2002.

MICHAEL G. RUMSEY
Acting Technical Director

ACKNOWLEDGEMENTS

The authors thank Anne Humphreys of the Learning Systems Architecture Lab at Carnegie Mellon University, Pittsburgh, PA, for graciously hosting the workshop. We also thank Johanna McKenzie of the Learning Systems Architecture Lab for her outstanding efforts in handling the workshop logistics. In addition, we greatly appreciate efforts by Phillip Loranger, Director of the DoD Biometrics Office, for his tremendous support and kind assistance in providing expertise in the area of biometric measures.

In addition, our thanks to Dr. Allan Pettie for his first-rate coordination within the Army Training Support Center and to Dr. Kathleen Quinkert for her excellent coordination within the Army Training and Doctrine Command.

EXECUTIVE SUMMARY

Research Requirement:

The Army is shifting certain training from a classroom-centric delivery of instruction to a learner-centric model. Soldiers who receive training in the workplace, at their residences, or other sites outside the traditional classroom increasingly will rely on the use of the Web or military intranets. Such reliance upon asynchronous distributed learning systems accentuates the need to identify various forms of training compromise, such as obtaining questions beforehand or enlisting a proxy for test taking in non-proctored, Web-based learning environments. Practical solutions based on recommended practices, procedures, and applications of special measurement technology need to be identified.

Method:

Solutions to training compromise were sought from experts in the areas of test security practices, training design considerations, public key infrastructure (PKI), biometrics, and legal perspectives. Experts presented potential solutions to training compromise at a one-day workshop. The workshop was followed by a brainstorming session during which the 31 invited participants from government, academia, and industry generated 40 potential solutions. An Army advisory panel assessed the solutions based on cost, feasibility of implementation, ease of use, reliability and accuracy, then developed a final list of recommended solutions.

Findings:

The advisory panel recommendations included: using affirmative obligations; live and virtual proctoring; multimodal biometrics and/or biographical information integrated into course design; implementing PKI to limit inappropriate access to courseware and tests; and considering test designs such as randomizing items, performance testing, time limits, limiting testing attempts, using "no print/capture" options, and tracking where test takers have been online. The recommendations are meant to function as general guidelines for solutions to training compromise. The usefulness of implementing any particular set of solutions is in large part dependent on the criticality of the training and testing under consideration.

Utilization of Findings:

This report is relevant to course administrators who are using or planning to use online distributed learning technologies for military education and training. The results and recommendations of this study were presented to representatives from the Army Training Support Center and TRADOC Headquarters on 21 February 2002, and the Total Force Advanced Distributed Learning Action Team on 29 March 2002. Based on this work, the Defense Acquisition University plans to implement certain recommendations, including: affirmative

obligation statements, requiring a user to type in passwords at variable intervals, and live proctoring at remote sites.

TRAINING ON THE WEB: IDENTIFYING AND AUTHENTICATING LEARNERS

CONTENTS Page

FOREWORD v

ACKNOWLEDGEMENTS vi

EXECUTIVE SUMMARY vii

INTRODUCTION 1

BACKGROUND 1

The Issue of Training Compromise 2
The Distributed Learning Environment in the Army 3
Implications/Impact of Training Compromise 4

WORKSHOP SUMMARY 5

Training Design Considerations for Identifying, Authenticating and Monitoring Learners 6
Test Security Practices and Issues 7
Public Key Infrastructure 8
Overview of Defense Biometrics Management Organization 10
Future Trends in Biometric Measures 14
Legal Issues—JAG School 15
Brainstorming Session 17

RESULTS 18
Rating the Proposed Solutions 18
Advisory Panel Meetings 20

ARMY ADVISORY PANEL RECOMMENDATIONS 21

REFERENCES 27

APPENDIX A: WORKSHOP ATTENDEES AND PRESENTERS A-1

LIST OF TABLES

Table 1: Articles 92 and 134 of the Uniform Code of Military Justice 16
Table 2: Training Compromise Solutions 17
Table 3: Matrix of Solutions by Factors 19

LIST OF FIGURES

Figure 1: A depiction of the PKI process....9
Figure 2: Fingerprints with identified minutia points....12
Figure 3: The radial mapping boundaries projected over an iris. 13
Figure 4: Cheating advisory statement 21
Figure 5: Student certification statement 22

TRAINING ON THE WEB: IDENTIFYING AND AUTHENTICATING LEARNERS

Introduction

Plans are in place to shift certain Army training from instructor-led classroom-centric delivery to a learner-centric model. Soldiers who receive training in the workplace, at their residences, or other sites outside the traditional classroom increasingly will rely on the use of the World Wide Web or military intranets. Much of this training will occur in the absence of an instructor, both physically and temporally. Reliance upon such asynchronous distributed learning systems increases the odds of various forms of training compromise, such as obtaining questions beforehand or enlisting a proxy for test taking in non-proctored, Web-based learning environments. The purpose of this study was to conduct a workshop to identify and prioritize potential remedies and safeguards to training compromise (i.e., cheating) in distributed learning scenarios.

How can it be determined whether the student online is the intended learner, particularly during individual testing? To begin to answer this question, remedies to compromise were sought from experts in various fields, such as commercial test centers, biometric measures (e.g., fingerprint identification and iris scanning), computer security, and other technical or commercial areas. Practical solutions were identified based on the information provided by the workshop presenters and through a brainstorming session of participants from industry, academia, and the government. These remedies were then prioritized based on deliberations and feedback from Army stakeholders, and are detailed in this study report.

Background

As a working definition for this study, training compromise, is considered to be the act of giving or receiving improper aid, such as: copying answers from another source; using notes or other references not permitted during examinations; knowingly allowing another to copy answers from an examination; collaborating with other individuals during testing, except as authorized; and having another individual act as a proxy. In the Army, the consequences of training compromise can be severe. For example, soldiers considered qualified to perform a task may not be, increasing the chances for "human error" during an operation. In terms of personal standards, cheating is considered misconduct within the military, as indicated by Articles 92 and 134 of the Uniform Code of Military Justice. These articles specifically indicate that both cheating and the failure to report knowledge of others cheating is considered misconduct. Cheating is also counter to Army values as described in FM (Field Manual) 22-100 Army Leadership. Specifically, the Army Value of Integrity states, "Do what's right – legally and morally."

It is important to state that compromise in Web-based training environments is not known currently to be a problem in the military. Of course, there is little critical training currently conducted online in the military. As it increases, so will opportunities for training compromise. The purpose of this study, then, was to explore solutions to potential problems, rather than to address an existing problem. It should also be noted that this study was conducted under the assumption that, in general, learners will "do right." In other words, this study was conducted

with the belief that the large majority of Army learners would not consider cheating as an option during training. Therefore, the focus of this report is on the benefits of creating an environment where the integrity of military skills is maintained, rather than how to catch those who cheat.

The Issue of Training Compromise

There is both anecdotal and empirical evidence that cheating occurs at the high school and college levels. There is further evidence to suggest that cheating among high school students is on the rise. Widespread use of the Web and the anonymity it can provide may be making cheating easier than it was in the past. For instance, a quick Web search on the key words "term papers" reveals nearly 150 sites selling or giving away book reports, term papers, and custom report writing services.

Several cheating scandals in military academies have been reported despite the honor codes in place at those institutions. For example, at the U.S. Naval Academy in 1992, 24 midshipmen were expelled, and 47 were punished after an investigation revealed their involvement with circulating advance copies of an electrical engineering exam (DeWan, 1994). During another electrical engineering course at West Point, 134 students resigned as a result of a cheating scandal reported in the Borman Commission Report (Borman, Johnson, Pye, Tate, Walker, Wilcox, Sussman, Kelly, Gray, Garrett, Holland, & Bacon, 1976). In this case, 823 second classmen were given take-home computerized examinations and, although they were given clear instructions to complete the tests independently, many students collaborated on the exam. These were not isolated incidents; other documented cheating scandals in the military service academies occurred at West Point in 1951 and in the Air Force Academy in 1965, 1967, and 1984 (DeWan, 1994).

In a recent study of 2,294 high school juniors, McCabe (2001) found student cheating in non-military academic settings to be prevalent. For example, 97 percent reported at least one questionable activity like copying homework. In addition, 86 percent of students admitted allowing another student to copy their homework, 76 percent reported getting answers or questions from someone who had taken a test, and 52 percent reported copying a few sentences from a Web site without referencing them. Although cheating is not a new phenomenon, the number of students who admit to some form of cheating has steadily increased over the past 30 years and may signal a shift in a cultural norm. McCabe (2001) suggests several ways to curtail cheating such as developing standards and expectations about cheating that are communicated to students and parents alike (such as an honor code), creating processes for handling violations, and requiring that students commit to adhering to the standards.

The Web provides students with the ability to research a wide range of topics without entering a library. The Web also presents students with ready access to hundreds of Web sites known as "paper mills," where students can trade papers or buy them for as little as $6.00 per page. McCabe (2001) found a greater incidence of plagiarism among high school students using written sources (34 percent) than Web sources (16 percent). The percentage of students reporting plagiarism of any kind was lower among college students in McCabe's study. However, anecdotally it seems that the number of students plagiarizing papers with the help of Web resources may be much higher. For example, a University of Virginia professor recently

found evidence of widespread plagiarism in a physics course (Argetsinger, 2001A). A total of 145 alleged cases of cheating were identified out of a class of approximately 500 students (Argetsinger, 2001A; Argetsinger, 2001B). Because of incidents such as this one, several universities now use anti-plagiarism services available on the Web in an effort to detect student plagiarism (Major, 2002).

McCabe's study is relevant to the military because high school students, as reflected in his survey, represent the primary pool of future enlisted service members. Similarly, the students accused of plagiarism at the University of Virginia are in a comparable peer group to a typical entry-level officer. Additionally, the increased use of the Web to conduct training in the military may increase the temptation to cheat. These points illustrate the need to develop remedies to potential compromise in Web environments prior to there being an actual problem.

The Distributed Learning Environment in the Army

The Army consists of three interrelated organizations with more than one million total members: the Regular Army, the Army Reserve, and the Army National Guard. Each is pursuing distributed learning in coordination with the others. The Regular Army is composed of approximately 480,000 full-time soldiers. Many are deployed overseas, but all need to acquire and maintain military skills and knowledge. The Army Reserve is composed of approximately 205,000 part-time soldiers who normally train 39 days per year. They are widely dispersed across the country, meeting and training for one weekend per month at a local reserve center and for two full-time weeks per year. The Army National Guard has more than 350,000 members who report primarily to the governors of their States and also meet 39 days per year, including two weeks of full time training.

The United States Army has a well-earned reputation as the premier training organization in the world. The Army has also long been a proponent of training innovations to foster improved effectiveness and efficiency that provide ready soldiers and units. Army doctrine considers training the linchpin of organizational performance as evidenced by the following quote from Army regulations:

> *Good training is the key to soldier morale, job satisfaction, confidence, pride, unit cohesion, esprit de corps, and combat effectiveness (AR 350-1, August 1981).*

Distance education has the potential to enhance Army organizational performance dramatically by increasing personnel qualifications in the unit and reducing the impact of skill decay by making training available when and where required. It is widely recognized as the method of choice for reducing costs while increasing flexibility, access and the number of learners reached. The potential for savings to the military services is tremendous, with the Army providing training to more than 335,000 students annually in residence (Office of the Program Manager, The Army Distance Learning Program, 1999). The ability to conduct pre-deployment, mission specific training under the tutelage of skilled subject matter experts can result in faster preparation for contingencies and can also level the playing field for the Reserve Component, and geographically remote organizations and learners by providing a standardized learning experience without walls or barriers (Freeman, Wisher, Curnow, & Morris, 1999).

The stated mission of the Army Distance Learning Program (TADLP) is *"To improve readiness by the delivery of standardized individual, collective, and self-development training to soldiers and units any time and any place through the application of multiple means and technologies."* To do this, the Army program must provide professional education and training on demand wherever soldiers are located. This includes permanent assignment locations and temporary locations in both developed and austere environments. It also includes soldier's work sites and, for selected events, their residences. Increasing the availability of training while maintaining standardization of learning outcomes is especially important for an organization with a worldwide mobile workforce of more than one million full- and part-time technicians and professionals (Army Public Affairs Office, 2001).

Types of training and education considered for distributed delivery include professional and technical skills, specific collective/team performance, and skills associated with fielding new and displaced equipment. Also required is training associated with adopting new business and operations practices (tactics and doctrine) and simulations. The Army's goal is to make 525 courses available via distributed learning by 2010, with from 30 to 45 courses adapted each year (Program Management Office, The Army Distance Learning Program, 2000).

The Army distributed learning environment is enabled by the TADLP, which primarily supports Regular Army and Army Reserve soldiers, and the Distributed Training Technology Program (DTTP) of the Army National Guard. Both programs are intended to provide access to technology and courseware. Currently the programs provide more than 800 high bandwidth, interconnected classrooms or digital training facilities (DTF). These DTFs are located throughout the United States and the world with the goal of providing a facility within 50 miles of 95 percent of potential students' duty station (Program Management Office, The Army Distance Learning Program, 2000). The typical high bandwidth DTFs provide seating for from 12 to 16 students for Reserve Component locations and Regular Army locations respectively. As of September 2001, more than 80 percent of soldiers are within 50 miles of one of the 431 completed facilities, achieved primarily through placing priority on high population density locations and integrating DTTP classrooms (Abell, 2000). Interestingly, in a recent survey of military personnel, 38 percent of enlisted soldiers and 49 percent of officers reported being extremely confident that they could complete a distributed learning course.

For the reserve component, distributed learning may be on the verge of becoming far more widespread. The National Defense Authorization Act for fiscal year 2002 included language for reservists to be compensated upon successful completion of a course of instruction undertaken by electronic-based distributed learning methodologies to accomplish training requirements related to unit readiness or mobilization. Furthermore, the compensation may be paid whether or not the course of instruction is conducted in the physical presence of an instructor. This means, for example, that reservists will now be able to take distributed learning courses from home and be compensated for their online time.

Implications/Impact of Training Compromise

Training compromise and the prevention of compromise in DL training environments have many implications, from the level of confidence that individuals have in the quality of DL programs to issues of military readiness. Distributed learning is sometimes thought of as less rigorous than regular classroom training, although the empirical research suggests that DL is at least as effective for learning achievement. Just as in the traditional classroom, it is important that DL training programs have mechanisms to ensure that training and testing procedures are not being compromised. Having solutions to compromise in place for DL training may improve perceptions about the rigor of DL courses. More importantly, it can provide a stronger guarantee that a soldier has been trained and can perform to standard.

Another reason to ensure course integrity is that when students cannot or do not cheat the playing field is leveled. In other words, it is fairer to students who never intend to cheat to have measures in place to ensure that others do not cheat. This way, all students are assessed on their actual performance and test scores represent actual knowledge for all students.

Different solutions to training compromise may be deemed appropriate depending on the criticality of the course. For example, a course that does not have a test administered at the end may not require implementing measures to prevent training compromise. On the other hand, a course that is critical, such as MOS training or courses that result in skill certification, may require a much more stringent level of control. This is especially true when completed training is used as a discriminator for highly competitive actions such as promotion or special assignment.

A final factor in controlling Web-based training compromise is that many Army courses are available to students outside the U. S. military such as the international students attending Army schools. This has two effects. First, it means that not all students are bound by U. S. military rules, regulations and ethics. Second, solutions to compromise need to be reasonable for civilians as well as military personnel. For example, a course should not be designed to require equipment or facilities that are accessible to only one group (i.e., if testing centers are used, they should be accessible to both military and non-military personnel).

Workshop Summary

The workshop entitled "Training on the Web: Identifying, Authenticating, and Monitoring Learners" was conducted on 14 November 2001. Workshop topics included an overview of the Army's DL program, an overview of the National Guard Bureau's DL initiatives, training design considerations, test security practices, public key infrastructure, biometric solutions, the future of biometrics, and a discussion of legal issues related to training compromise. Based on the presentations, all of the attendees took part in a brainstorming session that generated solutions to training compromise. When the Army advisory panel met to discuss a final set of recommendations, the discussion was directly related to the presentations.

A total of 31 individuals from industry, academia, and government attended the workshop. A list of the attendees and presenters appears in Appendix A. An overview of the

Army and National Guard Bureau initiatives was provided in the background section. The remaining presentations are summarized below. Following the summaries of the presentations, recommendations based on the presentations are discussed.

Training Design Considerations for Identifying, Authenticating and Monitoring Learners

Summary of the presentation by Dr. Mike Freeman, Director, Advanced Training Concepts, Computer Science Corporation, Atlanta, GA

It may be possible to include "gates " in the design of Web-based training that require learner authentication on a periodic basis. This timely authentication should not interfere with the flow of instruction, as a random check of learner authenticity might. Here, the focus is on the activities related directly to the learning process. A brief review of the type of interactions that occur during Web-based instruction is presented along with some considerations for where to place the gates.

Learning Interactions. Training design boils down to providing the right interactions at the right time. Wagner (1997) defines an interaction as reciprocal events requiring two objects (e.g., student and instructor) and two actions (e.g., an e-mail and a reply). Such interactions foster behaviors in which individuals and groups influence one another. Wagner also identifies 13 types of interactions that can occur in distributed learning, such as interactions to increase participation, to develop communication, or to receive feedback. The hallmark of interactions is that they must result in the transfer of knowledge or a change in intrinsic motivation.

Natural Points. Interactions provided for learning can also act as natural points for identification, authentication and monitoring of participants within the conversational framework of the learning activities. Instructional design can provide for validation actions at these points without unduly interrupting the flow or distracting from the intent of the learning activities.

Social Interactions. Providing social interactions in the learning environment can create a sense of community and personal involvement while allowing positive identification of learners. Creating opportunities to acquaint learners with each other, the instructor, and subject matter experts increases the situational awareness of each participant and decreases the feelings of isolation often associated with distributed delivery. Some examples are the inclusion of personal essays, chat rooms, social greeting time and instructor office hours in the virtual learning environment.

Continuous Assessment. Distributed learning can be an outstanding enabler of continuous learning because of the ability to participate while widely dispersed in time and geographic location. Learning can be accomplished as needed rather than in an episodic, higher directed fashion. However, in order to truly embrace continuous learning, the design must include the associated continuous assessment required to determine what is required and when. This continuous assessment interaction provides many more opportunities to gather information about the learner and increase the level of confidence that the learner has, in fact, grasped the required concepts.

Progressive, Comprehensive Learning Design. Progressive, comprehensive learning design starts with very basic concepts and expands them in both depth and breadth. This provides the opportunity to build on each learning interaction while increasing the learner's mastery. It also reduces the opportunity of a proxy participating for a student in order to pass a specific part of the training since a change in performance from earlier or later in the course would be highlighted.

Higher-Order Synthesis. Higher-order synthesis of knowledge results in learners understanding principles, concepts, and performance required in the context of their own job requirements. This requires application of basic concepts to novel situations in order to solve performance-based problems. The design of learning activities to produce and measure the higher-order synthesis lessens the opportunity for substituting answers because of the personal nature of the resulting learner performance.

Conclusion. Instructional strategies provide many opportunities to improve the identification, authentication, and monitoring of participants within the conversational framework of the learning activities without unduly interrupting the flow or distracting from the intent of the course. This can be accomplished by several methods, including the provision of validation actions, social interactions, continuous assessment, progressive/comprehensive development, and requiring higher-order synthesis.

Test Security Practices and Issues

Summary of the presentation by Mr. Ray Nicosia, Director of Test Security, Educational Testing Service (ETS), Princeton, NJ

Tests have been compromised for thousands of years, and will continue to be compromised. The first known standardized test was administered in China in 1000 B.C.; the test was a civil service exam. This is also where the first historical evidence of cheating can be found. More recently, according to one study, 97 percent of high school students have cheated on a test or copied homework from another student (McCabe, 2001). The purpose of this presentation was to discuss the current state of testing compromise as experienced by ETS, and to describe some of the solutions to testing compromise ETS has implemented. ETS administers 11 million tests such as the SAT or GRE in 180 countries in 25,000 test centers annually.

Cheating can be categorized in three basic areas: copying/communication, impersonations (proxy), and pre-knowledge. Copying or communicating occurs when a test taker looks at another test taker's answers, or when one test taker actively provides answers to another. Impersonation takes place through various means such as fake identification, switching answer sheets, or switching computers in computer-based testing (CBT) environments. Finally, pre-knowledge occurs when a test taker receives answers or questions to a test in advance.

In an effort to prevent cheating, three steps to test security have been suggested: prevention, detection, and remediation. For the first step, the following prevention methods were suggested:

- Have live proctors monitor exams.
- Have test takers sign an agreement during test registration stating that they will follow test security procedures (this also clarifies legal issues that may arise if a person is identified as cheating).
- Check identification.
- Provide lockers so nothing goes into the test center except the test taker.
- Count and secure test materials (for paper and pencil tests).
- Secure equipment (for CBT).
- Train staff of test administrators to follow prevention procedures.
- Seat test takers far enough apart (i.e., four feet), so that they can not see each other's papers.
- Maintain seating charts of test takers at each site (this can be useful for investigations).
- Provide a hotline to report cheating.
- Collect a handwriting sample and signed statement at the end of testing (this can be used later for verification if necessary).
- In CBT environments, record everything that goes on.
- Use computer adaptive testing in CBT environments.
- Use multiple test forms in paper and pencil-based test environments.
- Implement biometric measures such as iris scanning in CBT environments.

The second step for test security is detection. This involves such methods as monitoring test site scores to detect large differences from other sites or large retest differences for the same individual, monitoring the sites for missing test books, and receiving external inquiries such as calls from schools. One important component of the detection phase is maintaining detailed records of test scores and reported problems at each test site. When potential cheating is detected, further investigation is usually necessary.

Finally, remediation is the process of addressing cheating that has been detected and rectifying the situation. For this process, ETS has instituted a process wherein several three-person panels investigate questionable test scores. When a test score is in question, there are several available options. First, a decision can be put on hold in order to collect additional information. Then, a test taker can be retested or have their scores canceled.

In conclusion, there are several factors that can help prevent cheating. First, establish a policy about cheating and how it will be handled. Second, convey that policy to test takers and ask them to agree to the policy in writing. Third, keep materials and equipment secure. Fourth, train proctors and appoint a person in charge of security. Finally, document problems in a centralized database.

Public Key Infrastructure

Summary of the presentation by Dr. David Pass, Career Management Account Team Leader, U.S. Department of Labor, Washington, DC

The goal of this presentation was to discuss Public Key Infrastructure (PKI) as a system to identify computer users and authenticate secure transmissions of information across the Web.

PKI is a method of encoding and decoding messages sent over a computer network. Reliable methods for sending messages are required to assure the authenticity of a message and that the message is received fully intact only by authorized individuals.

PKI is one of many methods for encrypting messages sent over a network. In its most basic form, encryption includes using a single coding key, or a shared secret. When sending a message, a sender uses this single key to encode a message, and the receiver uses the same key to decode the message. One problem with the single key system is that a computer hacker who steals the key can decode the message, compromising its security (Schneier, 2000).

A more secure procedure involves "asymmetric encryption," where two different keys are used, one by the sender and another by the receiver. A public/private key method is a form of asymmetric encryption that can be used to ensure the security of a message. The public and private keys are two complementary codes, both of which are required for the process. What is encoded by one key can only be decoded by the complementary key, and vice versa. The private key is accessible only to a specific user, while the corresponding public key is available to anyone communicating with the specific user. The process of sending an encrypted message using PKI can be done either of two ways. First, a message (e.g., completed exam) is encoded with a private key that can only be read by a person with the corresponding public key (see Figure 1). This assures non-repudiation, knowing for sure that the appropriate person sent the message, since only the sender would have the private key. The inverse process is also possible; a person can encode a message with a public key, which can only be opened by a person using the corresponding private key. This assures that only the appropriate person receives the message.

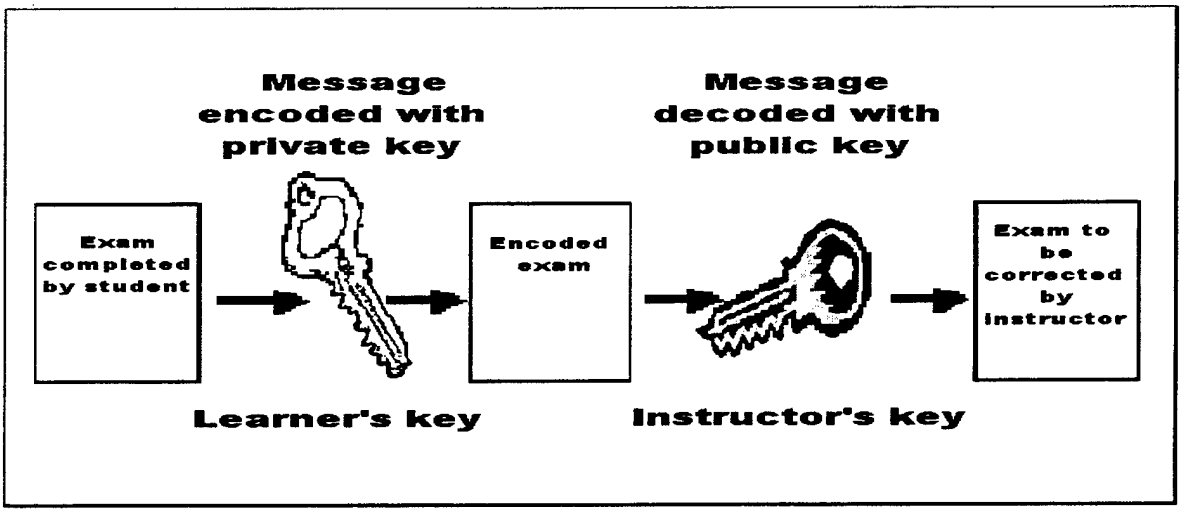

Figure 1. A depiction of the PKI process

One requirement of PKI is the use of a trusted third party called a certifying authority. The certifying authority sets up complementary public and private keys for users who must prove their identity. Only the specific user would hold the private key, and the corresponding public key would be made available to anyone authorized to receive that user's encrypted message.

Each user is assigned a unique pair of encryption keys. Besides being a repository of public keys, the certifying authority would also maintain a revocation list of compromised encryption keys.

In addition to the basic PKI, there are additional methods that provide increased security by requiring authentication of a network, a workstation, a user, or any combination of the above. One is S/MIME encryption, a standard for encrypting email. This involves encrypting a key and sending the encrypted key along a separate channel to the same person receiving an encrypted message. On the receiving end, the encrypted key is then decrypted and the key is used to decrypt the message. A second method is to use a HASH function, which is an algorithm to condense a file of any length to a HASH value of a specific length. For example, HASH values for a 1-page document and a 10-page document would be the same length but the contents would differ. The algorithm is unidirectional, in that the original documents cannot be derived from the HASH values. Then the encrypted message and the encrypted HASH value are sent along separate channels to the receiver. After both are decrypted, the sent HASH value must match a HASH value based on the sent message. If they match, the message has not been altered en route (Schneier, 2000).

The Career Management Account pilot program, an initiative of the U. S. Department of Labor, is currently using the PKI method to authenticate learners who wish to create an account for the purpose of storing and managing all of their lifelong learning and career information. The Career Management Account program is part of America's Career Kit, which was developed to assist people in procuring a job of their choice. In a Career Management Account, all of a person's work experience, training, and other related information is stored so the information can be easily shared with potential employers. This account is maintained and updated as needed. To access America's Career Kit visit http://www.eworkforce.org/careerkit/.

The use of PKI and other security methods allows for the creation of secure Career Management Accounts, a safe place to record lifelong learning and career development. The use of PKI also provides for a secure environment were personal information and course material is exchanged only between appropriate individuals. In the realm of distributed learning, the transmission of information must be secure. The use of encryption is one means to assure that tests, answer sheets, and training materials are sent and received only by the authorized individuals, and that the information is not accessed or modified along the way. This insures that the learning environment is not compromised.

Overview of Defense Biometrics Management Organization

Summary of the presentation by LTC Robert Bollig and Mr. Pat Miller, Department of Defense Biometrics Management Office, Falls Church, VA

Biometrics is the process of identifying people based on their physical/anatomical, personal, and/or behavioral characteristics. A few of the methods used today include fingerprints, iris patterns, signature production, voice characteristics, hand geometry, and face composition. These characteristics of a person are distinct, and can be converted into a digitized form through the use of computational algorithms. Biometrics are currently used by the U.S. Army to authenticate the identity of individuals.

The Department of Defense Biometrics Management Office, located in Falls Church, VA, is managed by the U.S. Army. For additional information, visit http://www.c3i.osd.mil/biometrics/. The Biometrics Management Office develops Department of Defense (DoD) biometric policy and coordinates DoD biometric services. As part of the Biometrics Management Office, the DoD Biometrics Fusion Center in Bridgeport, WV, conducts studies in the area of biometrics. The center tests commercial, off-the-shelf biometric products from more than 300 companies worldwide. Based on the tests, the center produces a list of biometric products that meet the platform requirements and usability qualifications of the DoD.

There are four steps in the process of using biometrics for identification: capture, process, enroll, verify. The capture process is where the device obtains the biometric data (e.g., fingerprint, iris image, handwriting sample). The data are then processed and encoded to an easily storable form. This encoded data can also be encrypted to provide a higher level of security. The enrolling procedure occurs the first time an individual's biometric data are obtained and stored in a local file. The verification procedure occurs when an individual's biometric data are compared to stored data to determine if a match has occurred. Biometrics offers assurance that a person is who he or she claims to be. In distributed learning, this is important because the instructor and student are not co-located.

There are some concerns with biometrics. For example, the technologies are not completely foolproof. There are two types of errors that can be made. The first is a false acceptance, when the biometric data of a confederate is accepted. The second is a false rejection, when the correct person is rejected as not matching his/her biometric profile. To lessen the chance for these errors, biometrics can be used in conjunction with a password, or more than one biometric can be used at a time to identify a person. Another concern is the security of the repository.

Below, the most common and/or promising technologies (fingerprints, iris patterns, facial composition, and handwriting) are discussed in detail. There are, however, some other forms of biometrics, such as retinal images, hand geometry, vein pattern on the back of the hand, and ear shape. The technology for these forms of biometrics either are still emerging and require further development to determine the feasibility of widespread use within the DoD, or will not be used due to the invasive nature of the measure. Presently, in some departments within DoD, fingerprint identification is being used to access computers and networks, while in other areas iris scanning and hand geometry are being used to limit building or vessel access. To secure a computer, a fingerprint system can cost approximately $100 and an iris scanning system approximately $250. When these systems are incorporated into a door access and alarm system, the cost can be as much as $10,000. Because this technology is still developing, prices are expected to fall in the future.

Fingerprint. Of the various biometric technologies, fingerprint scanning is the most mature method based on cost, reliability, and usability. A fingerprint is made up of curved ridges. These ridges have identifiable minutia points (e.g., end of a ridge, joining of two ridges). The set of minutia points on a fingerprint are unique to each individual.

In fingerprint identification, between 15 and 20 distinct minutia points in a single fingerprint are identified, and then the distance and angle between the key points are measured. The fingerprint is thereby encoded as vector measurements between these points. Many fingerprint-scanning devices are also able to determine if the finger is from a live person. Figure 2 depicts a constellation or polygon, showing distinct locations (minutia points) that are highly likely to be uniquely arranged for any individual fingerprint. The actual fingerprint is not stored but rather the polygon that connects the distinct characteristics of a fingerprint; therefore, the fingerprint image cannot be duplicated from the encoded set of vector measurements.

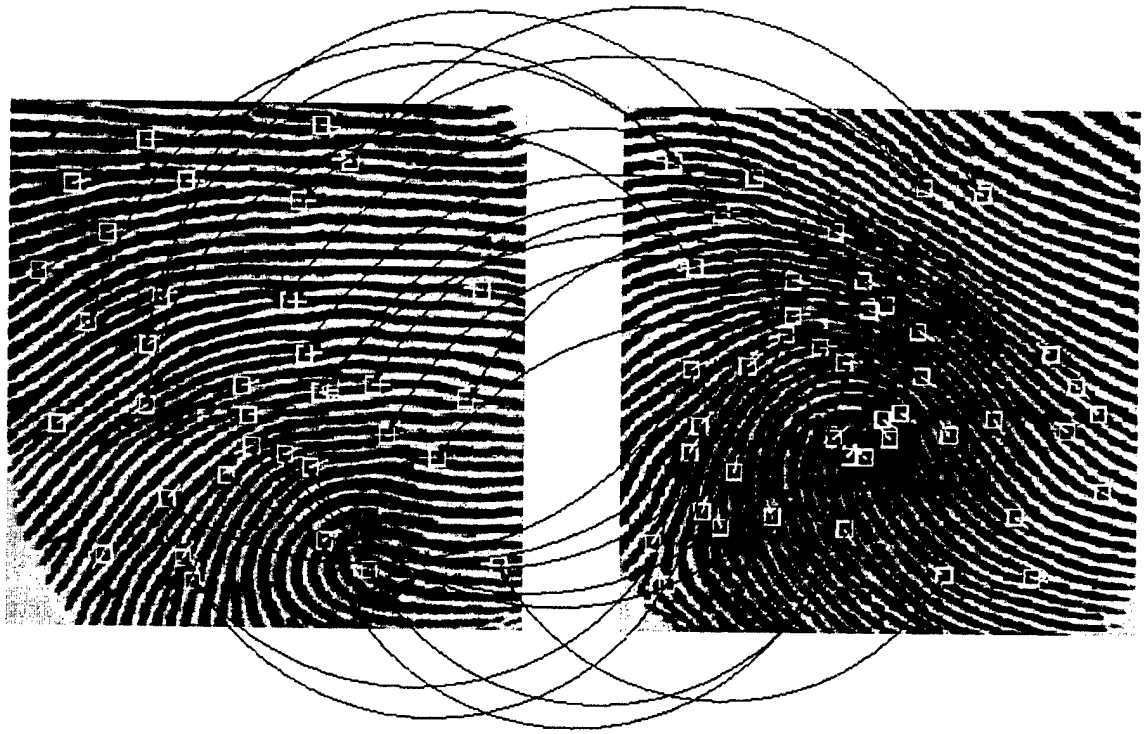

Figure 2. Fingerprints from the same finger, but taken at different angles. The lines link corresponding minutia points between the fingerprints

Iris. Scanning a person's iris (the colored part of the eye surrounding the pupil) is a method that is promising, and may be a preferred method in the future. In this procedure, the pattern of radial marks and their relative position in the iris are identified, as shown in Figure 3. Identification of these features remains consistent over a person's life. In addition, the iris pattern remains identifiable, even though the size of the iris changes as the pupil changes due to lighting. Scanning of the iris can be conducted through contact lenses, eyeglasses, sunglasses, and even gas masks.

Advantages of iris scanning are ease of use, accuracy, and the speed to take a repeated measure. For a person to be scanned, they need to be within approximately two feet of the camera that captures the iris image. It then takes a fraction of a second for the iris to be located,

and an additional fraction of a second for the boundary of the iris and the internal features to be mapped and converted to a 512-byte code. The use of a 512-byte code offers a high level of accuracy. Iris scanning technology is continually improving, and is, therefore, a very promising method of biometric identification.

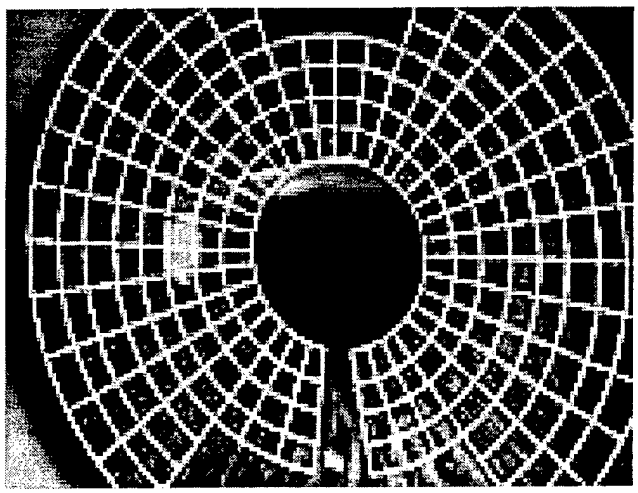

Figure 3. The radial mapping boundaries projected over an iris. The features within each segment of the radial map are recorded and encoded.

Face composition. The facial composition method identifies points on the face (i.e., eyes, nose, mouth) and then measures the relative distance between these key points. The relative distance and angles between these facial components can be converted into an alphanumeric code in a similar manner as fingerprints and iris patterns. These codes can be easily stored in a repository or compared to previously stored codes.

One advantage of facial composition is that it can be completed with the use of standard computer top video cameras, so there is little extra cost. A disadvantage is the current level of accuracy of the available systems. While the shape of faces is relatively stable, the aging process does effect facial composition, and the use of disguises can modify a person's appearance. Additional advancements are needed to make this a viable option for broad use by the DoD.

Handwriting. A person's handwritten signature has been used as a traditional means of identification. With current technology, however, handwriting analysis involves more than just the visual shape of the signature. In addition to the shape of the signature, the speed and pressure used to create the signature are measured. The inclusion of speed and pressure make this biometric much more difficult to forge than just the visual aspects of a signature.

To capture the signature, a digital tablet with a stylus is used to write the signature. With this tablet, speed, pressure, and timing are captured; not just the shape of the signature. All of these features are compared, making forgery very difficult and increasing security. For example, tracing another person's signature would be rejected by this technology since the speed and pressure of certain elements of the signature would not match the enrolled target signature. Digital tablets are not that expensive, and come as options on many laptops.

Future Trends in Biometric Measures

Summary of the presentation by Dr. Bojan Cukic, Assistant Professor, West Virginia University, Morgantown, WV

The Center for Identification Technology Research is a National Science Foundation (NSF) funded consortium of universities, industry, and government agencies focusing on all aspects of biometric technology. Due to the broad nature of the issue and the fact that no single university or organization had the capabilities to adequately address the issue alone, a consortium was developed. The center is closely involved with the DoD Biometrics Management Office and their Biometrics Fusion Center. The consortium's Web site is www.csee.wvu.edu/citer.

The center's mission is to conduct research with the goal of improving biometric technology and the ways in which the technology is used. For example, are the current algorithms for codification and identification the best, or can they be improved? Another goal of the center is to empirically validate claims made in biometrics. For example, are there really no two fingerprints that are identical? In addition, the center explores the use of new forms of biometric measures such as DNA, heartbeat pattern, and ear prints. Some of the current lines of research the center is working on are:

1) Liveness—the detection that the captured measure is coming from a live being. Many current devices are easy to spoof. For example, some fingerprint devices can be spoofed with clay models of a person's finger. Identifying liveness will decrease the possibility that an inanimate model or a disembodied body part is used to fool the sensor. Some of the possible solutions are simultaneously measuring skin resistance, pulse, or temperature while taking a biometric reading. For example, one non-invasive, software based method takes about 5 second to determine if a fingerprint has perspiration producing pores.

2) Multimodal systems—the use of more than one biometric to increase confidence with the result of the identification procedure. For example, using fingerprints, face recognition, and palm geometry in combination to authenticate a person's identity. The use of multiple biometrics increases the reliability of the verification process. There are still some unanswered questions, such as, what level of confidence is needed for each individual biometric measure to make the combined measure efficient. If two out of three measures are confident of a person's identity, is that acceptable?

3) Error estimation—the use of statistical analysis to determine appropriate levels of variability with each form of biometrics. In biometrics, a small level of variability is expected across measurements. This line of research is trying to determine acceptable levels of variation for different biometrics. Since slight variation from measure to measure is expected, an additional research question is how to deal with exact matches. An exact match might not be from the appropriate person, but instead from a model or a stolen measurement from a repository; therefore, should it be rejected and the person required to submit to a repeated measurement?

4) Template aging—researching the effects of aging on a person's biometric measures. How does the aging process affect biometric data? What are the effects of gaining 50 pounds on a person's facial configuration? For example, fingerprints do age and change slightly over time. This line of research will also explore the effects of lifestyle changes like gaining or losing weight, accidents, or cosmetic surgery.

5) Large scale biometric data—there are a variety of issues regarding the storage of large-scale biometric data. How should large repositories of biometric data be developed? Currently, there is no established policy. One of the concerns is the need for system-level security and network security if there is a central repository that will be used for matching biometric data. If someone was able to hack into a repository, Would they be able to pretend to be anyone they want to be? Another issue of concern is system assurance measures. What happens if a network goes down and the repository cannot be accessed?

While the five issues above are important to the effective use of biometrics as a form of identification verification, additional issues are sure to emerge. The center will continue exploring the use of biometrics and how the process of identification verification can be improved.

Legal Issues – JAG School

Summary of the presentation by SFC J. Arthur Wilde, Judge Advocate General School, Charlottesville, VA

The Judge Advocate General's School offers legal training for the Judge Advocate General's Corp, U.S. Army Personnel, and attorneys employed by the Federal government. The school also offers resources to the military legal community and develops doctrine for legal support of the Army. Information regarding the Judge Advocate General's Corp is accessible at (http://www.jagcnet.army.mil).

In the military, determining the consequences of compromising a distributed-learning environment is a function of command. A student is expected to follow the rules of a training situation, and when those rules are compromised, misconduct occurs. Cheating is immoral, unethical, and can be illegal; therefore, it should be considered misconduct. Because, "cheating" is misconduct, it can be treated as any other violation. When an act of cheating is revealed, commanding officers have wide latitude in investigating and determining guilt and/or punishment.

It is important that appropriate and inappropriate behavior is defined during a distributed-learning environment so clear limits are set. For example, in some learning environments, it may be acceptable to use a book while taking a test or to collaborate with other students when completing a project, while in other situations it may not. Defining what is and is not allowed informs the soldiers what is expected of them to include the ramifications for such behavior. This informs soldiers of the consequences if they choose not to follow the rules.

Table 1. Articles 92 and 134 of the Uniform Code of Military Justice

ART. 92. FAILURE TO OBEY ORDER OR REGULATION Any person subject to this chapter who- (1) Violates or fails to obey any lawful general order or regulation; (2) Having knowledge of any other lawful order issued by any member of the armed forces, which it is his duty to obey, fails to obey the order; or (3) Is derelict in the performance of his duties; shall be punished as a court-martial may direct.
ART. 134. GENERAL ARTICLE Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.

Articles 92 and 134 of the Uniform Code of Military Justice (UCMJ) indicate that cheating is misconduct, as shown in Table 1. In addition to cheating as an act of misconduct, soldiers who know about cheating but do not act accordingly are subject to penalties. Any student who is aware of other students who are cheating is bound to report the misconduct. Article 78 of the UCMJ states "any person subject to this chapter who, knowing that an offense punishable by this chapter has been committed, receives, comforts, or assists the offender in order to hinder or prevent his apprehension, trial, or punishment shall be punished as a court-martial may direct."

The process of dealing with a soldier who may have cheated starts with an allegation put forth against the soldier in question. If the commander sees fit, an investigation will be initiated. The investigation may start out informally, but at some point the commander may decide that, based on preliminary evidence, a formal investigation is required. The basic purpose of any investigation is to gather the facts with regard to a particular incident.

The investigating officer should conduct a proper and meticulous investigation. While investigating, the servicing judge advocate should be consulted regularly and Army Regulation (AR) 15-6 should be applied. When the investigation has concluded, a report of the findings should be completed, followed by recommendations. The findings lay out all of the evidence in a clear and meaningful manner. AR 15-6 states that findings "must be supported by a greater weight of evidence than supports a contrary conclusion." The recommendations of "next steps" must be based on the findings of the investigations.

After an investigation is conducted, proceedings may commence. There are three levels of proceedings: administrative, non-judicial and judicial. One aspect that differentiates administrative proceedings from non-judicial and judicial proceedings is the level of evidence needed for guilt. In administrative proceedings, the level needed is "a preponderance of guilt," while in both non-judicial and judicial proceedings the level is "beyond a reasonable doubt."

If a soldier is found guilty or admits guilt, the disposition of consequences is the final part of the process. Based on the severity of the misconduct and the level of evidence, the consequences of guilt can vary. After administrative proceedings, the options for disposition are at the discretion of the commander and include written reprimand, convene an academic board, terminate a soldier from the course, and/or adverse academic efficiency report. For non-judicial and judicial proceedings, the options include the above and more severe punishments. It should be noted that the UCMJ does not apply to Department of Army Civilians or others who may be taking Army Distributed Learning courses.

Brainstorming Session

At the conclusion of the presentations, the attendees participated in a brainstorming session. The purpose of this session was to generate a list of potential solutions to training compromise in online environments based on the presentations, discussions, and new insights. Ideas were generated along the lines of four topic areas: policies, biometrics, training design, and PKI. Table 2 shows the complete list of 40 ideas that were generated. At the conclusion of the brainstorming session, workshop organizers asked each participant to record what he or she considered to be the top five solutions to training compromise. Table 2 also shows the number of times a particular solution appeared on a participant's top 5 list. The most commonly chosen solutions were to have process control policies, use multimodal rather than single mode biometric measures, create real job conditions for assessments, and choose certification tasks carefully.

Table 2. Training Compromise Solutions

Policies	**# of times on a top 5 list**
Treat as process control	7
Choose certification tasks carefully (i.e., high stakes, types of courses)	6
Identity over privacy	5
Third party proctors	5
Is cheating a problem?	5
Live proctor	3
Assume people will "do right"	2
Assess learning process	2
Review historical data (of training compromise)	1
Advertise benefits (of not cheating)	1
What do we do if we catch cheaters?	1
Supervisor validation of performance	0
Affirmative obligation (tattle)	0
DL policy can influence residential courses	0
Biometrics	**# of times on a top 5 list**
Multimodal vs. single	7
Reauthentication (periodic)	5
Monitor surrounding environment (audiovisual)	4
Combination of technology should be based on situation	4
Focus on physical identifiers	2

Fingerprint seems to be the most mature technology	1
Ability of technology is questionable	0
Training Design	
Real job testing conditions (authentic assessments)	7
Adaptive test item generation	5
Random test item generation	4
Longitudinal testing (pre-, post-, later)	3
Focus on learning outcome	3
First make sure training works	3
Biographical inserts	3
Portfolio	2
More simulation vs. knowledge based	2
Teams/collaboration	1
KM=where is learner (context)	1
Live instrumentation	1
How to control the conditions?	1
Intelligent agent	1
Third order effects of software/automatic grading	1
Virtual private network	0
Personalized learning style assessment system	0
Technology should not degrade learning	0
PKI/DIG	
Modalities—cheap and easy	5
Positive, overt commitment (policy too)	4

Results

Rating the Proposed Solutions

There are positive and negative aspects to each of the proposed solutions. For example, among the biometric solutions, fingerprint identification is fairly inexpensive, while iris scanning is more costly. To capture the positive and negative aspects of the various solutions, each was rated by the authors on several factors. These factors include the cost of acquisition and implementation (including maintenance), the feasibility of implementation, the ease of use, the level of control, the reliability of the solution, and its accuracy. Ratings for the factors were developed through research and input from workshop presenters and other subject matter experts. Table 3 shows the ratings of each solution by rating factor. In this matrix, higher numbers represent positive attributes. A rating of 5 is considered most acceptable (e.g., low cost, easy to use, and reliable) and a rating of 1 is considered least acceptable (e.g., high cost, difficult to use, and unreliable).

Table 3. Matrix of Solutions by Factors

A rating of "1" for cost indicates high cost, while a rating of "5" indicates low cost, as low costs are generally considered desirable. Likewise, a rating of "1" for ease of use indicates the solution would not be easy to use, while a rating of "5" indicates that the solution would be quite easy to use. **Solution**	**Factors**				
	Cost	Feasibility of Implementation	Ease of Use	Reliability	Accuracy
Multimodal vs. single biometrics	3	4	4	4	5
Fingerprint	4	5	5	4	5
Iris scanning	2	3	3	4	5
Face recognition	4	3	4	4	4
Handwriting analysis	3	4	3	3	3
Biometric reauthentication (periodic)	5	5	5	5	5
Treat as process control	3	3	4	N/A	N/A
Choose certification tasks carefully (i.e., high stakes, types of courses)	4	5	N/A	N/A	N/A
Adaptive test item generation	1	3	3	4	5
Real job testing conditions (authentic assessments)	2	2	2	3	4
Determine if cheating is a problem	4	3	N/A	N/A	N/A
Use third party proctors	1	2	4	4	4
Prioritize identity over privacy	4	3	N/A	N/A	N/A
PKI/DIG	4	4	4	5	5

The solutions presented here could be implemented in many ways. For example, one solution is the use of multimodal biometric measures. This could be achieved by using fingerprint identification and face recognition technology. Both fingerprint and face recognition technologies are relatively inexpensive and can be easily installed on a soldier's computer and monitored by a course administrator. When multimodal biometrics are used in combination to provide verification of a students presence, the "false positive" rate is decreased, and chances of impersonation are lower. The use of multimodal rather than single-mode biometric measures can provide a greater level of confidence that the student is in fact present. It also may ameliorate problems with one mode such as if a student suffers a burn to the hands and is no longer able to use fingerprint identification, then face recognition could be used instead. In cases where civilians may be taking a course, a choice of biometric measures would help to provide access to the disabled in compliance with Section 508 of the Rehabilitation Act of 1998.

In addition to verifying a student's presence, face recognition technology requires a camera. It may be possible to use the camera to take a "snapshot" of the student. This snapshot could provide evidence on whether the student was alone while taking a test. This is, of course,

as with any prevention method, not foolproof, since a second person could simply stand out of the camera's view. However, the simple presence of the camera may create a heightened sense of being in a proctored environment. Finally, biometric measures can be implemented in such a way that students could be asked to re-authenticate periodically. This would prevent students from logging in and then walking away while a proxy completed course materials or tests.

Another method of identifying students during training and testing is to ask students biographical questions to which only they are likely to know the answers. In an online testing environment, this could be implemented through the use of a learning management system (LMS). Demographic information that is known or collected by the course administrator can be used as the basis of questions that are periodically inserted into the course (at a natural break in the content), and incorrectly answered questions could be followed with additional questions. If additional questions were answered incorrectly, the student could be logged out of the training event or testing module pending further verification. While this does not ensure there is no one else sitting with them, it may ensure that they are at least present.

One of the recommendations for testing is to use randomized test items. Using a bank of test items or, at minimum, one set of randomly ordered test items can help to eliminate testing compromise. This is not an issue unique to DL environments but, in this case, an electronic environment actually provides a better venue for randomizing test items than a paper-based environment. Having a bank of test items from which a subset can be drawn randomly is particularly important when students are given more than one opportunity to take a test. Finally, during online testing, using a "no print" option would prevent test items from being printed out and possibly circulated to other students.

Advisory Panel Meetings

Meeting 1. The day following the workshop, a panel of individuals called the "Army Advisory Panel" met to initiate discussions about the final recommendations for this study. The panel consisted of stakeholders in military distributed learning. The advisory panel agreed that the criticality of training should be taken into consideration when determining solutions to training compromise. In addition, the following solutions were discussed as possibilities for the final recommendations:

1. Use third party proctoring. One issue that was discussed regarding third party proctoring was how this may conflict with the "anytime, anywhere" training goal of Army distributed learning programs.
2. Use learning management tracking systems to collect metrics and to obtain affirmative obligations in computer-based environments.
3. Design tests using randomized items.
4. For computer-based testing, use "no print/capture" options, limit the number of times a person can attempt a test, implement a "test mode" on the computer, and/or track where the test taker has been online.
5. Implement PKI so only specific students can access courseware and tests.
6. Periodically verify the test taker through biometric or biographical measures.
7. When using biometrics, implement multimodal measures.

Meeting 2. In February 2002, the advisory panel met again to determine the final recommendations. The discussion focused on identifying pros and cons of each of the proposed solutions from the first meeting. Among the potential solutions a theme emerged that each recommendation would require careful thought before implementation to avoid interference with the learning process. The final recommendations, along with some of the pros and cons for each, are presented in the following section.

Army Advisory Panel Recommendations

The advisory panel concluded with several general recommendations, detailed here in no particular order, but accompanied by some of the pros and cons associated with each. The recommendations are meant to serve as broad guidelines, rather than specific instructions for implementation. For each one, practitioners must carefully consider its necessity and practicality.

Affirmative Obligations

The first recommendation calls for using affirmative obligations that reinforce a definition of misconduct. This involves presenting a statement to students that details what is considered inappropriate and appropriate behavior, and requiring the student to sign a pledge that they will not cheat. The Army currently uses a two-step affirmative obligation for some online testing. First, prior to testing, the pop-up window pictured in Figure 4 requires students to "click" OK to an advisory about cheating before continuing with the test. At the completion of the test, students must agree to a statement that they have not cheated in order to submit their test answers. That statement appears in Figure 5.

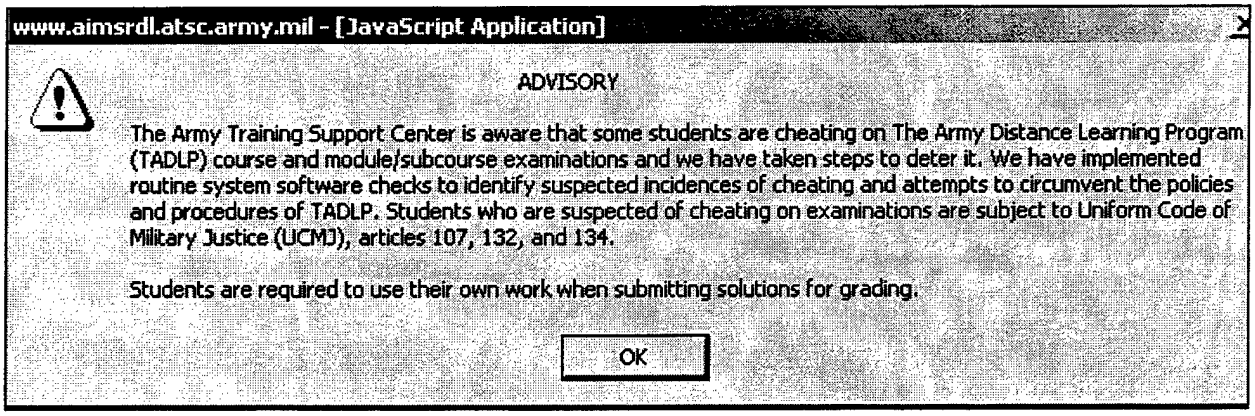

Figure 4. Cheating advisory statement

Using an affirmative obligation ensures that students understand proper conduct for training. This solution can also be implemented with little cost and effort. One possible disadvantage to the affirmative obligations is that, as training courses are increasingly

implementing collaborative techniques, there is a potential for these statements to be confusing to students. However, the statements should be tailored to a particular training environment.

In accordance with DA Pam 350-59, paragraph 1-30, I certify that the answers I submit are the result of my own work and that I have not had access to copies of answer sheets or solutions from others.

Pressing the submit button to process your examination is your assertion that the above statement is true.

Submit | Clear

Figure 5. Student certification statement

Proctoring

The next set of recommendations involves proctoring. There are essentially two types of proctoring: live and virtual. Live proctoring is the traditional, in-person monitored, test-taking environment. Live proctoring can occur for both paper-based and computer-based testing, but involves the student going to a specific location. Virtual proctoring, on the other hand, involves attempting to monitor students at remote locations during test taking. Virtual proctoring is typically thought of as occurring in computer-based environments. The panel had several recommendations regarding proctoring techniques.

The panel recommends the use of live proctoring for high stakes testing situations. Live proctoring may be the closest to a foolproof method for preventing compromise during testing. Within the Army, there are systems already in place that provide live proctoring, such as the use of test security officers. Outside the Army, there are several commercial and academic organizations that specialize in live third party proctoring for test administration. There are a couple of disadvantages to this solution. First, live proctoring interferes with the Army initiative of "anywhere, anytime" training because it requires students to go to a testing center. Second, this solution creates a loss of learner control, as students may not be able to immediately get to a testing center when they are ready to take a test. Finally, live third party proctoring administered outside the Army could be more costly than proctoring by test security officers.

In terms of virtual proctoring, the advisory panel recommends using multimodal biometrics and/or biographical information integrated into the course design. Biometrics can be used in a layered approach depending on the stakes of the test being given. For example, in very high stakes testing, a multimodal approach with both fingerprint identification and iris scanning is used. For medium stakes testing, a single biometric mode may be all that is necessary, while for low stakes testing, no biometric measures may need to be implemented. Either as an alternative or in addition to biometrics, students could be asked biographical questions during training and/or testing to help insure their presence. Unique biographical information could be obtained from student records by an LMS regarding courses the student has taken or other personal information of which others would be unlikely to have direct knowledge. This

information could be put into the form of questions that students would have to answer correctly and immediately to continue training or testing.

Virtual proctoring techniques are not foolproof, as they only require the presence of a test taker and do not insure that a proxy is not present. In addition, the requirement to provide biometric or biographic information during training or testing has the potential to interfere with the training atmosphere. Implementing such measures would need to be carefully integrated into training or testing to avoid such interference. The implications of applying such systems to the Army training infrastructure are unclear. Technical support for this type of a system could also be costly.

There are, however, several positive attributes of virtual proctoring, particularly biometrics. First, biometric technologies such as fingerprint identification are quite reliable. Second, biometric technologies are becoming very affordable, with fingerprint readers on the market well below $100 per unit. Finally, should the Army choose to implement biometrics, there is a great deal of information available through the Biometrics Management Office and the Biometrics Fusion Center. These organizations have been involved in extensive product testing and research, and they are willing to share their findings with other government agencies. Virtual proctoring seems to have great potential, but there are many issues still to be addressed regarding implementation of such systems.

Public Key Infrastructure (PKI)

The next recommendation from the advisory panel is to implement PKI to limit access to tests and courseware. PKI could be adopted in Army training as it is adopted Army-wide. Implementing PKI in training could provide the added benefit of creating ready access to a career management account that could be used as a transcript to document a soldier's education. This recommendation is not likely to be implemented in the short term, as it does rely on a change to the current infrastructure.

Test Design

The final set of recommendations involves test design. The advisory panel identified several test design issues that could be used to decrease the likelihood of training compromise. Some of these solutions are unique to Web-based training, and some are not. The first test design recommendation is to randomize test items and/or randomize response options. This could be done in several ways. For example, a set number of test items could be administered with the order in which they appear varying with each test. Alternatively, the response options for each test item could be randomized, so the placement of the correct answer could appear in any position, creating the potential for enumerable test forms. Drawing items randomly from a pool of test items could achieve an even greater level of test security. These randomization techniques could be implemented individually or in conjunction with one another. All three randomization techniques eliminate the usefulness of a "test key" that could be passed from one student to another. However, there is still the possibility of the content of test items being remembered by students and passed along to other students. Randomizing by pulling test items from a pool of items helps to alleviate the possibility of test items being passed around.

Developing a pool of test items can be costly and time consuming, as this process involves generating many test items, pilot testing them, evaluating their psychometric characteristics, and designing appropriate randomization methods to ensure that equivalent test forms are produced.

Another recommended test design technique is to use performance-based testing. This would make cheating more difficult without making test taking more difficult. In fact, as long as we can determine who is taking a performance-based test, pre-knowledge of test content becomes almost irrelevant as the ability to perform a task is being tested, and successful completion of the test (assuming the test is designed well) indicates that the test taker is, in fact, able to perform the task. Pre-knowledge of test content in this case would only help a student prepare and learn to perform a particular task. However, this technique is more costly to develop than the more traditional multiple-choice test, and it involves more time of subject matter experts.

The next set of test design recommendations involves setting limits in the test-taking environment. First, time limits could be set. The idea behind this is that if an appropriate time limit were set, test takers would not have time to complete the test if they were to spend their time looking up answers in reference materials. However, this technique would involve a greater amount of development time, as setting an appropriate time limit would involve careful pilot testing. Two additional testing limits that could be set are limiting the number of times that a student can attempt to take a test and using "no print/no capture" options. These techniques would limit the possibility of students remembering or copying test items. This solution may be limited by the capabilities of the LMS being used.

The final test design recommendation is to implement a test mode on the computer to track where a test taker has been online. This would provide evidence when cheating does occur. The presence of such a system itself could serve as a deterrent to cheating. However, the implementation of this type of technique could again be limited by the LMS. Additionally, this could create a cumbersome data storage requirement. Each of the test design recommendations has the potential to decrease compromise in testing environments. As with the other solutions, the stakes of the testing should be balanced with the time and cost of implementation.

Conclusion

The set of recommendations generated by the panel provides a framework for implementing solutions to training compromise. The recommendations are not meant as a step-by-step guide to foolproofing training and testing environments. The purpose was to identify remedies to compromise in Web-based training and testing environments that can be implemented without hindering learning and prior to any problems arising. It was the advisory panel's basic assumption and belief that soldiers generally will "do the right thing." The passive and active solutions are meant to level the playing field, dissuading potential cheaters while not burdening those who never intend to cheat. Both the implementation of these solutions and a more thorough understanding of the current state of cheating and the motivations behind it are important topics for future investigation.

The overall recommendation is a layered approach based on the criticality of the test under consideration. For example, in high stakes testing situations the use of multi-modal biometrics and/or live proctoring may be warranted. In a medium stakes testing situation, however, a single biometric measure or tracking the keystrokes of the test taker may be acceptable. Finally, in a low stakes testing situation no intervention beyond an affirmative obligation statement may be appropriate. The level of security would depend on multiple variables set by the course administrator, and the recommendations from this report can be used to determine methods of setting an appropriate level of security.

References

Abell, M. (2000, December). Soldiers as distance learners: what army trainers need to know. Paper presented at the meeting at the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC), Orlando, FL. Retrieved March 25, 2002 from http://www.tadlp.monroe.army.mil/abell%20paper.htm.

Argetsinger, A. (2001A). Technology snares cheaters at U-VA: Physics professor's computer search triggers investigation of 122 students. *Washington Post*, Section A, Page A1.

Argetsinger, A. (2001B). Honor panel struggles with 145 cheating cases. *Washington Post*, Metro Section, Page B1.

Borman, F., Johnson, H., Pye, K., Tate, W., Walker, J., Wilcox, H., Sussman, A., Kelly, T., Gray, D., Garrett, R., Holland, H., & Bacon, H. (1976). Report to the Secretary of the Army by Special Commission on the United States Military Academy. www.west-point.org/publications/borman.html.

DeWan, G. (1994). Failing grade for cheaters. *Newsday*, May 12, 1994. http://www.newsday.com/other/education/ny-cheaters-conflict.story.

Department of the Army (1981). *Army Regulation 350-1, Army Training.* Washington, DC: Department of the Army.

Major, L.E. (2002). The virtual battleground: How universities are tackling academic plagiarism on the Web. http://www.distance-educator.com/dn2.phtml?id=6018.

McCabe, D. (2001). Cheating: Why students do it and how we can help them stop. *American Educator*, Winter, 38-43.

Program Management Office, The Army Distance Learning Program (1999). *Memorandum dated 27 April 1999, Subject: Acquisition Strategy, The Army Distance Learning Program (TADLP) Modernized Training System.* Fort Belvoir, VA: Department of the Army.

Program Management Office, The Army Distance Learning Program (2000). *The Army Distance Learning Program Brochure*, Fort Monroe, VA: Department of the Army. Available at http://www.tadlp.army.mil/brochure.pdf

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* New York: JohnWiley & Sons, Inc.

Wagner, E. D. (1997). In support of a functional definition of interaction. *The American Journal of Distance Education, 8*(2), 6-29.

Appendix A: Workshop Attendees And Presenters

Attendee/Presenter	Organization
Millie Abel	**Army Training and Doctrine Command**
Craig Aldrich	ACT, Inc.
John Archield	Air National Guard
Jim Belenich	U.S. Army Research Institute
Robert Bollig	**Department of Defense Biometrics Management Office**
Brian Burton	HQ AETC/DOZA
Dojan Cukic	**West Virginia University**
Christina Curnow	Caliber Associates
Sean Donahoe	**National Guard Bureau**
Mike Freeman	**Computer Science Corporation**
Chuck Fullerton	Transforming Technologies
Keith Hanshaw	Northeast Counterdrug Training Center
Dominique Harrington	Department of Defense Biometrics Fusion Center
Anne Humphreys	Carnegie Mellon University
Greg Mclean	Department of Labor
Pat Miller	**Department of Defense Biometrics Management Office**
Ray Nicosia	**Educational Testing Service**
Richard Nuffer	Defense Logistics Agency
James Nugent	Naval Reserve
Ed Papke	Unites States Army Sergeants Major Academy
David Pass	Department of Labor
David Raes	Iowa National Guard
Melinda Reed	U.S. Army Training Support Center
Teresa Semel	ACT, Inc.
Leonard Shyles	Villanova University
Chris St. John	Defense Acquisition University
Ron Stump	Defense Acquisition University
Kenneth Vance	Department of Defense Biometrics Fusion Center
Arthur Wilde	**Judge Advocate General's School, Army**
Jeff Willden	Weber State University
Robert Wisher	U.S. Army Research Institute
Rich Yarger	U.S. Army War College
Alan Pettie	U.S. Army Training Support Center

Note: Presenters are listed in **bold.**