Fingerprinting Certification Cheaters (Oct 08)

Gene Radwin, Ed.D. of EMC Corporation

This article describes several steps that the EMC Proven Professional certification program has taken to protect the integrity of its exams. A brief description is provided of how EMC has identified sources of cheating and actions taken. The article focuses in on a recently introduced practice of seeding exams with types of questions that can "fingerprint" candidates who rely on stolen copies of exams. The power of the fingerprinting process is described in a report of recent results on one EMC exam.

Steps to Reduce Cheating

IT certification programs individually and via industry associations are seeking to address problems of cheating. Most programs are very careful to ensure that exams remain confidential as they are developed. Access to exams is on a need-to-know basis. Programs use secure communications channels to transmit exam materials. Some programs analyze exam results to identify suspicious patterns (e.g., high jumps in scores for a candidate on an initial testing and on a retest; testing centers which have results significantly higher than other testing centers). Programs also seek to close down websites that offer copies of their exams. Microsoft has pursued a well-publicized effort against one of the most notorious websites.

Protecting Proven

The EMC Proven Professional Program has been extremely proactive in addressing issues of security.

Security Audit: In 2005, the Proven Program had a third party firm that specializes in exam security conduct an audit of its exam practices. The audit found that Proven was employing many appropriate security practices (e.g., requiring NDAs of exam developers and limiting access to exam materials). However, the audit offered recommendations to improve security further and these were subsequently adopted, including:

· transmit exam files to test publishing vendors via secure FTP sites and use password protected files
· provide a secure environment for field SMEs to review exam questions
· create multiple forms of each exam, making it more difficult for cheaters because they can not be certain which questions they will actually be tested on.

Ongoing, Active and Regular Monitoring: The EMC Proven Program has also engaged third party firms to assist in efforts to improve security and reduce cheating:

One firm provides monthly analyses of Proven exam results for evidence of cheating and other improprieties. Using these analyses, the Proven Program Security Manager has

· barred Proven exams from being delivered at specific testing centers that did not adhere to appropriate security practices
· notified candidates that their results are suspicious

Another firm provides EMC with 24-by-7 monitoring of the world wide web to identify websites and other internet locations (blogs, etc.) that are offering illegal copies of Proven Exams. Based on the reports, the Proven Security Manager has

· had EMC's IT organization bar access on the EMC network to websites that offer EMC exams for sale

as these websites are identified

· requested that third party payment services (e.g., PayPal) and web hosting services stop doing business with firms that offer Proven exams illegally

Identified Leaky Faucet: In late 2006, EMC found that one of its exams was for sale on the web before anyone had actually taken the exam at a testing center. After purchasing the exam, EMC determined that it was the actual exam and that it was in the format created by the testing vendor, not in the format in which EMC sends the file to the testing vendor.

How could this exam have been stolen? A band of fraudulent test takers could not have memorized exam questions because no one had yet taken the exam. Nor could the exam files have been stolen from EMC.

EMC investigated and in the end found a significant "hole" in the security operations of one test delivery vendor. Individual testing centers, in parts of Asia, were signing up fake candidates under false names to take EMC exams. Once these phony candidates were registered for an exam, the testing center could download the exam files for duplication and sale.

Pinpointing Sources: During 2006, EMC expanded the reach of its program by contracting with a second test delivery company. EMC exams would now be easily accessible by candidates worldwide. However, EMC wanted to sure that by adding a second vendor it did not make it more difficult to discover the sources of stolen exams. Thus, EMC initiated the practice of slightly modifying the exams that are delivered by the two vendors. Insignificant, non-substantive changes were introduced to a subset of questions of exams. For example,

· one test vendor might have a question that began "Your customer needed to increase its storage capacity"

· the other vendor would have the same question written as "A customer needed to increase its storage capacity "

These minor differences have, in fact, demonstrated their usefulness. EMC has been able to use these differences to identify which vendor was the source of exams that were available on the net for sale,

Limits of current efforts

With all of the efforts and tactics that EMC had employed, a gap still remained. The processes that were instituted could not easily identify a single individual who had procured a copy of an exam ahead of time. The potential identifiers of single individual cheating were limited to time and to score jumps:

- time: if a candidate raced through an exam, answering questions at an extremely rapid pace, that would be a possible indication that the candidate had prior access to exam questions and answers
- score jumps: if a candidate's score rose significantly from one administration of an exam to another and if the two administrations were close in time, this also would suggest that the candidate may have obtained access to exam questions and answers before the second exam administration

However, a cautious cheater could easily defeat time as an indicator by simply slowing down. And score jumps would not be displayed if a candidate had access to exam questions and answers before taking an exam the first time.

Something else would be needed to "fingerprint" other potential cheaters.

Creating a fingerprint

Goal: design exams in such a way that people who cheat will have a pattern of results that differs from those who are honest

Would it be possible then to "help" cheaters leave fingerprints? Would it be possible to design exams in such a way that the results would be self-incriminating to "cheaters"?
To do so, consider how different groups can be expected to perform on a certification exam

"Type" of Candidate	Expected Score on Certification Exam
Honest, knowledgeable exam takers	High
Honest, unknowledgeable exam takers	Low
Dishonest exam takers relying on stolen exams	High

The certification questions themselves distinguish knowledgeable from unknowledgeable candidates. In effect, exam scores provide a "fingerprint" for who's knowledgeable and who's not.

Dishonest candidates, however, will score similarly to honest and knowledgeable ones. Certification exams, as usually structured, obscure cheating. The issue: could an exam be structured or questions created that would highlight cheating? Could questions be included on an exam that would distinguish honest and knowledgeable candidates from dishonest ones? Could a way be found to have cheaters leave their fingerprints?

What would be needed is simple conceptually: add questions to an exam on which honest and knowledgeable test takers would score differently from dishonest test takers. How, though, could cheaters be made to answer differently?

The cheaters of primary concern were those who rely on stolen copies of exams - copies which contain not only questions and distracters but also identify the correct answers as those answers have been keyed. What if the stolen copies could be subverted so that cheaters were relying on "bad" information?

The answer to this challenge was not in the question content per se but in how the answers were scored. Take as an example a simple multiple choice question:

How much is 2 + 3?

A) 4 B) 5 C) 6 D) 7

Anyone with knowledge of basic arithmetic would select "B" as the answer. However, suppose that the test key had identified "D" as the correct choice. In this situation,
people who know basic addition will select B and will be scored as getting this question wrong. However, if someone was relying on a stolen answer key, that individual would select D as the answer and get the question "correct." Consequently, an honest, knowledgeable person would answer the question one

way and a dishonest person, another.

Here, then, was a means to elicit a distinctive pattern for "cheaters" - add questions to an exam which were (1) easy and (2) which had the incorrect answer coded as the correct answer. Like Homer's Trojan Horse, these mis-coded, easy questions would undermine those who tried to use them. Honest takers would be scored as answering such questions incorrectly; dishonest test takers would be scored as answering them correctly.

Question Asked: How much is 2 + 3?	Answer Selected When …	
	"5" coded as correct answer	"7" coded as correct answer
Honest, knowledgeable exam takers select	"5"	"5"
Dishonest exam takers relying on stolen exams select	"5"	"7"

With a series of such questions on an exam, honest test takers and cheaters would have distinctive patterns on exams.

Type of Test Taker	Answer Pattern on …	
	Regular Certification Exam Questions	Trojan Horse Questions (Easy Questions Coded with Incorrect Answers)
Honest, knowledgeable exam takers	High	Low
Dishonest exam takers relying on stolen exams	High	High

Thus, adding easy questions that were incorrectly coded - Trojan Horse Questions - would make exams self-incriminating for cheaters.

These Trojan Horse questions would not be used in calculating a candidate's official score on an exam. They would be used to help identify cheaters.

The Power of Trojan Horse Questions

An exam would not need to have many such questions to be effective in identifying cheaters. Five to seven should suffice. For example, exam A has 50 real questions and 6 Trojan Horse [TH] questions. If someone scored 90% on the real exam questions, how likely is it that such a person would select the incorrect but coded as correct answers on the TH questions. The answer is very, very low.

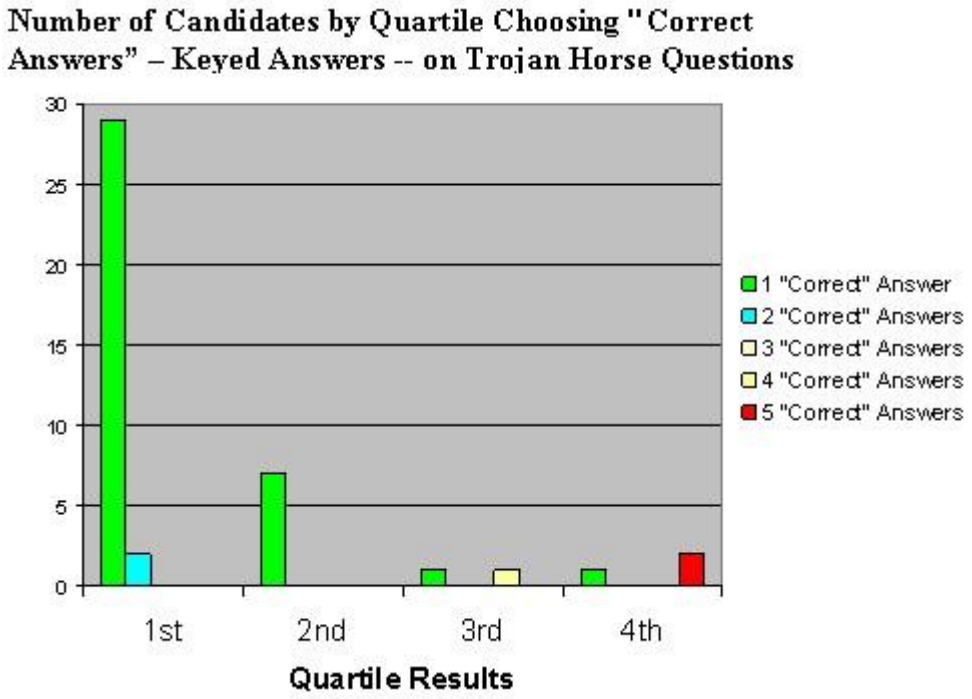
For someone who scored 90% correct on the rest of exam A, the odds of answering 6 of 6 or 5 of 6 TH questions as coded is 0.0000014. The odds don't improve much for someone who scored 80% correct on the exam.

Here, then, is a mechanism for shining a light on cheaters.

Implementation: The "Trojan Horse" strikes

The EMC Proven Program has begun adding Trojan Horse questions to exams. One exam had 5 Trojan Horse questions. These questions were selected from previous versions of the exam and were known to have very high pass rates --- the questions were demonstrably easy.

During a six week period, the exam was taken 650 times. The following table displays the results on the Trojan Horse questions by quartile.



As can be seen, 29 candidates from the lowest quartile answered one Trojan Horse question correctly (as keyed) and one candidate from this quartile answered two TH questions correctly. Since these are the least knowledgeable candidates, it is not surprising that more of them answered the TH questions correctly. However, the "easy-ness" of the TH question is evidenced by the fact that the vast majority of these less than expert candidates answered the TH questions accurately, and not as keyed.

In the next quartile, the number of candidates answering any TH question as keyed falls markedly - from 31 to 7. Again, this is another indicator of the fact that the TH questions are easy questions.

In the third quartile, the discriminatory power of the TH questions can begin to be seen. Only two candidates in this presumably more knowledgeable group answer TH question correctly. One candidate answered one such question correctly, a fact that can be attributed to random error. The other candidate answered four of the five questions as keyed. This candidate scored 88% on the rest of the exam. The probability of a person answering 4 of 5 Trojan Horse questions correctly when scoring 88% on the exam is approximately .0008. A small probability to be sure but debatable perhaps.

In the highest scoring quartile, we find results that are scarcely debatable. In this quartile, two individuals scored 98% on the exam and yet answered all 5 TH questions as keyed. These individuals, then, seemed to demonstrate high level proficiency on the exam content (98% correct) and yet they answered

5 very easy questions incorrectly. The probability = 0.0000003.

Here, then, is proof - DNA testing level proof - that these two candidates did not rely on their knowledge and experience to answer an EMC certification exam. Instead, these individuals were relying on the answers, illegally obtained, from the exam answer key. EMC is taking action against these individuals.

Conclusion

Trojan Horse questions offer a means then to turn cheaters' behavior against the cheaters. The tests that cheaters procure can be seeded with questions that will assist certification programs to identify those who cheat and to take appropriate action against them.

The TH questions also offer a means to identify the extent of cheating on certification exams. Such information will help the program management team to determine which actions are warranted to protect test sponsor assets.

The TH questions could potentially be used by exam test vendors to flag results at the time of testing. Criteria could be established whereby results could be flagged for action or withheld at the time of testing if a candidate scores a certain level or higher on an exam and answers a certain number of TH questions as keyed.

Trojan Horse questions can become one tool that test sponsors employ to reassert honesty in high stakes testing.

Test Publisher, ©2008 Association of Test Publishers