How data forensics help root out certification cheaters (Sep 08)

Linda Musthaler, 29 Sep 2008

Details on how data forensics analysis helps to find anomalous testing behavior that could indicate cheating

There's nothing quite like stirring the pot of controversy. Last month, I addressed the issue of cheating on certification exams. Specifically, I said that using "study aids" (i.e., stolen exams) that come from braindump Web sites could put a certification candidate at risk of being accused of cheating. The column was intended to inform people that many certifying agencies are now using data forensics to analyze test responses and look for extremely unusual behavior. As it turns out, people who use braindump materials often fall into this category. The ultimate penalty for cheating could be loss of certification with negative employment consequences.

This assertion led to a reader backlash, with some people suggesting that the forensic analysis is inaccurate and would ensnare people who did not cheat in any way, shape or form. Anonymous readers posted comments such as these:

* "…who validates the forensics (since this will destroy somones [sic] career for life)? In any investigation, there are always false positives. Legitimate people (even if only a few) will be caught unfairly. How will this be policed?"

* "We're supposed to believe that these tests are flawless? How are they going to handle it when they inevitably accuse an innocent person? The same way corporations always handle it, of course. Deny everything. Smear the person in the press. Throw lots of lawyers at them until they can't afford to go on. This sounds like another witch hunt."

* "Has anyone else seen or heard of this? Is the Microsoft cheating, a rediculous [sic] red herring? Or is there some kind of official [sic] document saying if you get all the answers right you'll be banned?"

Clearly I need to provide more details around my assertions on certification cheating, and especially the use of data forensics to uncover possible cheaters. (Oh, and for the person who suggested I must be on Microsoft's payroll, let me assure you that I am not and never have been.)

My sources for my information are the best they can be—people who work for the certifying agencies, the test centers and the data forensics company. (By "certifying agency," I mean any company or organization that issues a certification based on a candidate meeting specified requirements. Examples would be Microsoft, Cisco, CompTIA, Linux Professional Institute, etc.) These organizations all have a vested interest in seeing that the certification process is legitimate and fair to everyone, and that any cheating that exists in the process is eliminated.

I also referenced another article in Network World in which Peggy Crowley of Microsoft Learning, the department within Microsoft Corporation that oversees certification, stated that her company is updating its certification policy to include the penalty of a lifetime ban from the Microsoft certification program for all forms of cheating. Crowley says this includes the use of braindumps. (A "braindump" is an unauthorized distribution of a certification test which includes actual test items and their answers.)

Microsoft is not the only certifying agency that is re-evaluating its policy on exam security. New techniques and technologies that weren't even available a few years ago have made it possible to detect certification fraud. Certifying agencies are studying how or if their exam security policies need to change to accommodate these new capabilities.

The use of data forensics for certification exams is becoming common place among the certifying agencies, and not just in the IT industry. Caveon Test Security is one company that provides data forensics analysis as one of its test security services. Last week I spoke with Caveon president John Fremer and chief scientist and master statistician Dennis Maynes to learn more about how data forensics analysis helps to find anomalous testing behavior that could indicate cheating.

Fremer says the goal of using data forensics is not to catch cheaters; rather, the goal is to improve the security of the exams. Caveon and its clients (i.e., the certifying agencies) believe that catching and punishing cheaters is a deterrent that ultimately improves test security.

The million-dollar question on everyone's mind is, "How does data forensics analysis work?" Not wanting to tip his hat and reveal too many secrets to cheaters, Maynes explained the process in general terms.

A certification exam that is taken online generates a lot of data about how that exam was taken. For instance, the data points include how long a candidate lingered on each question; if the person first chose one answer and then changed to another; the sequence in which questions were answered; if two or more candidates taking the test at the same time have identical or similar results; and so on. This data is then analyzed to look for "extreme outliers"—something that doesn't fit the normal pattern of how most people would take the same test.

"We look for people who answer test questions in an unusual way," says Maynes. "An example of this would be answering a series of questions correctly in a very short time. This would be very suspicious, since the candidate wouldn't have enough time to read the questions and truly think about the answers."

In and of itself, this is not enough to say that the candidate cheated on his test. Perhaps he's a really fast reader, or he has taken the test before. Caveon also uses sophisticated statistical models to determine the probability of having extremely unusual results on a given test. If this litmus test indicates a low probability of having unusual results under normal (no cheating) conditions, then additional corroborating evidence is sought.

As an example, Maynes described a scenario where two candidates have extremely similar tests, indicating that the tests weren't taken independently. Caveon would use the science of item response theory to calculate the probabilities that two people worked together or didn't take the test independently. It's possible that one person was "the source" (i.e., a legitimate test taker) and the other person copied from him. Maynes points out that people can collude even when they take the test online. "The data speaks for itself," says Maynes. "We have an extremely high degree of confidence in what the data tell us."

Even armed with accurate data, Caveon doesn't point a finger and yell "Cheater!" Caveon provides the results to the certifying agency, which can do a further investigation into circumstances and determine what action to take with the certification candidate(s). Microsoft has said, however, that forensics analysis is so accurate that it will be used as the sole evidence for enforcement actions, including a permanent ban from certification. Because Caveon does not identify false negatives, Maynes could not give a definitive statement about the accuracy of Caveon's statistical models. Microsoft says the statistics it uses have a one-in-a-trillion chance of a false positive.

Data forensics analysis is just one protection against certification fraud. Caveon says one of its most popular services is a security audit, which is a review of every feature of a testing program. In this type of audit, Caveon identifies vulnerabilities and makes recommendations for any testing agency with a high stakes exam. Caveon also provides a Web patrol service in which it searches the Internet for evidence that exams have been posted online or that other people will take a test for another person.

"If we understand the mechanism of test theft, we can work with our clients to prevent it," says Fremer. For example, Caveon analyzes a test over time and looks for changes in test results that occur over that time period. It’s possible to correlate these changes to other occurrences, such as the posting of an exam on a braindump site. “We can make recommendations to the agency to update its test items,” says Fremer. These subtle changes in test results also factor into the forensics analysis.

Exam security is complex, but the challenges certainly aren’t limited to the IT industry. In public education, states are required by the No Child Left Behind Act to administer tests to evaluate the effectiveness of student learning. A compromise of these tests could result in public schools losing accreditation as well as funding. Fortunately, the techniques and technologies to improve exam security are getting better at addressing the problem, regardless of the industry.

Linda Musthaler is a principal analyst with Essential Solutions Corporation.