

Security In Language Testing

Mr. Paul Stevens
Mayflower College
Plymouth, UK

In such high-stakes, emotive testing, it is anticipated that some pilots and air traffic controllers will try to cheat in their attempts to achieve Operational Level 4. This paper looks at why they may do this, areas of test security which may be compromised and best practices in how to reduce the risk of cheating.

Little research has been published on security in language testing. This may in part be due to the fact that little has been done on the subject but it is also no doubt partly influenced by testing authorities' reluctance to admit that candidates cheat on their test and an understandable self-interest in not publicising how their test's security may be compromised.

However, our experience at Mayflower College in running IELTS examination centres for the past 11 years and our experience with Test of English for Aviation (TEA) over the past 12 months has lead us to conclude that some language test candidates do undoubtedly try to cheat.

Key factors determining whether a candidate will cheat seem to be:

- The candidate's desperation to pass the test – the higher the stakes the more the candidate is prepared to risk.
- The realistic options at the candidate's disposal to pass the test without resorting to cheating. If all the candidate needs to do to have a good chance of passing is a few days of hard study then s/he will more than likely do this rather than accept the risks of cheating. Conversely, if someone is obliged to take a test but has no hope of passing that test legitimately, then cheating becomes a more attractive option.
- The candidate's nationality / cultural background – attitudes towards cheating vary greatly according to nationality / cultural background, from a complete reluctance based on morals, values, shame and fear, to a laissez-faire attitude where attempting to cheat is partially tolerated, even expected; successful cheating is admired by peers and candidates feel they can act with a degree of impunity, whether they succeed in their cheating or not.
- The security measures in place to prevent cheating – if cheating is perceived to be easy then the temptation is too great for many to resist.

In testing to meet the ICAO language proficiency requirements the stakes could hardly be higher.

The results of the testing can have a significant impact upon people's livelihoods, careers and egos.

The situation is further fuelled by many controllers' / pilots' resentment of the imposition of these new language proficiency requirements – this resentment is based on the belief that they have been doing the job for many years and have never had any problems previously. In addition, such is the scale of this ambitious ICAO programme that it is inevitable there will be differences in the way people are assessed around the world. There will most certainly be stories of people receiving Operational Level 4 certificates when in reality their language competence does not merit such an award.

Learning a language takes time; there are few short-cuts and the deadline of March 2008 is looming large. Airlines and ATS providers have organisations to run, services to deliver, budgets to meet – they cannot simply roster everyone on English language instruction until everyone achieves Operational Level 4. As a result very few pilots / controllers are able to devote extended, intensive periods of time to improve their level of English. Under these circumstances a candidate who is currently at ICAO Elementary Level 2 in each of the six skills (Pronunciation, Interactions, Fluency, Structure, Comprehension, Vocabulary) has minimal chance of reaching Operational Level 4 before March 2008.

All this can lead to a pilot / controller feeling hard-done-by, victimised and with few alternative courses of action. This in turn can even result in that pilot / controller persuading himself that his attempts to cheat are morally defensible.

Our work to date in testing pilots / controllers leads us to conclude that in some countries it is extremely likely that the *majority* of pilots / controllers in those countries will NOT achieve Operational Level 4 by March 2008 if the testing process is carried out accurately and securely. There will be many people in the same difficult position; if some of these people decide to pool their resources (finances, influence, etc.) in order to cheat then the likelihood that they may succeed increases.

A lot of good work has been carried out by ICAO and others concerning the development of the descriptors, test design, criteria for examiners, etc. However, if a test is not secure then all the other good work is in vain.

The links of the “security chain” are many but key elements are:

People – many of us can be corrupted in the right circumstances – the offer of money, granting of favour, intimidation, etc.

Test Materials – some research surprisingly concludes that knowing the questions in advance does not always help candidates as much as may have been expected; nevertheless, this is not an argument to make candidates aware of the questions in advance!

Database – almost all tests will use a database of some description to record candidate data, test results, etc. If the database can be hacked then results can be changed and a test’s integrity falls apart.

Impersonation – people take the test on behalf of others; these impostors can be friends, relatives or people who are paid to provide the service.

Certificate – most testing bodies award hard copy certificates. Such is the sophistication of image editing software (like Photoshop) that counterfeit certificates are a concern.

What “best practices” can be employed to prevent cheating?

Solutions to an extent depend on the testing solution employed (whether it takes the form of a face-to-face interview, is computer-based, is delivered over the telephone, etc.) but there are some common elements.

Any system will only be as strong as its weakest link. It is possible to have everything in place (people, materials, etc.) but, for example, if an unauthorised person discovers the password to a database then everything falls apart.

People

Administrators, interlocutors, raters, technical support, signatories on certificates the advice is to choose them all very, very carefully, selecting as much for human qualities as for technical expertise. Security is simpler to control if the group of people is small and everyone is accountable. It is important to create a “culture” that this is VERY serious work; it is all too easy for people to think procedures are overly bureaucratic and to start to cut corners.

Ideally interlocutors and raters should not know the candidates they are testing. If the rating is done remotely (using a recording of the test) then best practice is to use numbers to identify the candidate (rather than the name of the candidate). The greater the distance that can be created between the candidate and his / her examiner(s) the better.

Test Materials

If any test materials are compromised they MUST be withdrawn and never used again. This is an expensive inconvenience but needs to be adhered to. If hard copies are used, good practice is that they are stored in a lockable cupboard within a lockable room. All test materials must be signed out and signed back in – if anything goes missing then it should be simple to trace it back to the person responsible.

Candidates will inevitably talk to each other about the questions they have been asked – it is impossible to stop this but demands that a test has a sufficient number of sets / versions.

The test venue also needs to be chosen carefully, to prevent, for example, tests being overheard.

Finally, steps need to be taken to ensure that candidates do not secretly record the examination / interview. The size of today’s digital recorders does not make this a simple task but as a minimum measure no bags or coats should be allowed into the examination room.

Database

Few people who are ultimately responsible for a test are also IT experts. Good practice is not to accept an IT developer’s claims that the system is secure – employ independent IT security experts to evaluate a system. The importance of the human factor in the security chain should not be underestimated however. Passwords are always a trade-off between something which is memorable and something which is difficult to guess or break.

If a database user leaves the password to the system on a Post-It note on his / her monitor then the time and money invested in getting the technical side secure is wasted.

Any data transfer (for example, candidate data, results, digital recordings of interviews, etc) should always be securely encrypted.

Recommended practice is to have paper copies of test data / results as well as computer data. This provides the facility of having a trail to compare the marks in the database with the marks awarded by the examiners.

Finally, a computer audit trail makes it possible to see who did what and when.

Impersonation

Test developers need to ask themselves, “how do we know that the person whose name appears on the certificate is really the person who took the test?”

As a minimum, ID checks (passport / identity cards) should be shown at the time of the exam. Basic training should be given to administrators / examiners in how to match a face to a photo (for example, looking at the distance between the eyes and the ears). Training should also be given to spot fraudulent identity documents.

If any part of the test is conducted in groups of candidates (for example, a listening exercise) then passport / identity cards must be placed on each person’s desk and be available for inspection by invigilators. Invigilators also need to check that the name written on the exam papers is the name which appears on the candidate’s passport / identity card – it is not unusual for candidate A to write “candidate B” on his / her examination paper and for candidate B to write “candidate A” on his / her examination paper.

With the Test of English for Aviation (TEA) the candidate is photographed immediately before the Test begins, the camera is connected to the computer and this photo is automatically uploaded into the candidate’s database record. We can therefore be sure that the person who took the test is the person whose face appears on that person’s certificate. The printing of the date and time on the photo serves as an extra security measure.

Certificate <http://www.maycoll.co.uk/aviation-english/images/teacert.jpg>

The issuing of certificates should be strictly controlled and ideally centralised. It is recommended that a certificate numbering system (preferably which includes some random numbers) is employed.

Original signatures are more difficult to forge than pre-printed signatures as are dry seals when compared to wet (ink) seals.

Tinted paper is more difficult to reproduce and watermarked paper is a recommended investment.

In conclusion, no system will ever be 100% secure.

The key notion here is “Affordable Security” - there will always a trade-off between cost and benefit.

However, there are many potential test candidates who appear to have ample motivation for cheating. They are relatively well paid, highly educated and not without status and influence.

If some of these people decide to cheat it will not be simple to stop them.

However, if a level 2 pilot or controller receives a level 4 certificate then we all have a serious problem.

— — — — —