

Understanding the Role of ePassports

Tim Moses
Director of Advanced Security
Entrust, Inc.



On 29 July, a robbery took place near Manchester. The result? A thief escaped with nearly 3,000 blank passports and related travel documents. Their value on the black market is thought to be in the region of £2.5 million.

These, however, aren't typical passports; they are "ePassports," the newest form of international border security document. They contain a silicon chip for storing the holder's biographical and physical details.

For varying reasons, ePassports have had critics over the years. This latest event gives them another opportunity to rehash arguments that ePassports do not provide absolute security. Quite clearly, the simple act of embedding a chip within a document doesn't transform it from an insecure document into a secure one. Only if the chip and its information are processed properly will it deliver the highest level of security of which it is capable.

A passport is not a ticket to a rock concert; mere possession of a genuine document does not grant entry. A passport is a credential that asserts the citizenship of an individual. In order to obtain entry, the genuineness of the credential must be established, and the person must prove they are the rightful owner and the credential is theirs.

Under attack

Attacks against the genuineness of a passport are known as "forgery attacks"; attacks against the ownership of the credential are "impersonation attacks." A digital signature, created by the UK Identity and Passport Service over the biometric dataset (which could contain fingerprints, iris scan data, and/or a facial photograph), held in the passport effectively addresses forgery attacks. Provided, of course, that the signature is verified.

Overcoming an impersonation attack requires a border agent to compare the biometric datasets in an ePassport with those of the individual carrying the document. The only forms of biometric data in widespread use today are facial photographs and physical characteristics such as height, eye colour, hair colour and skin colour. An impersonation attack requires a criminal to match a genuine passport to an impostor whose physical characteristics can be mistaken for those of the genuine passport holder.

Detecting such an attack relies, to a large extent, on the skill of the border agent, although tools are becoming available to help with this process. The duplication of the information in electronic form neither enhances nor degrades the accuracy of the process.

One particular variant of an impersonation attack is called a "cloning attack." It involves copying the contents of a genuine passport onto another passport. The only additional consideration is that the genuine holder may not report the loss of the passport and so it won't appear on a watch list.

The presence of a chip makes it practical to carry higher-entropy biometrics — fingerprints and iris scans, for example — which achieve lower false-positive rates than facial photographs. This will make it impossible, in practice, for a criminal to match an impostor with a genuine passport.

The ePassport evolution

Today's ePassports are the beginning of an evolution that will improve the reliability of travel documents, allowing governments to enforce laws aimed at improving the safety and living conditions of their citizens. This first generation of ePassports — commonly referred to as Basic Access Control (BAC) ePassports — only represents the initial stage of advanced border security initiatives.

Governments around the world are developing an even stronger standard for ePassport security. Protected by Extended Access Control (EAC) technology, future ePassports only will improve the methods of securing and authenticating biometric datasets. EAC ePassports will be deployed in the European Union (EU) member countries as early as 2009.

As of now, technology can only do so much, particularly when the human element is involved. These documents do not represent absolute security. Only the naïve would expect them to. They mitigate some of the vulnerabilities associated with paper documents. And, future generations of the technology will effectively address still more of those vulnerabilities.

We are stepping in the right direction. And even with the current security technology, ePassports are much more difficult to compromise than their previous paper-only counterparts. And that is a good thing.



About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organisations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call +44 (0)118 953 3000, e-mail emea.sales@entrust.com or visit www.entrust.com.