E-passports without the big picture

Date: 20 Feb 2006 - 13:00
By Professors Jaap-Henk Hoepman and Bart Jacobs, Radboud University Nijmegen, Netherlands

Professors Jaap-Henk Hoepman and Bart Jacobs, Computer Security, Radboud University Nijmegen, Netherlands, talk about the risks and the societal changes involved in the introduction of the E-passport.

Electronic passports are on their way. According to EU regulations member states have to start issuing passports with embedded chips that store a digital picture of the face of the passports holder before 28 August 2006. Digital fingerprints will be added later. These biometric measures should make it easier to make sure that your passport really belongs to you—and not to someone else.

The new chip in the passport has no external contacts: communication is wireless, but does require prior activation of the chip via a code that is derived from the so-called Machine Readable Zone (MRZ) at the bottom of the plastic page inside your passport. The introduction of these e-passports is one of the biggest IT-operations in the Union so far. It may seem a small change, but it isn't; it is remarkably complex and far reaching.

First of all, it is difficult to get the standards right. They are set by ICAO, the International Civil Aviation Organisation, in a compromise between many parties. Authenticity and integrity of the passport data are guaranteed by well-established security mechanisms. But confidentiality depends on the abovementioned chip activation. It has not been designed to satisfy the highest levels of protection. Eavesdropping on the wireless communication at a border crossing is possible. The data collected in this manner is encrypted, but not in the very best manner. The encryption can be broken offline because the number of options involved (derived from the MRZ) is limited. The fingerprints that are introduced in a next stage (in a couple of years) require an additional protection mechanism, developed by the EU itself. It is complicated, and involves a non-trivial exchange of certificates between states. Assuming such standards are implemented uniformly, suitable e-passport readers have to be introduced at border stations. And the resulting new checks have to be integrated into new procedures— for instance, on how to act when the biometry does not match, or when the chip fails. The introduction of the e-passport may also lead to major societal change.
We expect that the actual use in international travel of the additional options offered by the new e-passport will grow only slowly. It is by no means clear if biometrics works at such a wide scale. But what we can already see is that the pressure is building up to employ the new options also in other areas than border inspection. For instance, your bank may also wish to use the biometric options offered by the new passport—-in order to decrease identity fraud. Given the current set-up, it can access the digital facial image in your passport if you hand over the document. Accessing the (future) fingerprints will require additional certificates from governments. Will they give it to banks? Or to institutes in health care or social services? Or to casinos? Pilots to test the use of biometrics to combat social security fraud are already happening in the Netherlands.

The issue at stake is what is often called "function creep". The e-passport is designed for one purpose, but may very well end up being used for many other purposes. Is there any control? It is not clear. Certain countries, like the Netherlands, intend to create a central repository of all data, including biometrics, on the passports they issue to their citizens. The official goals of this database are to increase (1) the security of the passport, and (2) the effectiveness of national identification laws. It allows for more thorough checks when applying for a new passport, or for additional on-line verification of passports. It also allows for other, possibly non-intended, uses. For one thing it makes on-line identification possible.

Citizens can be identified and traced even if they do not carry their passport. It could also be used to solve more crimes. Fingerprint s found at a crime scene could be matched against the nation-wide fingerprint database. As far as we know, no concrete plans for applications like the latter exist. But they may become very hard to resist, once the enabling infrastructure is in place. Widespread use of biometrics will change the balance of power between states and their citizens. The current European standards for the protection of the fingerprints for instance solely focus on the use of these fingerprints for border inspection.

No provisions for the use of the passport in other situations are included. The security implications when the new passports will actually be used for other applications are unclear. Biometrics raises high hopes. But the technique is highly overrated. Two basic laws for ordinary password use are: change regularly, and avoid multiple use of the same password. Both laws are broken with the use of biometrics: you use the same "password", say a scan of your finger or iris, everywhere, and you can never change it - after it is compromised. Biometrics may actually lead to an increase of identity fraud via what we like to call "bio-phishing": fraudulently taking your biometrics in order to be admitted as you somewhere else.

The new passport should provide stronger proof of one's identity. Precisely this additional strength forms the basis for future applications. As a consequence, the value of the biometric data on the passport (related to the value of the assets they give access to) also increases. At the same time exposure of this
data is required on many more occasions. More applications imply more potential vulnerabilities. If the value of the biometrics increases and their exposure becomes more likely, then the risk of using these biometrics also increases. It is therefore very well possible that we arrive at a situation where the risk of using the new passport for identification becomes higher than current identification techniques. The paradox then is that with the widespread adoption of an apparently more secure passport, we actually may render ourselves less secure! What is needed is "the big picture": a perspective on identity management in modern societies, looking 10-15 years ahead. It is important to give citizens control over authentication, i.e. over what part of their identity they wish to disclose in which situation.

We can envisage a situation where everyone of us is constantly carrying a smart identity token, for instance in the form of a mobile phone, identity card, or implanted chip. A very basic rule is that in every situation, the environment should authenticate itself first. The token can then respond, based on a pre-defined or an ad hoc policy, determined by the user. For instance, only when it is clear that I am at home it may give away all my personal preferences. The environment may then require additional proofs---for instance via biometrics---before certain services are offered. The proof method should be proportional to the service level. Certain electronic identity checks may be enforced by law. Such future scenarios require a thorough rethinking of personal identities.

It will have to take privacy into account, not only in a one-sided manner as impediment to public security, but also as an essential element of personal security. For instance, if you, say as a politician, always broadcast your identity, you are vulnerable to e-bombs that only detonate in your presence. Personal identity management is fundamental in an increasingly connected world. The explicit use of personal policies makes life (again) a bit more complicated. But if we observe closely how high-school children manage and protect their contacts through mobiles, email, chat and instant messaging programs, we can already notice that the youngest generation has a much better grasp (than us) of virtual identities.

Professor Jaap-Henk Hoepman, www.cs.ru.nl/~jhh/ and Professor Bart Jacobs, www.cs.ru.nl/~bart/ are senior researchers and professors in computer security, at the Radboud University Nijmegen, the Netherlands. They consult the Ministry of Internal Affairs wrt. e-passports. This article reflects their own views.