TCSDAILY
TECHNOLOGY · COMMERCE · SOCIETY
A PUBLICATION OF TECH CENTRAL STATION

Passport Puzzle

By Evgeny Morozov : BIO| 21 Aug 2006

At a recent technology conference in Las Vegas, Lukas Grunwald, a German security expert, showed how a few hundred euros combined with some publicly available information helped him clone a German electronic passport that had been specially designed to eliminate just this sort of fraud. Since the technology is being adopted across Europe, the trick would work elsewhere. Some experts argue that his discovery is not such a big deal; that the risk level is akin to that of using a stolen paper-based passport; and that physical examination will almost always reveal the difference between the passport photo and the reality.

However, at least three major vulnerabilities exist. The first has to do with automatically-controlled check-ins, where there is no physical verification (something which is actively being discussed in Australia, but probably won't be introduced in Europe and America). Second, were one to look beyond passports, the identical technology is used in access cards for offices, student cafeterias, some libraries; there is very little (if any) physical control to match the person to the card there. Finally, there are privacy concerns about the mere access to personal data stored in the electronic passport (currently, decoding data from the electronic passport is not feasible, because it requires the possession of the passport to match the codes; this can be done just by reading the data manually).

Whatever the broader security implications of the flaw, the discovery has inadvertently exposed the European Commission's slowness in embracing innovative technologies and its poor coordination with the national technology policies of the member states. On paper, issues surrounding Radio Frequency Identification (RFID), the backbone of the new electronic passport system, seem to occupy a good portion of the agenda of Viviane Reding, the commissioner for Information, Society, Media. Since March, the Commission has been organizing numerous workshops with leading industry experts to debate the pros and cons of RFID technology, trying to grasp what regulatory environment would be required to encourage it - or at least not hinder it.

The Commission even placed the RFID debate in the public space by opening an online consultation process on its "Your Voice in Europe" web-site, where visitors can fill in a questionnaire and share their views about RFID. Also, the background paper presenting the results of the workshops eloquently highlights the nature of the debate and calls for a rather liberal approach to framing the legal debate.

Yet as the passport fraud story has demonstrated, member states prefer to simply proceed with embracing RFID instead of waiting for another green light from Brussels. This might have its advantages: among them, faster adoption and diffusion of technologies. However, given the current inchoate state of understanding of the risks to privacy and security associated with RFID, this might be as destructive to EU member states as it appears beneficial.

Suppose somebody manages to clone another German passport, but this time in a way that data on the cloned copy can be altered without alerting the authorities (something the current hack cannot do). Among other things, given the open borders in Europe, it would mean that the holder of the fake passport would be able to travel everywhere in the EU and even abroad quite freely. So, the flaw in the German system creates a problem for the rest of the EU, and it would have made sense for the Commission to have played a more proactive role in this process.

The same, of course, has been possible with fake "paper" passports. Yes, but we are missing an important point: the whole idea of launching an e-passport (which was, needless to say, rather expensive) was to *prevent* fraud in the first place. If the guarantees against fraud are so few, why should we bother?

This doesn't mean the European Commission or member states should bury the idea of using the e-passports. In part, they can't—because this would stymie their visa-free regime with the US. It seems that were it not for the pressure that the US levied on the national capitals by threatening to impose visas on holders of the old passports, the issue might have taken years to come to the wide public attention.

The looming question is not what will happen with RFID; the technology is here to stay. The question is how come it has taken the European Commission so many years to start talking about RFID in the first place? Germany rolled out its RFID-enabled electronic passport in October 2005 (it is not the only country to have done so) and the Commission expects to collect the results of its "Your Voice in Europe" campaign about the benefits of RFID only in September 2006, almost a year later.

Wouldn't it make more sense to consult the public first and then carry on with the implementation of technology in the member states? Instead, we get the European Commission, which, at least on the technological level, seems to operate independently of the member states. It wastes resources on collecting feedback for projects that have already been launched, thanks to pressure from the US. One can hardly call such an approach to managing technology "proactive".

The author is a TCS Daily contributing writer. He blogs at www.sharpandsound.com.