Biometric Blooper?
National Identity Cards Might Benefit From Two-Factor Authentication

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Regular readers may know that I detest passwords as a method of authentication and have leaned towards tokens and biometric authentication as more secure, less expensive solutions for identification, authentication and authorization. However, my friend and colleague Frank Platt, a distinguished expert in physical security and emergency management for the last 40 years, sent me an interesting e-mail message recently and I asked him if we could publish it for the readers of this column.

The remainder of this column is Frank’s (with minor edits):

* * *

The U.K. is planning to launch a national biometric identity card next year, along with a national database to include all the citizenry. This card will certainly be convenient when purchasing or banking or to quickly authenticate one’s identity. But the whole idea may be deeply flawed.

On June 8, the London _Daily Mail_ carried an article whose headline was “Mafia will steal millions of biometric identities, MPs warned.” [http://www.dailymail.co.uk/news/article-1024946/Mafia-steal-millions-biometric-identities-MPs-warned.html] The article covers a report to Parliament by Ross Anderson, [http://www.cl.cam.ac.uk/~rja14/] Professor of Security Engineering in the Computer Laboratory [http://www.cl.cam.ac.uk/research/security/] at the University of Cambridge [http://www.cam.ac.uk/] in England and a well-known contributor to the security community. His point is that criminals can easily steal biometric scans.

Once that happens, it is not possible to re-enroll the person whose identity is compromised. You can’t issue someone a new fingerprint [although MK notes that you can enroll another finger], or a new retina, or a new face. So once a person’s biometric data are compromised, they will have to be out of the proposed system forever. There are much better ways for secure authentication, he suggests – for example, using chips within an ID card, PIN numbers, and perhaps random keypads.

I too offer a suggestion (not knowing exactly what the U.K. has in mind): two-factor authentication. If a PIN is required when using the national ID card and also a keypad with random key locations, the PIN can then seed an encryption process. Since the authentication process will first assign each 0-9 number to randomly selected keys on the keypad, the encrypted packets will be different each time. Then, if an identity is compromised, the PIN can easily be reissued. The person recording the biometric scan does not know the PIN, so simply changing the PIN can reestablish security. A new finger won’t be necessary.
Next, here in the U.S., on June 5, President Bush issued Homeland Security Presidential Directive 24 (a.k.a. NSPD-59), “Biometrics for Identification and Screening to Enhance National Security.” [http://www.fas.org/irp/offdocs/nspd/nspd-59.html] It is interesting, timely, and well thought out. The “Purpose” paragraph is as follows:

“This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.”

This system can be very useful in that millions of existing fingerprints can be scanned into a uniform database. Nor do I see privacy as an issue because the information already exists; the only complaint can be whether interoperability is a bad thing. But still, a national biometric system will create the same weaknesses as the proposed U.K. system if only one means of authentication is used.

And also at issue are the announced plans for U.S. passports with embedded radio-frequency identification (RFID) chips to store biometric identification. Security researchers have raised serious questions about their reliability and resistance to cloning. [http://www.wired.com/politics/security/news/2007/08/epassport]

* * *

Frank Platt is founder and president of Office Planning Services, which was located on Wall Street for 20 years and is now a virtual consultancy headquartered in Stark, N.H. He can be reached at 603-449-2211 or e-mail. <mailto:fnplatt@aol.com>

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance [http://www.graduate.norwich.edu/infoassurance/] and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 Frank Platt & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.