NIST shows on-card fingerprint match is secure, speedy

April 2 2008

Tests show that wireless data transmission from a fingerprint reader to a match-on-card can be secure. Credit: Talbott/NIST

A fingerprint identification technology for use in Personal Identification Verification (PIV) cards that offers improved protection from identity theft meets the standardized accuracy criteria for federal identification cards according to researchers at the National Institute of Standards and Technology.

Under Homeland Security Presidential Directive 12 (HSPD 12), by this fall most federal employees and contractors will be using federally

approved PIV cards to “authenticate” their identity when seeking entrance to federal facilities. In 2006 NIST published a standard* for the new credentials that specifies that the cards store a digital representation of key features or “minutiae” of the bearer’s fingerprints for biometric identification.

Under the current standard, a user seeking to enter a biometrically controlled access point would insert his or her PIV smart card into a slot—just like using an ATM card—and place their fingers on a fingerprint scanner. Authentication proceeds in two steps: the cardholder enters a personal identification number to allow the fingerprint minutiae to be read from the card, and the card reader matches the stored minutiae against the newly scanned image of the cardholder’s fingerprints.

In recent tests,** NIST researchers assessed the accuracy and security of two variations on this model that, if accepted for government use, would offered improved features. The first allows the biometric data on the card to travel across a secure wireless interface to eliminate the need to insert the card into a reader. The second uses an alternative authentication technique called “match-on-card” in which biometric data from the fingerprint scanner is sent to the PIV smart card for matching by a processor chip embedded in the card. The stored minutiae data never leave the card. The advantage of this, as computer scientist Patrick Grother explains, is that “if your card is lost and then found in the street, your fingerprint template cannot be copied.”

The NIST tests addressed two outstanding questions associated with match-on-cards. The first was whether the smart cards’ electronic “keys” can keep the wireless data transmissions between the fingerprint reader and the cards secure and execute the match operation all within a time budget of 2.5 seconds. The second question was whether the “match-on-card” operation will produce as few false acceptance and false rejection

decisions as traditional match-off-card schemes where more computational power is available.

The researchers found that 10 cards with a standard 128-byte-long key and seven cards that use a more secure 256-byte key passed the security and timing test using wireless. On the accuracy side, one team met the criteria set by NIST and two others missed narrowly. The computer scientists plan a new round of tests soon to allow wider participation. For copies of the test report and details of the next test round, see the MINEX (Minutiae Interoperability Exchange Test) Phase II Web pages.

Notes:

*Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors. March, 2006.

** P. Grother, W. Salamon, C. Watson, M. Indovina and P. Flanagan. MINEX II–Performance of Fingerprint Match-on-Card Algorithms, Phase II Report. NIST Interagency Report 7477, Feb. 29, 2008.

Source: National Institute of Standards and Technology