SPYRUS

Fingerprints on Smart Cards

There have been a number of e-mails recently on the subject of fingerprints and smart cards, including the observation that such a card would inevitably have the user's own fingerprints on it, in addition to having the fingerprint template included in the smart card's memory. The question was raised whether the availability of the user's own fingerprints on the plastic card could invalidate the use of a biometric device and smart card for authorization and access control purposes.

SPYRUS recently participated in a series of three developmental trials to explore the feasibility of combining biometrics, PKI, and smart cards for the US Government's Biometrics Management Office. We were the technical lead for the third program, which involved extending the model to work with proximity cards used for physical access control. A certificate-based infrastructure was used, including the use of attribute certificates to certify the authenticity of the biometric templates.

So if I may, let me try to shed some light on some of these issues.

First of all, as I'm sure everyone realizes biometrics are not secret. At least most of them aren't, although retinal scans and scanners that pick up the venous pattern of the wrist are better than fingerprints and facial recognition systems in this regard. More to the point however, biometrics don't change, at least not much, and they are difficult to revoke – you run out of fingers after a while. As a result, the first time that a biometric image is scanned, that stored image could conceivably be used to mount a replay attack. As was pointed out, the overall threat scenario has to be considered in designing any particular security solution.

Second, it is not quite true that a biometric template is a one-way function, at least in the sense that those of us in the cryptographic community would think of it. It is a reduction of certain key attributes of the biometric characteristics, but it is not necessarily the case that it would be impossible to reverse the process. In fact, someone published an article on exactly that subject recently, where he took several facial templates and tried to reconstruct the face from the template. In this effort, he was significantly aided by an algorithm that provided a goodness-of-fit score, rather than a binary pass/fail indicator, and so he was able to manipulate various elements of his artificial face and use a hill-climbing algorithm to improve it. Some aspects of the face seemed to be ignored by the biometric algorithm, and therefore didn't produce particularly good results when compared to the original photo, but the more sensitive areas involving the eyes, nose, and lips were reproduced quite well. And obviously, the result was good enough to pass the acceptance test, since it was derived from it. So artificially reconstructing a biometric image is not impossible, merely difficult. Even if the algorithm didn't produce a goodness-of-fit output, it would still be possible to conduct an exhaustive search over the key parameters until you were successful, even if the false input didn't look anything like the real input – if it passes, that's good enough.

That brings me to my third point – that biometric templates need to be encrypted in storage and during transmission, and the encrypted template needs to contain a random value that is keyed to the individual subject somehow, or is at least unique. This is necessary in order to prevent a scan of a fingerprint database, looking for two templates that happened to be identical, or one that would match that of an attacker. And they should be digitally signed or otherwise protected against substitution.

Now, having said all of that, what is the risk that someone could "lift" a fingerprint off a plastic card and use it to impersonate a real finger? It wouldn't be impossible, but it wouldn't be trivial, either. With some of the older fingerprint readers, this would be quite difficult, because those readers scanned the finger using three different colors of light, one of which was the near infrared. The infrared sensor looks below the surface of the skin and picks up the subcutaneous capillary pattern, in addition to some portion of the surface image. That also provides protection against a severed finger, because the infrared is picking up the oxygenated hemoglobin, which is strongly reflective in the IR. Lose the oxygen, and you lose the pattern. And obviously, a fingerprint on the smart card doesn't pick up the subcutaneous pattern either.

The newer, less expensive devices generally rely on a capacitance sensor. A simple photograph won't work for a capacitive sensor – it would have to be a piece of plastic with the electrical properties of a real finger, and with 3-D molding to reproduce the real patterns of a finger. Is that impossible? Probably not – some kind of a photo-etching process might work.

With regard to whether smart cards have sufficient power to process a biometric live scan and perform a biometric match-on-card algorithm against a stored template, we (and other vendors) have demonstrated that they certainly can do that.

At present, the reason why no smart cards include biometric sensors is that most of the sensors currently available are too thick to fit within the banking card format. In addition, even if one were available that would be thin enough, there could be a real problem in meeting the bending and torsion requirements of the ISO 7816 card specifications – it seems doubtful that such a thin but large surface area sensor could withstand that kind of mechanical stress.

One the other hand, embedding such a device within a USB token, and certainly within a PCMCIA device, would be much simpler. How much would people be willing to spend for a FIPS 140-2 Level 3 USB crypto-token with an integral biometric sensor? And how soon do they need it, and how many would they be interested in buying?

With respect to the issue of replaying biometrics vs. the security of PINs, at the present I would worry a lot more about PIN and password replay than I would about a biometric replay, for the simple reason that spyware programs (a la the recent Kinko's attack) are all too ubiquitous.

But at least we can offer a real, off-the-shelf solution to that problem – the SPYRUS PAR-2 smart card reader. See http://www.spyrus.com/content/products/rosetta/PAR2.asp. This lightweight, portable reader also serves as a badge holder, calculator, and can be programmed to generate one-time passwords and for other applications.

Perhaps its best feature, however, is the keypad that provides a guaranteed private way of entering the PIN directly into the smart card. So long as the PIN for the device was entered that way when the card was first initialized, and every time the card is used thereafter, there is no way that the user's PIN can be intercepted electronically. For less than the cost of a nice dinner for two, you can have a FIPS 140-1 Level 3 Rosetta smart card, the PAR-2 reader, and the latest version of the Rosetta Executive Suite middleware. The PAR-2 will also work with virtually anyone's smart cards, although the secure PIN entry feature would require our drivers.

But even with that device, you have to have some caveats, among them protecting the PIN from observation while it is being entered.

Now, about the real-world performance of biometric devices. Some good independent evaluations have been done – see http://bias.csr.unibo.it/fvc2002/perfeval.asp for a description of the most recent evaluation procedures, and http://bias.csr.unibo.it/fvc2002/results.asp for the results. But this study only performed 4950 false acceptance comparisons, and the samples were all from a rather uniform sample of university students – no bricklayers, cosmetologists, burn victims or other subjects were included that might be prone to having unreadable fingerprints. And as industry representatives would be quick to point out, this was a form of interoperability test, involving the use of four different readers and several dozen algorithms, which biases the tests against the use of proprietary technique for enhancing the results when used with a specific reader.

As a rough rule of thumb, I would think that a False Acceptance Rate of less than 1 in 100,000 is probably achievable with a False Rejection Rate of a few percent, depending on the population sample. In comparison, a four digit, all numeric PIN, as often used for bankcards, is obviously much less secure against a random guessing attack, and may also be more vulnerable to a PIN caching and replay attack, as well as various social engineering attacks.

On the other hand, a six-character password that was machine generated and uses all 92 characters on the keyboard in a completely random manner would have a probability of a successful random guess of nearly one in a quadrillion. This assumes that the PIN wasn't pasted to the computer screen or compromised in some other way, or course.

Ultimately, the best approach would be to use three factor authentication, requiring possession of the card, knowledge of a reasonable length PIN, and a biometric that produces a decent FAR without too high an FRR. Is that overkill? It depends on the application, and the user's willingness to accept the risks vs. the costs.

Robert R. Jueneman
Sr. Systems Architect
SPYRUS, Inc.
rjueneman@spyrus.com
408/953-0700

SECURED BY SPYRUS™

Digitally signed by Robert R. Jueneman
Reason: I am the author of this document
Location: San Jose, California, USA
Date: 2003.07.28 15:33:35 -07'00'