Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 79 (2001)

Heft: 10

Artikel: The missing link between biometrics and cryptography

Autor: Aufreiter, Richard

DOI: https://doi.org/10.5169/seals-876584

Match on Card

The missing link between Biometrics and Cryptography

Biometric systems of various kinds have been around for quite some time. Despite the significant advantage of saving users from having to remember an increasingly large number of PINs, there has been little global implementation in real IT security applications.

The new capability of certain smartcards to verify the biometric templates of their rightful owner instead of a PIN, might now provide the missing link that hindered Biometrics for so long. Perhaps now, we can expect an explosion of cryptographic applications using Biometrics[1].

RICHARD AUFREITER

What is Biometric Authentication?

Nature has provided humans with many unique biological characteristics that allow us to easily recognise each other in everyday life. When used in computer technology, complex algorithms are needed to recognise and match biometric characteristics of users. However, the advantages are worth the effort since the usage of biometric identification systems for access control will relieve us from having to remember an increasing number of complex passwords and improve authentication security.
Many companies have worked over the recent years to make it possible for computers to identify humans by one of their unique characteristics. You can distinguish between passive ones that can simply be measured, for example

- Face
- Fingerprint
- Iris or Retina pattern
- Hand geometry or
- DNA

and active ones where the person has to perform a certain task, for example

- Voice
- Handwritten signature
- Typing behaviour

The question "Which is the best biometric method?" cannot easily be answered as it depends heavily on the application in focus. All methods differ in cost (mainly for the sensor), user convenience, accuracy, speed etc. Whereas DNA analysis might be very accurate in principle, it cannot distinguish between identical twins and the high cost and low user convenience makes it unsuitable for day-to-day business like PC access. Would you want to give blood every time you logged on to a Windows application? Voice recognition systems on the other hand are low cost, since they simply use a standard microphone as sensor, but can easily be overcome by a tape recorded voice. The same is true for face recognition. The system that might best be suited to IT security is fingerprint recognition. The sensors are now more cost-effective, foolproof and require a low-complexity matching algorithm.

How does Biometric Authentication work?

The principle is the same for all biometric methods. During a process called "Enrolment", the biometric characteristic of a user is measured and a so-called "template" of usually a few hundred bytes in size is computed and stored together with the user's name (ID) in some (hopefully protected) store on a PC or a smartcard. Usually it is not possible to re-create the original measurement data from this template, but this is also not needed.
During authentication, the characteristic of the user is measured again. The template is computed from the actual measurement and compared against the previously stored (enrolled) template. If they are similar enough it is assumed that the user with the ID stored at the enrolment is present (fig. 1 and 2).
A common problem for most of today's biometric authentication systems is if an attacker is able to replace the template or the ID in the database or alter the verification process. The system might then recognise him as a different user and grant access to him. This is a very real threat for all pure software based systems, as they exist today.

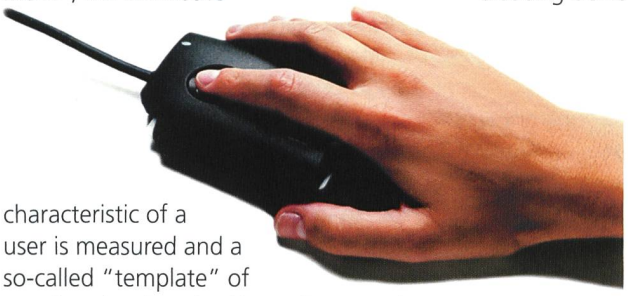

Figure 1. Biometric authentication will become the standard, convenient way of authenticating users to IT systems.

The Digital Identity and Electronic Signatures

Electronic signatures have become increasingly prevalent. Similar to a handwritten signature which represents the will of a person on paper, the electronic signature shall do the same for electronic documents. Electronic signatures allow to identify the user, ensure the integrity of e-mails, transactions and much more. However, electronic signatures require a secret key to be created and a corresponding public key in a PKI certificate to be verified. The most common algorithm for that purpose is RSA. Since a human person is unable to perform the complex calculations associated with an electronic signature, he needs to have a "signature creating device" like a computer with the key stored in a file on the hard disk or a smartcard that does the signing for him.
So how do these "signature devices" identify their rightful owner and protect his secret key from the rest of the world? Until now nearly all pure software solu-

[1] This article has been written as part of a series for ISSE 2001. For more information visit www.eema.org/isse or email: isse@eema.org

by a Biometric verification

Figure 2. A "template" of usually a few hundred bytes in size is computed and stored together with the users name (ID) in a smartcard.

tions as well as smartcards have protected access to the signature key by using a PIN. However, the PIN could intentionally or unintentionally be passed to some other person. Since the device accepts everyone who knows the PIN, you can never be really sure that a certain signature was created by a certain person, you can only be sure that it was created by a certain key.

Can I sign with my Fingerprint?
Unfortunately every biometric measurement, even that of the same user creates slightly different results. Since because of that the measurement itself cannot be directly used as cryptographic key or index in some databases, it must first be compared with a template for similarity. Biometrics can, however, be used to gain access to a signature key instead of a PIN. Since it is not possible to hand over biometric characteristics to another person as easily as a PIN, signature devices that protect their key with biometrics provide a greater certainty that only the rightful user can activate them.

The simple Way – Template Database
Most of today's cryptographic tokens like smartcards or software keyfiles (PKCS#12) are simply protected by a PIN. Their keys provide the basics for all kinds of IT security applications and protocols. In order to combine them with biometric authentication, the most straightforward way is to store the PIN, together with the biometric template, in a database or on the device itself in readable form. If the software detects that an actual measurement fits a template, it reads the PIN from the database and presents it to the cryptographic device. Although this appears very convenient to the user, it has a number of drawbacks for serious applications:

- The security of the device itself is still a PIN. If somebody knows it, he can access the device without running a biometric identification. He might need some alternative application for doing so, but this is no problem for an attacker.
- All the PINs of the devices are stored in a database which can in principle be attacked, whereas before they were only stored in the user's memory.
- The database must be accessible to perform the logon, which might become a problem for roaming users.
- To ask the user for a PIN in addition to his biometric characteristics eliminates the benefit of not having to remember a PIN and gains no true security benefit, since the device itself still relies on the PIN only.

The better Way – "Match on Card"
Smartcards have become increasingly significant in the IT security market since they offer a number of interesting properties:

- The data stored on a smartcard is tamper protected against analysis from outside.
- Smartcards can use keys to perform calculations like signatures without ever revealing the key itself to the outside world, not even the rightful owner. So smartcards cannot be copied, as opposed to software tokens.
- Smartcards are like small computers with the ability to identify their rightful owner. They usually do this by comparing a given PIN to a previously stored value. This value never leaves the smartcard and cannot be read by an attacker.

By the end of the year 2000 the first smartcards, capable of performing a complex biometric template comparison instead of a simple bit-by-bit comparison of a traditional PIN, became commercially available. These cards enable the user to authenticate himself by sending an actual measurement of his biometric characteristic to the card instead of a PIN. The card itself will verify it and grant access if the verification is positive. Using such a technique provides significant advantages both to users and application vendors:

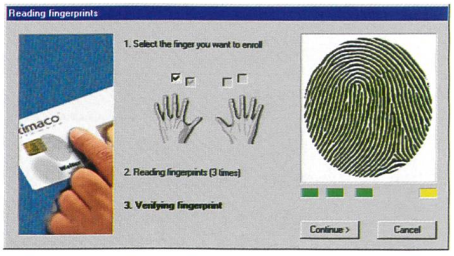

Figure 3. With Match on Card the user does not have to remember a PIN.

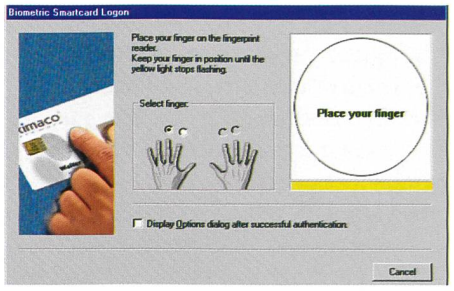

Figure 4. Smartcards are like small computers with the ability to identify their rightful owner.

- No PIN or biometric template is stored anywhere in a database where it can be attacked.
- Privacy concerns are overcome, since the biometric data is not stored outside the user's own smartcard.
- The user does not have to remember a PIN. With Match on Card this benefit can be achieved without paying the price of lower security, as it would be with the database approach, where the PIN is just "hidden" from the user.

Figure 5. The first set of commercially available applications based on Match on Card was shown this year by the German company Utimaco Safeware.

- There are significant advantages for roaming users since all data needed to authenticate the user is stored only on his smartcard, which he carries around with him. They do not need an online connection to some authentication server.
- Existing PKI systems and security applications can be used with little or no adaptation effort. Only the logon method changes, the rest of the cryptographic concepts remain intact. Proper PKCS#11 or cryptographic service provider (CSP) drivers can hide this from the application (fig. 3).

To achieve such a smartcard, a card vendor and a biometric vendor need to work together. The smartcard vendor needs to extend the operating system of the card with a biometric matching algorithm from the biometric specialist. Many large smartcard vendors like Siemens, Gemplus etc. are currently working on such technologies. The first commercially available solution was the combination of the Finnish company Miotec with the card operating system MioCOS and the Swedish company Precise Biometrics, who provided the biometric algorithm.
To fully exploit the practical benefits of this technology and to fulfil customers' security demands requires the added expertise of an enterprise that can build true IT security applications.
The first set of commercially available applications based on Match on Card was shown this year at CeBit by the German company Utimaco Safeware AG. Their product SafeGuard" Biometrics enables a whole range of professional IT security applications to make use of biometrically enhanced smartcards. Besides supporting Utimaco's own product range for file encryption, VPN or electronic signature, SafeGuard" Biometrics provides appropriate standard drivers to also enable common applications like Netscape, Microsoft Internet Explorer or MS Outlook to make use of true biometric logon to smartcards in order to sign and encrypt mails or authenticate SSL sessions (fig.4).

The Biometric Future
With its superior security advantages and seamless integration into existing security architectures, we can expect the new Match on Card technology, together with the rise in smartcard usage, to drive biometric authentication forward to become the standard, convenient way of authenticating users to IT systems. [4]

Richard Aufreiter *from Utimaco Safeware AG has dedicated his career to IT security. After graduating from University in Applied Mathematics and IT (majoring in multiprocessor system applications), he started in 1994 at Utimaco Safeware AG developing smartcard based, strong authentication systems under multiple operating systems. After several years as development team manager, he moved into Product Management and now heads a department for special customer projects and Biometrics.*
Latterly as project manager of the Utimaco SafeGuard" Biometrics solution, he has brought to market the first IT security system using "Match On Card" technology. Richard Aufreiter spoke at ISSE 2001 – Information Security Solutions Europe – which has been held from 26-28 September 2001 at QEII Conference Centre, London.

Zusammenfassung

Das fehlende Glied zwischen Biometrie und Kryptographie

Biometrische Systeme gibt es nicht erst seit gestern. Und trotzdem haben sie sich, obwohl sie es den Nutzern ersparen, sich eine immer grössere Zahl von PINs merken zu müssen, in realen IT-Sicherheitsanwendungen nicht wirklich durchsetzen können.
Die Fähigkeit gewisser Smartcards, statt der PIN das biometrische Abbild ihres rechtmässigen Besitzers zu prüfen, kann nun aber das fehlende Glied sein, das die Biometrie so lange behindert hat. Deshalb ist es durchaus möglich, dass sich die Zahl der kryptographischen Anwendungen, die auf Biometrie setzen, schon bald vervielfachen wird. Smartcards haben im IT-Sicherheitsmarkt in dem Mass an Bedeutung gewonnen, wie ihre Vielseitigkeit zugenommen hat. Gegen Ende des Jahres 2000 kamen Smartcards in den Handel, welche die Fähigkeit besassen, anstelle des bitweisen Vergleichs einer PIN den viel komplexeren Vergleich eines biometrischen Musters anzustellen. Diese Karten erlauben es dem Nutzer, sich auszuweisen, indem er der Karte statt einer PIN das aktuelle Abbild seiner biometrischen Merkmale schickt. Die Karte prüft sie und erlaubt den Zugriff, wenn alles in Ordnung ist. Von einer solche Technik dürfen sich sowohl der Nutzer als auch der Handel einiges versprechen.