

How secure is your biometric solution?

Magnus Pettersson, Mårten Öbrink

Precise Biometrics AB, Dag Hammarskjölds väg 2, SE 224 67 Lund, Sweden

26th February 2002

Abstract

Biometric solutions are installed frequently everywhere from airports to stock broker firms. There are various biometric solutions on the market, the question is: which biometric technology is best suited for my needs? This document is a security overview of different ways to use biometrics to secure computers, networks and digital information in general.

1 Introduction

What should the biometric device be used for? Is it only PC/network log-on? Is it to secure a signing key? Encrypt data? Enter a door? Sign a mobile transaction? These questions are important when choosing a solution. In this Whitepaper we will mainly address logical access, i.e. access to information. A basic application providing logical access is PC/Network logon using biometrics. For this purpose, storing the fingerprint at the local computer or server might be enough. Furthermore, in this case the fingerprint does not represent your digital identity on the Internet, only in your local environment. If the scope is PKI based applications (such as VPN, secure email etc) where a smart card is used for credential storage, that is also where the fingerprint template should be stored.

2 Computer security in general

To choose the appropriate level of security for a system is not an easy task. In most cases some kind of encryption is used, often using *PKI* (Public Key Infrastructure). This infrastructure relies upon digital certificates and the fact that each user has his or her own encryption key (called a private key), which must be protected. Via this key, access may granted to a network, a secure

email may be decrypted, a remote connection may be established to a company intranet etc. The private key is often stored on a smart card since this is a very secure storage medium and very hard, close to impossible, to tamper with. The smart card is protected by a secret, which traditionally is a PIN or sometimes a password. Instead of a PIN or a password, biometrics can be used to tie the identity to a physical person even stronger. However, this must be implemented in a secure way.

3 Different ways to implement biometrics

From a security aspect, the two important parts of a biometric system are

- Storing (on a server, in the PC, in the capturing device, in a smart card)
- Matching (on a server, in the PC, in the capturing device, in a smart card)

Depending on how these parts are combined, the security implications of the system are different. The table below is showing combinations of where the fingerprint is stored, and where it is matched. Some of these combinations are highly unlikely to ever exist in a commercial product and are therefore not discussed. These are marked with an X and will not be addressed further. (A server in this context is a hosted server accessed via the Internet).

Table 1: Combinations of where the biometric data is stored versus where it is matched.

	Store on server	Store in PC	Store in device	Store on card
Match on server	a	X	X	b
Match on PC	X	c	X	d
Match in device	X	X	e	f
Match on smart card	X	X	X	g

4 Security overview

a Match on server / Store on server

Matching on a server means matching in a protected environment. The administrator can monitor the security and detect attempted attacks on the system. The storage on the servers means that also the template is protected from tampering, at least from the outside. Getting users to store their fingerprint templates in a server out of their control may be hard; this requires that the party running the server is trusted. One security problem is the transfer of the template from the

capturing device to the server. This requires a secure Internet session or an intelligent way to solve the problem with cryptography. This solution also requires that a new infrastructure is built, which makes the solution difficult to deploy in large scale.

Conclusion

- + The administrator has full control of the fingerprint database
- The solution may be violating personal integrity
- The solution requires a whole new infrastructure to be built
- The fingerprints are transferred over an open network

b Match on server / store on card

In this case, the template remains with the user on a smart card, hence the problem with storing ones fingerprint template on a server out of your control is solved. The other problem with servers - the transfer of information across an untrusted network is augmented; now both the template and the input image must be transferred. In this case some kind of strong encryption should be applied to secure the transfer. This solution has drawbacks both with regards to security and due to the fact that a new infrastructure has to be built.

Conclusion

- The solution may be violating personal integrity
- The solution requires a whole new infrastructure to be built
- The fingerprints will be transferred over an open network unless an encrypted connection is used

c Match on PC / Store on PC

This is a common combination where the templates are stored on the users hard drive. This is also where the matching takes place. Since the PC is not a secure device there is an immediate threat that secrets such as templates or passwords may be stolen tampered with. Mobility may be a problem; the user can only log on to the computer where the template is stored.

Conclusion

- + The user has got control of his/hers own templates
- The PC is not a secure environment for template storage
- The solution is not scalable even on a local network

d Match in PC / store on smart card

Storing the template in a smart card but match in the PC eliminates some of the problems with variant (c). When a smart card is used it is often access to the protected area on the card that is critical. Access is granted if the correct PIN is sent to the card (the PIN is matched on the card). In this system, both the template and the PIN have to be transferred to the PC from the card, if the input image matches the template the PIN is sent back to the smart card to gain access. The template is not available for hacking at all time since it is stored on a card. But, the critical information (the template and the secret e.g. PIN) is sent to the PC from the card when matching. This means that both the template and the secret can be tampered with or stolen.

Conclusion

- + The user can carry his or her own template (stored in the smart card)
- + The user might use the fingerprint/smart card for accessing multiple devices
- The templates are exposed during verification
- The solution cannot be used for secure network transactions

e Match in device / store in device

In this scenario, no information is exposed in the PC since all information is stored in the device. This makes tampering with the template difficult. This means that the device is more or less personal since without it, I cannot reach my template.

Conclusion

- + The user has control over his or her own template
- + The template is never exposed (if the device is regarded as secure)
- Portability is limited since the template in the device itself and can not be accessed via another device

f Match in device, store on smart card

The roaming problem of (e) is solved here. The matching is also made in a safer place than the PC - the device itself. There is however still a PIN or password involved accessing the smart card. This means that this secret is stored somewhere - probably in the smart card. When the fingerprint matches, the secret is fed back to the card to gain access. Both the template and the secret can be

read from the card without restrictions, which means that the secret can be stolen.

Conclusion

- + The template can be accessed from any device
- + The user is in control of his/hers own template
- The template is exposed during verification (when transferred)
- There is a security hole when using the smart card for storage of certificates (PKI), as the secret to unlock the card is stored on the card and sent to the device before used to access the card

g Match on card / Store on card

Both matching and storing on the card mean that the sensitive data (the template) never leaves the card. There is also no secret to steal since a successful match enables the use of certificates on the card without the need of stored PINs or passwords. Even in the unlikely event that a card is tampered with; only limited damage is done since only that specific users credentials are hacked. An attack on multiple users means that the attacker must get hold of all users' cards This method is normally seen as the most secure way of biometrically securing computers, networks and digital information in general.

Conclusion

- + The smart card is made personal; it cannot be accessed without the appropriate biometric authentication
- + The templates are never exposed to a non-tamper proof environment
- + The user carries his/hers own templates
- + The solution works with a PKI (digital signatures, authentication over networks, encryption) without the need of new infrastructure

References

- [1] Pettersson M., *Match-On-Card Whitepaper* 2000, Precise Biometrics external publication.
- [2] Pettersson M., Öbrink M., *Ensuring integrity with fingerprint verification* 2000, Precise Biometrics external publication.
- [3] www.precisebiometrics.com

For Additional Information

www.precisebiometrics.com

Sweden, Lund

Precise Biometrics AB
Dag Hammarskjölds v.2
SE 224 64 Lund
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

Sweden, Stockholm

Precise Biometrics AB
Box 1223
SE 164 28 Kista
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

USA, Washington D.C.

Precise Biometrics Inc.
8300 Boone Boulevard, Suite 500
Vienna, VA 22182
USA

Tel: +1 703 848-9266
Fax: +1 703 832-0577
E-mail: infous@precisebiometrics.com

Entire contents ©2001 by Precise Biometrics AB. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden.