

Should You Care About Biometrics?

Executive Insight Series

Jonathan G. Gossels & Matthew Martin

Introduction

Why Should You Care About Biometrics?

Many organizations struggle with the problem of authentication; how users prove their identity in order to get access to applications or other IT resources. How strong or how secure does the authentication process need to be? Is the combination of a username and password sufficient? If not, should a token device – like SecurID or digital certificate be required? None of these solutions is without its problems.

In recent years, biometric technology has emerged as a practical alternative that offers a reasonable level of security. This brief paper offers some insight into the key benefits and critical limitations of the technology.

Understanding the term *biometric technology*

Biometric technology is increasingly finding its way from the world of high security applications into mainstream corporate computing environments. Why is that?

First, let's look at what is meant by the term biometric technology. Traditionally, that term is used to describe a whole class of authentication techniques that use physical characteristics either as a substitute for or in conjunction with a password to confirm a user's identity. Historically, fingerprints, retina images, and voice prints have been used.

In typical business applications, biometric usage is restricted to fingerprint analysis. Most users are understandably reluctant to put their eyes near any mechanical device.

Biometrics address ease of use, not security per se

The movement of biometrics into the mainstream is being fueled not solely by companies' desire to improve security per se, but by the recognition that biometrics can reduce user frustration. It is not uncommon in large enterprises for employees to have upwards of a dozen passwords to remember and as companies institute standards to ensure high quality passwords and require passwords to be changed regularly, that problem grows worse

both from a user's perspective and from the company's perspective. The administrative cost of resetting forgotten passwords and the lost work time can be enormous. User frustration increases as well.

What can you count on?

In a large enterprise, the old authentication maxim about something you have, something you know, and something you are degenerates to the following. Something you *know* really means something you forget, write down, or share. Something you *have* really means something you lose or leave at home. Only something you *are* remains the same.

Understanding the obstacles to adoption

There are three primary challenges inhibiting mass market adoption of biometrics for user authentication. They are:

- The output of the biometric readers must become standardized so companies can buy any brand of reader and not be locked into a single source

situation. The obvious endpoint on this path is that simple readers will be built into every keyboard, mouse or laptop.

- Biometric technology must be integrated with mainstream authentication systems. This would allow a single biometric authentication process to be used to log users directly into a full suite of applications and resources. Today, a two step process is usually needed. The biometrics technology is used to authenticate a user to a credential bank. Then, custom software performs the logins to the underlying applications and systems such as NT or Novell.
- The third challenge is enhancing the biometric software to

offer necessary administrative services. For example, many of today's systems store the biometric information on the user's hard disk. What is needed is a way to store that data centrally and securely so it can be properly backed up and managed.

Comparing security and looking to the future

What level of security does a typical fingerprint-based biometric device provide? False acceptance rates are often in the one per million attempt range. That is comparable security to a six digit PIN but less than a well constructed six character password.

Pilot deployments in large organizations have shown that this level of security is often sufficient to satisfy an organization's security requirements for a large number of its users and applications. In those cases, the organization has been able to greatly reduce user frustration and lower administrative costs.

Biometrics is a set of technologies well worth watching.

Matthew Martin is Vice President of Security Engineering for JPMorgan - Chase

Jonathan Gossels is President of SystemExperts Corporation

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Network-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com

info@SystemExperts.com