

Biometric Password Automation in the Enterprise – Issues and Solutions

Author: Harvey Bondar, Vice President

A DigitalPersona® Whitepaper

August 2004

For more information, please contact:

DigitalPersona, Inc
805 Veterans Boulevard
Redwood City, CA 94063 USA
650-261-6070
www.digitalpersona.com



Table of Contents

Introduction.....	1
The Problem with Passwords.....	1
Password Costs	2
Government Regulations/Customer Concerns	2
Alternative Authentication Solutions.....	2
The Answer to the Authentication Dilemma	3
Features That Ensure Security and Ease of Use.....	3
Unprecedented Control Across an Organization.....	4
The Value of Biometric Password Automation.....	4
About DigitalPersona.....	4

Introduction

Passwords were introduced in the 1960s to provide protection for the information stored in computers. They are still the most prevalent method of authentication even though they represent the weakest link in the security chain. In fact, according to the Computer Emergency Response Team (CERT), 80 percent of the security attacks they investigate are password related.

The proliferation of local area networks and the Internet has added to password security issues. Connections to other computers internally and externally give users access to unprecedented quantities of information. They also open the door to ever more sophisticated attacks on passwords and the information they protect.

In response to the growing risk to information security, organizations continually develop more complex password schemes and implement stringent policies to enforce them. However, despite these efforts, unauthorized users are still finding ways around passwords and policies and into computers and networks.

Those unauthorized users are not always outsiders. A 2000 CSI/FBI computer crime survey revealed that 71 percent of unauthorized break-ins were by corporate insiders. That same year, a Cap Gemini Ernst & Young survey published in Bank Technology News showed that in-house staff commits 84 percent of bank fraud.

This whitepaper addresses the problems associated with passwords in today's organizations and describes how fingerprint biometric technology can be an effective solution for improving security by eliminating the vulnerabilities and costs of password based security.

The remainder of this paper describes:

- The problems and costs of passwords
- Alternatives to passwords
- How fingerprint authentication systems work to address problems with password-based systems
- Enterprise features of DigitalPersona's fingerprint system
- Results of DigitalPersona's system in today's organizations

The Problem with Passwords

Most issues associated with password security arise because control of passwords is in the hands of users. Given the choice, users overwhelmingly choose passwords that are easy to remember, assign the same password to multiple applications and keep their passwords for months or years. If users are required to select more difficult-to-remember passwords or are required to change them frequently, they often write them down, compromising the secrecy of the password. Sometimes they even post passwords on their monitors or tape them to their desks so that they can remember them. Users also share passwords with colleagues – and not just occasionally. According to information provided by PentaSafe Security Technologies in a CNET news article in 2002, four out of five workers will disclose their passwords to someone in the company if asked.

In attempts to prevent password compromises, companies develop security policies that specify parameters for passwords and rules for using them:

- Passwords must at least some specified number of characters long and must contain a combination of letters, numbers and symbols
- They must be changed quarterly, monthly, weekly or even more frequently
- Access to each application must be controlled by a separate password
- Passwords must be memorized

While rules like these seem logical from a security perspective, the fact is that they are difficult for people to follow, difficult to enforce and not very effective. Complex password protection schemes are simply not practical for users or for the IT departments that must enforce them. Frequent password changes intended to improve password protection serve to exacerbate the problem. These practices make passwords even harder to remember, increasing the likelihood that users will compromise their secrecy by writing them down.

Password Costs

The more complicated the password protection, the more expensive it is to implement and support. According to Andreas Faruke, head of Deloitte and Touche's Identity Management Services in Canada, the typical enterprise spends an average of \$150 USD per user per year to support password resets. That is \$150,000 spent annually in an organization with just 1000 users, an expense that could be virtually eliminated with a truly effective, easy-to-use, easy-to-implement authentication solution. In fact, the Department of Defense achieved a 90% reduction in password related help desk calls after a biometric deployment. Furthermore, the costs reported here don't even factor in lost productivity and the forensic costs of investigating breached security. Add the frustration of end-users and administrators and you end up with the Molotov cocktail of security.

Government Regulations/Customer Concerns

Government regulations are creating additional pressure to provide better security for private information. For example:

- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to establish security standards that will protect customer information from internal and external threats and unauthorized access via networks and online systems.
- The Health Insurance Portability and Accountability Act (HIPAA) mandates that individually identifiable health information must be kept private and secure. HIPAA, as written, affects virtually all health care-related information created or received in virtually any medium by the health care industry or an employer.
- The Sarbanes-Oxley Act of 2002 requires a need for higher security standards for data that is financial or confidential. According to this Act, any public company may be liable if it has not taken adequate steps to protect this type of data. Many existing password and security policies would not be considered sufficient under Sarbanes.

Laws such as these, coupled with stiff penalties for non-compliance, have forced impacted industries and government agencies to take a closer look at their information security protocols. Compliance with legislation is not the only source of pressure in the areas of data and information security. With the increase in the amount of business being conducted electronically, customers and clients are also demanding safer, more secure communications. Jupiter Research in 2002 found that 80 percent of Internet users would like to see enhanced authentication methods implemented to replace the typical password methods most often used. The role of passwords and consideration of alternatives that are more secure and reliable are key focuses for electronic commerce.

Alternative Authentication Solutions

Over the years, numerous alternatives to traditional password based security have emerged. Organizations have turned to solutions such as tokens, smart cards and Single Sign-On (SSO) to address the weaknesses of password-based systems. Tokens and smart cards offer an added level of security but also add complexity and cost. Tokens are difficult to use and like smart cards, they require a significant upfront investment in deployment and integration with the organizations' applications and network infrastructure. In many cases, tokens and smart cards have been relegated to users who travel or work remotely or who are working with the most sensitive information.

Single Sign-On (SSO) has grown in popularity because of its ease-of-use for the end-user. However, providing a single entry point via a password to multiple systems makes an organization far less secure than a separate password for each system. And organizations are often surprised to uncover the hidden costs and challenges associated with setting up SSO systems. This includes the significant costs required to integrate with each application. To address the security risks of SSO, many organizations feel compelled to introduce a Public Key Identification (PKI) infrastructure, thus adding more complexity in implementation, IT management and user requirements.

These solutions such as SSO, tokens, etc. are covered more extensively in another paper by DigitalPersona: "Eliminating the Password Nightmare: A Comprehensive Review". This whitepaper may be found on DigitalPersona's web site at the following address:
<http://www.digitalpersona.com/docrequest/reqform?doc=15>.

The Answer to the Authentication Dilemma

Fingerprint authentication technology addresses security issues other password protection schemes cannot. Fingerprints are a credential that can't be forgotten, and are not easily shared. Using fingerprint authentication for access control helps ensure that only authorized users can gain access to personal and sensitive information. Protecting access with fingerprints also makes it possible to provide an accurate and documentable audit trail, an important consideration in organizations that must comply with HIPAA, Gramm Leach Bliley Act and/or Sarbanes-Oxley regulations.

DigitalPersona Pro is a biometric fingerprint password automation solution that takes password management out of the hands of end-users. Replacing password entries (and memory requirements) with a simple touch of a finger eliminates the high costs, administrative overhead and security risks associated with traditional password-based protection. It is convenient and cost-effective to implement and manage, easy for users, and most importantly, more secure.

Here's how it works: through the touch of a finger, a user is automatically authenticated against their centrally managed fingerprint credentials in Active Directory. Provided their fingerprint credentials match, their user name and password, and any other logon credentials required for any application or web service are automatically and securely submitted without ever having to type in a password.

DigitalPersona Pro is fully integrated with Microsoft Active Directory (AD), allowing organizations to maintain an identity management system for all of their users. All user information can be maintained in the

network directory for easier management of passwords and better control of security.

Virtually any application can be configured easily to run with DigitalPersona Pro: there's no need to customize applications. Because DigitalPersona Pro is integrated with Active Directory and it includes easy-to-use administrative set-up, the installation can be deployed in as little as a day.

Features That Ensure Security and Ease of Use

Among the features that differentiate DigitalPersona Pro are its password management features and centralized authentication control. Using an "Identity Lockbox" feature, which is a secure and encrypted location within the Microsoft Active Directory, DigitalPersona Pro automatically stores and manages user logon names and passwords for each application a user accesses. Each lockbox can only be "opened" by the person whose fingerprint is registered for it.

Since a simple touch of a finger on a sensor is all it takes to identify a user and gain access to the appropriate lockbox, users no longer must remember passwords, which means there is no need to write them down. Furthermore, a fingerprint cannot be easily shared or duplicated like a password, so the risks of social engineering attacks are dramatically reduced. Additionally, for applications or environments for which there is a high threat of malicious attack, two-factor authentication, a combination of fingerprint authentication and a password or PIN, can be put in force.

DigitalPersona Pro can also be configured to automatically create and assign a randomized password for each application a user accesses. When this option is selected, passwords are automatically entered, created, updated and stored using the DigitalPersona Pro system. This password randomization capability further enhances security because the end-user doesn't know their password: the password can be substantially more complex than a user-selected password and thus protect organizations against brute-force or dictionary attacks.

With DigitalPersona Pro, end-users no longer have to store and remember the myriad of passwords required to log into their applications.

There is little chance that they will forget their fingers when they come to work for the day. Help desk calls plummet. The whole login experience – to the network, to applications and to web services/web sites - is made convenient and users claim, fun!

Unprecedented Control Across an Organization

DigitalPersona Pro includes administrative tools that provide central control of authentication and password management policies. DigitalPersona Pro integrates with Microsoft's Active Directory and Group Policy Object administration tools to allow IT personnel to set authentication policies and enable password randomization for specific applications or users. A wizard-based tool allows administrators to create templates which can fingerprint-enable all Windows, Internet or custom applications. IT administrators can create these templates without the need for programming or professional services assistance. If the need arises, the seamless integration of Pro with Microsoft Active Directory makes it possible for administrators to delete a user's access to all applications simply by deleting that user's Identity Lockbox within Active Directory.

DigitalPersona Pro's fingerprint password automation solution scales to organizations of any size. The complete system consists of a fingerprint sensor as well as workstation and server software. Organizations large and small have found the set-up to be straight forward and far less costly than supporting passwords, where whole Help Desks are assigned to handling expired and forgotten passwords. Rite-Aid is rolling DigitalPersona Pro out to 3,500 stores and DigitalPersona Pro is being used in a consumer banking application with several million customers. The DigitalPersona system is proven to be an effective solution for improving security and convenience for organizations big and small.

The Value of Biometric Password Automation

DigitalPersona Pro's fingerprint password automation solution delivers a combination of security, convenience, ease-of-use and management tools that far outstrip traditional password protection. It provides reliable virtually

impenetrable security for an organization's most sensitive most vulnerable data, yet is the easiest and most cost-effective authentication available.

In addition to security gains, organizations like the Headquarters of the U.S. Department of Defense (DoD) are finding DigitalPersona Pro also saves money. The DoD reported their DigitalPersona Pro implementation has cut 90% of password-related calls into their Help Desk. In fact, DigitalPersona's fingerprint-based system can pay for itself in as little as six months.

Keep in mind that DigitalPersona Pro fully leverages existing investments in Microsoft platforms and in an organization's existing password managed infrastructure. DigitalPersona Pro's fingerprint password automation solution is applied on top of these systems; thus, there's no need for extensive professional services to change applications and networks to support fingerprint biometric technology. However, the benefit of putting passwords into the background is that organizations are no longer vulnerable to end-users who simply cannot comply with password policies and practices in a secure manner. With DigitalPersona Pro, password-based security systems are a thing of the past.

Organizations like Rite-Aid, the DoD, Cargill's Law Department, Sutter Health/CPMC, The Banker's Bank, the Toronto Blue Jays, and many more that have deployed DigitalPersona Pro, are proving that fingerprint-based systems are a reliable, scalable, and easier-to-use form of security for enterprise organizations.

About DigitalPersona

DigitalPersona is the leading provider of fingerprint recognition systems for enterprise and mainstream computing. Founded in 1996 and headquartered in Redwood City, California, DigitalPersona distributes its products through OEMs, VARs, and resellers worldwide. DigitalPersona is a Microsoft Managed Partner and has strategic partnerships with other major computer and peripherals manufacturers. Further information is available at www.digitalpersona.com.

© 2004 DigitalPersona[®], Inc. All rights reserved. DigitalPersona is the registered trademark of DigitalPersona, Inc. in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.