



## **Solving the Weakest Link: Password Security**

A Comprehensive Review

A DigitalPersona® White Paper

By Vance Bjorn, CTO

February 2005

DigitalPersona, Inc.  
1+ 650.474.4000  
[www.digitalpersona.com](http://www.digitalpersona.com)

## Table of Contents

Introduction.....	2
Passwords: The Weakest Link.....	2
The Cost to Organizations.....	3
Alternative Authentication Solutions.....	4
Complete Fingerprint Authentication.....	6
A Look At ROI.....	7
Summary.....	7
About DigitalPersona.....	7

## Introduction

Ensuring the security and privacy of digital assets is one of the key concerns facing corporations today. The need to safeguard these assets from both internal and external threats has never been more urgent. The Computer Emergency Response Team (CERT) reported over 70,000 security incidents in just the first 6 months of 2003.<sup>1</sup>

While IT spending on security continues to rise to meet these increasing threats, every new technology solution that is considered must deliver significant return-on-investment (ROI) and leverage existing technology to be justified in these tough economic times.

Passwords are still the most pervasive tool used to secure today's organizations. As the number of passwords per employee increases, the likelihood of them being forgotten rises. As a result, the costs of managing password-based security represent a growing burden for most organizations. (Figure 1)

- 40% of all help desk calls are for forgotten passwords.
- Each year companies spend up to \$200-\$300 per user trying to maintain secure passwords.
- Up to 15% of annual IT budget is spent on information security.

**Gartner Group**

**Figure 1: The cost of passwords**

Even more problematic, the increased dependence on password-based systems has not resulted in reduced vulnerabilities for organizations. Because many end-user password management practices can't be policed, loose practices lead to passwords being stolen, shared or intercepted.

This paper proposes a new approach to improving security in today's organizations which involves eliminating the use of passwords among end-users.

The remainder of this paper describes:

- The problems and costs of password practices in today's organizations.
- The strengths and weaknesses of most existing security solutions: passwords, tokens, single sign-on, etc.
- How implementing fingerprint recognition technology achieves complete authentication.
- The ROI of fingerprint authentication solutions.

## Passwords: The Weakest Link

Security experts tell us to start by identifying the weakest links in our systems, and to work on improving the security of those elements to mitigate risk. For many companies, password authentication is the weakest link in the security infrastructure.

According to the Computer Emergency Response Team<sup>2</sup> (CERT), 80% of the security attacks they investigate are password related. The vulnerabilities of password-based solutions stem from a combination of the following:

- Humans aren't perfect and cannot be relied upon to maintain a process that is highly rules-based.
- Other, more "job-related" processes compete for attention.
- Certain insiders or outsiders are intentionally looking for ways to compromise the solution.

### *Humans are fallible and predictable*

Passwords only work when individuals use them correctly. Despite established guidelines, the human element often results in a number of common password problems.

---

<sup>1</sup> RED HERRING, "The Global Security Gap", 11/5/03. [www.redherring.com](http://www.redherring.com)

---

<sup>2</sup> CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

- Easy passwords: Users tend to set passwords based on words that they can remember easily, making them easy for hackers to guess. Simple password cracking programs can find many whole word passwords quickly.
- Single passwords for many systems: To avoid remembering many passwords, people often use the same passwords across many systems – including insecure sites where passwords may be sent in clear text. A single password, once cracked, may open many doors.
- Accessible passwords: Longer passwords containing different kinds of characters are harder to crack. They are also harder to remember, prompting many users to write them down often in accessible locations. Strong passwords also result in more Help Desk calls to reset forgotten or expired passwords, in addition to increased employee downtime. The less convenient security is, the more likely it is to be bypassed.
- Accommodating or gullible people: Passwords are subject to social engineering attacks. Four out of five workers surveyed by the security company PentaSafe Security Technologies would give their password to a coworker. A convincing caller can often extract passwords over the phone.

Password issues	Solved?
Written down and easily accessible e.g. Post-it notes	✓
Easy to remember, easily guessed	✓
Single passwords for multiple systems and applications	✓
Stronger passwords increase password resets and support requirements	✓
Subject to social engineering attacks	✓

**Figure 2: Eliminating passwords solves a number of problems**

*One compromised password is often enough*

To make matters worse, many attackers only need to find one password to a system to then employ other measures to gain access to data or systems. One password failure may be sufficient to compromise overall security on every system to which that user has access. It's a frightening

thought, but your information systems are only as secure as your least responsible user.

## The Cost to Organizations

The following examples indicate how large a problem it is for organizations with passwords:

- Too many passwords to remember: “The 2002 NTA Monitor Password Survey found that the typical intensive IT user now has 21 passwords, and has two strategies to cope, neither of which is advisable from a security standpoint: they either use common words as passwords or keep written records of them. The survey found that heavy users maintain up to 70 passwords. Forty-nine percent write their passwords down or store them in a file on their PC. The research shows that 84 percent of computer users consider memorability as the most important attribute of a password, with 81 percent selecting a common word as a result.”
- People talk: “[A recent study] found that four out of five workers would disclose their passwords to someone in the company, if asked. That's the good news. Another study by the same company found that nearly two-thirds of the workers polled at Victoria Station in London gave the pollster their passwords when asked. Their reward? A cheap pen.”

### User Productivity and Support Costs

Arguably, most users will securely manage their identity data (credentials): creating secure passwords and hiding their passwords and/or tokens from others. Unfortunately these conscientious users will inevitably forget their password or token and generate a support call. As users are given access to more accounts, the number of passwords they must manage correspondingly rises.

Between 25-50% of calls into help desks are for password resets and each of those calls cost from \$20-38 per incident. In many cases, the actual cost of a password reset goes beyond the support call costs.

- Loss of employee productivity and effectiveness: When an employee is unable to login and contacts support, the employee experiences downtime and decreased productivity. In a call center environment, this results in less representation on the phone and less customers being assisted.

- Impacts mission critical operations: In hospitals where medical records must be quickly accessed from a shared PC at a nurses' station, stopping to get a password reset compromises patient response time.

## Alternative Authentication Solutions

Since standard password practices are not providing sufficient security for today's organizations, alternatives have surfaced. Organizations have explored everything from making password policies stricter to adopting tokens to using biometrics.

### Stricter Password Policies

Traditionally, user authentication means providing a user ID and a password – a technique that has been in practice for decades. Although incremental improvements have been made to this basic process, such as not sending clear text passwords over networks and requiring "stronger" passwords, the fundamental approach has not changed. Password's weaknesses are well known and are the primary methods by which network security is compromised.

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall... The weakest link in the chain is the people"

**Kevin Mitnick, Oct. 2002, BBC Interview**

The approach of requiring frequent changes and applying complex requirements to passwords tends to backfire, since people forget the new passwords and are even more apt to write them down. Password security policies rely on end-user cooperation, and strict policies motivate users to compromise security. Those who comply tend to generate higher support costs due to forgotten passwords. It's a catch-22, with stricter policies actually lowering overall security.

### Single Sign-On

Single Sign-On (SSO) products simplify the management of password credentials by allowing a single password to provide access to all applications. Ideally, this would eliminate the management of all password credentials, except for one, and give the user free access to all applications with only one logon.

In reality, there are several drawbacks that limit the viability of SSO for many companies. Most SSO solutions require an administrator / programmer to perform complex scripting for each application to be supported. This work is often multiplied over time as applications are updated and their logon screens change.

Furthermore, many security experts consider SSO less secure than using separate passwords. This is because SSO still relies on the end users to create and maintain a secure password and only one password is required to access all of the users' accounts (sometimes called "Single Break-In"). In the end, the combination of high cost of ownership and continued reliance on an end-user to securely manage a password, limit the viability to all but a few organizations.

### Password Self-Reset

Password self-reset solutions have recently gained a lot of attention in light of the growing password problem. These solutions reduce help desk calls for forgotten passwords by allowing users to reset their own passwords without calling for support.

Password self-reset products do not address the source of the security problem; end-users still must create and maintain (manage) a number of secure passwords.

Additional downsides of these solutions are:

- (1) they are not turnkey and often require immense professional services projects to support the integration effort required for each application, and
- (2) while they do significantly reduce help desk costs associated with forgotten passwords, end-user productivity is still impacted as they must perform the password reset.

## Tokens & Smart Cards

Strong authentication solutions typically use a token/smartcard in addition to a password to authenticate users. This is known as “two factor” authentication. Increasing the number of required credentials (factors) is a broadly accepted method of increasing security.

Token- / password-based authentication solutions have been commonly used but limited to where the added security can justify the cost and burden. There is a large upfront and ongoing cost to deploying and managing tokens or smart cards: these solutions typically require setting up and maintaining a private key infrastructure. Users often forget the keys or leave them at their desks. Traditional strong authentication solutions also do not support all applications and do not tightly integrate into the native network directory and management infrastructure. These issues have limited the deployment of token and smart card authentication products only to users who require secure remote access.

## Fingerprint Authentication

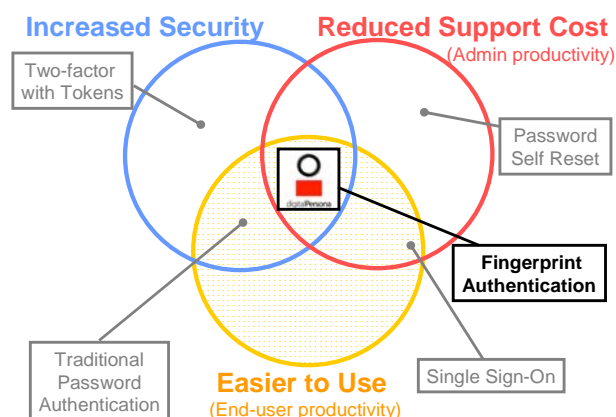
Fingerprint authentication avoids many of the security issues addressed in this paper. In particular, fingerprints are less susceptible to human error.

- Fingerprints cannot be "guessed," shared or written down.
- Users don't have to think up a "strong" fingerprint, so security of the metric doesn't depend on human effort.
- People can't "forget" their fingerprints – eliminating a common source of Help Desk calls.
- Because biometrics technologies use a physical characteristic instead of something to be remembered or carried around, they are convenient for users and less susceptible to misuse than other authentication measures.

## Alternatives Reviewed

Figure 3 reviews various options pursued by organizations to reduce the vulnerabilities of their systems. Many of the tools discussed in this whitepaper such as single sign-on, tokens and password resets fall short of achieving their desired end: increasing security without radically increasing inconvenience and costs.

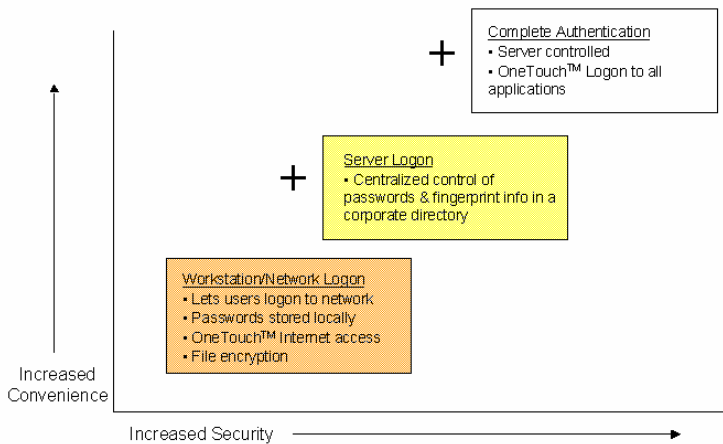
Figure 3



Regardless of how secure a new technology promises to be, if it's hard to use or inconvenient for end-users, it won't be accepted. Organizations face a tough challenge, trying to address increasing security threats without hampering productivity and while keeping IT costs down.

Fingerprint authentication sits squarely in the middle of the three circles in Figure 3. As discussed in this paper, fingerprint authentication eliminates the reliance on users to manage their authentication credentials (passwords, tokens, etc). The touch of a uniquely identifiable finger is applied to make each system more secure. Because it's not possible to forget a finger, fingerprint authentication solutions are much easier to use than most security options on the market today.

**Figure 4: Fingerprint Configurations**



## Complete Fingerprint Authentication

Figure 4 conveys how different fingerprint authentication configurations can produce varying levels of convenience and security benefits:

**Workstation/Network Logon:** Fingerprint authentication solutions installed locally on desktops improve security and convenience. With Windows® integration, users simply touch their finger to the reader and they can be quickly authenticated and logged onto the network. There's no need to remember or type in user account and password information. The information about the user's finger is encrypted and stored locally. The desktop is secured by a solution that cannot be copied, shared or discovered.

Within DigitalPersona's authentication solution, users can take further advantage of fingerprint technology by using OneTouch™ Internet to teach the fingerprint reader to know the logon information of any of their Internet applications. Users can apply their finger and logon quickly and easily anywhere on the Web.

**Server Logon:** Consider storing and matching fingerprint templates on a centralized server. Organizations have even greater control over network logon by moving the authentication process to a secure administrator-controlled environment. It's also possible to take advantage of administrative tools that come along with corporate directories.

**Complete Authentication:** The recommended approach is all of the above plus providing OneTouch™ Sign-On access to any application. No custom integration is required as it uses the existing password infrastructure. A user merely

places their finger on the reader and automatically is logged into all applications, thereby taking password management out of their hands entirely.

Organizations are more secure with a complete fingerprint authentication solution for these reasons:

- End-users are no longer involved in password management. Passwords are automatically applied when they touch their finger to a reader.
- Compromising end-user password practices (e.g. writing them down, sharing them, etc.) are eliminated.
- Audit trails and other tracking tools provide further information on access to applications, which helps meet regulatory compliance.

## Fingerprint authentication and Microsoft Active Directory

Fingerprint authentication can be integrated with Microsoft Active Directory (AD) to take advantage of AD administrative tools and fully integrate with an organization's identity management program.

If integration with a single corporate directory is not feasible, administrators can deploy fingerprint recognition for a division or department, using Active Directory Application Mode (ADAM).

## Enhance system security with multiple factors

Additionally, it's worth considering other measures to reduce risk for high security environments and users. Fingerprint authentication can easily be enhanced with additional security layers (a practice called "multifactor").

1. Add multiple fingerprints to an authentication scheme. This is essentially a no-cost solution, although it requires users to use the readers twice for each authentication.
2. Add a password or PIN to the fingerprint authentication solution for high security applications. Again, this makes it significantly more difficult for an intruder to gain access.

These additional factors can be used to protect specific applications or data, or even classes of users. For example, accounts with administrative privileges could require both a fingerprint and a password. These individuals are likely to be better about password usage than the general population, and the combination of a password and fingerprint raises the bar.

## A Look At ROI

Over the last five years, the costs and viability of fingerprint technology have developed to a state where enterprises can, and are, taking a serious look at the technology for password replacement and enhanced security.

Fingerprint authentication solutions can literally pay for themselves in help desk savings alone. The typical enterprise spends an average of \$150 per user per year to support password resets, according to Andreas Faruke, head of Deloitte & Touche's Identity Management Services in Canada.

There are additional cost savings in user productivity which are harder to measure. If a user on the road can't access the network because they've forgotten a password, then they've lost productivity for that entire period. Embezzlement, fraud or other losses due to unauthorized access can be even further costly to a business.

Considering that fingerprint authentication is more convenient, easier to use and more secure, the decision to go with fingerprint recognition technology is an easy one for many organizations.

## Summary

Passwords are even less secure today, despite more stringent requirements such as 90 day expirations and strings that must be a certain length. Passwords should be managed automatically, where humans aren't required to remember or keep track of them.

Fingerprint authentication creates a more secure environment by requiring users to prove who they are in the most natural way. An individual's fingerprint is mapped to their credentials on a server where identities can be tracked and mapped to their provisioned applications. The whole fingerprint authentication process is more convenient, more reliable, and thus less costly overall. Best of all, fingerprint authentication solutions are much more secure.

## About DigitalPersona

DigitalPersona<sup>®</sup>, Inc. is a leading provider of fingerprint authentication solutions for the enterprise, developer and OEM markets. Founded in 1996 and headquartered in Redwood City, Calif., DigitalPersona designs, manufactures and sells turnkey solutions that resolve password management problems while improving security and regulation compliance.

DigitalPersona has strategic relationships with key market-making manufacturers and resellers including Dell<sup>®</sup> Inc., Hewlett-Packard Company, Microsoft<sup>®</sup> Corporation and Intel<sup>®</sup> Corporation. The company's flagship solution, DigitalPersona<sup>®</sup> Pro, includes DigitalPersona's award-winning fingerprint reader and software application suite, and is used by leading organizations such as the U.S. Department of Defense, Rite Aid Corp., Cargill Incorporated, Telefonos de Mexico S.A. ("Telmex"), the United Bankers' Bank and Sutter Health Network/CPMC.

Additional information is available at [www.digitalpersona.com](http://www.digitalpersona.com).

© 2005 Digital Persona<sup>®</sup>, Inc. All rights reserved. DigitalPersona is the registered trademark of Digital Persona, Inc. in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.