DigitalPersona™ U.are.U® Pro Biometric Authentication Solution

Extending Network Security to Users' Fingerprints

For More Information Contact:

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

Contents

Overview *1*
Passwords: Imperfect and costly in practice *2*
Improving security with fingerprint biometrics *3*
U.are.U Pro biometric authentication system *3*
Reducing authentication costs with U.are.U Pro *4*
Putting the last mile in place with U.are.U *7*

Overview

User authentication and authorization processes are the gatekeepers to your business systems, connecting users to the broader security infrastructure. Problems with the user authentication process can compromise the security of your business systems. The best designed system and application security is of little use if an authorized user gives their password to someone over the phone.

User authentication is proving problematic and costly for many organizations. The situation is analogous to the networking world, in which the "last mile" that connects users to a high-speed infrastructure can be the most difficult and costly to implement. Until we can better handle the last mile of the security infrastructure, the entire infrastructure is at risk. According to the Computer Emergency Response Team (CERT), compromised passwords are involved with 80% of the security problems they investigate.

There is a better way to handle user authentication. Biometric technologies identify individuals based on their physical characteristics. The technology has matured in recent years, and is now ready for mass adoption. Fingerprint biometrics are a viable and practical alternative for user authentication, even for small and mid-sized organizations.

DigitalPersona offers complete biometric authentication solutions – reducing the cost and risks associated with password authentication. Applications range from personal computing to corporate networks to web-based services:

U.are.U Personal	A personal security solution for home computers and small businesses. It lets you switch Windows XP user profiles easily and replaces the use of passwords for frequently-visited web sites. You can also encrypt and lock files with your fingerprint –useful for protecting data on mobile laptops.
U.are.U Pro	A complete, plug and play solution for biometric authentication in the corporate network, including networked administration tools for security administrators.
U.are.U Online	An Internet service that integrates fingerprint biometrics in e-signature security solutions for online services providers. Available either as a hosted service or as server software.

Passwords: Imperfect and costly in practice

The traditional method for authenticating users is using passwords. The theory is simple; if a password is known only to a specific user, then someone providing that password must be who they claim to be. In practice, however, passwords are both insecure and costly.

Password security depends on individuals using them correctly. Research shows that people routinely fail to do so, making the same common errors:

- *Setting passwords to predictable or easy strings.* In an effort to remember their passwords, many people choose obvious or simple password strings. Password cracking software can automatically guess many passwords, particularly those set to whole words.

- *Writing down passwords.* To protect against password theft, companies often require "stronger" passwords with more special characters. These passwords prove more difficult to remember, so people sometimes write them down – often at their workstations.

- *Using the same password across many systems.* People often set the same password on multiple systems – even frequently visited web sites. A hacker having discovered a password on one system is often able to gain access to many other systems.

- *Giving away passwords*. We should know better, but in a recent survey by security company PentaSafe, four out of five people would give their password to someone who worked in their company. Passwords are vulnerable to social engineering attacks.

In addition to the security issues, passwords create administration costs. The more frequently you make people change their passwords, the more likely they are to forget them. According to industry analysts, forgotten passwords can account for between 20 and 50% of a typical company's Help Desk calls. The higher range probably represents organizations with stronger password requirements.

More significant, but harder to predict, are the losses that could be prevented with fingerprint authorization. These include:

- *Loss due to embezzlement or fraud*. With security breaches on the rise, the risk of this loss increases annually. These actions can result either in direct losses or increased insurance premiums.

- *Loss due to outage from a malicious attack*. The direct cost of downtime depends on a business. Web site downtime can cost $50,000 per hour for an average retailer, and millions per hour for large financial institutions. (Source: the Meta Group)

- *Loss due to data on stolen laptops*. Some laptop thieves work airports and ransom the data on laptop hard disks back to the company or its competitors.

Improving security with fingerprint biometrics

Biometrics use physical attributes to confirm an individual's identity. Fingerprints are a tested and proven method for authentication, and can be implemented using relatively low cost sensors.

Fingerprint biometrics eliminate many of the security problems associated with passwords.

- People cannot forget their fingerprints, so there is no need to write them down or call a Help Desk for a reset.

- Fingerprints cannot be "guessed" by an outside hacker. There are simply too many possible variations. Although it is theoretically possible to lift someone's latent prints and fool the scanner, it is in practice difficult to do, and requires a sophisticated attacker in close proximity to authorized users.

- Fingerprints are less vulnerable to social engineering attacks. No hacker can easily call someone else and ask for a fingerprint over the phone. It is difficult to "tell" someone else your fingerprint – you would have to actually put your finger on a sensor to give an unauthorized person access.

The savings in Help Desk calls alone can easily offset the hardware costs of the fingerprint scanners. (See the cost analysis section that follows.) More importantly, biometric authentication makes you less vulnerable to significant losses from security breaches.

U.are.U Pro biometric authentication system

Although fingerprints have been in regular use for a century as a means of identification in law enforcement, the use of fingerprints in a networked computer infrastructure is much more recent. Fingerprint sensors that work well in a controlled law enforcement climate do not necessarily meet the needs of users authenticating over insecure networks.

The DigitalPersona U.are.U biometric authentication system is designed specifically to handle the needs of networked user authentication, addressing the security, privacy, usability, and cost concerns of this environment.

End-to-end security and privacy. Unlike other fingerprint solutions, the U.are.U sensor never sends unencrypted data, even between the sensor and the computer to which it is locally attached. All communication between the sensor and a trusted authentication server takes place on an encrypted, challenge/response link, so data cannot be intercepted and examined or re-used. In addition, fingerprint information is always private. The product never sends or stores a fingerprint image; the U.are.U templates cannot be used to recreate a fingerprint image.

Convenience and usability. The U.are.U fingerprint sensors are simple and convenient to operate. They can read prints from individuals young and old, in less than perfect conditions, with fingers placed at varying angles on the sensor. Setting up the system to identify your fingerprint is a simple process.

Flexibility. The DigitalPersona products integrate easily into different computing environments, whether you are installing on a Windows XP workstation or creating fingerprint authorization for online services.

Cost-effectiveness. Despite the small hardware investment involved in fingerprint scanners, the U.are.U biometric systems save you money relative to password authentication. The following section outlines cost savings for a sample organization.

Reducing authentication costs with U.are.U Pro

Fingerprint authentication using the U.are.U Pro solution is more cost-effective than most password authentication schemes in practice. The savings are due to the reduced cost of administering lost passwords, the reduction in losses due to password-related security breaches, and user productivity gains.

To illustrate this point, we'll consider a sample organization of 200 users connecting via networked workstations, at home or in the office, to company computer systems.

We will make a number of assumptions to create our cost analysis. All of these assumptions are conservative estimates based on either industry standards or analysts' estimates of costs.

- *Cost of password resets*
  The Meta Group estimates that Help Desks receive 1.75 calls per user per month, and 30% of those calls are for password resets. For our 200-person company, this translates into 105 forgotten password calls per month.

  Let's take a more conservative approach and say that only one quarter (50) of the users call for password resets each month. Analysts estimate that a password reset call costs $38 in Help Desk and System Administration time. The total cost per month is then $1900, or $22,800 per year for our sample company.

  This cost scales as your number of user scales. Using the same formula, the per person cost is $114 per year.

- *Cost of embezzlement, fraud, or other losses due to unauthorized access*
  This cost is infrequent, but can be significant when it does occur. Let's assume our sample company has only one event in ten years, for a $1 million loss. Given the fact that security breaches are on the rise, this may be a conservative estimate. This generates a yearly cost of $100,000.

- *Cost of downtime due to attacks caused by unauthorized access*
  Compromised passwords leave your system vulnerable to malicious attacks that may shut down vital systems. The cost of downtime varies between businesses. Let's assume that the downtime cost for our company's site is $30,000 during business hours, and that they experience 2 hours of this downtime every 2 years. This translates into an annual cost of $30,000.

- *Productivity costs of passwords*. Even when things work well, each system logon using passwords takes some time – the time is lengthened for stronger passwords. Assume that each user logs on to 4 systems each day, and that the logon takes 13 seconds for the strong passwords, and only 3 seconds for the U.are.U login. At a loaded salary cost of $40, each second is worth just over a cent.

  For each user, the savings of using U.are.U instead of passwords is then $.10 per logon. If each user logs on to various systems 10 times each day, the savings is $1 per day. For a 250-workday year, that's an annual productivity savings of $50,000 for a 200-person company.

  This cost also scales with your number of users – for larger companies the productivity costs are proportionately greater.

Using these assumptions, the total costs for password authentication for our company exceed $200,000 annually:

	200-person password authentication costs
Password resets	$22,800
Financial losses/fraud	$100,000
Downtime	$30,000
Productivity costs: logons	$65,000
Total cost per year, 200 person company	**$217,800**
Cost per person per year	**$1,089**

Compare these costs to the cost of the U.are.U Pro fingerprint authentication system. Including the server software, the fingerprint scanners, and the software seats, the total hardware/software costs come to approximately $200 per person, or $40,000 for the sample company. Ongoing technical support is an additional 18%.

	200-person U.are.U Pro installation
Password logon time	$15,000
U.are.U hardware/software	$40,000
Technical Support	$7,200
Total cost first year, 200-person company	**$62,200**
Cost per person first year	**$311**

The solution cost is $47,200. If we include the login time of 3 seconds per login, using the same assumptions listed above, then the total cost of using the U.are.U solution is $62,200.

If we compare the total costs, the first year savings alone are over $150,000.

	Password Authentication	*U.are.U Pro*	*First year savings*
Total costs	$217,800	$62,200	$155,600
Per person costs	$1,089	$311	$778

The cost of password resets alone pays for over half of the solution in the first year. Note that these are first year costs only; the savings in the second year would be even greater with the U.are.U system, as there are no new hardware costs.

Larger companies would experience greater savings in both password resets and productivity for logon time, costs which scale with the number of users. For example, we estimated that password resets cost $114 per user per year, while logon time is $250 per user per year.

	Password resets	*Productivity costs: logon*
Per person	$114	$250
200-person company	$22,800	$50,000
500-person company	$57,000	$125,000
1000-person company	$114,000	$250,000

Putting the last mile in place with U.are.U

Returning to the "last mile" analogy, DigitalPersona's fingerprint authentication systems extend the security infrastructure right to your users' fingerprints –