Enhancing Security with Biometric Authentication

Protecting Valuable Systems and Data with the U.are.U® Product Lines

For More Information Contact:

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

Contents

Overview: User Authentication *1*

What's your threat model? *1*

Passwords: A source of numerous threats *2*

One compromised password is often enough **3**

There are many ways to compromise passwords **3**

The attack doesn't even have to be specific to you **3**

The benefits of biometrics *3*

Potential threats to biometric authentication *4*

"Fooling" biometrics: Fake fingers and latent prints *4*

What about intercepting fingerprints? *5*

Enhance system security with multiple factors *6*

Summary *6*

Overview: User Authentication

User authentication is an essential part of your overall information system security. Traditionally, user authentication means providing a user id and a password – a technique that has been in use for decades. Although we've made incremental changes to this basic process, such as not sending clear text passwords over networks and requiring "stronger" passwords, the fundamental approach has not changed. Its weaknesses are well-known and exploited daily.

Biometrics offer a new, better approach to user authentication. As passwords are probably the weakest link in your network and system security, this is one new technology that you may want to adopt rapidly. Since password-based security attacks continue to escalate, the risks of standing still are only growing.

The DigitalPersona™ U.are.U biometric authentication solutions provide convenient and secure user authentication to the desktop, in a networked environment and over the web.

U.are.U can be used by itself or in conjunction with other credentials to suit the needs of organizations requiring even higher levels of network security. A two- or three-factor authentication scheme that includes fingerprint recognition is extremely difficult to fool.

This paper discusses and compares the threats to networked computer systems using traditional, password-based authentication and the U.are.U biometric authentication.

What's your threat model?

Security professionals test security measures against well-defined *threat models*. In other words, what are you protecting your data and systems from? Unless you can identify the threats, it is very difficult to decide if security is adequate.

For most businesses, potential threats include:

- Privacy attacks, in which outside individuals gain access to private information
- Disruptive attacks that compromise business data and/or systems
- Subversive attacks, in which an intruder manipulates the system into non-legitimate activities. Transferring money inappropriately would be an example.

The authentication component of your security infrastructure works with the authorization processes to control access to data and systems. The main threats to these components include outside users gaining access by impersonating authorized users, and legitimate users impersonating other users with different authorization levels. Because user authentication is the gateway to your data center infrastructure as a whole, the potential risks are significant.

In evaluating the security of any authentication technology, you have to consider risks specific to your business.

What kinds of attacks can be launched, and can you protect against them?
Who are your potential attackers?
What kinds of resources will they dedicate to an attack? Time? Money? Both?

If your business works with sensitive government material, for example, your potential attackers may have significant resources available to them. For most businesses and most security breaches, the threat model is less daunting – a disgruntled or dishonest employee, a bored teenager running scripts, or someone with a grudge against your industry in general.

With that in mind, let's compare the potential risks of passwords and fingerprint biometrics.

Passwords: A source of numerous threats

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 (CERT), 80% of the security attacks they investigate are password-related. The password model is fatally flawed at this point. Since it depends on human behavior, it is rarely implemented perfectly and consistently, and there are a large number of people ready and eager to exploit its weaknesses.

Humans are fallible and predictable.
Passwords only work if individuals use them correctly, all the time. Alas, they rarely do, resulting in a number of common password problems.

- *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 some users to write them down in accessible locations. Strong passwords also result in more Help Desk calls for forgotten or expired passwords. 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 someone else in the company. A convincing caller can often extract passwords over the phone.

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.

There are many ways to compromise passwords
The list of potential threats is long.

- The most obvious attack is simply guessing the password. It shouldn't be possible, but many people set passwords to simple strings, or leave them set to a default value.
- Password cracking programs have remarkable success at finding a reasonable number of passwords on many systems.
- Hackers can intercept passwords sent to an insecure site or sent in clear text over a network.
- You can buy an inexpensive device at a local electronics store to track keyboard operations. A disgruntled employee could easily attach the device to someone's computer without it being detected, and intercept passwords.
- Some e-mail viruses automatically send password information back to an originator of the virus. This wouldn't have to be a broad-based virus – someone could modify an existing virus to target your systems.

The attack doesn't even have to be specific to you
Many attacks on businesses and web sites are propagated broadly across the Internet, not against specific targets. Individuals who create scripts to exploit known or published system weaknesses are sometimes referred to as "script kiddies" and may blanket the Internet with attacks. Your potential base of attackers isn't terribly sophisticated; the efforts of a few, technically advanced hackers can be magnified thousand-fold.

For example, a recent attack took advantage of null or default passwords for the system administrator account on Microsoft SQL Server – spawning a whole class of worms that scanned for this vulnerability and exploited it when possible.

The benefits of biometrics

Biometric authentication strategies avoid many of these security flaws. In particular, they are less susceptible to human error.

- Fingerprints cannot be "guessed"

- A user doesn't have to think up a "strong" fingerprint, so the security of the metric doesn't depend on human effort.
- People can't "forget" their fingerprints – eliminating a common source of Help Desk calls.
- It's very difficult to give someone else your fingerprint. (See the discussion of lifting fingerprints below.) Biometrics are less susceptible to social engineering attacks than passwords.
- Because biometrics 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.

Potential threats to biometric authentication

Fingerprint biometrics have a very different threat model than passwords. Using the U.are.U biometric authentication system, an individual logs on to a system or network by putting their finger on a sensor, which communicates with a trusted authentication server.

Potential threats to user authentication using this model include:

- Someone "fooling" the fingerprint sensor with a fake finger.
- Someone intercepting the fingerprint information and either changing or re-using it.
- An unauthorized person gaining access to an authorized user's PC or the network

We'll address each of these potential threats separately. But notice that the possibility for mis-use and human error is much smaller than with passwords. People cannot forget their fingerprints, set them to something easily guessed, or give them to someone else. And they are quite difficult to retrieve over the phone.

"Fooling" biometrics: Fake fingers and latent prints

We cannot argue that it's impossible to fool a biometric authentication system. *Any* technology is vulnerable to attack, given the right conditions, plenty of time and resources. To determine the relevance of the threat, you need to understand what is involved in creating a fake finger that will fool a fingerprint system.

To fool the fingerprint system, you need the fingerprint of a legitimate user. Either you need a willing user who lets you use their fingers, or you have to lift a latent print.

With a willing authorized user, you probably can create a fake fingerprint without a great deal of trouble or specialized chemicals and equipment. Of course, with the help of authorized users, *any* authentication scheme can be compromised. This is, happily, a pretty unlikely case.

Lifting latent prints is more difficult, and requires an investment of both time and resources:

- You have to know which finger or fingers are used for authentication, and be able to get a good print of those fingers.
- Next you have to "lift" the latent print, which requires specialized chemicals.
- Finally, you translate the two-dimensional print into an accurate three-dimensional model.

Potential attackers for the fake finger attack must meet the following requirements:

- The right expertise and equipment to create the fake finger.

- Proximity to an authorized user to get the print. This is not an attack that can be launched from a distance.

- Knowledge of the specific target. This attack can't be launched remotely on a wide range of users. Someone who creates a fake fingerprint has a very specific purpose in targeting your systems.

Note that this group represents a significantly smaller number of potential threats than people who can launch a password attack. There are no script kiddies for this one – and creating the fingerprint is probably just as difficult the third or fourth time as the first, so there are no "economies of scale" in repeating the attack.

If this threat model concerns you, there are easy and relatively inexpensive ways to further "raise the bar" with fingerprint authentication – we'll describe those below.

What about intercepting fingerprints?

DigitalPersona's U.are.U biometric system is designed to authenticate users over network and Internet connections, meeting the needs of today's increasingly web-based businesses. This is a very different model than fingerprint sensors installed in secured locations (such as those used by law enforcement). The DigitalPersona system protects privacy and security of fingerprint data in an inherently insecure environment.

One way to compromise fingerprint authentication is by intercepting data between the sensor and the authentication server at any point along the way. The DigitalPersona sensor is unique in the industry, as it never sends unencrypted data over the network. It creates a challenge/response, encrypted link between the sensor device and a trusted authentication server to protect the integrity of the data. The data cannot be captured and replayed later, as the challenge/response link is time-sensitive.

U.are.U protects the privacy of your employees, as well as your customers and business associates when they use it to access your data, network or web site. In fact, U.are.U stores fingerprint templates, not fingerprint images. Images cannot be recreated from templates, and the templates themselves are stored in an encrypted format.

For more information on electronic security, see the technical white paper "Enterprise Security Architecture for Biometric User Authentication Systems" available on the DigitalPersona web site.

Enhance system security with multiple factors

If the fake finger threat model concerns you, there are several ways to reduce the risk of this kind of attack. The easiest is to enhance fingerprint authentication with additional security layers.

1. Add multiple fingerprints to your authentication scheme. While lifting one print may be easy, lifting several, from different hands, can be challenging. This is essentially a no-cost solution, although it requires users to use the sensors twice for each authentication.

2. Add a password or PIN to the biometric authentication. 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, you could require accounts with administrative privileges to log on with 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 is significantly more difficult to defeat.

There are techniques for rejecting fake fingers in the fingerprint scanner itself. These include some combination of pulse oximetry, flowmetry, thermal profiling, skin impedance. Adding two or more of these measures to the scanning device makes it very difficult to create a fake fingerprint that works.

However, these measures add to the cost of the hardware and may have other side effects, such as additional false rejections and a longer fingerprint scan time. Adding these metrics could put fingerprint sensors out of the price range of small and mid-sized businesses that need the improved security of fingerprint authentication.

Summary

The DigitalPersona U.are.U biometric authentication system offers authentication that is convenient, cost-effective, easy-to-use, and difficult to defeat. Fingerprint systems have a more restrictive threat model than passwords. It's much more difficult to lift a latent print and create a fake finger, for example, than to guess an obvious password or to attack a system with a simple password cracking program. Fewer people have the resources and capability to do so, and the attack must target a specific user in the organization.

If you are concerned about potential malicious attacks using fake fingers, then you can take several steps to augment biometric identification with additional security factors. Regardless, the best way to improve the security of your overall networked infrastructure and data center systems may be to implement biometric authentication throughout the organization.

Your fingerprint is more uniquely yours than any password you may create. Today, your signature serves to identify you in the world of paper-based transactions. Fingerprint biometrics offer the same level of convenience, with the security and privacy necessary in the world of digital transactions and interactions.