

“The Role of Biometric Technology And Single Sign On Solutions As An Alternative To Passwords At Your Place Of Business”

Overview of Previous Article

Our last article reviewed some of the business factors that an emerging business owner needs to take into consideration before implementing a biometric system at their place of business. In particular, such factors examined were conducting a security audit; examining the Rate of Return On Investment by implementing a pilot project; and examining the possibilities of a multi-modal security solution.

Also reviewed were the biometric standards or metrics that you, the emerging business owner need to take into consideration when evaluating products from various biometric vendors. The False Reject Rate and the False Accept Rate are important metrics that need to be evaluated before deciding upon a biometric system for your place of business.

All of the previous articles on biometric technology have examined the tools available from the standpoint of physical access entry applications. However, biometric technology is starting to play a pivotal role as an alternate solution to the use of passwords in business today.

This article is divided into the following sections: (1) The importance of information in business; (2) The role of biometric technology and single sign on solutions; (3) An example of the benefits and advantages to be gained by single sign on solutions.

The Importance Of Information In Business

The information we possess at our company or place of business is one of the greatest assets that we can have, whether it is the customer database or market intelligence about our competitors. However, as business owners, we tend to put much less emphasis on trying to protect this information from internal attacks than external attacks. One of the greatest weaknesses and perhaps one of the greatest threats to our information are the employees themselves-especially the “clueless employees” who don’t mean real harm, but are not trained in proper security procedures.

This is particularly the case with the use of passwords, and the lack of password entropy. For example, employees tend to leave their passwords on Post It Notes sticking to their computer monitor, or share their passwords with other employees. Or, if your employee has access to multiple areas of information at your place of business, thus requiring multiple passwords, the chances for password misuse are greatly increased.

Also, passwords can be easily cracked, if your employees do not put enough creativity in creating them: such as using a birthdate, nickname, or even using the word “password” as a password itself. As a result, this has increased the costs for password maintenance and reset. In fact, the cost now to maintain a password for one employee is \$250 per year.

While this may sound like a small amount, this cost can increase as your business grows and you have more employees.

The Role Of Biometric Technology And Single Sign On Solutions

You can use biometric technology as an alternative to passwords-literally, your fingerprint becomes your password. This has great benefits to you, as an emerging business owner. Employees will not have to remember multiple passwords, and the costs of password administration will be greatly diminished. You could even technically eliminate the use of passwords completely by employing biometric technology.

The use of biometric technology as an alternative to passwords has been referred to as "Single Sign On Solutions." This is so because you need to sign on only once in order to gain access to the shared resources. The most commonly used biometric technologies for Single Sign On Solutions are fingerprint recognition devices. Also, iris recognition technologies are utilized, but to a lesser degree.

The Single Sign On Solution device (if it is a fingerprint recognition device) usually comes in three different formats: (1) Installed on a keyboard; (2) Installed on the mouse; (3) Or a dedicated device (such as a miniature stand alone fingerprint reader). Single Sign On Solution devices which employ iris recognition technology usually come in the form of a small camera, which can be easily mounted on top of a server or workstation. To see pictures of actual single sign on devices (a keyboard and a stand alone USB device), please visit www.htgadvancessystems.com/Advance/products/index.html

Software comes with the Single Sign On Solution device, to allow for either local authentication (for example, your employee logging into their workstation), or centralized authentication (authentication occurs at a centralized point, namely the server). There are drawbacks to centralized authentication, as discussed in the previous article (to see this article, please go to www.technologyexecutivesclub.com/artbiometricsbusinestechicalfactors.htm). Local authentication tends to be much cheaper (typically less than \$150 per device), as opposed to centralized authentication which can be more expensive, because of sever software licensing and maintenance fees. Most emerging to medium sized businesses tend to use local authentication, because of these costs.

There are numerous vendors for Single Sign On Solution technologies. Among the established vendors are Identix, Inc. (they offer a keyboard, laptop, and dedicated fingerprint recognition devices), BioLink Technologies International, Inc. (they a offer a fingerprint recognition mouse), and Digital Persona (they offer dedicated fingerprint recognition technology). The primary vendor for the iris recognition devices is Iridian Technologies, Inc.

An Example Of The Benefits And Advantages To Be Gained By Single Sign On Solutions

As an emerging business owner, there are a number of benefits that can be gained by implementing a single sign on solution. These benefits can be categorized into security, price and convenience. One of the best examples that illustrates these benefits is that of a retail setting. Take for example that you own a retail store, which sells numerous products to customers. Also, you have 10 store employees who work for you. At this store, also assume you have a number of Point of Sale (POS) systems, such as five of them. These Point of Sale systems require your employees to enter a username and password as a means of authenticating themselves into the system.

In terms of security, you have probably set up a security policy which forbids your employees from sharing or writing down their passwords. But the reality is that your employees will write down and/or share their passwords with other employees (I have actually seen this happen on many instances, having been in the retail world). After you become aware that several breaches have occurred, much of your time, as the business owner, is then wasted in tracking down, reprimanding, and resetting the passwords of the suspected employees. However, if you had implemented a single sign on solution (such as fingerprint recognition), this scenario probably would not have happened. Fingerprints are unique to each individual, so therefore, unlike passwords, they cannot be written down, shared, or stolen. Also, by using a single sign on solution, the chances of money being stolen from the Point of Sale system also diminishes. For example, suppose employee #1 told employee #2 their username and password, employee #2 could feel tempted to cover their tracks and steal money by using the username and password of employee #1. By using a fingerprint single sign on solution, each employee is held accountable for their own Point of Sale register, because fingerprints cannot be shared.

In terms of price, there will be costs associated with implementing a single sign on solution, but bigger gains can be realized in the long term. For example, to implement five fingerprint readers (for five Point of Sale systems) at this retail store would cost about \$750 (going on the assumption of \$150/unit). The costs associated with password administration would be \$2,500 per year (for 10 employees, going on the assumption that the average cost of password administration is \$250 per year per employee). Thus, you the business owner, would realize a savings of \$1,750 per year.

In terms of convenience, there is much to be gained. The enrollment and verification processes occur very quickly, with the proper training given to your employees. In fact, verification can take less than one second, which is obviously much quicker than typing in a username and password at the Point of Sale system. This can be a great benefit during the peak times of retail business, when your customers need you the most. For example, as the check out lines build up, your employees will be wasting time in typing their username and password. And if they have forgotten their password, you will have to go back to your office to administer a password reset. With a fingerprint sign on solution, this wasted time will be eliminated, your employees can process transactions faster, and as the owner of the retail business, you can devote much more time and energy

to your valuable customers. Password administration in itself can also be a hassle and a time consuming process. As the business owner, you have to actually write the password security policy, implement it, and make sure it is enforced. With a fingerprint single sign on solution, all of this is eliminated. Finally, single sign on solutions come right out of the package-meaning they can be very easily installed for local authentication. The entire installation process can be thought of as “Plug and Play.”

Our next article will examine implementing a two tier or “multi-modal” security solution for your place of business.