



N•CYCLES

software solutions

Enterprise Biometric Security

A framework for using biometric security in the
enterprise.

January 2003

Hunter Purnell

Dan Marks

| |
|--|
| 65 Germantown Court |
| Suite 205 |
| Cordova, TN 38125 |
| Phone 901-756-2705 |
| Fax 901-758-1597 |
| www.ncycles.com |

Table of Contents

| | |
|--|----|
| Table of Contents | 1 |
| The Enterprise Defined | 2 |
| Biometrics: Life Measures..... | 3 |
| The Case for Biometrics in Enterprise Security | 4 |
| Convenience | 5 |
| Security..... | 5 |
| Usability..... | 6 |
| Present State of Enterprise Biometric Security | 6 |
| Handprint..... | 6 |
| Fingerprint | 7 |
| Retina | 7 |
| Iris | 8 |
| Voice/Speech..... | 8 |
| Handwriting/Signature | 9 |
| Face..... | 9 |
| Movement Patterns | 10 |
| Example Enterprise Scenarios..... | 10 |
| Web Portals..... | 10 |
| Single Sign-On (SSO) | 11 |
| Inter-Enterprise | 12 |

The Enterprise Defined

There is a narrow view of the enterprise that exists today that only includes the network and computer realms within an organization. In order to have an end-to-end sense of control over your users and assets within a particular organization, the view must be broadened a bit. The enterprise should, at a minimum, include the following realms:

1. Physical
2. Network
3. Computer

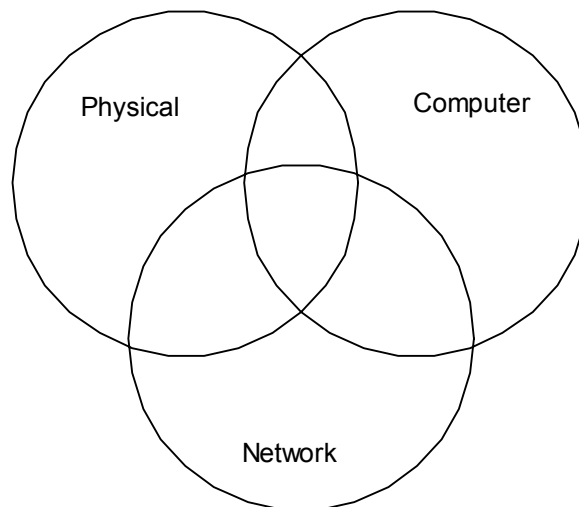


Figure 1

Securing the physical realm consists of protecting a facility or a tangible asset from entry or use. For example, a building is secured from entry, typically, with a lock that requires a key for ingress. Usually securing network and computer assets are grouped together. They are related but very different concerning the task of securing them. The network provides a gateway of use for a computer asset. The network is the first line of defense against unauthorized use of a computer asset. It is an all or nothing proposition when it comes to securing it. An individual can be given rights to access it or denied rights to access it. The computer asset is not that simple. The computer realm can be further broken down in to the following sub-realms:

1. Login
2. Application
3. Data

The login security of the computer asset protects it from any unauthorized access. Again, like the network asset it is all or none. Application security is applied to each individual application that is being run on a computer asset. Each application should have security mechanisms that grant or deny access to the use of the application. This sub-realm is a bit different in the sense that it does not exhibit the all or nothing access characteristics of the previously discussed realms. Security for the application asset is going to depend on who you are and where you are (internal or external). For example, a manager (who you are) will have access to the payroll function of a web based corporate enterprise application that an employee would not have. Also, it might be a requirement for some types of sensitive functions on the same application to be "hidden" if the manager is accessing the application from his home computer versus his office computer. Finally, data is the last realm. The data will typically be the most sensitive part of the entire system. This sub-realm also exhibits the characteristic of access being based on who you are and where you are.

Finally, consider some broad grouping characteristics of security challenges that are employed in the enterprise:

- Something I know (password, PIN)
- Something I have (token, smart card, certificate, etc.)
- Something I am (fingerprint, face, voice, etc.)

In a modern enterprise security system, all three of these broad groupings will be employed. The user's actions and level of desired access will dictate the security policy employed and determine the mix (one, some, or all) of security challenges.

Any single layer can be made more secure by increasing the complexity of the challenge. However, stronger security can also be less convenient for users. Therefore the right mix of challenges and complexity of the challenge will depend on the particular need.

Biometrics: Life Measures

As the name biometrics suggests, the idea behind this emerging technology is to map measurements of human physical characteristics to human uniqueness. If this can be accomplished in a reliable, repeatable fashion, the verification and identification of human individuals by machine becomes a reality. To that end, biometrics is a fusion of human physiology, pure mathematics, and engineering. The idea of biometrics is very simple to grasp, but the implementation can be daunting and very difficult to realize. The difficulty does not come from the gathering of the actual measurements but from the analysis of these measures. As with most pattern recognition problems, more data can always be gathered. The problem is what to do with it after it has been gathered. Enough measurements have to be taken to assure uniqueness of each individual. There is a fine line not having enough data and having too much. Too much data can cause an "aliasing" effect, where individual uniqueness is lost.

Also, the application of the biometric device has important ramifications on how much data should be collected. Simply verifying someone's identity is much less complex than identifying a person. Verification vs Identification might seem like semantics, but think about the difference between checking someone's driver's license photo and recognizing someone in a packed room who you've never met. Verification involves having someone tell a biometric system she is Jane Doe and then using one or more set of biometric information to verify that

she is in fact Jane Doe. Identification would be Jane Doe walking up to a set of Biometric sensors and being recognized as Jane Doe. If you have seen the movie *Minority Report*, the mall stores biometrically identify Tom Cruise as he moves from store to store. The increased complexity of identification means that reliable identification is still some years away from being perfected, which is why the Superbowl elected not to try to use Biometric identification techniques. On the other hand verification is extremely reliable today and for some security applications is quite appropriate for either increased security or ease of use.

Depending on the application and objective, different “form factors” are more appropriate. The predominant biometric form factors today are:

1. Handprint
2. Fingerprint
3. Retina
4. Iris
5. Voice/Speech
6. Handwriting/Signature
7. Face
8. Movement patterns (i.e. typing, walking, etc)

The Case for Biometrics in Enterprise Security

The use of biometric verification and identification have so far been limited to a few Hollywood movies. The public seems to view biometrics as futuristic if not scary, even though these technologies have been around for the past several years. The reality is this: the form factors discussed in this paper are real and work. The issue becomes how to apply them appropriately. Companies want to rush to the market with a really cool technology without a real problem to solve. This is the case with early biometric solutions. The early implementations were burdened with the fact that they were not as reliable as hoped for and prospective customers did not see the need to deploy yet another security technology that at the time only looked like a fancy replacement for passwords during computer or network login. This is all beginning to change. The important thing to focus on is the *application* of the technology. The technology is much more robust than it was in years past. Some of the technologies, fingerprint for example, are beginning to put up 99% correct verification rates.¹ Some of the technologies, such as facial and speech recognition, will always be plagued by ambient environmental factors such as lighting and limited bandwidth communications channels (cell phones). These technologies will not be able to function alone in an enterprise security system, but can be an important part of group of technologies that are used in conjunction with one another to strengthen the whole (see the future section of this document). With all of this said, let's look at a few factors to consider when applying biometrics.

¹ Reference the latest fingerprint recognition “shoot-out” in which Bioscrypt scored 99%+.

Convenience

This will be the number one factor for most customers concerning the deployment of a biometric system. Security systems will be forced to become more stringent in the days to come. This means that, at the low end, password policies will be modified to increase the frequency of changes to a user's password. Most organizations today are forcing users to change passwords at least every thirty days. Most of these policies also do not allow the user to reuse the past 5 passwords. This causes a user one extra headache and a reason to circumvent the security practices. This also causes more calls to the help center to reset forgotten passwords. Frustration rises and time wasted to achieve the higher level of security. Passwords are also going to become longer and be machine generated. This will really cause user frustration and lost of efficient use of protected physical/computer/network assets. The password is the predominantly deployed verification mechanism in all of enterprise security today. The password is considered "something that I know". The convenience provided by a biometric device that represents the user's identity ("something I am") mapped to the user's password or PIN is very high. If the user obtains use of a physical/computer/network asset only using a biometric, the convenience of the security system is greatly increased. Also, the security of the system can be bolstered without affecting the user. The password could be changed every 10 minutes and made to be 32 characters long, if the security policy so demanded. The user would only have to bring their biometric along.

Security

Incorporating biometric devices into the enterprise security architecture increases security by eliminating the ability to share passwords and making it much more difficult to counterfeit or steal the security key. The level of security provided by a device also depends on the number of "reference points," which are the individual metrics taken in each scan. For instance, Iris scanners capture 200+ while fingerprint readers typically capture around 80. However, the effectiveness of the reference points also depends on the algorithms used as well. More reference points can mean more false negative identifications. In other words, better accuracy can actually result in rejecting the right person. While more reference points theoretically means a better "signature," it can also mean that there are more chances for failure in the secondary scan. This problem is more pronounced in difficult environments or where ambient noise or light can impact the scanning environment. The original Iris scan could store all 200 points correctly, but if the person using the device is not positioned correctly, then the scanner could not pick up each reference point properly. The individual sensitivity settings on a device controls whether it will err on the side of caution (rejection) or convenience (acceptance). Setting the sensitivity too high can result in too many False Rejection Rate (FRR) and setting it too low can increase the False Acceptance Rate (FAR). When used with multiple form factors, lower individual levels can provide fewer false acceptances or rejections because of the multiple points of reference.

Since biometrics rely on "something you are," obviously other people will not be able to use them. Some movies have included examples of killing a person and then using the deceased's finger, hand, etc. In *Mission Impossible*, someone used a molded rubber copy of a person's hand. Both of these approaches would be extremely difficult if not impossible to use to defeat even today's biometric sensors. In the future, multiple form factors will be used at the same time to reduce the likelihood even further. Multiple form factors refers to using, say, fingerprint, voice, and movement pattern recognition at the same time to make it even harder to effectively counterfeit someone's identity.

Usability

Various biometric sensors require more or less involvement on the users' part. Even more importantly, the nature of the signatures collected impact the ease of enrollment and implementation of the equipment. Another more important aspect of usability is whether a device is intrusive or non-intrusive. Intrusive devices such as retina, fingerprint, and handprint require users to touch or be very close to the sensor. Non-intrusive devices such as iris, facial recognition, and voice generally can operate at less intrusive distances. The level of the intrusiveness varies by device (fingerprint is much less intrusive than a retina scanner). As we discuss the various form factors, we will comment on the particular usability challenges inherent in each choice.

Present State of Enterprise Biometric Security

This next section provides an overview of the main types of device "form factors" available for practical use today. Each one is in various stages of refinement, although all have some useful applications. In addition to discussing each one, we will also rate them along the same dimensions defined above: Convenience, Security, and Usability. Of course, your particular circumstances may modify these ratings, but by providing an overall sense of the relative characteristics, we hope to provide a better idea of the general tradeoffs among the devices.

Handprint

Handprint is probably most familiar from spy movies where top-secret rooms have a pad for handprint use. While the actual details are different in reality, the basic idea is the same. Handprint is usually most appropriate for fixed physical locations requiring very high assurance of identify since it combines the hand biometric with essentially five different fingerprint biometrics. Fairly large physical assets such as buildings are necessary simply because of the size of the sensor. Imagine how awkward a full hand print sensor would be on a desktop let alone a notebook computer. The security and reliability can be even further enhanced by combining a handprint with really any of the other form factors. Cost is another factor limiting use of handprint readers to mostly larger physical assets. The system vendors typically specialize in door lock type systems. While there are many vendors incorporating handprint readers into attendance or security products, the main provider of the underlying technology is Recognition Systems. We see handprints continuing to be used primarily for the traditional applications in for data rooms, sensitive office zones/buildings, national security/intelligence facilities, and vaults. However, handprint reader use for normal commercial and light industrial building access is waiting for identification algorithms to become reliable so that building managers can stop issuing access cards.

| | |
|-------------|----------|
| Convenience | Moderate |
| Security | Moderate |
| Usability | Moderate |

Fingerprint

Fingerprint biometrics involve a finger size identification sensor with a low-cost biometric chip. Fingerprint provides the best option for most uses of biometric verification, especially attached to specific computer and network assets. The relatively small size and low cost allow them to be easily incorporated into devices and are fairly reliable. Many PC manufacturers are experimenting with integrating the devices either on keyboards mice, or the actual computer case. Dell seems to be the furthest along although all are working on it. For now, actual implementations have used third party devices such as **Identix, Authentec, Veridicom, Secugen, Sony, or Infineon**. Most stand alone fingerprint readers sell for \$75-150/each at retail, making it one of the most affordable form factors. I have worked on an implementation for a large pharmacy benefits manager using the **Authentec device**. In addition, many integrated devices such as time clocks are incorporating biometric fingerprint readers.

Fingerprint biometric devices must be distinguished from simple fingerprint recorders. Some banks are starting to implement simple fingerprint recorders to provide more security in check cashing operations. This is simply taking a snapshot of the fingerprint to aid in tracking and prosecuting check fraud. We have assisted clients in running feasibility studies using both recorders and actual biometric verification devices. Most choose to run pilot programs and/or implementations with the biometric verification devices because of the greater security and convenience it provides.

| | |
|-------------|----------|
| Convenience | High |
| Security | Moderate |
| Usability | High |

Retina

Retina scanning involves examining the unique patterns on the back of a person's eye. The retina is the part of the eye that translates light into the electrical impulses sent to the brain. Because of the complexity of current scanners, most retina biometric devices require a relatively large footprint. Some manufacturers are working on ways to install or simply place retina scanners on top of computer monitors. However, most are still used to protect fixed physical assets. Using a retina scanner is also less convenient because the user must position himself a certain distance away from the scanner and then rest his or her head on a support or look into a hood. This is necessary in order to effectively read the *back* of the eye.

The leading provider of Retina scanners is EyeDentify, the last time we checked, EyeDentify had pulled its Retina product off the market in order to try to reduce the cost from around \$2,000/unit to more like the \$400-500 range.

| | |
|-------------|----------|
| Convenience | Low |
| Security | High |
| Usability | Moderate |

Iris

Iris scanning is similar to retina, but the scanner is looking at the unique patterns on a person's iris. This is the "colored" part of the eye and is visible. Retinas are on the inside back of the eye ball. A key benefit for Iris over Retina is that iris scanners do not need to be nearly as close to the eye and do not need the eye to be as precisely positioned.

The leading provider of Iris scanning hardware is Panasonic and Diebold has experimented with adding iris scanners as an integrated option in part of its line of ATMs.

| | |
|-------------|----------|
| Convenience | Low |
| Security | High |
| Usability | Moderate |

Voice/Speech

Biometric verification using speech is uniquely appealing simply because no specialized recording device needs to be used. Biometric verification using a voiceprint is completely a matter of the algorithms and analysis software. This opens up the possibilities of being able to use it for phone-based applications such as voice response systems and time card entry.

The possibility of using voice verification to make secure remote data reporting applications more convenient in the criminal justice and healthcare industries is extremely promising as well. Sexual Offender databases could be made much more reliable if each offender had to call in periodically to provide updated contact information. The entry could be authenticated via his or her unique voice pattern and recorded. Any offenders who missed their deadline to call in would be flagged for further investigation. In healthcare, people on home care or hospice could use voiceprint secured telephone systems to report progress or request prescription refills. In a similar way, home care nurses could use voiceprint authenticated systems to report after each patient stop.

Voiceprint biometric identification has been developed most extensively by the NSA in order to assist in electronic espionage, but as commercially available software continues to evolve, then an increasingly wide range of applications will become feasible. This will primarily enhance the convenience of voice-based authentication systems as well as enable new applications. For instance, marketers would love to enhance telesales centers with the ability to identify the caller by his voiceprint in the first few seconds of a call in order to supply the telesales agent with all available information about that individual. This would reduce the inaccuracy of relying on caller id to guess who is calling.

| | |
|-------------|----------|
| Convenience | High |
| Security | Moderate |
| Usability | Moderate |

Handwriting/Signature

Biometric verification via handwriting or signature must be distinguished from simple signature capture pads. Unlike a signature capture pad which simply records an image of what the person wrote, biometric enabled capture pads actually record the pressure, distance of strokes, and speed of writing. These data points enable biometrically verifying whether the person writing the signature is indeed the same person who supplied the original enrollment sample. Depending on the threshold settings used, the biometric device could flag potential forgers. Even if a forger duplicated the exact image of a signature, the pressure and speed would be different from the genuine signature. However, the tradeoff between false positives and false negatives is particularly fuzzy here because people vary the way that they sign their names, particularly at earlier ages. Setting the threshold too tight will cause genuine signatures to be rejected. Setting the threshold too loose will let forged signatures pass.

Biometric signature verification is particularly interesting to the financial and legal communities because it is substantially less obtrusive and requires less behavior modification. It still feels like a signature – just digitally captured. However, for frequent authentications such as computer and network logins or physical asset access, signatures are less ideal because they just take longer than simply using a thumbprint reader.

Vendors of signature verification solutions include Cyber-Sign and Communication Intelligence Corporation.

| | |
|-------------|----------|
| Convenience | Low |
| Security | High |
| Usability | Moderate |

Face

Face recognition involves scanning the unique features of a person's face. Because some aspects change over time, this is a less reliable form factor. Face recognition is less attractive for up-close verification than for long distance identification. Once a person is close enough to a physical asset in order to get a high quality biometric scan, other form factors are viable and are currently much more reliable. However, eye, hand, and finger are practically worthless at distance and the quality of voiceprint identification degrades rapidly with distance. Therefore, face recognition holds the most promise for remote identification. Security teams for Super Bowl XXXVI considered using rough forms of facial identification to help spot terrorists, but shelved the idea because of the current limitations. It will be several years before remote facial recognition can be cost-effectively used to monitor workplaces or remote physical assets.

Similarly, non-security applications for facial recognition are probably even further off mainly for privacy reasons. CRM specialists drool at the thought of being able to record and then use facial prints to identify customers when they enter a store or restaurant.

| | |
|-------------|------|
| Convenience | High |
| Security | Low |
| Usability | Low |

Movement Patterns

The Movement Pattern biometric form factor is a little harder to grasp. It involves monitoring the way that a person moves (types, walks, etc.) and guessing their identity. The measurements involved are more complex because they must combine spatial and time series data. Also, the scanning required to accurately read the movements still depend on ensuring a consistent angle of observation. The subject must walk by the sensor at the same angle as the measurements are taken. For this reason, typing is probably the most promising current form factor since the observation area is relatively fixed.

| | |
|-------------|----------|
| Convenience | High |
| Security | Moderate |
| Usability | Low |

Example Enterprise Scenarios

Web Portals

The most obvious scenario for biometrically securing a web portal is for online banking or online financial aggregation. As larger banks such as Citibank and Bank of America continue to push account aggregation, these two areas will gradually merge. Consumers may be more willing to aggregate their online accounts with an institution that protects the aggregation point with biometric verification. This could potentially increase the switching costs for users even further by making it harder for consumers to change account aggregation points, if not entire banks. Currently, customer loyalty is highest for consumers using online bill payment and this could increase by securing it through biometric authentication.

However, the traditional mega portals are also strong contenders to benefit from biometric security. Yahoo, AOL, and MSN are all trying to push different single sign on strategies to make it harder to use competing services. Yahoo has the Yahoo ID and Microsoft has Passport. However, adoption has been slower than each company would prefer perhaps because users are hesitant to trust one particular entity as their online gatekeeper. At least part of this fear is that it makes their personal information more susceptible to compromise since it is consolidated in one single location. There are other privacy reasons, but the security reason is a major factor.

However, the major factor affecting all of these scenarios (and severely limiting the adoption by other types of public web portals) is the simple question of enrollment and access. Before a biometric can be used, it must be enrolled (recorded). Enrollment can be either handled in a secured location or remotely via "self-enrollment." Both have limitations. Physical enrollment provides the best assurance of security because a person must travel to a physical location and present some other type of identity verification to the person handling the enrollment. This provides the highest probability that John Doe's biometric is indeed John Doe. Self-enrollment involves generating a temporary password that John Doe would use to log in for the first time and then use his or her local biometric reader to enroll. This is more convenient, but introduces a greater probability of fraud. Identity thieves could still steal personal information and open an account using the self-enrollment approach. It is much more difficult with physical

enrollment. Physical enrollment would be very costly for the true web portals unless they contracted with some other type of business such as Kinkos that already has a communications infrastructure and a national presence. However, this would still not be as secure as true physical enrollment. Banks would probably have the easiest time implementing physical enrollment because most already have branch networks near or within the areas where customers live and work.

Access might be a harder problem to overcome, at least at current biometric scanner prices. One of the benefits of web portals is that they provide almost universal access, from any internet-connected computer. Current biometric devices are not compatible with each other. This means that if a bank wanted to offer biometric security for its internet banking that it would have to physically ship a compatible biometric scanner to the consumer who would then have to install it before using it. Even if the bank wanted to invest in the ability to handle a variety of form factors and manufacturer's devices, the user would still need to access his or her account from a computer using a device that was compatible with the one that he or she used to enroll on. This means that if John Doe enrolled on his home computer, he could most likely not check his account balance on his office computer, let alone a friend's computer. The access problem will not be solved until a global standard for biometric signatures is agreed upon or a single device manufacturer obtains massive market dominance.

Mainly because of the current incompatibility of devices, we do not see widespread use of biometric security for public web portals for quite some time. More limited use within enterprises are certainly more feasible, but still present problems anytime that a user would need access to the portal from a computer from outside the enterprise.

Single Sign-On (SSO)

Traditional single Sign-On initiatives are concerned with consolidating every computer-based authentication into a single set of credentials so that a person only has to remember one password or token. However, biometric security devices allow the concept of single sign-on to extend to the physical layer as well. A person would only have to enroll once to let his or her biometric characteristics give access to every door, computer, or application that he or she needs access to. Fingerprint readers make sense in this environment because they can be deployed relatively cheaply and in a variety of different type of locations. More importantly, they can all be integrated into the underlying network, computer, and physical security systems. It is feasible for an organization to have a central enrollment point for biometric verification of both network passwords and physical security doorlocks. In order to be effective, the company must be able to control the access privileges and in order to be administratively cost-effective, they need to be integrated with network, application, and physical security systems. In our work for the pharmacy benefit management organization, integration down to the application level was critical to achieve the security benefits sought without slowing down the workflow involved. The client wanted to be able to have pharmacists "sign-off" on a particular case via intra-session fingerprint verification. It could have extended to other applications or even the physical level just as easily. We believe that as other organizations attempt to take advantage of the security advantages provided by biometric verification, the flexibility to integrate directly down to the application level will be critical to avoid impacting workflow speed and operator frustration. The necessity of making verification dependent on an almost infinite different combinations of business rules increases the need to have complete control over the device and identity storage methodology selected within the enterprise.

Inter-Enterprise

To our knowledge, no financial institutions are actually using real-time biometric identity verification at the time of transaction mainly because of the enrollment problems. In order for it to be feasibly convenient, a person would need to be able to enroll once and then authenticate a transaction at many if not all potential transaction locations or websites. A couple of start-up companies are offering biometric verification-based check-cashing systems to localized retail stores (primarily liquor stores and grocery stores). Most of these systems require separate enrollment at each location and are not integrated with the rest of the enterprise. However, BioPay provides a inter-enterprise solution to biometrically verify check transactions. The company has inked a deal with Kroger to run tests with a centralized database so that customers can use a variety of Kroger locations after enrolling only once. The system is sufficiently integrated to allow customers to both cash checks and verify check purchases with a biometric signature. BioPay is attractive because it offers a centralized database of bad check writers that depends on the biometric signature and not the particular account number or name.

We see two different primary uses for for fingerprint verification evolving: 1) centralized 3rd party inter enterprise transaction facilitators and 2) enterprise specific workflow security.

The first case will be for verification of identity, primarily in consumer-focused transactions. Consumers would rather enroll once with a trusted provider and then be able to use verification devices at a variety of transaction origination points. Consumers will be reluctant to enroll at all unless they trust the institution enough to safeguard their most private financial and/or medical information. Also, consumers will quickly become annoyed if each institution requires separate fingerprint enrollment because of the relatively larger hassle of having to be physically present to enroll. Besides the check cashing/payment security that BioPay provides, ATM transaction security is another prime example of a situation where a centralized provider will make sense, unless a biometric signature interchange standard emerges. For biometric verification to make sense to consumers, they must be able to enroll at their home institution and then use any ATM. Prescription identity verification is another area where a centralized 3rd party verification system makes economic sense because a patient needs to pickup prescriptions from a variety of locations and providers. They would rather not enroll with each chain separately, although with the consolidation in the pharmacy business this may become less of an issue.

For intra-enterprise security applications, the details of the implementation can be controlled within an organization while the scope of integration and application replacement will depend on the scope of the organization and the desired level of deployment.