

The Use of Biometrics to Combat Identity Theft Over Virtual Private Networks

The term Identity Theft most often calls to mind the assumption of one's identity when someone co-opts critical personal information. There are other types of Identity Theft however. The form of identity theft with the most impact on business entities is the compromise of legitimate users' authentication credentials by another, thereby exposing corporate information and resources to an illegitimate user. The growing deployment of Virtual Private Networks (VPN) throughout the business community has created a significant risk to corporations from this type of Identity Theft. This paper discusses the threat potential of this type of Identity Theft and explores Biometrics as an alternative for securing this vulnerability.

Executive Summary

VPN's are being deployed at breakneck speed as large organizations seek to take advantage of the cost savings to be realized by switching from leased line WAN to the public internet and Small and Medium Businesses (SMB) now have a cost effective way to connect remote and virtual offices. Yet in their fervor to capture the cost and competitive advantages afforded by implementing VPN's, many organizations unwittingly increase their exposure to security risk by failing to secure the great weak link in their security infrastructure – the Username/Password.

Despite the protection afforded by the encrypted VPN tunnel and security policies at the firewall, when deployed without strong user authentication, companies increase the risk that someone will penetrate their corporate LAN by posing as a legitimate user by compromising a username/password. Ultimately, how does one insure that a remote user is who they claim to be? Generally, one strengthens the authentication process by adding additional 'factors'. The factors most often used today are "What You Know" – e.g. a password and "What You Have" – e.g. a hardware or software 'token'. The advent of practical biometric technology now offers the IT manager a third authentication factor – "What You Are".

The inconvenience and complexity of basing an Authentication System on "What You Know" and "What You Have" often means that security personnel end up with a system having an increased cost and reduced security benefit than what was expected. Biometrics on the other hand, provide a system that is both more convenient and more secure meaning that ultimately, the security manager has the opportunity to adopt an authentication method that provides a greater ROI when one considers both the security and ease of use and a lower TCO when one considers the reduced administration costs.

This paper explores the limitation of Authentication Systems based on "What You Know" and "What You Have". It investigates the option of employing Biometrics for authentication purposes and, in reviewing the biometric technology life cycle, discusses why Biometric Authentication has come of age as a cost effective alternative for the IT Manager, SIO, CIO and CFO.

The Growth of VPN's

The proliferation of VPN's is truly remarkable yet not unexpected when one considers the cost saving involved. Many large organizations are replacing their Wide Area Networks built upon Frame Relay and ISDN links and are realizing substantial savings that can be had by using the public internet rather than private leased lines. Also, many Small and Medium sized Businesses (SMB) who could not afford to implement leased lines now have a cost effective means to provided connectivity between remote offices. VPN technology coupled with the web-savvy businesses of today has created virtual corporate communities where Remote Offices, Mobile Users, Customers, Partners and Suppliers all have access to segmented portions of the corporate network, thereby creating an more efficient and efficient means of communicating with these various corporate stakeholders.

Because of the Capital Expense (CAPEX) and Operating Expense (OPEX) cost savings and the competitive advantages afforded by VPNs, the consensus estimated from various research groups indicated that the global VPN market will expand from US\$10 billion in 2003 to US\$35 billion by 2006.¹ This is a Compound Annual Growth Rate of over 50%!

The Inherent Risk of VPN's

The tremendous growth in the deployment of VPN's brings with it an incredible security risk. But where is this security risk? Any security strategy is limited by the vulnerability present in its weakest link. Let's explore the VPN architecture in search of the chink in its armor. First, we have the Firewall. All VPN's require a Firewall. Firewalls are necessary to keep unwanted packets out of the local network when connected to a public network. Given the large choice and wide range of capabilities of Firewall products on the market, this area of the VPN should not present an extraordinary threat.

What about the VPN tunnel itself? Most VPN's are implemented using IP-SEC protocol. This protocol provides security over the network and transport layers of the VPN. The IP-SEC protocol allows administrators to define lists of applications and networks to which users will have access as well as IP Addresses, ports and protocols that are authorized for use over the VPN tunnel. Emerging protocols such as Point-to-Point Tunnel Protocol and Layer 2 Tunnel Protocol provide additional security over the VPN tunnel. Hence, no extraordinary vulnerability lies here.

Finally, lets examine the VPN User Authentication. User authentication for establishing a VPN session is normally controlled at the firewall. Although some sort of Challenge-Response mechanism is required to authenticate a user, the default method of user authentication is the simple Username/Password. Herein lies the great vulnerability of VPN and most other network security strategies.

The great risk in the deployment of VPN's is that they extend the weak link of the Username/Password beyond the perimeter of the corporate walls. Companies, in their headlong drive to take advantage of the cost advantages of deploying VPN's and comforted by the security afforded by the Firewall and VPN tunnel, are deploying VPN's without shoring up this weak link.

In the days of leased line WANs or when SMB's operated only closed networks, the username/password was an adequate authentication method because it effectively carried with it some level of physical access control. To breach a corporate network, a hacker first had to gain physical access to a machine on the corporate LAN or WAN.

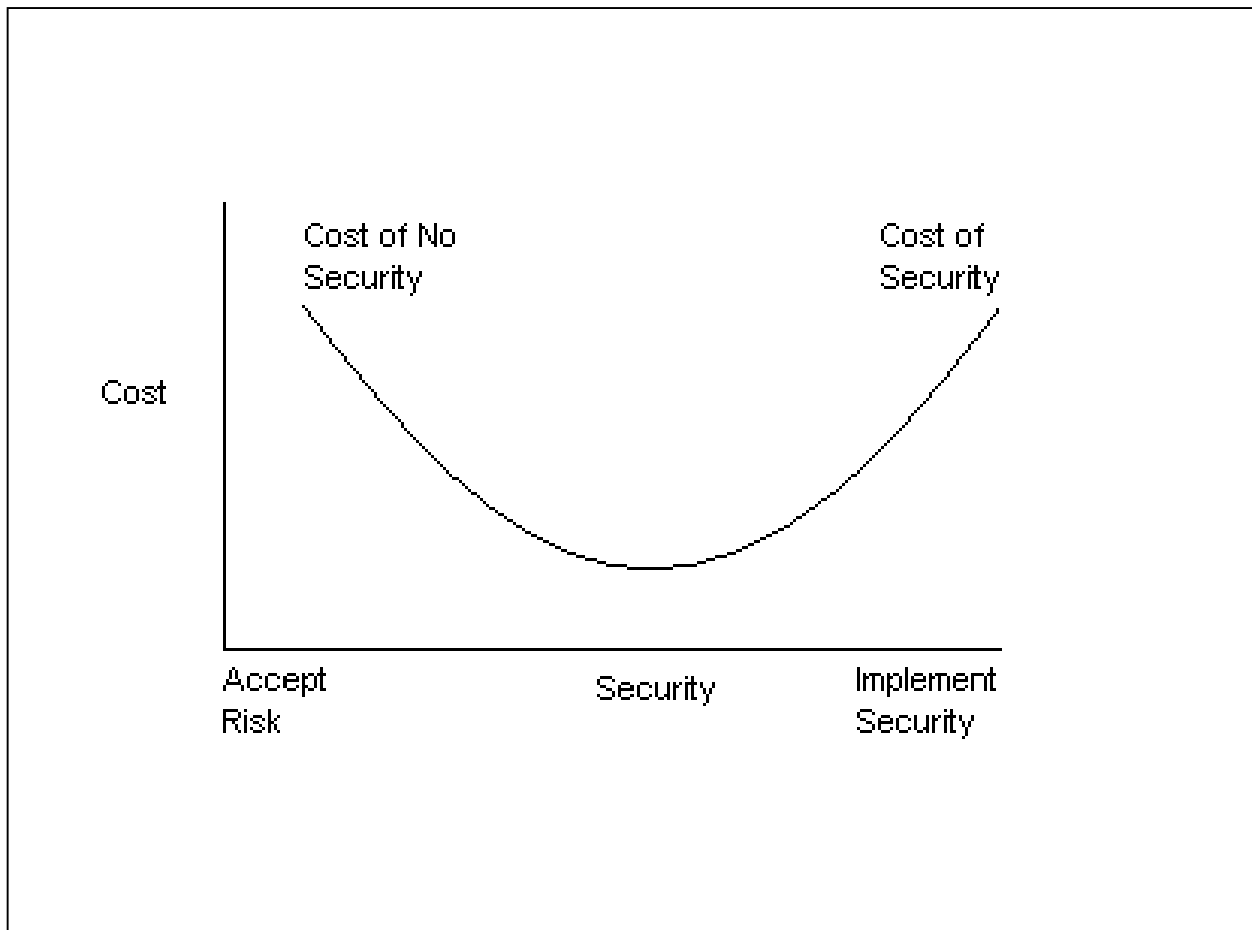
However, today, when one considers the millions of user who access corporate networks over VPN connections, any one who implements a VPN without implementing some form of strong authentication is putting their business at serious risk. Now a malicious user, from any comfortable location, can attempt to penetrate the corporate environment through the username/password vulnerability. Armed only with the name of employees, a hacker can certainly guess a valid username. Then, by employing simple dictionary or social engineering attacks, a hacker will invariably be able to log into the network over the VPN.

Securing the Username/Password Vulnerability

¹ Forrester Research, Infonetics Research, Ovum Research Group.

So clearly, some form of strong authentication must be used if one wishes to deploy a VPN. But what methods are available today to provide strong authentication?

Central to the discussion of various strong authentication schemes is the concept of the Cost-Security Curve associated with the Risk Management Decision. As seen in the accompanying diagram, companies make decisions about securing their infrastructure based on the real and perceived costs associated with accepting risks (Risk Acceptance) or implementing security (Risk Averse). Let us assume that corporations make these decisions on a purely economic basis and without personal emotion. The actual shape of the curve varies by company and is influenced by their assessment of the cost of the data and information they are protecting as well as the cost and security provided by the various security approaches employed.



Given this model, let's examine the approaches used by companies on opposite ends of the spectrum. The first are companies who place a low value on the cost of intrusion. Such a perspective would tilt the curve such that the cost of No Security is lower than the Cost of Security. Thus, they are unwilling to make large expenditures to secure their infrastructure.

For these companies, the predominant method of securing user authentication is to create various Password Policies and Procedures. Such policies include requiring users to select passwords of a minimum length, requiring user to change passwords periodically, etc.

There are two particular problems with this approach. The first is that such a program is difficult to both administer and enforce. The result is the company's assessment of the Cost of No Security is lower than the realized cost. Again, research shows the costs associated with passwords can be significant in terms of both loss of productivity and administrative overhead. Password related problems can account for 30-40% of all internal helpdesk costs while companies can lose US\$300 or more per user per year in lost productivity as users struggle to remember forgotten passwords or sit idle while administrative personnel reset their password.²

The second problem with this approach is that by its nature, it creates a situation where security and convenience are at polar opposites. The stronger the password policy, the more inconvenient it becomes for the end user. This has two ramifications: First, lost productivity and administrative headaches soar. Second, the process is subject to being subverted by the end user and the security benefit of such an approach is lost. Users invariably have a difficult time remembering strong passwords. This results in various undesirable behaviors. For example, users employ simple algorithms such as pre-pending the current date to a standard password or posting the password of the week on their computer monitor or forgetting this weeks password and requesting administrative assistance. These problems create a situation where not only the cost of No Security has been underestimated, but the security benefit of the solution is over estimated. The end result is that the company is not on the desired location on the Cost-Security Curve.

Now, lets examine the situation faced by companies on the other end of the Cost-Security Curve. These companies value their electronic assets very highly and see the cost of implementing security as a cost effective means of protecting these assets. Consequently, the Cost-Security Curve is tilted such that the Cost of Security is less than the cost of No Security.

Companies that fall into this category generally favor implementing some form of 2-factor authentication.

Let's briefly review authentication factors. Strong authentication is generally implemented by increasing the authentication 'factors'. There are 3 authentication factors that can be employed today. These factors are: '*what you know*', '*what you have*' and the newest factor, delivered by the advent of biometrics, '*what you are*'. It is important to note, that these factors may be used in any combination and the number of factors in and of itself, does not yield a good measure of the effectiveness of the system. Put another way, not all X factor solutions are created equal. For example, comparing two 2-factor authentication systems, one based on *What You Know* (a Username) and *What You Have* (a Token) and the other based on *What You Know* (a Username) and *What You Are* (A biometric fingerprint), we would all agree that the 2-factor system that requires a biometric provides a stronger authentication method.

Most 2-factor authentication systems are based on *What You Know* (a password or PIN), and *What You Have* (a token). The following is the typical process used with the 2-factor authentication token:

- A user, prompted for a username and password, enters their static username and a password, provided by the token, consisting of a string of seemingly random numbers.
- The Username/Password is delivered across the network to the authentication server.
- The server uses the Username to find the user's record in its database, and then compares the Password to one generated using the same key used by the token. If the passwords match, the user has been authenticated.

This authentication method has some deficiencies that result in the company not being on the intended point along the Cost-Security Curve. Like the problems associated with strong password policies, 2-factor tokens have problems that cause companies to overestimate their security value while underestimating the costs associated with their implementation.

Let us examine these issues in some detail.

First, understand that this method authenticates the token, not the user. There is still no guarantee that the person employing the device for authentication purposes are who they claim to be. Methods to authenticate the user of a token vary from none at all (a

² Sources: IDC and Renee Woo, Giga, March 2001

hardware token is inserted in a computers USB port and the user need not enter any password) to PINs that are pre-pended to the seemingly random numbers generated by the token. In either case, lose of a token is cause for concern as in the case of a former, an illicit user can gain immediate access to the network and, in the case of the latter, cracking a 4 digit PIN will yield the same result.

Beside the security vulnerability created when tokens are lost or stolen, sharing is also a problem that may be encountered. This problem is especially unsettling because studies have shown that the greatest financial damage done to companies is by the intentional, inadvertent access of internal employees.³ Such an example would be a user who accidentally reboots a critical production server or deletes records in a database for which they should not have access.

Besides problems with tokens being lost, stolen or shared, 2-Factor Tokens are inconvenient to use. This creates the simultaneous problem of inflating the cost of the solution while lessening its security value.

Entering long strings of random number is a time consuming, error prone process. Time spent by hundreds or thousands of users typing and retyping passwords costs companies real money. Not only is there the hourly cost of the employee to consider, but also if presumably, the employee is generating more revenue then they cost, real money is lost because this is time that they are not being productive.

Inconvenience also leads to the problem of users bypassing the system altogether. Ask yourselves; do your company executives use 2-factor authentication? Not likely. Surely, they may have been issued the tokens, but the requirement to use such a device has been turned off at the server. They view their time as too valuable to be inconvenienced by such an approach. Or perhaps they had forgotten their token while on a business trip. Late at night, far from the office, unable to connect to the network to download a crucial sales or investor presentation, they have awoken the network administrator with a strong admonition to disable the token security on their account. This is particularly ironic for two reasons: First, a person impersonating a member of the executive team over a VPN will likely have access to information assets that are much more valuable then the typical employee. Hence the cost of a potential breach is much more expensive. Second, this mindset intentionally ignores the fact that, although a typical employees activity might be worth less than the activities of an executive on a strategic basis, there is a real dollar cost associated with their time. Multiplying this by the volume of employees using the system, and costs can be substantial.

Finally, let us examine the issues associated with 2-Factor authentication systems that increase the estimated of the cost of acquiring this security solution.

First and foremost are the costs of administering such a solution. In a large organization, these solutions require a dedicate administrator to manage the deployment and tracking of tokens. Tokens need to be enabled and disabled as employees join and depart the company and tokens are lost and replace. Then there is the late night calls from the executives as mentioned in the preceding paragraphs.

Next there is the cost of administering the user database. This leads us into our next discussion: the Authentication Server.

Virtually every 2-Factor authentication system *requires* its own authentication server. The reason for this is quite simple. In order to authenticate the passwords generated by the token, the same password must be generated on the local network. The value proposed by the 2-factor vendors is predicated on dynamic passwords. That is, the password is changed after each use or on some periodic schedule. Granted, dynamic passwords would be of tremendous security value if you could authenticate the user, but as stated previously, 2-factor systems authenticate the token, not the user.

The high cost associated with the administration of the authentication server is why 2-factor systems are generally not deployed in small or medium sized organizations. These costs include the initial cost of the hardware, the administration costs to maintain the server, the costs to integrate the solution into your existing network and authentication system. Finally, as the user base grows,

³ CSI/FBI 2003 Computer Crime Report.

hardware costs grow, replication of the user database becomes an issue and the administration of token devices for growing number of users becomes more complex and time consuming.

All these issues conspire to move the right half of the Cost-Security much higher and to the left as the cost of security increases and the security value decreases.

Biometrics as an Option for Strong Authentication

In our prior discussion we alluded to the use of biometrics for providing a unique ‘*What You Are*’ factor for a strong authentication system. We will now explore the benefits of utilizing biometrics for providing strong authentication over VPN access.

Simply defined, biometrics is the measure of a unique physiological trait. This can include fingerprints, finger-scans, hand-scans, retinal scans, iris scans, etc.

How do biometrics compare against the other forms of strong authentication discussed? Our prior discussions portend that biometric authentication is both more secure and more convenience than other forms of authentication.

Consider the issue of security. Your biometric information cannot be lost, stolen or shared. While some would argue that a particular biometric could be impersonated, these arguments do not address the cost or likelihood of doing so. On an intellectual basis, one could make the argument that any authentication system can be compromised. But we must consider the practical potential of impersonating ones biometric. And if a particular biometric does not yield the desired security level, one can increase the security by changing the biometric or requiring additional factors.

Next, consider convenience. Using biometrics, one does not need to enter password or usernames of any kind. In a typical example, a user would simply lay their finger upon a finger-scan device and would be authenticated as who they are. Because of the ease of use involved with such a system, users would have no desire to circumvent the system and because it is actually easier then entering a username and password, the benchmark by which all users judge a system, they would actually be more willing to adopt and use the system.

Before we proceed any further, let’s examine the perceived limitations of biometrics and in doing so investigate the basis for these impressions to determine their relevance for the IT executive.

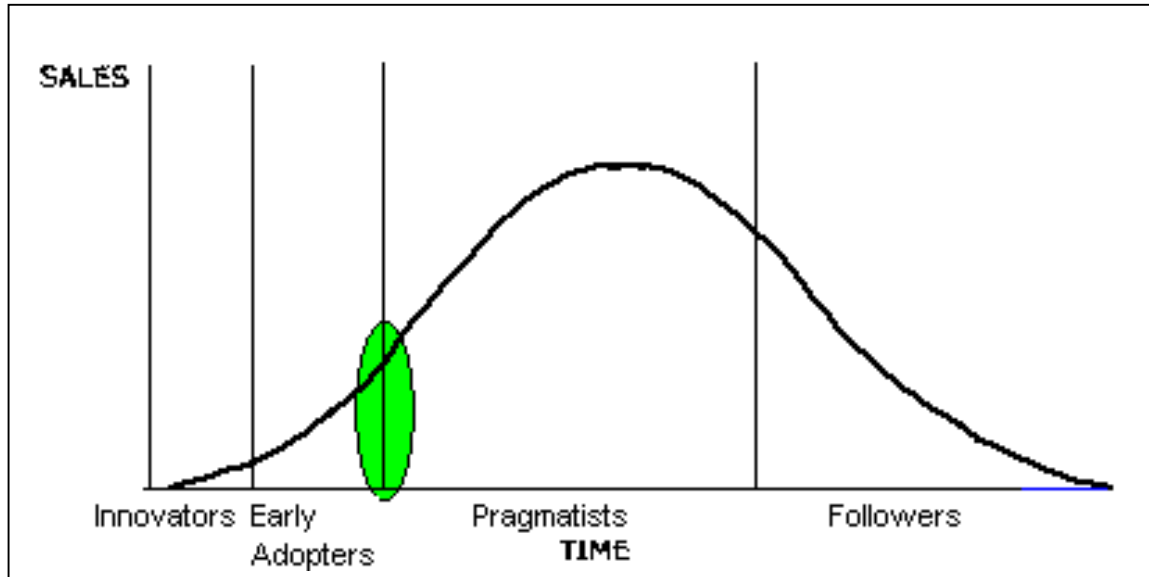
Practicality of Biometrics as an Authentication Method

Prior to having this discussion, a brief review of the technology adoption lifecycle and a dating of biometrics within the life cycle are warranted. To simplify the discussion, let us define the technology adoptions lifecycle thusly: Technology Innovators, that is, the people who create the technology are its first users. Next, the Early Adopters embrace the technology. These adopters generally have a compelling need or are visionaries who are seeking a competitive advantage. They tend to adopt technology to solve a specific problem either Economic, Political, Regulatory, Environmental, Social, etc. The next adopters are the Early Followers who I will call the Pragmatists. Pragmatists adopt technology purely as a business decision. This decision is based on ROI and TCO. Lastly, the Followers adopt technology. This group adopts technology only after its use is well established. Although they gain a general benefit from employing the technology, this group can never gain the competitive advantage of technology because by this time, “everyone” is using it.

As far as biometrics within this technology adoption lifecycle, the indications are that we are in the transitory period between the Early Adopters and the Pragmatists. This is shown in the graph below. Certainly, there are many examples of biometric applications by Early Adopters. Within these examples are rooted many of the myths, misconceptions and fallacies concerning the use of biometrics. Which is why I have chosen to review this lifecycle. There are also many examples of biometric applications for the Pragmatists. In fact, it is my opinion that biometrics have come of age for the Pragmatists, certainly I believe this to be true for the applications with which I am familiar.

Now let us examine the suitability of Biometrics in applications for the Pragmatist.

Accuracy



The first question to be asked concerning biometrics is: How accurate is it?

Before reviewing the technical aspects of this question, it should be pointed out that many stories concerning the limitations of biometrics are rooted in the experience of the Early Adopters. For example, facial recognition of unwilling participants at public events is an incredibly difficult task. Yet, because of the compelling need for security, these systems have been deployed to limited success and their novelty make them newsworthy. The need of the Early Adopters and the needs of the Pragmatists are quite different. So to, are the systems developed to accommodate each group. When developing a system for a Pragmatist IT manager, one need not concern themselves with the problem of unwilling participants. The point here is that when judging the suitability of biometrics for a particular application, we must make sure our notions and biases are based on relevant examples.

To understand the technical aspects of the answer to the question of accuracy, let me review some of the basic concepts used to measure biometric reliability and accuracy.

FAR: False Accept Rate – The rate at which a system mistakenly accepts the biometric credentials of another.

FRR: False Reject Rate – The rate at which a system mistakenly rejects valid biometric credentials of a user.

ERR: Equal Error Rate, the rate at which FAR=FRR.

It should be noted that FAR and FRR have an inverse relationship. For most biometric systems, FAR and FRR are dependent on an Acceptance Threshold. For simplicity sake, we can think of the Acceptance Threshold as how close a live biometric reading needs to be to a stored biometric reading for the credential to be considered 'identical'.

In comparing various biometric systems, ERR is typically used as a comparative value. While this makes for an interesting academic comparison, it is of limited value to the Pragmatist. Think of the Acceptance Threshold as a dial on a biometric system. As the dial is turned down, FAR increase, FRR decreases and security suffers. As the dial is turned up, FAR decreases, FRR increases, security increases but the user becomes inconvenienced. A practical system is not deployed at the ERR. It is deployed

according to one's preference along the Cost-Security curve. If one can adjust the Acceptance Threshold dial to eliminate FAR and incur a FRR of 1 in 100 authentication attempts, the system is a practical and cost effective solution.

The other concept to be discussed when one discusses biometric accuracy is the concepts of Identification versus Verification. In Identification, we are trying to match a specific biometric against a database of size N. If the error rate for the particular biometric is X, the error rate of the total system is $N \times X$. Verification on the other hand is the process of verifying whether or not a user is whom they claim to be and involves matching a specific biometric to a specific stored record of that biometric.

Given this background, we can appreciate that a practical biometric authentication system will utilize Verification over Identification and will generate a FAR/FRR that is both convenient and secure.

Vulnerability

I have previously discussed the vulnerability of biometric system and will only summarize the discussion here. Because of the cost and effort one would incur to compromise a Biometric System, it is not a *likely* scenario. Yet we realize that likelihood of an attempt to compromise a system is based upon the value one would receive upon successfully doing so. Because any system can eventually be compromised, all security systems are ultimately based upon measure-countermeasure. Biometrics systems provide multiple countermeasures such that, as a technique, it can be adopted to the level of security required for the particular applications. Such countermeasures could include switch from one form of biometric to another, requiring multiple biometric samples, combining biometric data with PINs or tokens, etc.

Deployment

Biometric systems have a reputation of being difficult to deploy. This reputation is firmly rooted in the experiences of the Early Adopters. By and large, the biometrics deployed by Early Adopters were Physical Access Control systems. These systems possess one key liability: Central Enrollment. As part of the security process surrounding the deployment of these systems, users were required to report to the central authority, prove their identity and become enrolled in the system. The coordination and effort involved in such a task can be quite significant depending on the size of the system user base.

Again, designing and evaluating a biometric system requires an understanding of the problems unique to the application. For the IT Pragmatists, biometric system can provide self-enrollment by the use of a more traditional authentication method to initiate the enrollment process. Such a methodology provides an acceptable positioning along the Cost-Security curve for the IT Pragmatist during initial deployment.

Integration

The reputation that biometrics possess for being difficult to integrate into a users environment is another perception that is firmly rooted in the experience of the Early Adopters deploying Physical Access Control Systems.

These system deployments were typically integration projects of a core biometric technology into an existing infrastructure which itself, was largely proprietary in nature. Hence, these systems generated a high cost in the specialized consultancy required to make them operationally.

Today, the IT Pragmatists can find shrink-wrapped, plug and play solutions to meet their strong authentication needs. Again the experience of the Early Adopter is not relevant to the situation faced by today's IT manager.

What to Look for in a Biometric VPN Authentication Solution

So what should a biometric authentication look like? What features and functions should it provide to accommodate the needs of users? In our prior look at authentication systems, we looked at solutions for both ends of the Cost-Security curve. Can biometrics provide the flexibility to meet the needs of not only these users but those in the middle of the curve as well?

The following list provides question that one should ask the vendors of a biometric solutions. The answers to these questions will help you determine where you belong along the Cost-Security Curve and your vendors' ability to accommodate you.

Deployment

Question	Ramification
Can the system be deployed by the end user or is administrative assistance required?	The system should provide a simple Windows InstallShield installation mechanism.
Can the system be remotely deployed by an administrator via MSI or another software distribution mechanism?	Large organization will achieve cost savings through remote software distribution.
Does the system provide Plug and Play installation of the biometric hardware?	Users should be able to install the hardware without administrative assistance.
Does the system support User Self-Enrollment?	The system should provide ease of deployment through self-enrollment.
Does the system support Central-Enrollment?	The system should allow for tighter security through central enrollment.
Does the system provide seamless integration with popular VPN clients? Which ones?	The system should provide seamless integration with VPN clients. Products tightly coupled with a client API risk future compatibility issues and an inability of the vendor to handle many different interfaces.
Does the system provide seamless integration with my existing Authentication Database? Which ones?	The system should be compatible with popular authentication database, i.e. Active Directory, LDAP, etc.

Security

Question	Ramification
Does the system provide a strong 3-Factor Authentication Requirement?	What you know, What you have, Who you are.
Does the system allow for a configurable Biometric Template Size?	The system should provide the ability of the user to configure performance versus security versus convenience.
Does the system allow for administrative configuration of the Biometric Decision Threshold?	The system should provide the ability of the user to configure performance versus security versus convenience.
Does the system integrate with my existing Authentication System? Which ones?	The system should integrate with your existing authentication systems: LDAP, Active Directory, Radius, Cisco ASE, etc.
Does the system provide multiple Single Sign On (SSO) Features?	System should provide the follow SSO features: <ul style="list-style-type: none"> - Single Biometric Authentication logs the user onto client machine and allows VPN access. - Biometric Authentication required for the user to log onto Client Machine and separate Biometric Authentication is required to establish VPN connection
Does the system provide 3-Factor Biometric Authentication only for the purpose of establishing the VPN tunnel?	Biometric credentials should never be exposed and should never be transmitted across the network.

Does the system provide Encrypted storage of User Credentials on the Client?	User credentials should be stored securely on the client machine. Biometric credentials should never be exposed and should never be transmitted across the network.
Does the system provide Tamper Resistant credential storage on Client?	The system should be tamper resistant and provide the following protection: <ul style="list-style-type: none"> • Replay Protection • Intrusion Detection • Attack event notification

Integration

Question	Ramification
Does the system overlay my existing Authentication method?	The system should leverage the existing authentication system. For example Username Password, Digital Certificates, etc. Users risk long integration projects and vendor obsolescence with systems that require a replacement of the existing system.
Is the system independent of any one biometric technology and devices?	As biometrics continues to make rapid advancements, vendors should be able support the most suitable biometric for the clients application.
Does the system provide seamless integration with existing authentication dB?	The system should integrate with existing authentication systems: LDAP, Active Directory, Radius, Cisco ASE, etc.

Productivity/Ease of Use

Question	Ramification
Does the system obviate the need for user-entered username/password?	The system should support simple biometric input mechanisms.
Does the system provide Fail-Safe Operation if Biometric Device is removed or fails?	The software should operate in a fail-safe manner.
Does the vendor provide easy to use Software Manual?	Is the vendor documentation clearly written, easy to understand and follow?
Does the system provide an Online Knowledge Base Access?	The vendor should provide on-line help resources.
Does the system provide multiple Single Sign On (SSO) Features?	The system should provide the follow SSO features: <ul style="list-style-type: none"> • Single Biometric Authentication logs the user onto client machine and enables VPN access. • Biometric Authentication is required for user to log onto the Client Machine and a separate Biometric Authentication is required to establish VPN connection.

Authentication Server

Question	Ramification
Does the System support both Client Only and Client-Server configuration?	Support for client only provides SMB users a cost effective solution while Client-Server configuration provides added security of one-time password for Risk Averse users.
Does the Server provide Central Management of User Credentials?	The system should provide intuitive interface for managing user access rights.

Does the Server provide Biometric Audit Trail Report?	Basic reporting of user access should be provided.
Does the Server provide Tamper Resistant credential storage?	User credentials should be encrypted and protected.
Does the Server support multiple Security Policies?	The system should support security policies such as: <ul style="list-style-type: none"> • One-time Passwords • Re-authentication Scheduling • Credential Retirement Scheduling • Random Secret Enrollment Capable
Does the Server provide Intrusion Detection and Prevention?	The system should provide the following protection: <ul style="list-style-type: none"> • Replay Protection • Intrusion Detection • Attack event notification

Conclusion

Biometric technology is entering an exciting period within its adoption lifecycle. Biometrics has evolved to the point where because of the cost of acquiring the technology, its convenience and low administrative overhead, it provides information managers and executives a Low Total Cost of Ownership and a high Return On Investment. This makes biometric solutions a viable alternative for addressing the strong authentication needs of the IT Pragmatist in businesses of virtually any size.

About the Author

Phil Bochey is Vice-President of Sales and Marketing for SureID. Mr. Bochey has 20 years of IT management experience. Formerly with Micromuse, Automatic Data Processing, and General Instrument, he has performed in several key management positions in Software Development, Marketing, Professional Services and Partner & Alliance Management. His accomplishments include running his own successful professional services company, Product Management for Next Generation Access Control Systems for Broadband Cable Systems, building a profitable Professional Services Partner business, Managing Key Product Integration programs for customer solutions and Implementing an International Channels Program.

About SureID

SureID is a market-leading provider of User and Identity Management solutions. Their flagship product, SureID-Remote uses the latest in biometric technology to secure VPN access with an authentication method that is both stronger and more convenient than passwords, PIN's, tokens or Smart Cards. Delivering security solutions since 1985, the SureID team consists of information and security veterans with decades of experience delivering enterprise security. These solutions are used by the defense industry and Fortune 1000 Companies including: Checkpoint Systems, Target, SAP America, Unisys, Wells Fargo, American Greetings, FMC Chemical, and Jason Roberts. The SureID product suite leverages patent pending BIO3 and BIKE impenetrable biometric security technologies to provide a scalable, reliable, plug-and-play strong authentication solution. To find out more about the SureID Suite of Products, visit our web site at <http://www.sureid.com/>.