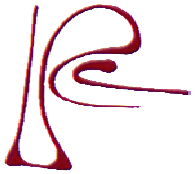


L.. F. Coppenrath
& Associates

Biopassword® Technology Overview

1 Technology Overview

1.1 Biometrics

Biometrics is a field that recognizes that we are all different in our physical makeup, and it is possible to identify people based on these differences. Hair color, height, and the sound of a voice are all examples of how people are different from each other. Combined, these differences create our identity and make us unique from each other. Biometrics measure aspects of our make-up, and uses those measurements in order to identify us.

The principle of biometrics is to use some unique characteristic to identify whether the person is who they say they are. Biometrics works by matching or verifying a person's unique traits with stored data in two categories: physiological characteristics and those that are behavioral. Physical indicators include iris, fingerprint, facial, or hand geometry. Behavior types are usually voiceprints, keystroke dynamics and handwritten signatures.

Biometric technologies, tools for measurement of a biological or behavioral trait, can be categorized as static, dynamic or continual. "Static" refers to measurement of a trait that requires no action at the time of verification. "Dynamic" refers to measurement of a trait while action is taking place. A written signature, for example, can be measured statically or dynamically.

Most biometric technologies require special hardware to convert analog measurements of signatures, voices, or patterns of fingerprints and palm prints, to digital measurement, which computers can read. BioPassword on the other hand, is software only, and relies only on an external existing keyboard to produce a digital measurement binding it to a standard user id and password procedures.

1.2 Keystroke Dynamic Technology

Typing biometrics is more commonly referred to as keystroke dynamics. Keystroke dynamics looks at the way in which a person types or pushes keys on a keyboard. This method is based on the typing characteristics of the individuals such as durations of keystrokes, and latencies between keystrokes, inter-keystroke times, typing error frequency, force keystrokes etc. Specifically, keystroke dynamics measures two distinct variables: "dwell time" which is the amount of time you hold down a particular key and "flight time" which is the amount of time it takes a person to travel between keys.

The original technology was derived from the idea of identifying a sender of Morse code using a telegraphy key known as the "fist of the sender", whereby operators could identify senders transmitting a message by the rhythm, pace and syncopation of the signal taps.

During World War II, the Army Signal Core identified that an individual keying rhythm on a telegraph key was unique. In the early-'80s the National Science Foundation and the National Bureau of Standards in the United States conducted studies establishing that typing patterns contain unique characteristics that can be identified.

Keystroke dynamics works by monitoring both the rate of typing and intervals between letters when typing in a password.

Benefits: Verification is based on the concept that how a person types, in particular their rhythm, is distinctive. Even if intruders guess the correct password, they cannot type it in with the proper rhythm.

Drawbacks: If someone is in the lab with you, for example, they could possibly observe someone's key clicks when typing in a password. However, once an imposter is removed from the environment, (causing a lapse in memory), the imposter is unable to replicate the legitimate biometric template.

Applications: BioPassword technology for User Authentication and Access Control when logging on to the Windows NT operating system.

Biometrics keystroke dynamics technology utilizes - the manner and rhythm in which each individual types passwords and logon codes – to create a biometric template. It measures the keystroke rhythm of a user in order to develop a template that identifies the authorized user.

1.3 BioPassword® Technology

BioPassword technology uses statistics to take a measurement of the differences in how we type, and uses that measurement when verifying different people. In this approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both internal and external attackers. This analysis is transparent to users while they are trying to gain system access via a password-authentication mechanism in the normal way (by entering a user ID and password string).

The technology was originally developed by SRI International (formerly Stanford Research Institute) between 1979 and 1985 in an effort to create a computer-based security access and identification procedure that would present greater protection than keys, cards, passwords or codes. BioPassword uses a patented keystroke dynamics technology (a proprietary algorithm to make biometric measurements of a keyboard user's individual typing rhythm) when they enter a password. BioPassword adds a transparent layer of authentication during the login process. Currently there is no competition for BioPassword using the keystroke dynamics due to our patent covering the proprietary nature of the algorithm, process and methods.

The process measures the unique typing style of an individual computer user. BioPassword captures the stroke and dwell time of each character typed and hashes this information with an algorithm creating a biometric template. This biometric template is invoked each time a computer user logs on using their user name and password and compares the new logon with the stored biometric template. BioPassword either accepts or rejects access based on the Euclidian distance derived from the administrator setting the users individual security level.

This user-specific unique rhythm is stored as a biometric template and compared when a user logs into a system with a password or ID. The user's template is developed when they register in the system by typing an ID and password, providing sufficient samples to make the biometric template unique. During the enrollment period the system learns the user's keystroke rhythm. The procedure takes only about a minute to complete. Once installed, BioPassword requires both domain authentication and biometric signature (rhythm) comparison before access is granted.

1.4 BioPassword® LogOn for NT®

BioPassword LogOn for Windows NT is the first implementation of the BioPassword technology for the Windows NT O/S as a more secure layer for Windows NT's Graphical Identification and Authentication (GINA), the component of the network client that handles user logons. BioPassword LogOn for Windows NT is a client-server based software product designed to offer the thousands of businesses running the Windows NT platform an added layer of biometrics security.

BioPassword LogOn for Windows NT works in conjunction with the existing Windows NT logon process to enhance user authentication process (verifying the identity of a user who is logging onto a computer system) within the security features on NT networks. BioPassword LogOn for Windows NT uses existing Windows NT account information, binding a biometric template to the password. When a client attempts to log onto the domain server, the user name and password are compared to the stored biometric template.

The Windows NT Server retains all user management. By incorporating BioPassword biometric technology with the use of user names and passwords, BioPassword LogOn for Windows NT maximizes network security.

BioPassword's product features enhance the following GINA subroutines:

Constant, automatic Password logon monitoring, every time the computer is booted up or unlocked.

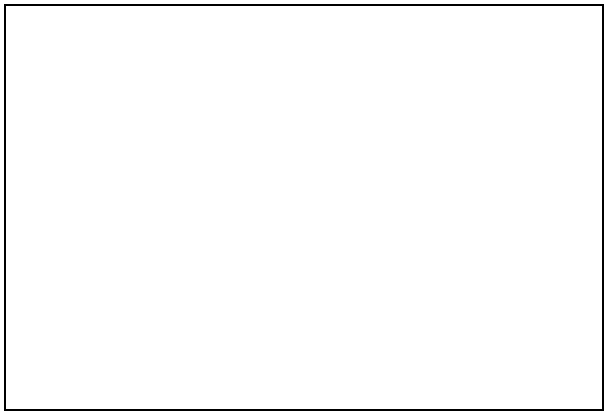
Maintains existing NT Security Logon/Log off Options for maximum security when you're not at your computer, that include a system lock feature, a system shutdown and reboot feature, a shutdown feature and a shutdown and power off feature.

Flexible Security Settings, so that, as appropriate, the administrator can tailor the level of security on each NT client on the network. BioPassword Logon gives you the ability to set an individual User biometric Security Levels. There may be circumstances where a user requires authentication Security Level either higher or lower than the default System Security Level. Levels range from:

Level 1 - minimum security, allows for a minimum degree of accuracy (essentially turning off BioPassword signature checking)

Level 9 - maximum security, requiring complete accuracy

Complete and invisible integration with the Windows NT client-server program for seamless biometrics security.



click here for enlargement

BioPassword LogOn for Windows NT consists of two components:

Server software (bioserver.exe) This component stores the biometric measurements for a user's username and password and authenticates them when a user logs on.

Client software (bioclient.exe) This component collects and passes on to the server, the user's biometric signature. It also displays the BioPassword LogOn for Windows NT logo on all Windows NT dialog boxes identifying biometric verification is used.

BioPassword LogOn for Windows NT is the only software solution that can authenticate a user at time of logon. It is easy to install and administer, saving support time and costs. It is not intrusive to the user, allowing for user acceptance and therefore usage. It works with existing process, making the deployment faster.

2 Testing Methodology

Biometric technologies have been in development over a period of decades. Users and vendors alike have looked to find a common measurement to compare and contrast the performance of one technology over another for the purposes of evaluation. Lack of standards and independent testing are the weak points of these technologies.

The National Institute of Standards, BioAPI Consortium, The Biometrics Consortium, and The Association for Biometrics among others, are aggressively addressing the area of standards. In addition to benefiting from a more receptive market and emerging standards, biometrics technologies like BioPassword also now have many more years of research, development and testing behind them.

The challenge of course is that the commercialization and deployment of biometrics over a broad range of environments is not well documented so one is forced to rely on vendor-produced specifications and documentation. This is one reason it is so difficult to compare biometric types against one another, let alone the same types of biometrics.

In order to create a comparative benchmark some work has been done by independent agencies using some common measurements. The following terms are used to describe biometric performance and are recognized as common measurements are:

FTR (Failure to Enroll Rate) - the ability of the biometric to enroll a biometric for a user.

FAR (False Acceptance Rate) - the rate an imposter could be verified or identified by a biometric.

FRR (False Rejection Rate) - the rate a legitimate user is rejected by the biometric.

ERR (Equal Error Rate) - Cross over point when FRR = FAR.

There are two basic concerns in these technologies: the error tolerance and the storage of the templates. The setting of the error tolerance of these systems is critical to their performance. Ideally False Rejection and False Acceptance errors should be low and the manufacturers should quote them both. FAR and FRR are two measurements which can produce widely varying results dependent on the environmental issues such as physical location, type of user, and security level setting.

Several environmental issues have an effect on these numbers and their characteristics. First it should be noted that there might be a difference between the ideal lab-controlled environment and a real-world implementation.

Another factor that may affect the FTR is if a biometric is intended to be used by users that use a keyboard in their current login process (like BioPassword) and is tested with users who cannot type you could produce two numbers. A FTR of 0 would result, where 100% of the users type on a keyboard in their day-to-day work verses a random sample of people off the street who may or may not have ever used a keyboard. It's possible that 2 out of a hundred people may fit this profile and therefore produce a FTR of 2%.

It should also be noted that FAR and FRR are generally mutually exclusive. Meaning that if the FAR is high the FRR is lower. And if FRR were lower then the FAR would be higher. This is true also for different threshold settings of the software. There is an important measurement, or ERR where the FRR and FAR are equal. This is the measurement, which really describes the strength of the technology.

In order to validate the technology you need to lab-test all versions of the biometric in all operating systems and environments, including SDK versions. This is not really practical and may even ignore the favorable environmental suitability of a particular biometric type.

2.1 Testing History

In 1980, the National Bureau of Standards (NBS) in Gaithersburg, Maryland, sponsored a study of the concept by the Stanford Research Institute (SRI) which concluded that computer keystroke authentication of 98% accuracy (equal 2% Type I and Type II errors) could be achieved from typing name and password alone and, when more extensive typing data was available, error rates could be reduced to even lower levels.

Rand Corporation drew similar conclusions about typewriter keyboard dynamics in a study sponsored by the National Science Foundation. In late 1980 Rand published a paper defining the practicality of this. This report is found under: Gaines, R. Stockton et al., "Authentication by Keystroke Timing: Some Preliminary Results", Rand Co., R-2526-NSF, 5/80.

2.1.2 SRI Findings

In 1984, a feasibility study conducted by SRI and sponsored by the National Bureau of Standards (NBS) concluded even relatively short typing sequences of 15 to 20 strokes were sufficient for good identification authentication of typists. Lab testing demonstrated that a 2% FRR and FAR could be achieved by typing an 8-character user name and password. The test was done with 35 IBM PCs in a large corporate network. The system functioned while users performed normal work.

Performance was evaluated using the point of equal Type I and Type II errors. For ongoing work the system correctly differentiated individuals with 98.1% to 98.5% accuracy. For logon alone, keystroke dynamics had been previously shown to be 98% effective using an eight character ID and eight-character password.

SRI used a CICS environment to provide a measure of performance in a menu-driven, screen-oriented application and achieved equal Type I and Type II error rates of 1.9% (98.1% accuracy.) These rates are based on measurements where the testers were given the logon ID and password and were allowed unlimited tries.

During the SRI lab-test the BioPassword algorithm demonstrated a 98.4% crossover rate producing a FRR of 0 for users who are familiar with a keyboard. In 1989, the Net Nanny Software International Inc. (NNSII) acquired all rights, patents, trade secrets, trademarks, and copyrights associated with BioPassword. The US Patent Number is 4805222.

2.1.3 Original Hardware Device

The National Institute of Standards and Technology (NIST) administers the Computer Security Act of 1987, and develops standards and guidelines for security in federal government computer systems. Military-related computer security guidelines were outlined in a Department of Defense publication known as the "Orange Book". The original design and development of the BioPassword product addressed both the Orange Book and NIST guidelines in designing the product's functionality.

BioPassword was offered as a hardware solution, in the form of a chip that was installed in the IBM PC/XT/AT/PS2 or a similarly configured clone. The keystroke dynamics technology for the hardware product is actually based in software; the algorithms and program was burned into an Erasable Programmable Read Only Memory (EPROM) chip on the circuit board. The hardware product was developed and used in the XT Personal Computer in the mid 1980's. This hardware device was capable of handling 6 independent users on a stand-alone PC (Non-Networked.)

Considerable respected and qualified input was sought out in the testing phase of the hardware devices and initial technology. In 1987 a group of potential customers from major federal agencies and the commercial sector were assembled to create a Preferred User Advisory Group to test and provide further input with respect to the product. Alpha testing on the hardware device, called BioPassword Access 2000, took place in 1987 and Beta testing went on through 1988.

The following companies and organizations participated in various stages of Alpha and Beta testing:

AT&T Development Corp., Bell Labs, CIA (Central Intelligence Agency), Cargill, Chase Manhattan Bank, Chemical Bank, Commercial Credit, DCA (Defense Communications Agency), DIA (Defense Intelligence Agency), Department of Labor, Dupont, Exxon, FBI (Federal Bureau of Investigations), Federal Reserve Bank, First Boston Corp., GE Capital, General Mills, Geodynamics, Hughes, IRS, JP Morgan, Lockheed, Los Alamos Scientific Labs, Manufacturer's Hanover Bank, Merrill Lynch, National Bureau of Standards, NSA (National Security Association), New York Stock Exchange, Nixdorf, Paine Webber, Social Security Administration, US Air Force, US State Department, and Wells Fargo Bank.

After a series of beta tests of prototype systems, it was felt that the most useful system would be one where initial verification of the typist would be adequate, with an ability to periodically check that the same person was still typing.

2.2 Current Testing

NNSII invested a great deal of research and development in making BioPassword core technology entirely software based. The company has now taken the hardware device, re-written the software to run under the Windows NT operating system, and scrapped a hardware solution in favor of a "software only solutions".

2.2.1 BioPassword® for NT 4.0

In 2000, BioPassword cleared an important hurdle in the authentication of the user after passing the Financial Services Technology Consortium (FSTC)/International Biometric Group (IBG) Comparative Testing program. This program gauged the real-world performance of leading biometric technologies in the two fields of greatest interest to financial services professionals - IT security and e-commerce.

With the participation of the FSTC, comprised of leading banks, financial services providers, research laboratories, universities, technology companies, and government agencies, IBG's testing is the standard for the comparative performance of biometric systems, helping to clarify the often-confusing world of advanced information security. IBG qualified BioPassword as a valid biometric solution.

Samir Nanavati, a partner with International Biometric Group, said Keystroke dynamics is a viable technology because it requires minimal training and no special hardware. It also inhibits employees from sharing passwords - a common way security is breached. Net Nanny, he said, is the only company that has brought this technology to a commercial stage. In an industry where new companies quickly come and go, it's considered a real player, he said. "As far as the approach that Net Nanny has taken, it's a respectable one," Nanavati said. *[Seattle Times, March 22, 2000]*

"Over the past 12 months all of the biometric technologies have finally come down in price, finally have incorporated standards, finally have adequate accuracy and finally work," says Samir Nanavati, a partner with IBG. "Specifically for keystroke biometrics, the accuracy was not there, but now it is." Nanavati says the other key for success is tight integration with NT. *[CNN December 26, 2000]*

Controlled testing in the past 6 months, as well as observations at PC Expo and COMDEX 2000 have shown support for previous testing numbers. More credible third party testing will support the previous lab test and validate the optimized environment for BioPassword LogOn for Windows NT.

2.2.2 Next Steps

In order to produce meaningful values to validate the BioPassword LogOn for Windows NT we have approached and are exploring running independent testing programs with the following third parties:

The International Biometric Test Center at the University of San Jose.

Sandia Laboratory at the Department of Defense.

The International Biometric Group in NYC.

Arthur Andersen.

IBM ASP Test Lab in Beaverton, OR.

3 Statistical Analysis

3.1 Passwords

It is important to recognize that keystroke dynamics, when layered on user ID and password, incorporates the statistical probability of password access control. Using a statistical formula, we can represent the probability of a security breach with the use of passwords alone.

Selecting a password randomly from 100 possible PC keyboard characters (upper and lower case) that is unknown to an unauthorized user, the probability of a successful password occurrence is P=(1/100)n where "n" denotes the character length of the password. If the probability of selecting a proper password is independent of the probability of a security breach, then this will result in the probability of success as $\mathbf{(1 - (1 - (1 / 100)^n)^t)}$ where t = the number of tries. The mathematical formula $\mathbf{1 - (1 / 100)^n}$ will essentially equate to zero, implying that without knowledge of the password, there is little or no chance of a security breach.

Unfortunately in the real world this is not the case. Users share their passwords; write them down, select easily guessed passwords and users seldom change them unless they are forced to do so. The vast majority of passwords can be determined far too easily by intruders especially if written on a post-it-note stuck to the computer.

3.2 Keystroke Dynamics

This technology provides a unique level of security for logon and passwords. BioPassword technology measures in milliseconds, the timing between keystrokes using our proprietary algorithms to generate the biometric signature. To illustrate the unique statistics of keystroke dynamics, the following formula may be used:

$$P_r(1 \le x \le t) = \sum_{x=1}^{t} \frac{t!}{x!(t-x)!} P^{x} (1-P)^{t-x}$$

"t" = number of tries.
P_r = Probability of success.
"x" = number of successes in "t" tries.

If "P" equals .01% or .0001 based on the decision criteria mentioned earlier then the following table shows the tries vs. the probability of a security breach based on the binomial distribution of P=.001.

"t" (tries)	Probability of a Security Breach
1	.00001
3	.00003
5	.00005
7	.00007
9	.00009
100	.001

When the probability of a security breach, in the above example, is multiplied times factors in the above table, one can see that even with full knowledge of someone's password, the security of a system is still within the acceptable limits because of keystroke dynamics. The proper design of a keystroke dynamics security system can provide additional deterrents to an impostor. An example of the effectiveness of a keystroke dynamics device can be assessed using the following assumption:

Logon Name = known!
Password = known!
Decision point = .01% or .0001
False rejections = 3%
Tries before lockout = 6 attempts
Lockout time = 5 minutes

Every 6 attempts result in a probability of 1 in .0006 of successful access or 6 times in 10,000 tries! The system locks for 5 minutes every sixth try, or must be released by the system administrator, who would notice the attempt. If a 5-minute lockout were implemented, the system would be locked for (10,000/6) x 5 minutes or approximately 140 hours before a successful keystroke dynamics match. This is certainly a deterrent.

User ergonomics and environmental created issues, such as user position, hands to keyboard geometry, artificial or enhanced nails, digital dexterity, physical ailments (arthritis, swelling, and injury, as examples,) or protective layers (including bandages, gloves, and keyboard membrane covers) can create influencing variables preventing successful BioPassword logon. Fortunately, the BioPassword administrator has the ability and control to modify the tolerance range of acceptance allowing logon on an individual need basis.

4 Summary

The use of passwords is heavily entrenched into computer access systems worldwide, so it makes sense that better password management is required. It also opens opportunities for complementary technologies, which can enhance password systems and make them more secure. One such solution is the combination of passwords and biometrics.

As biometrics becoming more accepted within Enterprise IT security, keystroke dynamics will become recognized as an unobtrusive, non-invasive and very cost effective solution. Keystroke dynamics only electro-mechanical requirement is a computer keyboard, which has been perfected over many years of engineering.

Today, NNSII has re-engineered keystroke dynamics into a software only biometric solution for user authentication in modern computers. BioPassword LogOn for NT is NNSII's first commercial biometric product specifically designed for the Windows NT server platform authenticating client users accessing the network.

BioPassword technology provides a number of benefits to both IT professionals and the user base and differs from other biometric technologies in a number of ways:

Ease of Use - BioPassword is a transparent system, which uses the familiar keyboard. Users adapt to using BioPassword quickly because it is easy and unobtrusive.

End-user - Transparent to users after login. Passwords are difficult to remember. From an administrative side, BioPassword can reduce periodic user name/password updates or, in some instances, eliminate the need for monthly "user name/password" updates. BioPassword is transparent in operation and requires no additional hardware or training. What this means is an inexpensive biometric solution that can limit who can access a company's network even if a user name and password are compromised.

Value - BioPassword is software-based, requiring no external hardware. Simple and inexpensive to deploy, BioPassword is as easy as installing a new program. The economic advantage becomes apparent very quickly when cumulative employee time loss is tracked for user name/password monthly maintenance. And, compared to other biometric solutions, there are no additional costs associated with BioPassword Logon such as supplemental hardware, hardware and software training, or hardware upgrades and modifications.

Flexible and Scalable - Systems administrators using BioPassword can easily expand the number of users who are required to authenticate themselves. Integrating and strengthening existing security systems. Third-party software solution providers will be able to incorporate BioPassword technology into existing environments and products. BioPassword will offer the market the easiest biometric technology to incorporate into a wide variety of products and network architectures.

BioPassword presents a unique approach to improving the security of passwords and User Authentication. Password typing is the most widely used identity verification method in Web based electronic commerce. Due to its simplicity, however, it is vulnerable to imposter attacks. Keystroke dynamics and password checking can be combined to result in a more secure verification system. In a "one to many" environment of the internet and electronic commerce, BioPassword enhanced verification whether, a digital signature or an authenticated transaction, can provide a simple biometric layer that can bind the user to a digital signature or transaction in such a manner that no other biometric technology can offer.

BioPassword technology can be distributed and implemented over a wide electronic geographic and demographic expanse without new hardware, learning how to use new hardware, maintenance, or incurring additional hardware expense.

The emerging biometrics based identification and authentication technology is applicable to areas of

Banking security such as electronic fund transfers, ATM security, e-commerce, check cashing, credit card transactions, etc.

Physical access control such as airport access control, sensitive zone access control, defense, etc.

Customs and immigration such as passport control, authentication of visa, etc.

Voter identity such as a voting machine that will not allow the voter to access the machine without automatic positive identification of the voter against his or her voter registration record (5) telecommunications such as cellular bandwidth access control.