BIOMETRIC SIGNATURE ID
IDENTITY PROOFING SOLUTIONS

Gesture Biometrics

A Game Changer for Remote Identity Authentication

-White Paper-

Prepared by:
Biometric Signature ID
708 Valley Ridge Circle
Suite 8
Lewisville, TX 75057

Document No.: **0000016**
Release date : **Updated March 2015**

Gesture Biometrics: A Game Changer for Remote Identity Authentication

Editor: Jeff Maynard - CEO & Founder

Welcome!

With nearly 5M uses in 3 years, significant year after year % growth, use in 70 countries, Top 20 Ed Tech Company Award, New Product innovation of the Year Award and chosen by the White House (versus 180 other companies), Biometric Signature ID's innovative technology is quickly becoming the market leader in the field of online identity protection.

We all get skittish about our privacy and security, especially as we remotely access a digital asset such as a bank account, e-commerce site, healthcare portal or an online exam. When an institution has a breach we lose confidence and many of us will switch to another institution or merchant. These data breaches can quickly lead to identity theft and fraud, sometimes within hours. The underground economy is very vibrant and clean credit cards with security codes can sell for as much as $50.00 per card[1]. Credit card companies have some protection against fraud for us (less protection for debit cards) but nobody pays us for the huge time, emotional drain and aggravation that fraud costs us personally. We should all expect and demand that our e-tailers or other providers of remote services use higher security that allows only the registered user access to their digital asset.

We all know PINS and passwords are not enough security as a single credential and we see the evidence of this every day with the announcements of yet another data breach. Before I talk about biometrics what are our other choices to secure our virtual identities?

Non-Biometric security technology

- Tokens (thumb drives that fit into our USB ports or flash different access codes),
- Cards like Bingo cards, Access/proximity cards, Smart cards loaded with personal Information (mostly available in Europe for ATM's only),
- Multilayer strategies that combine layers/matrixes of something you know. Some of these strategies combine options such as verifying the "identity" of the device you registered with (example your pc), analyze patterns of behaviors (i.e. make money transfers at a certain time), look at geo-locations or use multiple pins and passwords etc. In some cases these technologies might be transparent to users until out of ordinary behaviors are recognized,
- Mobile phones that use a onetime password to unlock your account,
- Security questions of various flavors called in-wallet or out of wallet questions,
- Government issued documents such as driver's license with your photo, birth certificates etc. that must be faxed or scanned.

What do all these security technologies have in common? A poor user experience. Take each one of these choices and ask the questions:

- Whether they can be forgotten, stolen or borrowed and how do you replace if lost?
- Then add the convenience factors like extra cost, how accurate are they, how do you know if the person who registered for the card, device or document is the same person who now possess the item?
- How do we know if the security answers to questions are not easily available from researching on the internet?
- Multilayer security (not multifactor) and analyzing behaviors (these have the privacy groups up in arms) have been responsible for failing to protect commercial clients.
- How many devices do you have to register and what happens when you add/modify equipment and operating systems?
- What about poor reception, different age groups not wanting to use SMS texting to receive a password, we are still shocked (think TJ Max scenarios), to trust a still vulnerable mobile network, work phone may restrict personal access, are the phones themselves secure….

Recently, University of Washington researchers ran subjects through several types of authentication. They then asked for feedback on the usability and perceived security of a new biometric authentication technique that identifies people based on their eye movements. "How humans interact with biometric devices is critically important for their future success," said lead researcher Cecilia Aragon, Ph.D., an associate professor of human-centered design and engineering. "This is the beginning of looking at biometric authentication as a socio-technical system, where not only does it require that it be efficient and accurate, but also something that people trust, accept and don't get frustrated with."[2]

Besides obvious limitations, the BIG issue with these current technologies is that they have NOT been able to protect us. The levels of identity theft and cyber security issues is at all-time highs in spite of these technologies. So what is the problem? Simply stated they do not authenticate the individual - the physical person, they only verify that a person (could be anybody) has possession of the device, answer, card or document.

So how do these technologies compare to using biometrics? Big difference. Biometrics cannot be borrowed, stolen or forgotten. They are a part of you. There are major differences however in the user experience that limits specific use cases. Let us examine the two types of biometrics.

Physical biometrics examples are fingerprints, iris scans, face scans, DNA and more recently vein scanning [2, 12, 13]. They are best suited for accessing physical buildings for example and are not well suited for logical access (PC, mobile, tablet). Since we are discussing remote (logical) access are these useful for this application?

- Physical biometrics require special hardware to scan/receive your input. This adds high cost and inconvenience that is nearly insurmountable. Are you supposed to carry around a reader for every device, for every app?

- Who supports the training of how to use/add these devices, how do they get to you, who do you call if any issues?
- High failure to enroll rates create poor user experience and limit use. For example, somewhere between 5-10% of some populations will not be able to enroll their fingerprints due to lack of ridges in their fingertips (smooth or very rough skin).
- Ineffective hardware readers can produce up to 50% or more false positives. Companies lose out because the system is no longer effective as a security technology. Even worse if the system does not recognize current users /employees will stop using them or vigorously complain they cannot get in. This affects work productivity as users will flood the help desk with calls and then do little work while they wait for answers/resets.
- Poor lighting and the fact that some parts of your face (ears and noses which contain cartilage and also elongate due to gravity) continue to grow all your life, reducing effective comparisons over time.
- Big issue is if your fingerprint is your new log in passcode how do you perform a password reset? Answer with a lot of difficulty.

Behavioral based biometrics also called dynamic biometrics consist of voice, keystroke and signature gestures.[3, 13] Welcome to the future! This class of biometrics requires no additional special hardware like readers to activate. This means that in the case of signature/gesture biometrics all you need is a finger, or a mouse to log into the software and create your unique passcode. You even get to bring your own device(s) and can create multiple secret passcodes respecting different screen sizes. This patented software only biometric is called BioSig-ID.

BioSig-ID works by having the user draw or sign their passcode (usually 4 letters or numbers) on a drawing area that appears on the screen of the device they are using. After inputting, the software collects your unique pattern of length, angle, speed, height, number of strokes and stores this in an encrypted database. Upon subsequent log ins if the patterns match we confirm that the person who registered is the same person trying to access the digital asset (bank account, healthcare portal, exam). Only the same user who has successfully authenticated themselves against a previously created enrollment profile can proceed. Imposters will not be able to proceed as they have to duplicate your unique passcode. (Example 1)

One additional feature of the BioSig-ID software is the ability to move the requirements for accuracy. One size does not always fit all. If the institution desires to ratchet up the accuracy that is required for their users, we can do this. We increase the accuracy needle. BioSig-ID can even modify the needle by group within a group or for individuals allowing maximum flexibility.

However the compromise is that the user experience can be affected. Moving the needle is a function of what you are trying to protect and how many times your users are accessing their accounts. Our analysis tools run reports to determine what the optimal accuracy levels are in the user base by device so we can advise our clients. More about this in a later section.

User experience, accuracy and scalability

The real secret to user uptake is a positive user experience. If it is too expensive, too intrusive, takes too long, is inconvenient, does not work every time, is too difficult, you have to carry something, wait too long to get enrolled and a host of other factors you will have limited use and fail to achieve your objective.

Independent tests have confirmed that BioSig-ID is three (3) times more accurate (99.97%, 0.0003% false positive) than the federal government guidelines.[4] Moreover, the level of false negatives at 99.78% means the software works extremely well for its intended purpose of blocking those who are attempting to access using your credentials and recognizing current users. Few upset customers with BioSig-ID as these extremely positive levels means users will not experience "password rage" and the software will be well received. This was confirmed in follow up surveys from first time users across a wide spectrum of ages, locations, gender who reported a 98% positive experience rating.[5] In fact, nearly 45% also found the software entertaining/intriguing. BioSig-ID uses a self-service password reset using its patented "Click-ID image software" SMS and e mail and this reduces help desk calls to below 1%.[5]

Keystroke biometrics by comparison in an earlier lab test by the same testing company was found to be 27X less accurate then BioSig-ID and did not meet the minimum acceptable standards[6]. No similar work using independent lab testing has been published with voice. It is very likely voice authentication will never match the positive results found with BioSig-ID due to physiological sameness (i.e. brother, sister, family) and differences with multiple microphones and speakers. Voice's strong spot is verifying that a person is human so they can answer questions. A great use for voice is in call centers to replace human operators.

The user experience is the final denominator. The vertical global growth of mobile device access is a critical security issue spanning users, commerce, enterprise and government. BioSig-ID software enables BYOD (bring your own device) and strong multifactor authentication. For each device a user can create multiple secret passcodes respecting different screen sizes. Users can even modify their secret passcodes specific to each device. For example they can also create a passcode based on their mood or disposition. Experts feel many of us use at least three types of signatures - one legible for official documents, one for sign off with credit cards and one that nobody is supposed to understand. BioSig-ID software allows the user to set up a passcode for all these.

Security and API

BioSig-ID communication is secured using common transfer protocols, e.g. SAML 2.0, SSO-I/O, oAuth and OpenID. Utilizing Flash and HTML5, BioSig-ID will work with virtually any current device today. In higher education BioSig-ID has already integrated with seven (7) of the top learning management systems including those using LTI 1.1. Scalability of this SaaS based technology is not a problem. Like a Google SaaS system, when too many users challenge the system it may slow down until more servers are added.

Continuous and randomized authentication

One new security field that is fast emerging is continuous and randomized authentication. Perhaps the best way to explain this is by example. With our higher education clients, the BioSig-ID software can be placed as a "gate or door" when the student registers for school or a course, signs in for interactive discussions, signs in for actual coursework or a gradable event. To reduce the opportunity for working

together and fraud, unexpected challenges can be placed at various points in course delivery. Students will not know in advance *when* they will need to verify their identity. This severely reduces opportunity to enlist the aid of someone else to sit with them to take an exam. Using a combination of time, location, activity and history, BioSig-ID audit trails offer an extra continuous assessment and real time event notification (RTEN) to identify suspicious activity and can shut down access to the account.

Random/unexpected identity challenges increases the confidence level (Level of Assurance) that the registered user is the same person who accesses the account or online asset. But there are other benefits of using the BioSig-ID software to increase assurance levels. BioSig-ID is a both multifactor and multilayer in one product. This uniqueness is due to being a dynamic biometric but also because of the way the software was designed. This means you really do not need any other security factors like "Something You Know" (another set of PINs or passwords, security questions) or "Something You Have" (hardware tokens, cards etc.). These combined with "Something You Are" (always a biometric like BioSig-ID) is the new gold standard described as multifactor authentication (MFA)[7]. Congress is mandating its agencies to use MFA where they must offer users 2 of the 3 something you have, are or know as the new security protocols.

In contrast, fingerprint biometrics, security questions or tokens for example, require another factor and this means another company may have to be involved to complete it being classified as multifactor. This introduces a new level of complexity any time you try and get multiple companies to work together.

Continuous authentication is like the Holy Grail. It is illusive. It will also be intrusive yet is being advocated by agencies such as Defense Advanced Research Projects Agency (DARPA)[8]. The way to measure success of the security chosen for identity authentication is to analyze the audit trail history.

Audit trail and suspicious activity reporting

Ok is there anything else that needs consideration before selecting your choice of security for logical access? A big Yes. You need the ability to analyze a user's history of authentications over time. BSI has advanced security access by using a service intelligent analytic platform that dashboards client and administrative reporting. Using real time event notifications (RTEN's), user suspicious behavior can be identified for administrative action. We see the combination of biometrics and behavior analytics as the future to monitoring user online access and preventing/identifying fraud. (Example 2, 3).

Again the best example is to describe what BSI has created to monitor a user's activity for our higher education clients.

BioSig-ID provides an audit trail including the time and date stamp of user sign in, course/instructor name, from what city/state/country, IP address and multiple details about their activity. In addition to being a key asset in identifying potential academic cheating, such audit trails are now imperative as both the department of education and schools move to reduce the skyrocketing financial aid fraud occurring (estimated at over $1B annually or 4% of all financial aid given out). Verifying WHO a student actually is over time speaks legions in determining the user experience. The data details out the changes that develop over time and compares this to averages and creates a flag for intervention. In this way, our clients have used data to identify cheating and to help confirm financial aid fraud [5]. Using sophisticated reports we baseline a client's unique user experience and suspicious activity events thereby creating a custom tool for each client.

Here are two examples of fraud identified through the BSI neural net analytics in higher education.

1. Our client asked us to run some forensics on a student who was acing their exams but doing very poorly on the quizzes/tests and other work. We ran the student through our neural net and found that there was another 5 student (emails) who were verifying their identity using the same IP location, same time, same classes, same device used etc. We did a full analysis on these students and found the same passcode was being used. We also found an instance where one student tried to verify identity and seemed to "forget" they used a different passcode for this fictitious student. They quickly made the change after failing to verify their identity. We determined that there was one or two real students involved and they were creating fictitious students identities and verifying their identity (using the same passcode for all). We reported this to our client. Most federal student aid requires no credit check and comes with few restrictions on how the money is spent. The likely fraud involved for 5 students using Pell Grants may run to $25,000 in just this one instance.

    - In some cases, students have the ability to apply multiple times for aid and at other colleges. To receive money they have to remain in the course until the date they receive their financial aid check (called the census date). They are supposed to be "academically active" from enrollment to this date. Some of our clients use the BioSig-ID verification and attendance reporting to monitor non active students.

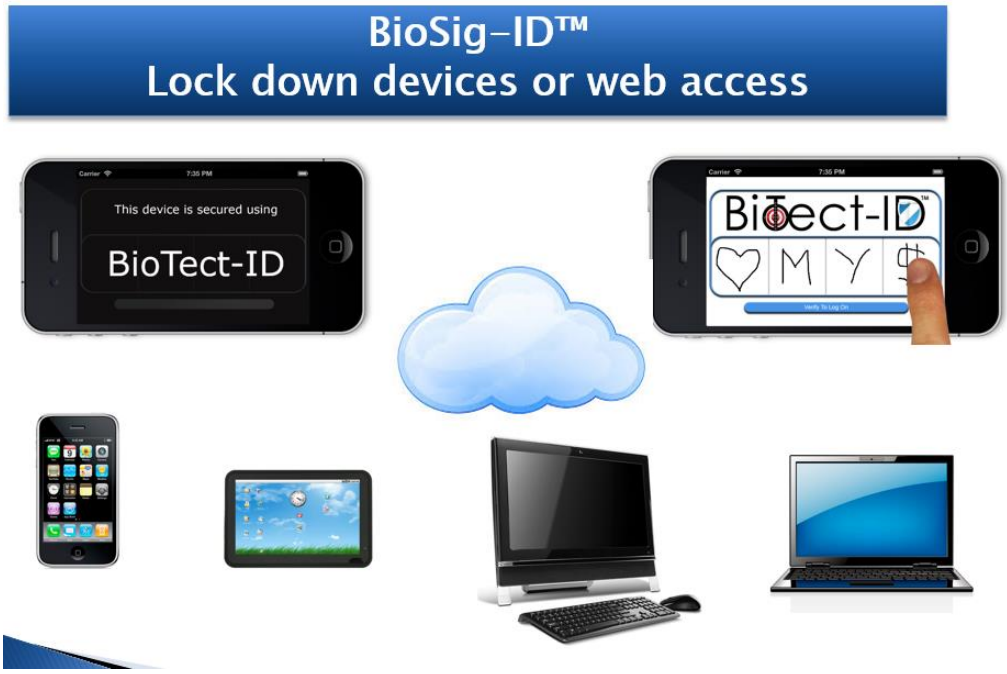
    - Here is a simplified version of how fraud is perpetuated. If the student stays in the course (versus getting kicked out), they will receive the difference in their Pell grant (call it $5,000) less their tuition that the school keeps (call it $1,000) = an expense check issued to them for $4,000.00. They receive this money and since schools have limited or no physical contact to verify the student's identity or attendance they can usually pocket the money for themselves and then disappear. Improper payments surrounding Pell Grants were over $829M as reported by the Dept. of education and probable direct loss was $187M in federal student aid [9, 10, 11].

2. We received a request from a client who suspected that a number of students were working together in a nursing course to get better grades. We ran the BSI neural net with these names over the previous few months and found some rich data. They were all verifying their identity from the same IP location, same provider and same class and within minutes of each other. We crossed matched this with exams times and found common times where they authenticated their identity. We then looked at the right and wrong answers to the questions and found they were the same. We were able to identify 6 students in what was found to be a fraud ring where a third party was helping the students take exams and providing coaching.

The BioSig-ID gesture biometrics can stop an imposter from immediately accessing your valuable digital assets and accounts. Combined with analytic reporting, the technology provides the teeth to flag certain target behaviors and report these to the client. The ability to provide our clients with evidence history of all the events surrounding the authentication activity is a powerful tool to combat fraud and ensure compliance with evolving regulations.

BioTect-ID™ - iOS, Android and Windows Mobile app/using BioSig-ID

Using the technology of BioSig-ID™, BioTect-ID™ locks down mobile devices and workstations by either replacing or supplementing the device's native lock screen. BioTect-ID™ binds the physical person to the device and only after successful authentication using BioSig-ID will device access be allowed. Identity credentials can be stored locally and updated through a service on the local network via Wi-Fi. Use cases include, securing consumer devices, gating employees' access to corporate mobile devices, tablets and workstations. Using the SaaS style configuration that we suggest allows for administration to monitor and change device access ability and reset passwords. Optional forensic audit trails show illicit attempts to gain access to the devices.



This configuration also allows for direct access for administrators allowing for easy re-provisioning for new users.

Summary

The concept of "drawing" a passcode to capture biometric gestures, without any need to purchase expensive hardware, is very innovative. In mere seconds and with only 3-4 characters, BioSig-ID™ software will establish whether the person who registered for the account is the same person who is attempting access. Identity verification in this SaaS based model is now used in over 70 countries.

Mandates from governments, enterprises and security federations to eliminate user name and passwords are advancing higher security options. All are looking at Multifactor Authentication. Passwords are not going away anytime soon. But they will be increasingly combined with another security factor(s) that will undoubtedly include biometrics especially software only ones. Being recently chosen by the White House NSTIC initiative to use BioSig-ID to prevent identity theft online is recognition of this unique technology. When you can combine the positive user experience, bring your own device, high accuracy and ease of use, you know you have a winning combination. Try it for yourself on our website, or call us and we will send you case reports or other information.

On our web site we offer a $500.00 reward for anyone who can break the passcode written by another user. This passcode is "Mom" – we actually show you a picture of what it looks like. Thousands have tried none have managed. http://biosig-id.com/goverify

BioSig-ID is a game changer. Use it to take control of your virtual identity.

More about the Editor:

Jeff Maynard, Founder and CEO of BSI, is the creator of several patents for gesture biometrics. Mr. Maynard is a respected and sought after speaker on the application of dynamic biometrics. He has been a guest lecturer at University of Texas-Dallas Business School, UTD Business School-New Business Competition Judge, a speaker at: 20 conferences, the Texas Technology Executives Network, the Technology Executive Network Group, CEO Net Weavers Group of Dallas, COIT Association for the Oklahoma Universities and Colleges, Finovate, WBT and is a regular presenter at University of North Texas division of MIS graduate studies. He is a writer for Blogger News.net, has been quoted and interviewed by many leading newspapers, radio and blogger sites and has published works on dynamic biometrics in the trade journals/magazines: Smart Card and Identity News, A&S International, Biometrics Technology Today and Nextgov.com.

White papers include: "Student ID Verification – What Institutions Need to Know" "Gesture Biometrics - A Game Changer for Remote Authentication", "Student Identity Proofing Solutions", "Internet Based Identity Proofing", "Online Signing Technology Using uSignOnline™" and "How to Integrate Software Biometrics in E-Prescribing".

Case Reports published include: "Use of BioSig-ID for Identity Verification from 1893 Online Students", "Case Report from University Maryland University College", "University of Texas System Case Report", and "Houston Community Colleges Case Report".

Update: BioSig-ID technology has been featured in: Security Newsletter, Security Product, US Tech Watch, Security Today, Dean and Provost, Enrollment Management Report, Community College Week, Successful Registrar, SecureID News, A&S International, Nextgov.com.

References:

1. Herb Weisbaum, 5 Lessons learned from Target security breach, NBC News, December 27, 2013.
2. Rick Nauert PhD, John M. Grohol, Psy.D, Technology to Replace Passwords Fails User Tests, Psych Central,. July 17, 2013, Funded by the National Institute of Standards and Technology: http://psychcentral.com/news/2013/07/17/technology-to-replace-passwords-fails-user-tests/57302.html
3. Study Report on Biometrics in E-Authentication 8/21/2006 Ver. 0.5- Conducted with NIST, the Office of Management and Budget (OMB) and the International Committee for Information Technology Standards (INCITS).
4. Biometric Signature ID Version 2.0, BioSig-ID User Authentication Solution Using Gesture Biometrics for Ease of Use, Enrollment Accuracy and Protection Evaluation. Tolly Group report # 211104, January 2011,

5. Data on file, Biometric Signature ID
6. BioPassword Enterprise Edition 3.2 Accuracy Evaluation of Keystroke Dynamics January 2007. Tolly Testing Report 207233
7. FFIEC Guidance for e-authentication using multifactor for online banking, October 12, 2005 and FFIEC Supplement June, 2011.
8. Kathleen Hickey, Dump passwords, use biometrics instead, says DARPA, Defense Systems, March 23, 2012.
9. Josh Mitchell, Wall street Journal. Student-Aid Scams Targeted by Schools, Government. Updated June 23, 2013, available at: http://online.wsj.com/news/articles/SB10001424127887323300004578557393479395544
10. Kathleen S. Tighe, Inspector General, Dept. of Education, , January 2013, The Inspector General's FY 2013 Management Challenges, available at: http://www2.ed.gov/about/offices/list/oig.
11. Testimony of Inspector General Kathleen S. Tighe U.S. Department of Education Office of Inspector General before the Subcommittee on Labor, Health and Human Services, Education, and Related Agencies Committee on Appropriations, U.S. House of Representatives - March 19, 2012
12. NIST SP 800-32 Section 2.2.4
13. National Institute of Standards and Technology, US Department of Commerce, Annual Report 2006, Computer Security Division – page 25

Example 1: Failure to validate identity using a bio-signature

Example 2: Activity captured in the BSI Audit trail

Activity Captured

BSI
BIOMETRIC SIGNATURE ID

Custom Detail Report

From: 10/2/2013 **To:** 10/2/2013
UserID:

User Name	Time	Signature Data	Client IP	Device	Context	Action	Succ	Acc.	App
jeff100212 @test.com	10/2/2013 12:22:26 PM		71.244.56.54 Coppell, TX, United States	None	Enroll	Create User	✓	0	Biosig-ID
jeff100212 @test.com	10/2/2013 12:22:49 PM	2 9 2 0	71.244.56.54 Coppell, TX, United States	Mouse	Enroll	Create Profile	✓	100	Biosig-ID
jeff100212 @test.com	10/2/2013 12:23:00 PM	2 9 2 0	71.244.56.54 Coppell, TX, United States	Mouse	Enroll	Create Profile	✓	92	Biosig-ID
jeff100212 @test.com	10/2/2013 12:23:09 PM	2920	71.244.56.54 Coppell, TX, United States	Mouse	Enroll	Create Profile	✓	96	Biosig-ID
jeff100212 @test.com	10/2/2013 12:24:15 PM	2920	71.244.56.54 Coppell, TX, United States	Mouse	Validate	Validate Profile	✓	98	Biosig-ID
jeff100212 @test.com	10/2/2013 12:24:30 PM		71.244.56.54 Coppell, TX, United States	Mouse	Validate	Validate Profile	✓	95	Biosig-ID
jeff100212 @test.com	10/2/2013 12:24:45 PM	2 9 2 0	71.244.56.54 Coppell, TX, United States	Mouse	Validate	Validate Profile	✗	26	Biosig-ID

Example 3: Neural net analytics for client reporting

Time, location, activity, history reports understand user experience and fraud potential.