

AUTHENWARE™ CERTIFIED FOR SECURITY

A SUMMARY OF THE INTERNATIONAL BIOMETRIC GROUP'S CERTIFICATION OF AUTHENWARE™

Executive Summary

Since 1996, the International Biometric Group (IBG) has provided technology-neutral, vendor-independent biometrics services, strategy, and solutions to government agencies, systems integrators, high-technology firms, and financial services organizations. IBG's Comparative Biometric Testing (CBT) is the industry's longest-running benchmarking test, complying with all published US and International biometric performance standards.

The Biometric Performance Certification program measures the accuracy and usability of commercial biometrics technologies such as AuthenWare™, a breakthrough second-factor authentication solution. AuthenWare utilizes a combination of biometric security algorithms, known as "keystroke dynamics," as well as a series of other behavioral and environmental heuristics to create a unique personal security pattern for each user of a system or application.

The following document summarizes the results and findings from IBG's standardized CBT Group 7 test that reviewed AuthenWare. Through the standardized CBT tests, IBG certified AuthenWare as meeting its mandated accuracy and usability criteria. The IBG's CBT Group 7 Testing results provides important comparative data that will assist AuthenWare customers and prospects as they assess the accuracy, performance and impact of using AuthenWare as a second-factor authentication solution in their organization.

IBG's performance test reports and certification lists are used by hundreds of government agencies and commercial entities in support of procurement and partnership decisions.

What was measured?

The IBG CBT's objective is to evaluate the usability and accuracy of biometric systems in terms of the following:

- **Match rates:** measures a systems' ability to correctly distinguish between genuine and impostor comparisons;
- **Enrollment and acquisition rates:** measures a systems' ability to successfully enroll and acquire samples from Test Subjects;
- **Level of effort:** measures a systems' ability to successfully enroll and acquire samples from Test Subjects with minimal transaction durations and repeated attempts / transactions.

What was not measured?

The IBG CBT only evaluates biometric systems' usability and accuracy. While an important comparison, for AuthenWare this only evaluates a portion of the overall solution effectiveness. In addition to a keystroke dynamics biometrics system, AuthenWare incorporates numerous other heuristics and environmental factors to authenticate users such as the IP address, screen resolution, browser version, normal time of use, and many others. These additional factors play an important part towards ensuring that AuthenWare accurately distinguishes one person from another to confirm a valid identity.

CBT Testing Methodology

IBG utilizes a sophisticated CBT evaluation platform that includes seven enrollment and recognition laptops / workstations, 11 storage and processing servers, IBG’s Test Management System (used to manage test subject IDs, visits and data), and IBG’s Data Analysis Application which generates, captures, and matches accuracy results.

The tests conducted on AuthenWare utilized 184 separate test subjects. Each subject participated in four separate sessions. During the first session, participants enrolled in AuthenWare’s keystroke dynamics biometric system; the three following sessions were utilized for repeat-visit recognition analysis. After the testing period was completed, a total of 7,731 keystroke signatures were analyzed (4,851 genuine attempts and 2,880 hacking attempts). Test subjects enrolled through a master account utilizing four test type rules (See Figure 1).

Figure 1.

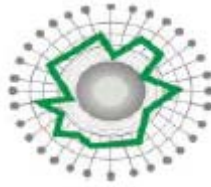
Test Type Rules		
Test	Login Convention	Password Convention
Type 1	Numeric email (e.g. 06001@ibgweb.com)	Three (3) common English words; 12 char. minimum; no spaces (e.g. bluebirdeats)
Type 2	Two (2) common English words; 8 char. minimum; no spaces (e.g. jumpingwhale)	Three (3) common English words; 8 char. minimum; no spaces (e.g. bluebirdeats)
Type 3	Two (2) common English words; 8 char. minimum; no spaces (e.g. jumpingwhale)	Three (3) common English words; 8 char. minimum; with spaces (e.g. blue bird eats)
Type 4	Two (2) common English words, plus “.subject”; no spaces (e.g. jumpingwhale.subject)	Three common English words; 8 char. minimum; no spaces (e.g. bluebirdeats)

AuthenWare Test Subjects were pre-registered with a unique userID (corresponding to their first session visit) and a randomly-generated password (e.g., users were unable to choose their own userID or Password). Additionally all of the Test Subjects participated in the test using an identical hardware and software environment.

It is important to point out that in a real-world customer deployment scenario, users would select their own userID and password (or at a minimum, their own password). Users develop “muscle memory” as they type and re-type their keystroke credentials over time. Additionally, the likelihood of each user having an identical hardware and software environment is very low for even the largest customer implementations. As such, these facts alone would dramatically enhance the uniqueness of each AuthenWare users’ typed patterns in a real-world situation.

Unfortunately, IBG’s testing methodology is unable to incorporate a meaningful way to evaluate these types of situations. See Figure 2 below for a representation of the AuthenWare unique user pattern.

Figure 2.



The AuthenWare Singularity PatternSM represents a user's unique typed pattern.

Within the CBT, there was no ability to accommodate bringing back test subjects each day, and it was not feasible to ask users to provide real userID, password and other login data because this would be exposed to other test subjects executing “impostor” attempts. As such, IBG pointed out the following in their CBT findings:

“It is very likely that real-world performance for AuthenWare will be even more robust than was observed [in the CBT].”

Results - Accuracy and Performance Findings

IBG evaluated the usability and accuracy of AuthenWare’s biometric authentication system, measuring the results for six performance metric categories. These categories are the following:

- (a) Failure to enroll rate (FTE)
- (b) Transactional failure to acquire rate (T-FTA)
- (c) Median enrollment transaction duration
- (d) Median recognition attempt duration
- (e) Transactional false match rate (T-FMR / FAR)
- (f) Transactional false non-match rate (T-FNMR/FRR)

IBG’s CBT certification of AuthenWare’s second-factor authentication accuracy and usability was performed at Security Level 3.¹ The CBT findings for AuthenWare include:

Usability

- The Failure to Enroll Rate (FTE) as certified by IBG was 0% (meaning all of the IBG Test Subjects were able to successfully enroll and be managed by AuthenWare)
- Median recognition times for users was < 11 seconds, including the time it took for them to type their userID and password

Accuracy

- The False Rejection Rate (FRR) during the first attempt as certified by IBG was only 3.26%
- As such, 96.74% of the first valid attempt by users to login were accepted

¹ AuthenWare offers customers Five Security Levels – 1 being the most “forgiving” level of security and 5 being the most secure. Level 3 was tested since it is the median level in terms of securing user access.

Figure 3 below provides the reader with a more complete review of AuthenWare’s biometric accuracy and usability outcomes.

Figure 3.

Performance Metrics					
Type	Sub-Category	Metric	Definition	AuthenWare Results	Certification Granted / Denied
Usability Metrics	Enrollment & Acquisition Rates	Failure to Enroll Rate (FTE)	Were any test subjects denied enrollment?	0% were denied enrollment.	GRANTED
		Transactional Failure to Acquire Rate (T-FTA)	Did the software fail to capture keystroke and environmental data?	0% of data was left un-captured.	GRANTED
	Level of Effort	Median Enrollment Transaction Duration	What was the median time needed to complete the biometric pattern training and /or enrollment?	< 80 seconds; To obtain enrollment AuthenWare requires a user to key in a userID and password 10 times.	GRANTED
		Median Recognition Attempt Duration	How much time is needed to analyze the biometric?	< 11 seconds; This includes the time (in seconds) that the user took to type in their userID and password.	GRANTED
Accuracy Metrics	Match Rates	Transactional False Match Rate (T-FMR / FAR)	How often were non-authorized users allowed to gain access?	< 3.26% of unauthorized attempts were granted access.*	GRANTED
		Transactional False Non-Match Rate (T-FNMR / FRR)	How often were authorized users denied access?	< 3.20% of authorized attempts were denied access	GRANTED

NOTE: Test subject “hackers” were provided with access to valid userID and passwords as part of this test. Typically, these userID and passwords are unique and not readily available to each user.

It is noteworthy that in a real-world implementation of AuthenWare, the product is used to augment a company’s primary security efforts. As such, the results found here would be even more outstanding in a live customer situation. Additionally, in the event they are needed, AuthenWare customers can easily provide users with several alternatives to solve situations such as False Acceptances and False Rejections directly within the system itself (such as offering them a second try, sending them a “One Time Password,” or a combination of both, etc.) In this way, AuthenWare customers can completely tailor the security environment as desired to further refine their results.

Analysis of the Findings and Results

Since the IBG test only measured the performance and accuracy of the biometric portion of AuthenWare, we conducted further tests to measure the impact of incorporating the heuristics and other environmental factors that the product uses into the IBG findings.

The Effective System False Rejection Rate is defined as the rate of false rejections that result after executing not only the initial biometric test, but also any additional attempts managed by business rules, One Time Password submissions and other decision mechanisms provided by the full AuthenWare system.

Security Level 5 is the most secure level of protection offered. AuthenWare offers a variety of ways for customers to tune FAR and FRR rates to within their desired tolerances. For example, while not specifically tested by IBG, at Security Level 5, AuthenWare achieves a False Acceptance Rate (FAR) of only 0.198% and a FRR of 8.19% using the same initial biometric test parameters.²

Offering the user a second opportunity to attempt validation reduces the FRR to 2.459%. If this second authentication attempt is also rejected, incorporating a third validation opportunity reduces the FRR even further to that of 0.738%. Adding a one-time password (or another validation check such as requiring the user to enter a pin number, etc.) would lower the effective System FRR to a worst-case scenario of only 0.00738%.

The implication of this is that 99.9915% of valid user logins will be authenticated as valid users. This means that less than one in every ten thousand authentication attempts would require any additional assistance outside the system (such as third factors, call center or other out of channel identity verifications). Many customers see a dramatic reduction in call center and help desk costs related to this innovative technology.

² Using the IBG test parameters for Level 3 as a baseline, AuthenWare correlated the IBG database with its larger test sample to extrapolate these findings.

Table of Effective System FAR and FRR results:

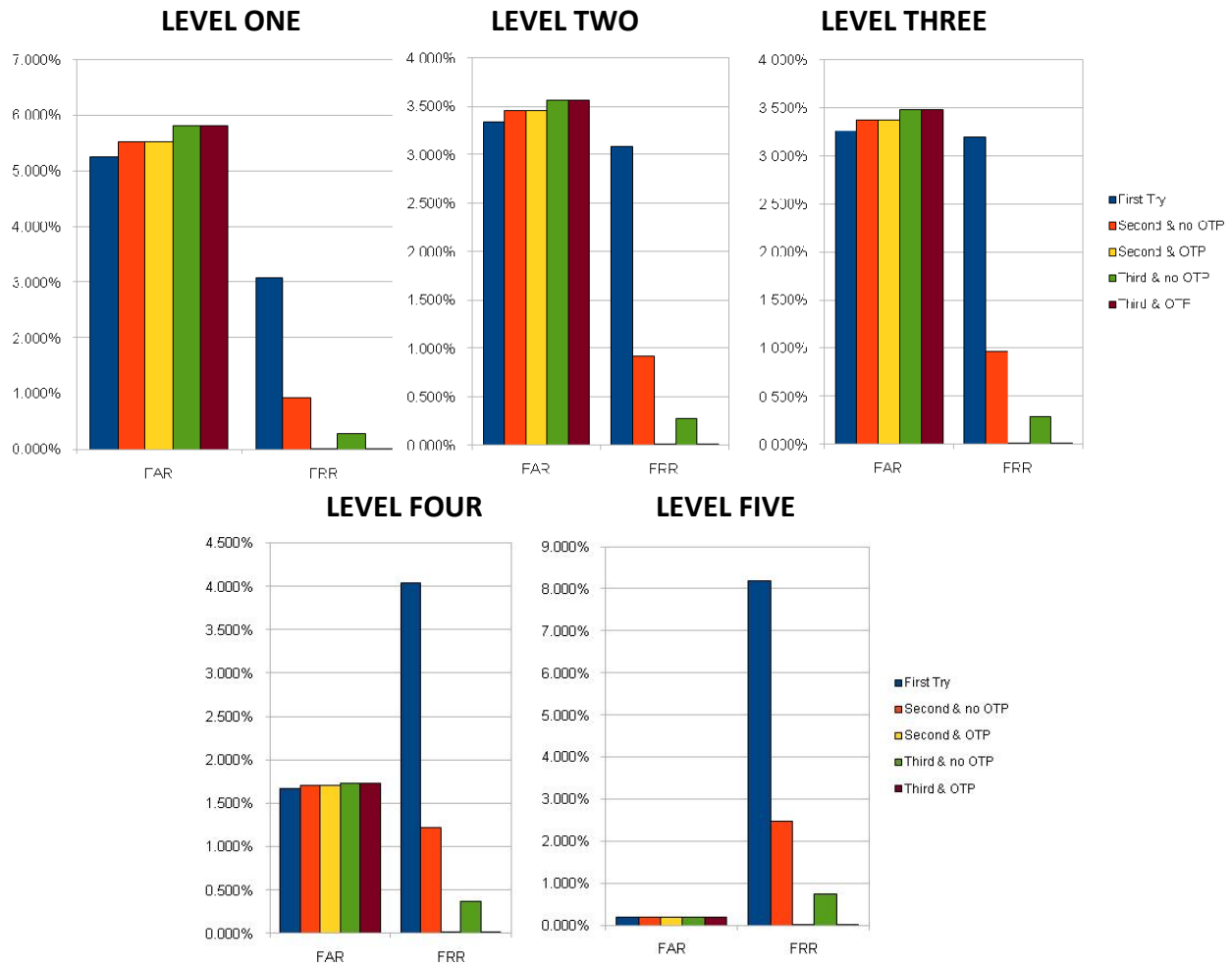
Figure 4. Summarizes the expected FAR and FRR rates – using only userID and password during a failed login procedure.

Security Level		First Attempt	Second Attempt	Third Attempt
1	FAR	5.249%	5.524%	5.814%
	FRR	3.088%	0.926%	0.278%
2	FAR	3.340%	3.451%	3.566%
	FRR	3.088%	0.926%	0.278%
3	FAR	3.260%	3.366%	3.476%
	FRR	3.200%	0.960%	0.288%
4	FAR	1.671%	1.699%	1.727%
	FRR	4.043%	1.213%	0.364%
5	FAR	0.198%	0.198%	0.199%
	FRR	8.198%	2.459%	0.738%

Figure 5. Summarizes the expected FAR and FRR rates – utilizing a userID and password and incorporating one additional validation check (a one-time password) during a failed login procedure.

Security Level		First Attempt	Second Attempt with OTP	Third Attempt with OTP
1	FAR	5.249%	5.524%	5.814%
	FRR	3.088%	0.009%	0.003%
2	FAR	3.340%	3.451%	3.566%
	FRR	3.088%	0.009%	0.003%
3	FAR	3.260%	3.366%	3.476%
	FRR	3.200%	0.010%	0.003%
4	FAR	1.671%	1.699%	1.727%
	FRR	4.043%	0.012%	0.004%
5	FAR	0.198%	0.198%	0.199%
	FRR	8.198%	0.025%	0.007%

Figure 6. Reliability Graphs Reflecting FAR and FRR for each Security Level



Conclusions

AuthenWare takes authentication and verification to a new level. Unlike other two-factor methods that can be bypassed, stolen, spoofed, phished or pharmed, with AuthenWare there is nothing for the users to forget, nothing for them to lose, and no reason for them to call the help desk. This technology can be deployed instantly to massive numbers of customers, requires no additional hardware, and is totally unobtrusive. It is simply one of the most accurate and effective implementations of biometrics in the market today.

The complete methodology, findings and other CBT details related to AuthenWare and other biometric technologies are available in the official IBG public report of CBT Group 7. To review the entire CBT Group 7 report, please visit www.biometricgroup.com, or contact us at info@authenware.com.

About AuthenWare™

AuthenWare™ Corporation is a leading provider of keystroke biometrics software. The Company's innovative authentication solution recognizes valid users through a unique personal security pattern coupled with behavioral and environmental characteristics. The solution lets authorized users in while keeping hackers out. AuthenWare is a global company headquartered in Miami, FL with offices around the world. Tens of millions of people use the Company's products every day in a variety of industries including financial services, government, transportation & logistics, manufacturing, telecommunications and retail.