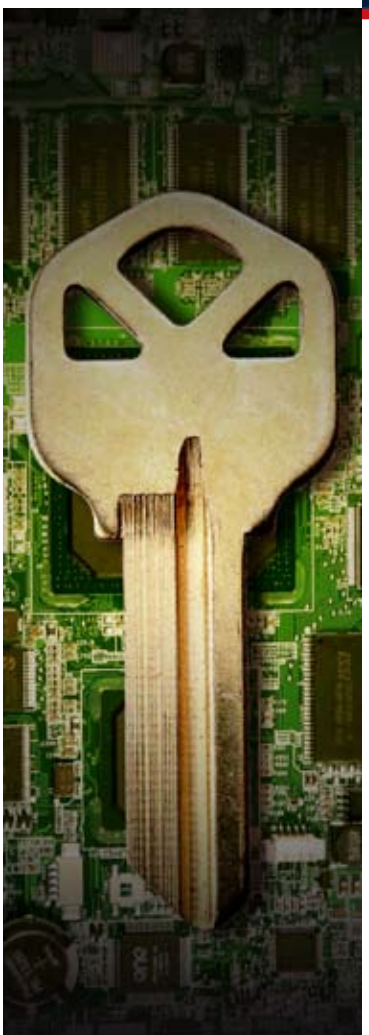
AuthenWare™
Security Redefined.



With AuthenWare® you can be sure that:

- **Potential fraud is identified and prevented**
- **Operation is undetectable to users**
- **Complements existing Web Fraud Detection software**

Detecting and Preventing Web Fraud

Utilizing AuthenWare® as an Early Fraud Detection Solution

Background

Online transactions are increasing exponentially for businesses such as financial institutions, online retailers, telecommunications providers and others. Unfortunately, online fraud is growing at an even faster pace, primarily due to user impersonation. No longer is the verification of users through username/password and challenge-response questions enough. With today's proliferation of spyware, phishing, keylogging and other cyberthreats, this simpleton approach is just not working. To prevent fraud losses, avoid regulatory action and prevent erosion of customer confidence, organizations must incorporate better ways to ensure the security of its online users.

While increased security is needed and demanded by companies across the globe today, there is an even more pressing need for tools that can assist them with early fraud detection and prevention. Some organizations have teams of specialized fraud detection personnel that continuously monitor online transactions to identify suspicious behavior and are currently armed with tools such as session surveillance software, computer fingerprinting technology and others. The obvious goal is to detect potential fraud and prevent it from occurring instead of after the fact.

Solution

AuthenWare® is state of the art software that helps companies dramatically increase security, stop identity theft, and reduce Web fraud, keylogging and other system breaches. It uniquely identifies the rightful owner of username/password credentials as they are being entered to make user validation easy, cost-effective, and reliable. It does so through an innovative system that combines keystroke dynamics and other heuristics to deliver strong security and forensics. The AuthenWare solution is very accurate and completely transparent to end users regardless of application, device or operating system – they just type in their credentials as they would normally do.

AuthenWare introduces a completely different way to assess fraud – it reviews the user's keystroke typing pattern. By working in concert with existing authentication and validation methods, this advanced biometric approach ensures that the user is the valid owner of the credentials presented. It adds a real-time online dimension to existing identity validation checks, with little to no impact on the real end-user. And AuthenWare will complement and integrate with any existing Web Fraud Detection software that an organization already has in place.

How it Works

AuthenWare validates user identity by using a series of biometric security algorithms that record and measure a person's unique typing patterns, as well as other behavioral and environmental heuristics. These biometric security algorithms enroll users into the system upon login by training the user keystroke pattern – known as the AuthenWare Singularity Pattern™. Once trained, AuthenWare's engine will compare the user's current session login typing pattern to the keystroke pattern that is stored in the database.

As an Early Fraud Detection tool, AuthenWare operates in a 'stealth' mode – undetectable to users. By doing so, AuthenWare will allow any user who enters credentials for an account to successfully log into that account. The system can be implemented to perform this level of authentication for a specific transaction, user or group of users, as well as at the application or system levels. If the keystroke pattern matches, then the user is permitted to proceed as they are normally authorized.

However, if the current typing pattern does not mathematically match the stored pattern for the user, then AuthenWare can trigger a real-time alarm to the company's Early Fraud Detection team notifying them that the system has been compromised. Similarly, rules can be set in AuthenWare to force the offending user unknowingly into a different environment – commonly referred to as a 'honeypot' – where the team can monitor their actions for forensic purposes, legal action or other desired results.

AuthenWare is highly accurate, and offers numerous settings to accommodate the unique needs of any organization. At the highest setting, false positives within AuthenWare have been certified at a mere 0.19%. As such, AuthenWare helps to better focus the efforts of the Fraud Detection department by enabling them to pursue only those instances where the likelihood of an actual fraud event is high.

AuthenWare provides four useful parameters to assist an organization's Fraud Detection team with their analysis:

1) The system result (whether it is or is not the rightful user)
2) Certainty percentage rate – a score calculated from the mathematical comparison of the pattern stored within AuthenWare to the particular login event.
3) User pattern quality (high quality implies more certainty).
4) Which user pattern was last evaluated in the case of multiple patterns per user – a user may log into the system from different computers or types of devices, such as a keyboard or smart phone.

Training the AuthenWare Singularity Pattern is accomplished in one of two manners and is entirely dependent upon the company's goals and customer policies:

- Using the "Progressive Mode" where the training is completely transparent to the user (e.g., no alert is returned until the user logs in 10 times).
- "Quick Mode," by requesting that the user log in 10 times in a row.

In the latter case, the rightful user is aware that the AuthenWare system is in place. This may be desirable to some organizations, since the higher-level of security (alerts will be issued) is immediately in place from the very first login onwards.

Integration with Other Web Fraud Tools

AuthenWare is packaged as a 100 percent service-oriented architecture (SOA) compliant Web services server. As such, AuthenWare can easily integrate with, and complement the functionality of existing tools such as Arcot, Actimize, RSA, 41st Parameter and other Web Fraud-related technologies. Evaluating the user-oriented keystroke patterns of AuthenWare, combined with the computer device-fingerprinting capabilities of these tools allows organizations to more accurately identify valid user attempts, even when they are coming from a different location or device.

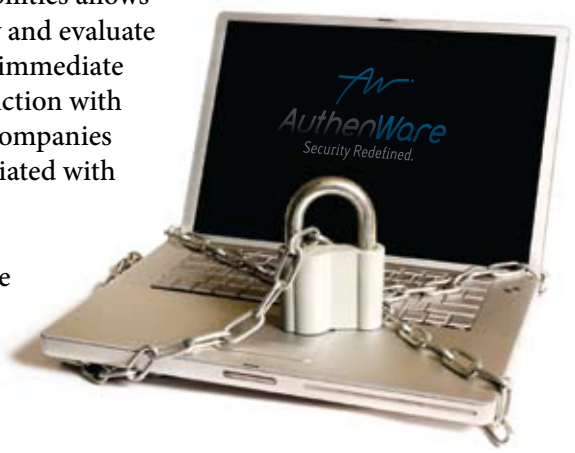
Benefits of AuthenWare for Early Fraud Detection

Incorporating AuthenWare as an Early Fraud Detection solution offers companies the following benefits:

- For users logging in from a different computer, but with a correct keystroke pattern, surveillance becomes unnecessary, since it is the rightful user;
- When both the computer device-fingerprint and user keystroke pattern are suspicious, the fraud detection team can be confident (with a nearly 100 percent certainty) that fraud is being attempted through a different computer;
- When the computer device-fingerprint is correct, but the user keystroke pattern is suspicious, there is an especially delicate fraud situation – quite possibly the thief has stolen the rightful user's equipment or has accesses the equipment at the user's workplace or home;
- For transactions deemed a risk by the organization's Web Fraud or other rules engine, it is possible to initiate additional keystroke pattern account verification later in the transaction cycle to further validate the user through passphrase or reentry of password;
- Similarly, the addition of keystroke pattern verification step later in the transaction cycle can help confirm that a request is coming from a validated user and not a Man-In-the-Middle or Man-In-the-Browser attack.

Conclusion

Utilizing AuthenWare's keystroke pattern capabilities allows Early Fraud Detection teams to rapidly identify and evaluate specific occurences of potential fraud and take immediate action. Whether used stand-alone, or in conjunction with computer device-fingerprinting technologies, companies can now easily determine the level of risk associated with any type of online transaction.



AuthenWare offers organizations a comprehensive solution that dramatically reduces the effort and cost of fraud detection, while greatly improving their ability to stop the culprit in his or her tracks, before any damage occurs. AuthenWare - Security Redefined.

About AuthenWare®

AuthenWare® Corporation is a leading cybersecurity software provider. The Company's innovative tokenless authentication system delivers strong security through a combination of keystroke dynamics, behavioral and environmental characteristics to minimize identity theft, web fraud and other system vulnerabilities. The AuthenWare solution creates a unique personal security pattern that recognizes authorized users while keeping hackers out. AuthenWare is 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, healthcare, telecommunications and online retailers.

For more information, visit www.authenware.com.

AuthenWare™
Security Redefined.

AuthenWare Corporation
1221 Brickell Avenue, 9th Floor
Miami, Florida 33131
T: +1 305 377-8768
F: +1 305 374-6146
info@authenware.com
www.authenware.com