

Authernative Granted U.S. Patent for User Authentication System Operation Modes

REDWOOD CITY, Calif., Oct. 14 (SEND2PRESS NEWSWIRE) – Authernative, Inc., the developer of innovative [user authentication and identity management](#) technologies, announced today that the United States Patent and Trademark Office has granted the company a patent for operation modes in a user authentication system. The newly issued U.S. Patent No. 7,577,987 titled, “Operation modes for user authentication system based on random partial pattern recognition” (“the Patent”) describes a system of operation modes for self-service account administration of a “what user knows” based authentication system using random partial pattern recognition.

The Patent builds on Authernative’s portfolio of user authentication patents by covering the operation modes for secure self-service set-up and self-reset of user accounts and authentication credentials. The patented system enables users to securely set-up and reset accounts and authentication credentials including usernames, e-mail addresses, personal profiles, security questions, temporary credentials, password credentials, and other authentication credentials used in a single- or multi-factor authentication based on random partial pattern recognition.

The security tiers and features offered by the newly patented system enhance the well known benefits of online self-service user authentication systems such as reduced support costs, anytime/anywhere access, and increased productivity. The result is an unparalleled secure self-service account administration that is immune from the security challenges and attacks plaguing user account login, set-up and reset. For example, security questions are commonly used for resetting passwords, but they alone do not provide sufficient security because they can be compromised or guessed by identity thieves. By contrast, Authernative’s system protects against such back-door attacks by providing multi-tier account reset security, where at least two tiers must be successfully traversed before a user can reset the account.

The account login and reset security is further enhanced by random partial pattern recognition authentication, where the authentication server never challenges the user to provide the full secret pattern (authentication code such as a password, PIN, or graphical pattern), but instead requests a session-specific random subset of the secret pattern (“One Time Pattern”™ (OTP)). This significantly reduces the credential’s entropy leakage and renders one-time authentication responses difficult to compromise, protecting users’ credentials against phishing, key logging, brute force, Trojan horse and other spyware attacks. Moreover, the method’s virtual reference grid and the scalable combinatorial capacity of the secret pattern provide high security against guessing attacks, while delivering a simple and more engaging user experience.

Authernative's patented system also provides multi-tier account set-up security options including temporary credentials, out-of-band delivery, and account release options. Additionally, the system logs all account administration and authentication events enabling automatic or human monitoring to detect unusual account administration activity, conduct forensic research, and meet regulatory compliance. This patent adds to the protected intellectual property and technology foundation for the company's AuthGuard® user authentication product.

AuthGuard® offers a suite of one-factor, layered, and multi-factor authentication to meet a variety of security and usability requirements. AuthGuard® user authentication is electronically mass deployable, has scalable security, high usability, low total cost of ownership, and efficient integration/customization options with legacy environments.

The product provides fully automated operation modes for secure login, set-up, and reset of all AuthGuard® authentication methods including enhanced password, graphical password, one-time challenge one-time response, out-of-band, one-time pin, and secure in-band authentication. The AuthGuard® crypto security of data-in-transit and data-at-rest is assured by the CrossSecure® Authernative® Cryptographic Module that has been FIPS 140-2 certified by the National Institute of Standards and Technology (USA).

Authernative's granted patent solidifies the company's ability to provide innovative, secure and cost-effective user authentication solutions. With identity theft, cyber crime, and data breaches escalating to an all time high, enterprises, government agencies, online service providers, and consumers can benefit from the AuthGuard® authentication product to secure access to networks, extranets, portals, applications, data and devices.

About Authernative, Inc.:

Authernative is a leading provider of innovative software security solutions offering identity and access management capabilities including authentication, authorization, administration, and auditing. The company's products are used to prevent unauthorized online access to confidential data, protected resources, and financial transactions. They allow organizations to lower the cost of providing, deploying and managing user authentication for enabling e-commerce, e-government, and regulatory compliance.

More information: www.authernative.com.

News issued by: Authernative, Inc.



Send2Press® Newswire

Original Image: https://www.send2press.com/wire/images/09-1014-Autherntv_72dpi.jpg

#

Original Story ID: (5395) :: 2009-10-1014-004

Original Keywords: AuthGuard user authentication, CrosSecure, patent, security, encryption, multi-factor, Government, Identity management, phishing, compliance, identity theft, Authernative, e-commerce, US Patent 7577987, One Time Pattern, regulatory compliance, tech patents Authernative, Inc. Redwood City California