

THE RHYTHM OF SECURITY

STRENGTHENING LOGIN ACCESS WITH ADVANCED KEYSTROKE DYNAMICS SOFTWARE

FÉLIX RACCA, FOUNDER AND CHIEF TECHNOLOGY OFFICER OF AUTHENWARE

 **AuthenWare**™
Security Redefined.



“Every American depends—directly or indirectly—on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal well-being.”

—Sen. Barack Obama, July 2008



INTRODUCTION

It is difficult today for many to imagine living outside of a tri-screen household – television, computer, and cell phone. Certainly, these devices bring unprecedented access and efficiency to businesses, critical infrastructures, and military operations; however, in the process of advancing convenience, security is compromised.

In 2008, 285 million consumer records were breached, and the financial repercussions of compromised online data rose to nearly \$1 trillion. Such augmented expenditures are a result of the expanding web of electronic networks which will entangle over 1 trillion devices at the conclusion of 2009.

In response to the cybersecurity pandemic, CIO's and IT executives have moved to construct more complicated firewalls and password rules, but have thus far failed to widely adopt a stronger authentication infrastructure. As a result, Internet crimes dramatically rise, and their effects are only perpetuated by increasingly sophisticated cybercriminals who execute intricate attacks.

In the search for a stronger online archetype, network access points must move beyond identifying a third-party factor (i.e., a password, key fob, etc.) and toward authenticating the administrator of such devices.

1 IDENTITY PROBLEMS IN THE CONNECTED WORLD

Every day, 10 million new web pages are added and 55 billion emails sent. Social networks that contain real-time updates of our everyday activities have expanded to millions of users. Facebook alone hosts more than 275 million individuals and adds to that number by approximately 1 million every day. Further, 15 percent of mobile phones purchased last year were smart phones, enabling millions of global citizens to easily connect to each other.

Certainly, the expanded interconnectivity encourages convenience; however, it often surpasses the capabilities of today's security apparatuses which inevitably lead to identity and data theft. The security vulnerabilities are a derivative of multiple societal and technological occurrences.

Saturation of the Username and Password Paradigm

The average Internet user today holds approximately 30 accounts that are accessed with a keyed-in password or PIN number. The buttress of the username/password security structure, however, is originality. Each account should have different login credentials that utilize a unique combination of letters, numbers and symbols. Such data should also remain completely confidential, as security is further compromised each time the passphrase is recorded — electronically or physically. Because of the Internet's proliferation, such rules have become nearly impossible to implement, and the method has thereby developed into an outdated paradigm.

Sophistication of Hacking Technologies

At the same time, cybercrime has developed into a \$105 billion underground industry. Even amateur hackers can access advanced key loggers that trace the activities of infected computers, or implement spyware that sifts through files and sends back any data that appears to be a username and password. More sophisticated cybercriminals develop their own botnets, malware, and viruses that leach into electronic systems and often create entire networks of infected computers that can be activated and effectively shut down even the largest websites.

The Forfeiting of Privacy

Social networking sites have saturated cyberspace with personal information that users have opted to make public. As such, even secret security questions (where you were born, your mother's maiden name, etc.) are ineffective as Internet users often choose to grant the public access to a vast majority of that information.

End-User Malpractice

Despite continual media coverage and awareness efforts, 11 percent of adults do not install security software on their personal computers and 45 percent only utilize data protection programs they can access for free, according to a recent study. Even amidst the April 2009 Conficker virus scare which produced worldwide headlines, one-in-ten Internet users did not take the necessary steps to protect corporate or personal computers from the virus.

Creation of a Security Black Hole with Password Sharing

The secrecy of passwords — and the security of a network — is often willingly compromised in the workplace. It is not uncommon for employees to share login information with colleagues to better service clients when out of the office, and although illegal, many businesses even encourage coworkers to share passwords for online accounts in order to save money on subscriptions. However, the exploitation of that shared username and password can greatly compromise the entire internal network, as hackers need only one weak link to infiltrate and access the entire system.



THE NEED FOR PROTECTION—15 percent of mobile phones purchased last year were smart phones, enabling millions of global citizens to easily connect to each other.

2 NON-CONVENTIONAL ALTERNATIVES

Longer passwords and additional firewall rules compromise security as IT directors and end users rarely implement the complex structures properly. For example, many firewalls require administrators to effectively manage tens of thousands of rules. If even one rule is foregone, the entire system is made vulnerable.

As such, online infrastructures that combine multiple aspects of an individual's electronically measurable identity create stronger systems that authenticate the user rather than simply verify a particular password. Specifically, there are three means to recognize an individual online – by what they know, what they have, and how they act.

What the Individual Knows

This element has evolved into a traditional mode of identification, encompassing techniques such as the requirement of a valid username/password or an appropriate security question answer. As previously mentioned, this identification factor often acts as a significant security vulnerability due to the proliferation of personal information, explosion of data sharing, and sophistication of hacking technologies. Nonetheless, it remains a convenient and user-friendly form of identification.

What the Individual Has

Whether it is a USB drive, magnetic card, or key fob, this approach requires individuals to carry a tangible device in order to identify themselves. Such a technique is often effective when utilized against social engineering and data theft. However, physical objects are undoubtedly subject to misplacement and theft. If lost, individuals must wait until a new gadget is generated – costing time and financial resources.

Digital certifications are also components of this identification method. In many cases certificates can be downloaded by simply logging in with the correct username and password. As such, an online thief can easily mask their computer as if it was the valid user's device, and thereby gain access to any applications that require the certificate.

How the Individual Behaves

Analyzing how Internet users conduct themselves (also termed the science of biometrics) is the only identification element that also provides authentication of the user, as it measures aspects of the individual's behavior or being that cannot be separated from the account's owner. Specifically, this approach includes physiological (i.e., fingerprint analysis and retinal scans) and behavioral (i.e., voice recognition and keystroke dynamics) biometrics.

In many cases, biometric authentication requires additional hardware, such as scanners or digital recorders. The exception is keystroke dynamics which is a software-based application that grants or denies access according to innate typing patterns and behavioral heuristics.

3 OBSERVING BEHAVIORAL KEYSTROKE PATTERNS

Keystroke dynamics applications automatically combine two of the three electronic identification elements – what a person knows and how they behave. Specifically, such technology will review the dwell time (duration a key is held down) and flight time (period between keystrokes) of an entry. Without the correct username and password in conjunction with an accurate behavioral typing pattern, access is denied.

The concept was developed over a century ago. Just 20 years after the first telegraph transmission was sent in 1844, operators became attuned to the unique tempo and rhythm of their colleagues, gaining the ability to identify the sender by their distinct pattern.

By World War II, such authentication methods became a practical art. With a methodology termed as “the fist of the sender,” trained ears could identify the unique manner which Morse code communication was tapped out, adding an ancillary layer of confidence in the messages that were relayed. In the midst of battle, practiced communicators could distinguish a friend from an adversary.

Until recently, only an acute ear could come close to identifying these patterns. However, next-generation keystroke dynamics software allows individuals to be authenticated by their typing cadence with a level of accuracy beyond anything human senses can observe. Further, the digital monitor can track and adjust to the dynamic process of keying in the same data numerous times, ensuring long-term accuracy.

KEYSTROKE DYNAMICS APPLIED

Utilizing AuthenWare's® technologies, individuals can continue to identify themselves with a traditional username and password. While users may not even recognize a difference at the login site, the analysis conducted behind the scenes is starkly different. Rather than measuring what is keyed into a text field, the software will analyze how information is typed and the environment in which it was typed in. Specifically, AuthenWare's version of keystroke dynamics technology implements the following elements:

Fuzzy Logic

Humans are not binary creatures. Our built environment, mood and level of concentration create a multitude of variables in typing rhythms and cadences. As such, AuthenWare measures credentials with natural, "fuzzy logic" to achieve optimum accuracy. The algorithmic function allows the security server to analyze data as a multi-valued object, capturing the fractions of a variable rather than simply the whole number value.

Singularity Comprehension

Similar to how each individual has distinctive birthmarks, keystroke patterns contain one-of-a-kind elements that easily distinguish one typist from another. Under this principle, AuthenWare pinpoints "singularities" and utilizes these unique tendencies to augment distinctions between one typist and the next.

Behavioral Heuristics

This technology considers more than just direct keystroke patterns, carefully calculating typical activities taken by the valid user. Specifically, AuthenWare includes a behavioral heuristics engine which analyzes mouse movements, typical typing mistakes, Internet browser versions, and preferred times of use, among other factors.

User Notification Systems

If credentials are breached and an invalid login is attempted, the registered user will immediately be notified of the suspected violation, in addition to ensuring that the hacker is blocked from account access.



CONCLUSION

With 1.6 billion users, the Internet has changed the world's methods of operation. An email, blog post, or Twitter update can spread news and information from one continent to the next at the click of a button. Still, security vulnerabilities limit innovation's application.

The means of access Internet users have become accustomed to simply identify the correct sequence of letters, numbers, and symbols. However, authenticating the typist behind those seemingly opaque keystrokes will fortify security procedures while maintaining the user-friendly attributes of a customary username and password.

By blending the conventional "what the user knows" identification model with the innovative "how the user behaves" authentication method, online security is fortified and the effects of identity theft can be minimized, ensuring a safe application of next-generation communication technologies.



ABOUT AUTHENWARE

AuthenWare® Corporation is a leading cybersecurity software provider focused on fighting identity theft. 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.

