DATA SECURITY MANAGEMENT

THE FIFTH FACTOR: BEHAVIOR PROFILING OPENS NEW POSSIBILITIES FOR WEB ACCESS CONTROL

Bob Forbes

INSIDE
The Authentication World Today; The Fifth Factor: How You Behave; Benefits of Trust-Based Authentication; The Active Information Agent: A 24/7 Security Expert; Trust Systems Open the Doors to Change

INTRODUCTION
The Internet continues to revolutionize E-business, not solely through direct consumer sales, but by enabling companies to share enormous amounts of information with a wider, distributed user base. New information partnerships enable creative synergies at all levels of business, signifying an exciting time of growth and change. And in this new business environment, to the nimble go the spoils.

However, increased openness means increased risk. Threats to corporate data security loom perilous. The total annual cost of online security violations tops $15 billion, with nearly 60 percent of attacks coming from internal sources. Recent surveys of U.S. corporations show that 85 percent reported security breaches in the last six months, with two thirds of those leading to direct financial losses.

To be successful, a company must protect its valuable information assets and ensure that

PAYOFF IDEA
Currently, all authentication systems rely on one or more of the following four identification factors: what you know, what you have, who you are, and where you are. Now, behavior profiling, a new technology that aims to address these complicated issues, offers a way to significantly boost the confidence level of conventional authentication methods while providing a cost-efficient alternative to existing hardware-based approaches. This flexible, software-based security layer can also significantly ease integration of newer authentication methods.
distribution of its crucial data is secure. Simple password or cookie-based authentication procedures — the way most people access their networks today — do not provide sufficient protection to meet current threats. No amount of password complexity or IS diligence will prevail in the face of users who leave their ever-changing passwords on a Post-it® in their cubicles. Unfortunately, with current solutions, the old IS joke rings true: the best security is “No One Gets In.”

Achieving a significant level of strong network security currently requires costly investments in client authentication hardware such as smart cards, tokens, or biometric readers. Different units of a company often have different security needs, leading to implementation of incompatible technologies as each struggles to meet their individual requirements.

The result is a tangle of competing systems that require custom programming efforts, tangential to a company’s core proficiency, that deplete precious resources. Of greater importance (in a world where the quick succeed) is the challenge of integrating the hardware authentication systems of potential new partners. This often requires additional customization, adding an unnecessary hindrance to new business initiatives and growth.

Now, behavior profiling, a new technology that aims to address these complicated issues, offers a way to significantly boost the confidence level of conventional authentication methods while providing a cost-efficient alternative to existing hardware-based approaches. This flexible, software-based security layer can also significantly ease integration of newer authentication methods.

THE AUTHENTICATION WORLD TODAY

Electronic authentication — the process by which a person attempts to gain access to a network — attempts to answer two basic questions about a potential system user: (1) who are you? (identification), and (2) are you who you claim to be? (authentication). Different types of authentication technologies answer these questions with differing levels of confidence. The level of confidence, or trust, required from a given authentication system before it provides a user access to data is related to the value of the information; the more valuable the asset being protected, the higher the level of confidence needed before it can be released.

Currently, all authentication systems rely on one or more of the following four identification factors:

- **What you know.** Currently, 90 percent of authentication systems employ “what-you-know” technologies such as a password, PIN, social security number, mother’s maiden name, etc.
- **What you have.** So-called “key-based” systems rely on a smart card, token, or digital certificate.
• **Who you are.** Biometric systems, such as voice analyzers, iris scanners, and fingerprint readers, match client-side physical identification with an existing biological profile.

• **Where you are.** Location-based systems are tied to the computer, not the user, and can analyze such information as the originating phone number of a computer, its IP address, and, in the case of some wireless mobile locators, its geographical location.

Each factor employed alone has drawbacks and limitations, as do systems that rely solely on one factor. For example, the level of security provided by “what-you-know” systems is directly related to the difficulty required to steal or obtain the user’s information. Higher levels of security are obtained by increasing the complexity of passwords and by resetting them on a regular basis. “What-you-have” systems require distribution of costly client-side hardware, both keys and readers, with security related to users’ ability to retain (not lose) their identifying key. “Who-you-are” systems also require expensive hardware deployment and system integration.

The most recently introduced approach — “where-you-are” systems — is tied to the computer, not the user. Therefore, security is dependent on the inaccessibility of the machine requesting access.

Higher levels of security are achieved through the combination of these four factors; redundancy adds confidence. Two-factor authentication is more secure than one; two factors across categories are exponentially more secure. For example, a password and a biometric return a much higher level of confidence than do two “what you haves” (e.g., a smart card and a token).

Adding one of the higher (non-password) factors to an existing authentication system can be expensive and complicated. Most require client-side hardware or software that then must be integrated into the existing network, sometimes requiring writing to special APIs to ensure seamless operation. Client-side systems require training and put the responsibility for maintaining security in the hands of the user. Because security is not their core competency, these users require ongoing support — from key replacement to frequent password resetting.

Increased numbers of errors and exceptions — the denial of service to qualified users — invariably lead to higher administrative costs. These issues get amplified in an extranet situation, when the system is open to new business partners.

**THE FIFTH FACTOR: HOW YOU BEHAVE**

Behavior profiling (BP) introduces a fifth parameter — how you behave — that expands the authentication universe and opens up a new range of possibilities for strong security. Simply put, behavior profiling tracks details — such as habitual time of transaction, frequency of access,
typical usage pattern, user origin, role within the company, and others — to build and maintain a dynamic “profile” that represents each user’s normal behavior. Once the profile is defined, active information agent (AIA) software compares a user’s current attempt to access the network against a historical record of his or her previous attempts.

The evaluation of a behavior profile returns a third type of response — a modifier — that can be weighted to reflect those behaviors most likely to provide identity assurance. Introducing a behavior profile modifier into a security system provides an opportunity to reconceptualize the basis of strong authentication, thinking of it now in terms of trust. A trust-based approach creates a new, dynamic environment in which to secure your data.

Trust-based authentication assigns each asset — including applications, data, or network access itself — a “trust threshold” that must be met before access is granted. Each authentication factor in use is assigned a level of trust that represents the relative confidence that the evidence it presents confirms a user’s identity. Access to a given asset requires a combination of factors to meet the trust threshold assigned to it.

Unlike pass/fail systems, there is no single, unique action required to pass. Unlike biometrics, there is no single template to which to compare current input. Instead, a trust-based system can achieve a measurable level of confidence in a variety of ways by combining any of the five authentication factors.

Here is an example. Staff accountant Dave accesses his financial application at 8 every morning from his desktop computer using his password. Hacker W*Rez did a brief cubicle cruise yesterday and managed to steal Dave’s newly issued password (Dave’s IS department frequently resets its passwords in an attempt to improve security; Dave frequently forgets them). Today, when Dave arrives for work, he tries to log in but cannot recall his new password, which he swears he wrote down somewhere.

In a traditional situation, Dave would need to call IS to reset and reissue his password. Instead of an absolute pass/fail condition, however, a dynamic trust system allows for varied means of achieving adequate authentication. Because Dave is logging in from his normal location at his normal time, his behavior profile earns him enough trust that he is who he claims to be to earn him a second chance. The system presents Dave with a challenge response question that he answers correctly. Because a “what-do-you-know” factor plus the trust value of his current behavior equals the asset’s required trust threshold, Dave is immediately given access. He suffers no downtime and requires no tech support or help desk intervention.

That night, Hacker W*Rez attempts to gain access from a different location using Dave’s stolen password. While the password works, his behavior is inconsistent with Dave’s behavior profile, so he does not
achieve the trust level required for access. He, too, is offered a challenge response question, which he cannot answer, and access is denied. With no additional effort on Dave’s behalf, the standard password-based authentication system is rendered stronger.

From a security standpoint, behavior is very difficult to reproduce, hack, or steal. It exists in the background, out of the user’s knowledge or control, so there is no chance a “Post-it pirate” like W*Rez could steal it. Duplicating it requires a potential hacker to perform extensive system monitoring to learn his target’s habits. Dynamic trust lets the good guys in (even when they are not perfect) and keeps the bad guys out (even when they think they are).

**BENEFITS OF TRUST-BASED AUTHENTICATION**

Shifting to a trust-based/behavior profile paradigm provides a range of possibilities not previously achievable in typical authentication systems. In other words, Dave’s password plus his behavior-profile trust score might be high enough to enter the accounting program, but not the upcoming corporate profit/loss (P/L) statement, which today requires a higher trust level to access. Tomorrow, if we want to make the P/L available, we do not need to reclassify Dave (and 16 other accountants in his department), or worse yet, equip them with smart cards and readers. We simply lower the trust level assigned to the P/L report. This greatly simplifies asset security management and allows the protection of only sensitive information. Assigning the proper level of security to each resource minimizes costs, improves the user experience, and stops the security leaks that can impede the growth of business.

As seen in Dave’s situation, long, multiple character-type passwords with short reset periods — required to counter trust deficiencies inherent in passwords — mean more forgotten passwords. A trust-based system increases ease of access, especially in cases of altered or forgotten credentials, by automatically providing a second chance to log in. This reduces errors and exceptions that can account for up to 40 percent of all help desk calls. By providing an alternate means of boosting password security, behavior profiling permits shorter, easier passwords that require fewer resets. Password resets account for the highest ongoing cost of network security.

When passwords are forgotten, the dynamic nature of a trust-based system also allows for user self-service. To make changes to a system, the security level needed to access an administration screen must be greater than the security level being changed. By employing alternate means of trust generation, perhaps by combining the trust earned from predictable behavior with that from two challenge questions, a user can achieve strong enough verification to modify his or her account, further reducing security administration costs.
All the decisions required to implement these processes happen in the background and are completely transparent, with no active user behavior required. Therefore, no training, hardware rollout, or infrastructure ramp-up is required.

THE ACTIVE INFORMATION AGENT: A 24/7 SECURITY EXPERT

At the heart of a trust-based behavior profiling system is an active information agent (AIA). Applying computational models from cogitative neuroscience, the AIA actively manages the network authorization apparatus in real-time, automatically adjusting the security level of various assets based on the nature of transactions and the presence of possible threats. It is like having a staff of full-time security experts monitoring your network 24/7.

Essentially a sophisticated analysis tool, the AIA monitors multiple variables — such as a user’s behavior profile, profiles of similar users, and known patterns of fraud — to dynamically adjust the trust level of the user attempting to gain access. In the example of the accountant, Dave is able to access applications at his usual time with just his password and normal behavior pattern because the AIA automatically raises his trust level at that time. If he wants to log in after-hours, his trust level will be lower, and additional trust — in the form of higher authentication — will be required. Similarly, as Dave’s behavior profile grows, his expected behaviors are assigned higher levels of trust, allowing him greater access with less interference.

At the same time it is dynamically managing trust levels and behavior profiles, the active information agent is also working to determine the best means of meeting the required level of acceptance criteria. These decisions, made in response to an administrator’s preprogrammed priorities, help optimize not only the user’s authentication experience, but also the efficient operation of the entire network.

Rules-based authentication systems — those tied to a specific authentication method — cannot assess the probability of a user’s validity and substitute an alternative authentication procedure.

The AIA is pretrained with basic knowledge such as known patterns of security attack and the difference between the natural behavior of users and the systematic behavior common to automated network assaults, but it also “learns” as it grows. By constantly sifting and refining its data, it becomes capable of increasingly powerful predictive decisions. Unlike traditional authentication systems that become more vulnerable with increased exposure (necessitating those frequent password changes), an AIA-based system paradoxically becomes more secure over time, self-optimizing as it builds ever more accurate behavior profiles of its users.
The AIA tracks not only individual user patterns but also the patterns of a group, such as “Accountants.” Thus, new users can be added to this type of system and achieve relative confidence quickly if they are bootstrapped by their group pattern. This can significantly decrease the time the AIA needs to build a unique profile and achieve strong predictive success.

When the system does encounter suspicious activity, it can be instructed to provide a range of responses, including adjustment of an asset’s trust threshold, administration notification, detailed logging, and complete denial of access. It can also adjust security levels in response to the presence of a known threat.

All of this simultaneous activity occurs without the need for human monitoring. The AIA automates a vigilance that would take several hundred full-time security experts to achieve. But because the software acts as a single agent, all security administration can be performed through a centralized interface accessible over the network from any location.

TRUST SYSTEMS OPEN THE DOORS TO CHANGE

A behavior profile-based trust system opens the doors to a level of flexibility and adaptability previously unattainable (or attainable at great cost and complexity) by traditional authentication systems. Each type of traditional authentication method — biometric, passkey, informational — generates a specific type of coded information in response to input. Some return binary data, some metric, still others categorical or textual. Each output is like a specific language. This requires a traditional network, and all of its shared applications, to be customized with a series of APIs capable of understanding each input language.

To visualize this, imagine a company that builds docking ports for space stations. Each ship wanting to dock at the station requires a different docking mechanism (API) to achieve an airtight, secure connection. So in addition to building ports — the company’s core proficiency — one must also finesse unique docking mechanisms for each type of ship that may want to dock at the station, plus unique mechanisms for any new ships that might be introduced in the future. The only alternative would be to dictate precisely what type of ship can dock at the station, thus limiting the use of the station to only one kind of ship and potentially stifling innovation.

A behavior profile-based system — and all the assets protected within it — speaks a single language, the language of trust. The AIA can understand the various types of output coming from different authentication modules, all essentially different mathematical expressions of confidence, and convert them into levels of trust the system understands. It acts as a sort of universal translator that allows a company to integrate all its existing authentication modules, plus any future ones, into a functioning whole nimbly, seamlessly, and transparently.
In the space station metaphor, you equip all your docking ports with a single mechanism (trust) capable of adapting itself to any ship that might want to use the station. Instead of making ten, or twenty, or thirty different types of docking devices, you make one. This frees you from the responsibility of maintaining and adapting your equipment to shifting future demands and allows you to concentrate on your core competency, building docking ports. And just as importantly, it allows your customers and partners to fly and build any kind of ship they want. At your space station, all are welcome and all are secure today.

A trust-based system acts as a transparent layer between crucial network applications and existing security systems. Being software-based and residing in a turnkey system easily married to existing servers, AIA/trust technology presents a single sustainable infrastructure. This immediately eases integration with diverse existing authentication modules, and greatly facilitates compatibility with new business partners and opportunities. It eliminates the need to write additional APIs as the network expands, reduces future maintenance liability, and eliminates the need for hardware uniformity. As a bonus, trust systems even provide security where none currently exists, essentially extending “docking” services to those older ships that were not equipped to dock at all.

CONCLUSION
The increased and very real threat of data crime necessitates higher security for many networks that previously seemed safe. Software-based behavior-profiling technology represents a compelling alternative to current authentication technologies. As a sustainable infrastructure solution, it provides a high level of security, unprecedented flexibility, and dynamic security management at a price point far lower than traditional hardware-based solutions. It also provides users with an almost transparent experience designed to let the good guys in (and keep the bad guys out) with a minimum of downtime and inconvenience.

When thinking of security and its relationship to the growth of a company, remember that you do not put brakes on a car to go slower, but rather, to go faster.

Bob Forbes is executive vice president of Authentor Systems Inc., a provider of Web access management and authentication systems.