WHITE PAPER

Practical Methods for Improving Authentication

An Osterman Research White Paper

Published June 2013

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Organizations need better methods of authentication for their users to access corporate applications, systems and data sources during the normal course of their work. To validate this thesis, Osterman Research conducted a survey in early June 2013 with members of its survey panel. The survey found that:

- The typical user accesses a median of 10 different applications or systems during a normal workday.
- 14% of users identify current access methods as "painful" – they would like a better or easier way to access corporate resources; another 68% feel that their access methods are reasonable, but could use improvement.
- 82% of respondents sometimes use the same login credentials for multiple systems, resulting in greater risk for their organizations.
- 33% of respondents need to have login credentials reset more than four times per year simply because they forget their username and/or password for the applications and systems needed to do their work.
- The more applications that users must employ in their work, the less satisfied they are with the methods available to access them.

KEY TAKEAWAYS

- There is a wide range of authentication methods that organizations can employ to grant their users access to the applications, systems and data sources that they must use during the course of their work. These methods range from simple username/password authentication to sophisticated, risk-based methods and can also include "multi-factor" authentication to include physical devices users carry (like cards, phones or security tokens).
- Authentication carries with it a natural tension between the ease of use that users would like to have when accessing corporate systems and the high degree of security that IT would like to impose in order to mitigate the risk of unauthorized access.
- The growing number of applications, systems and data sources – coupled with the Bring Your Own Device and Bring Your Own Credentials phenomena – is increasing the risk that organizations face because of the reduced level of governance that IT departments have over access to corporate systems.
- The goal of any organization should be to find the appropriate balance between robust password management, ease of use and security of corporate assets.

Organizations need better methods of authentication for their users to access corporate applications, systems and data sources during the normal course of their work.

ABOUT THIS WHITE PAPER

This white paper discusses important aspects of good authentication practices, the options that organizations have available to them when attempting to balance ease of use with robust security, and recommendations for improving authentication. The white paper also provides a brief overview of its sponsor, SecureKey Technologies, and their relevant offerings.

A REVIEW OF AUTHENTICATION METHODS

BASIC METHODS

There are a number of relatively basic methods for accessing applications and systems, including username/password combinations, challenge/response systems and image/pattern methods, as discussed below:

- **Username/password**
  The combination of a username and password is the most commonly used authentication method and the one with which almost all users are familiar and comfortable. Because this is such a simple authentication method and can be hacked by determined criminals, it is acceptable for accessing information assets that are not critical to an organization. Its advantage is familiarity and ease of use, but it has two primary disadvantages:

  - The ability for hackers to easily guess users' passwords.

  - Many users will employ the same access credentials for multiple systems, so determining the username/password combination for one system will grant access to multiple systems. For example, in the survey we conducted for this white paper, 82% of respondents indicated that they sometimes use the same username/password combination for multiple applications or systems.

- **Challenge question/response**
  A challenge/response system requires answering a question that has previously been entered into an authentication system. For example, many banks require account holders to provide information like their father's middle name, city of birth, city of marriage, name of best man or maid of honor, or street lived on as a child. If the challenge question cannot be answered successfully, the individual is not given the opportunity to enter their password.

  This form of authentication is more secure than a simple username/password combination because it requires individuals to possess additional information beyond just a username and password. It is not entirely secure, however, because unauthorized parties could still guess or otherwise determine responses to the challenge questions. For example, because many users share a great deal of personal information on social media sites, they may inadvertently publish the answers to challenge questions in Facebook or similar posts.

- **Images or patterns**
  Some applications or systems will require the user to enter letters and/or numbers that are provided in an image in addition to their username and password. This form of authentication, also known as CAPTCHA[i], can prevent robots or automated dictionary attacks from penetrating a system because these tools are generally incapable of identifying text in images. Despite this, some have successfully defeated CAPTCHA systems[ii]. At least one vendor is providing image-based CAPTCHA, but this approach has yet to be widely implemented.

MORE SECURE AND SOPHISTICATED METHODS

Other, more sophisticated methods of authentication include one-time password tokens, out-of-band authentication, seals and certificate-based authentication:

- **One-time password tokens**
  One-time passwords (OTPs) are a better and more secure form of authentication. With this approach, a password is continually changed, each password being available for only a single access attempt. OTPs can be provided via SMS/text messaging on a mobile device, on a USB flash drive, via traditional postal mail[iii] or with some other physical method of delivery. OTPs are much more secure than traditional authentication systems, but can be vulnerable to phishing attacks[iv].

- **Out-of-band authentication**
  Out-of-band (OOB) systems use two different networks to authenticate users, such as a computer network that a user is trying to access and a mobile provider's network to which the user has access. Many banks, for example, use OOB to transmit authentication information via a telephone when they attempt to access their accounts through a Web site. OOB is a reasonably strong form of authentication, since an unauthorized user would require access to both

In the survey we conducted for this white paper, 82% of respondents indicated that they sometimes use the same username/password combination for multiple applications or systems.

networks to hack into an account. However, it has the disadvantage of being more cumbersome for users to employ. Plus, some OOB systems have been defeated - a variant of the Zeus botnet, for example, has successfully been able to defeat OOB authentication when used for banking purposes.

- **Seals**
  Seals are used by some banking sites and employ an image presented to the user that he or she has chosen when setting up access to the site. This element of mutual authentication gives users the confidence that the site asking for their credentials is not an impostor Web site, thereby helping to prevent spoofing. However, seals can be subverted by man-in-the-middle attacks.

- **Certificate-based authentication**
  This method of authentication continues to be a popular mechanism, allowing mutual authentication between parties. While certificate-based authentication is not without its difficulties (such as scaling to large numbers of users), it remains a reliable and trusted form of authentication.

THE MOST SECURE METHODS

The most secure methods of authentication include biometric solutions and multiple-factor authentication:

- **Biometric authentication**
  Biometric authentication uses a scan of a fingerprint, face, iris, finger length, voice, typing rhythm or some other unique, biological or behavioral characteristic of an individual who is authorized to access an application or system. These systems have the advantage of being difficult to spoof by unauthorized parties, but false rejections are possible, which makes them unsuitable in many situations.

  For example, a user who has cut his or her finger and then attempts to access a system via a fingerprint scan, or who is more stressed than when they provided their voiceprint might be rejected. A user whose typing rhythm is being checked might have a different rhythm while holding a cup of coffee, when using an unfamiliar computer or when they are tired. Also, if a user's password changes, old rhythm baselines may no longer be usable and the user would need to retrain the system. Consequently, while biometric authentication can be useful, it is often not desirable.

- **Multi-factor authentication methods**
  Methods that use combinations of the methods described above, such as a username/password combination in conjunction with a smart card, are among the most secure methods of authentication. Using multiple factors can provide more security than a single method can provide, but adding factors to the authentication process can be more cumbersome for authorized users. Tokens and smart cards are often used as part of a two-factor or multi-factor authentication system. This method has the disadvantages of higher initial and ongoing administration costs, and a physical component of the authentication (e.g., a smart card) that can be lost by end users. However, multi-factor authentication is quite familiar to most users because it is commonly used when accessing bank accounts through an ATM.

THE NEED FOR BETTER AUTHENTICATION

FOCUS HEAVILY ON THE USER EXPERIENCE TO IMPROVE SECURITY

A critical consideration for any organization's authentication management strategy is its usability. Although the usability of authentication will vary based on a number of factors, such as the number of systems to which individuals have access, the

A critical consideration for any organization's authentication management strategy is its usability.

sensitivity of the information they contain and even the corporate culture, the following should be considered important components of a sound authentication management strategy:

- **Calendar reminders**
  These will remind users to change their passwords at pre-determined intervals, such as every 30 or 90 days. Calendar reminders are an important security tool not only because they improve security by reminding users to change passwords at regular intervals, but because they can also reduce user frustration by eliminating the "surprise" of a forced password change at an inopportune time.

- **Password reset**
  A password-reset capability can make authentication more usable, particularly for users who access systems only occasionally. By permitting users to reset their own passwords without the intervention of IT, an organization will realize the benefit of making the system more usable, while also reducing the number of help desk calls. Plus, by eliminating a barrier to the use of corporate applications and systems, a password reset option helps in user adoption, such as when IT is attempting to have users employ a new system. Obviously, safeguards must be put in place for automated systems, but they are an essential element to ensure that applications are accessible and usable.

- **Password recovery**
  Using a password recovery system, users get to see their password or a hint when they are offline. This is very useful for individuals who seldom access an application or system or otherwise forget their password. Password recovery allows users to gain access to a system without having to return to an office (which can be an IT requirement for highly secure systems) or reconnect to the corporate network.

- **Password meters**
  These will test the strength of passwords by offering a score of a password's strength. Although password meters provided by unknown sources should not be trusted because of their potential to be used by cybercriminals, password meters from known sources can be a good method for educating users about the security of passwords they select. They make password quality more understandable to the average user by offering immediate feedback on the quality and wisdom of their password choices.

It is essential to move beyond the status quo for authentication. What may have worked just 12 months ago may not work today as a result of several factors, not least of which is the BYOD phenomenon.

It is essential to move beyond the status quo for authentication. What may have worked just 12 months ago may not work today as a result of several factors, not least of which is the Bring Your Own Device (BYOD) phenomenon. For example, in a survey conducted by Osterman Research in February and March 2013, we discovered that most of the iPhones and Android smartphones in use in the typical organization are personally owned. Moreover, employees in the majority of organizations have deployed tools like Dropbox and are storing corporate data in the cloud using access controls that may not be appropriate for the data stored there. Consequently, organizations need to place a high priority on evaluating their authentication capabilities and adjusting them as needed.

CREATING GOOD AUTHENTICATION POLICIES AND PRACTICES

Most organizations try to implement good password practices, such as requiring users to create strong passwords or employing a limited-strikes system to prevent unauthorized users from gaining access to a system. However, it is vital that an organization implement authentication capabilities that are appropriate to the applications and data that are being accessed, the user base of employees or non-employees who are given access, the mobility of the workforce and so forth. For example, students who access a system to see their grades or admissions records – and that will access a page that shows only an identification number – typically would

need only a username and password to access this system. By contrast, a defense contractor's system that allows individuals to make changes to confidential information should require accessors to go through a more rigorous authentication process. This might include using a username/password plus a physical token-based scheme that will prevent access after two failed attempts.

Making the issue more difficult is that most corporate users, as well as consumers, must access multiple systems that require authentication. For example, the Osterman Research survey conducted for this white paper found that the average user accesses a median of 10 different applications or systems during the normal course of their work.

Therein lies the basic tension in establishing a good authentication management system: systems that are easy for users to access will put sensitive corporate data assets at risk of unauthorized access, but authentication procedures that are too rigorous will make systems much less usable. The goal, then, is to match the authentication procedure with the sensitivity of the application or database being accessed in order to achieve a proper balance between usability and security. Users should be involved in helping to define the authentication solution so that it meets their requirements and ensures that users will be willing to use it. Users are best served when they are active participants in providing which trusted credentials work best for them. User convenience is increased, cost of service is decreased, and the assurance level is also increased.

A NEED TO FOCUS ON USABILITY AND BEST PRACTICES

Every organization should continually focus on the evolving needs of their business and regularly monitor and evaluate the balance between authentication usability and security for every system to which users have access. The goal is to move beyond the status quo of traditional authentication management and instead find the right balance between the often-competing interests of usability and security. Although relatively few IT organizations have the luxury of abundant time or resources to undertake these regular evaluations, they can implement risk-based authentication or similar schemes, solutions that will significantly improve both the access to and security of key corporate data assets.

Every organization should continually focus on the evolving needs of their business and regularly monitor and evaluate the balance between authentication usability and security.

BYOD MEANS USERS HAVE MORE CHOICES

As discussed above, the BYOD phenomenon that has taken significant hold in most organizations further complicates authentication management because users simply have more devices and applications available to access corporate applications, systems and data resources. Similarly, the Bring Your Own Credentials (BYOC) problem that is part and parcel with BYOD also makes things more tricky for IT and business decision makers because, as with devices and applications, users have more control over authentication practices than perhaps they should.

BYOD and BYOC can result in a reduced level of governance that comes from IT's loss of control over personally owned devices and how users access corporate systems, the data that is sent from and stored on these devices, and the potential loss of intellectual property that can result from the physical loss of a device that cannot be wiped. BYOD and BYOC clearly complicate the issue of authentication management, but it is an issue that decision makers must address.

IMPROVING SECURITY THROUGH RISK-BASED AUTHENTICATION

RISK-BASED AUTHENTICATION DEFINED

Risk-based authentication simply means matching the level of authentication required to access a resource with the risk that is inherent in the access. For example, an insurance agent who accesses a corporate system to get up-to-date information on the company or its products can, in most cases, employ a username and password

because the information being accessed is not highly sensitive or confidential. If the information were accessed by an unauthorized party it would create little risk for the company. However, if the agent must review corporate records from a customer's portfolio that includes their annual income, medical history, investments and other sensitive content, this would require a much stronger level of authentication because of the sensitivity of the information, the highly regulated nature of that aspect of the company's operations, and the risk inherent in an unauthorized party gaining access to this data.

IMPORTANT ELEMENTS OF RISK-BASED AUTHENTICATION

There are a variety of elements that are involved in developing and managing a risk-based authentication system:

- **Profile user behavior**
  The initial step in establishing a risk-based authentication scheme is evaluating user behavior. This may include data such as the time of day at which users access an application or system, the IP address from which the user accesses the system, the platform used to access the system, and other key pieces of data. It is important to note that while much of this information may not be a reliable form of authentication when used by independently, using a number of these elements in combination to create a user profile is a useful way to authenticate users.

  Creating a baseline of user behavior over time is essential in both creating a credibility score for each user and in detecting anomalies in user behavior that might indicate a possible security breach. As just one example, if an employee accesses a corporate system over a long period of time only on weekdays and only during work hours, but then attempts to access the system at 2:00am on a Sunday morning, this type of anomaly can be used to indicate a possible hacking attempt and a requirement for more rigorous authentication.

- **Create an authentication score for each user**
  The next step in the process is to create a credibility score for each user that will be used to determine the authentication method appropriate for a particular application or situation. For example, a user who regularly attempts to gain access to a system only on weekdays, from an IP address that is managed behind the corporate firewall, and that is attempting access using an IT-provided desktop computer from his or her office in San Francisco will generate a good authentication score. However, if the same legitimate user who attempts access at 6:00am on a Sunday morning from a Starbucks Wi-Fi hotspot in Brussels using an iPad will most likely generate a lower score because the behavior is out of the ordinary. A lower score can signal possible cybercriminal activity and so can indicate that a higher level of authentication is required.

- **Link the score with the risk of the transaction**
  Next is to match each user's credibility score with the sensitivity of the data someone is attempting to access and then adjusting the authentication method in real time based on that score. For example, a brokerage firm might use a simple, risk-based authentication system when account holders attempt to gain access to their account information. Upon initial access to the system, the user will be required to enter his or her account name, followed by a challenge question, followed by his or her password. Subsequent access from the same computer will require only the account name and password. However, if a customer accesses the account from a different computer, the challenge question will again be asked.

- **The need to block malicious activity in real time**
  The ability to employ a rule engine that can block access, trigger an alarm, contact a supervisor or take some other appropriate action is the primary benefit of monitoring user behavior. If admins can view access attempts on a real time dashboard or be alerted to things like multiple invalid username errors in a short

There are a variety of elements that are involved in developing and managing a risk-based authen-tication system.

period of time, this could result in an alert sent to an administrator so that the situation can be investigated.

It is important to note that risk-based authentication works well in environments with high traffic because there are a large number of data points (access times, locations, platforms, etc.) from which to build a baseline of "normal" behavior that can be compared to potentially anomalous behavior. However, risk-based authentication is not as useful in low traffic situations simply because the number of data points available may not be sufficient to create a reliable baseline of normal behavior.

WAYS TO IMPROVE AUTHENTICATION

WHERE IS AN ORGANIZATION ON THE SECURITY CONTINUUM?

The initial step in improving authentication and overall risk management is to determine where the organization is on the security continuum:

- **Good**
  Robust password management
- **Better**
  Robust password management combined with good usability
- **Best**
  Robust password management, good usability and very high security

This is particularly important as users migrate to both IT-deployed and personally selected cloud applications. Organizations need to satisfy both the usability of their authentication capabilities and reduce the risk to their critical systems and data assets.

EVALUATE THE REQUIREMENTS OF THE BUSINESS OVER TIME

Next, decision makers need to evaluate the current requirements of the business and how these will evolve over time. For example, as users become more mobile as part of formal or informal telework initiatives, or as they increasingly use cloud-based applications, they will access corporate data and applications from IP addresses that are not managed by the IT department. Plus, they will attempt access from IT-supplied platforms and personal devices, such as smartphones or tablet computers. This means that credibility scores must evolve over time to the new norms of how users attempt access.

Moreover, organizations must continually monitor the risk levels associated with data assets, corporate systems and other tools that users may employ in response to regulatory requirements, advice from legal counsel, recent data breaches, cybercriminal activity and other factors. For example, a corporate database may contain non-sensitive data that can safely be accessed using only a username and password. However, a change in an organization's offerings or a new industry regulation may mean that sensitive data will be added to the database, increasing the risk of inappropriate access of that content store.

DETERMINE THE APPROPRIATE BALANCE BETWEEN RISK AND USABILITY

It is also important to strike the right balance between the risk of unauthorized access to sensitive applications or data and the ease with which those systems are accessed. For example, when access is locked down too tightly, false positives can occur and lock out legitimate users, potentially with damaging impacts on employee productivity or customer relations. Plus, too much security for a particular system – such as a requirement for very strong passwords that are virtually impossible to

Organizations must continually monitor the risk levels associated with data assets, corporate systems and other tools that users may employ.

remember – can actually increase risk because many users will write down their login credentials or they will not use the system as often as they should.

IMPLEMENT THE RIGHT TECHNOLOGIES

Finally, it is important that the appropriate technologies are deployed so that the best balance between security and risk can be achieved. The decision process should include a review of all available technology solutions, including on-premise, cloud-based and hybrid solutions.

SPONSOR OF THIS WHITE PAPER

SecureKey is a global leader in building identity and authentication ecosystems. We make it easy to incorporate strong authentication into a wide range of online, mobile and in-person identity and authentication applications for financial services, government, healthcare, converged commerce, and extended enterprises. Our groundbreaking, cloud-based briidge.net™ platform combines powerful, device-based security with federated authentication to enhance privacy, create trust, and increase convenience for consumers – using devices and credentials they already have. SecureKey is a Privacy by Design (PbD) Ambassador based in Toronto, Canada, with backing from leading technology, payments and mobile network operators.

SecureKey is dedicated to the principle that proving your identity, or perhaps more importantly, protecting it – should be easy. We put the user at the center of identity and authentication solutions to help business and government enhance privacy, create trust, and increase convenience for users – using devices and credentials users already have!

briidge.net™ is SecureKey's groundbreaking, cloud-based identity and authentication platform that combines strong, device-based security with privacy-enhanced federated authentication.

briidge.net™ Enterprise – provides step-up multi-factor authentication in combination with existing user ID and password or card-based enterprise credentials.

- Provides strong protection against man-in-the-middle, browser-in-the-middle and other impersonation attacks
- Uses devices and credentials users already have, enabled with briidge.net™ DNA
- Easily integrates into online or mobile applications with minimal administrative overhead
- Highly scalable and cost-effective for the mass consumer market
- Simple, convenient user experience – Click, Snap, or Tap

briidge.net™ Exchange – combines strong, device-based security with privacy-enhanced federation.

- Reduces password reset and re-registration costs for infrequently used services like government, utilities, and telecom self-service
- Uses social media or other 3rd party credentials with enhanced security and privacy
- Simple, convenient user experience – Click, Snap or Tap

For more information about SecureKey products and solutions, please visit www.securekey.com.

www.securekey.com

twitter.com/SecureKey

info@securekey.com

---

[i] Completely Automated Public Turing Test to Tell Computers and Humans Apart
[ii] http://www.cs.sfu.ca/~mori/research/gimpy/
[iii] http://en.wikipedia.org/wiki/One-time_password#Paper
[iv] http://paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html