Authentication in the Enterprise: Current and Changing Requirements

An Osterman Research White Paper

Published August 2009

Sponsored By PistolStar

OSTERMANRESEARCH

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

Why You Should Read This White Paper

Organizations of all sizes possess information and a variety of other electronic assets, including email data stores, corporate portal document repositories, customer relationship management systems, desktop productivity suites, financial systems and a host of other tools and capabilities. These systems contain a growing quantity – and a growing proportion – of most companies' sensitive information, trade secrets, financial records, contracts with clients and a wide range of other data types.

Add to this the proliferation of points for accessing corporate data, including desktop computers, laptops, netbooks, smartphones, employees' home computers, etc.; not to mention that employees access these resources from corporate offices behind the firewall, from hotel rooms while traveling, from their local Starbucks, from their home wireless networks and other locations.

The data assets managed by most organizations vary widely in their value and in terms of the consequences that can ensue if the data is leaked inadvertently or maliciously. For example, an email sent from a clerical employee's Hotmail account while at work is unlikely to be as valuable as an attachment sent by a firm's chief financial officer to an external auditor. However, the growing sensitivity of corporate data makes breaches increasingly risky. For example, the authentication trends survey that we conducted for this report showed that 53% of those involved in managing their organizations' IT infrastructure are concerned or very concerned about data breaches from external sources. Further, 27% of those surveyed are more concerned about these data breaches than they were just 12 months ago.

THERE IS DEFINITELY ROOM FOR IMPROVEMENT

Because of the sensitivity of information maintained within most corporate data stores, organizations must employ authentication mechanisms to protect these systems and their content from access by unauthorized parties. Authentication mechanisms vary widely in their efficacy at protecting content, in their ease of use for end users, and in the cost of maintaining them. Further, as the quantity of electronic content grows, as this data becomes more sensitive, and as hackers and others with malicious intent become more adept at penetrating defenses, authentication mechanisms will have to keep pace in order to protect corporate data from those that should not have access to it.

However, most organizations realize that their authentication capabilities leave much to be desired. For example, the authentication trends survey that we conducted for this white paper asked, "Overall, what grade (A, B, C, D or F) would you give to your current authentication management?" Only 5% of respondents gave their organization an "A", while 54% gave themselves a "C" grade or lower.

ABOUT THIS WHITE PAPER

This white paper discusses the current state of authentication and trends that Osterman Research sees as shaping the future of authentication. We also discuss the results of a primary market research survey conducted in July 2009 specifically for this white paper in which we queried corporate decision makers about the current state of authentication and the problems that their organizations are having with their current mechanisms. Finally, we discuss the relevant offerings of PistolStar, the sponsor of this white paper.

The Status of Passwords Today

PASSWORDS ARE PERVASIVE…

Virtually all of us use username/password combinations to access work-related and personal systems, including our corporate email system, Twitter, Facebook, corporate portal document repositories, customer relationship management systems, networks, Web portals, file servers, and the list goes on. For example, in the authentication trends survey that we conducted for this white paper, we found that the average user accesses a mean of 12.3 different password-protected systems on a typical day at work. Some users have more, some have fewer, but all of us access a large number of systems for which we need some sort of authentication to gain access.

….BUT THEY HAVE SECURITY DRAWBACKS

However, password-protection, while necessary as a basic form of authentication to various systems, has several drawbacks:

- Users typically use the same password to access multiple systems. For example, in the authentication trends survey that we conducted for this white paper, we found that 85% of users at least sometimes use the same password to access more than one system. This means that if a hacker, or even a well-meaning co-worker, learns the password for access to one corporate system, he or she has most often gained access to most or all of the other systems to which that user has access.

- Even if passwords are used correctly and one unique password is used for each system, users find this to be difficult and cumbersome to manage. For example, our survey found that 61% of users report that they have too many passwords to remember. Further, 62% of users report that they have forgotten at least one username and/or password during the past 12 months, and 19% have had to call the help desk to retrieve it.

- Because users often create passwords that are easy for them to remember, such as their birthdate or a common word, passwords are easy for hackers and others to guess. This allows hackers or others to guess user's passwords or use a dictionary attack to attempt to gain access. For example, in a high-profile case earlier in 2009, the password of a well-known US politician was guessed and an unauthorized party gained access to sensitive emails.

The Growing Concern Around Protecting Access to Critical Data

INCREASING NUMBER AND SCOPE OF DATA BREACHES

There are many tools and systems from which confidential or sensitive information can be sent in violation of corporate policy, or that can be accessed by unauthorized third parties. These include:

- Corporate email systems used on desktops, laptops, mobile devices and home computers.
- Consumer and enterprise instant messaging systems, including Web-based chat tools
- Personal Webmail accounts used at work
- Thumbdrives and other portable storage devices
- Social networking tools like Facebook and LinkedIn
- Other Web 2.0 applications, including wikis and blogs
- File transfer protocol (FTP) tools
- Skype and other consumer-oriented VoIP tools
- Peer-to-peer file-sharing tools
- Message boards and forums

As a result, there are a large number of data sources and communications tools that organizations must monitor closely in order to protect corporate data from accidental or unauthorized distribution, although email and instant messaging are clearly the most important channels to monitor given their pervasive and much more frequent use by employees than most other tools.

THE RISING LEVEL OF RISK IN THE TYPICAL ENTERPRISE

Data breaches can be *very* expensive: for example, an Osterman Research survey found that if a data breach were to occur in which disclosure of the breach would have to be made to customers and other external contacts, nearly two-thirds of organizations estimated that a single such breach would cost their organization at least $100,000, not to mention other operational costs, damage to their brand and other problems.

Organizations that do not properly address data protection can suffer a variety of problems, including:

- **Loss of intellectual property**
  Email systems, file transfer systems, instant messaging systems, blogs, wikis, Web tools, thumbdrives and other tools are used to store, send and receive confidential information. The result is that trade secrets, designs, proprietary processes and other knowledge assets can all be compromised if not adequately protected.

- **Loss of reputation**
  If an electronic communication system is used in violation of corporate policy, an organization can suffer serious damage to its reputation.

- **Compromise of corporate security**
  A failure to properly monitor outbound communications can lead to a variety of security-related problems, including compromised PCs acting as zombies for sending spam and consumer instant messaging clients that can spread worms and malware. There are a variety of tools commonly used in the workplace that bypass conventional security defenses, including Skype, peer-to-peer file-sharing software and chat tools.

- **Violation of statutes and compliance requirements**
  By not adequately monitoring and managing access to corporate systems, organizations can run afoul of a wide variety of statutes that require data to be protected and retained.

An example of the last point above is California's SB1386 (the Database Security Breach Notification Act), a far reaching law that requires any holder of personal information about a California resident to notify anyone in the state whose information may have been compromised in some way.

HACKERS ARE MORE ACTIVE THAN EVER

There are a variety of ever more sophisticated attacks being directed against corporate networks. For example, modular Trojans – also known as multi-stage downloaders – operate on a simple principle: a small Trojan first disables local anti-virus software or other security defenses. Once those tools are disabled, a second-stage of the attack downloads any of a variety of threats, including keystroke loggers, worms or other software typically designed to take control of the platform. Attackers who successfully disable anti-virus defenses are free to download virtually any sort of malware, including old viruses and other threats, since these will no longer be detected. Keystroke loggers can be a potent method of obtaining confidential information and gaining access to even more corporate systems, particularly if the authentication mechanisms for those other systems are weak.

Phishing is becoming more targeted, spoofing businesses that have smaller customer bases (e.g., local banks) to increase the effectiveness of the social engineering tricks used. Phishing will also continue to expand beyond online banks to include more retailers, online gaming and other online sources that process confidential account information.

THE INCREASING SOPHISTICATION, CREATIVITY AND CLEVERNESS OF HACKERS, BOTH INTERNAL AND EXTERNAL

Many of the newer and more sophisticated threats are being directed against financial institutions, in large part because there are enormous amounts to be gained from criminal activity directed against these companies. However, there are organizations in many other industries that can suffer enormous financial loss if access to their systems is inadequate.

The profit motive has dramatically exacerbated the threats faced by users of email systems, corporate networks and any of the growing variety of communication, networking, storage and productivity tools used in the workplace. Because significant profits are available to spammers, phishers, criminal networks and others, many people have been attracted to this “market”. Further, because profits from malicious activities are substantial, they can be used to fund newer and better methods for circumventing defenses against their attacks. The growing numbers of criminals – some inside organizations – that are able to capture passwords and break authentication methods are being aided and abetted unwillingly by users and IT departments. For example, users who employ the same login credentials for multiple systems and IT departments that require only weak authentication, even for critical business systems, are assisting criminals, albeit involuntarily.

ORGANIZATIONS MUST IMPLEMENT STRONGER AUTHENTICATION

The result of all this is that organizations must implement stronger authentication methods. For example, for systems that contain highly sensitive content multi-factor authentication methods should be used instead of the simple login credentials that are most commonly used today. An example of multi-factor authentication is one with which almost all of us are familiar: access to automatic teller machines (ATMs). To gain access to an ATM, one must have access to two factors of authentication – an ATM card (something you possess) and a personal identification number (PIN) (something you know). The benefits of this two-factor authentication method are that a) even if one authentication factor is lost, access to bank funds is still protected; and b) the use of two points of authentication allows the PIN number to be simpler (usually just four digits) than it could be if only a single-factor authentication system was used.

Examples of stronger authentication methods include:

- Strong passwords, such as those that must include upper and lower case letters, numerals and punctuation symbols. While still a password, strong passwords are more difficult to guess and are less subject to compromise from automated dictionary attacks or hackers’ attempts at guessing.

- Token-based authentication, an example of which is an ATM card and PIN combination. This type of authentication includes more sophisticated methods of access control, such as challenges (e.g., a question) provided by the system, but users can forget the answers to challenge questions.

- Another form of token-based authentication is the use of physical devices that contain one-half of an access code that automatically increments at regular intervals. Tokens have the advantage of more robust security, but physical tokens can be lost.

- Biometric authentication, such as the scan of a fingerprint, retina or voice. Biometric authentication offers more robust security for many applications, but can result in a greater number of false rejections.

THERE IS AN INCREASING NEED FOR ACCESS CONTROL

In addition to the need for much stronger authentication methods than today's common username/password access control, there is a need for much better access control to corporate systems and other capabilities. For example, organizations should implement systems that can provide sophisticated access control functions, including:

- The date of each user's last login or login attempt
- Each user's login time
- Each user's time spent on a system
- Reports on when users change their passwords
- The strength of users' passwords and when users choose weak passwords

Much better and more detailed access control, coupled with more robust authentication, can result in greater security for corporate systems and reduced risk.

The Impact of Regulatory Compliance

US REQUIREMENTS

There are a variety of requirements in the United States to protect sensitive and confidential information. Many of these requirements are at the Federal level, but most states have passed data breach requirements, as well. Some of the leading compliance requirements include the following:

- **HIPAA**
  The Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses the use and disclosure of an individual's health information. It defines and limits the circumstances in which an individual's protected health information (PHI) may be used or disclosed by covered entities, and states that covered entities must establish and implement policies and procedures to protect PHI. Penalties for violations are up to $25,000 and $1.5 million, depending on when the violations occurred. Further, an individual who knowingly obtains or discloses individually identifiable health information may face a criminal penalty of up to $50,000 and up to one-year imprisonment.

- **GLBA**
  The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

- **Regulation S-P**
  Regulation S-P has been adopted by the US Securities and Exchange Commission (SEC) in accordance with Section 504 of the GLBA. This section requires the SEC and a variety of other US federal agencies to implement safeguards to protect non-public consumer

information, and to define standards for financial services firms to follow in this regard. The rule applies to brokers, dealers, investment firms and investment advisers.

OTHER REQUIREMENTS

There are a number of other requirements that require the protection of data, including the following:

- **Red Flag Rules**
  Part of the Safeguards Rule, the Red Flag Rules requires financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft.

- **Federal Trade Commission's proposed security breach notification law**
  In April 2009, the Federal Trade Commission proposed a security breach notification law focused on electronic health information. The rules, covering notification to individuals and federal regulators, would apply to vendors of personal health records and entities that offer products or services through Web sites of such vendors.

- **American Recovery and Reinvestment Act of 2009**
  There are provisions in the current US economic stimulus legislation (American Recovery and Reinvestment Act of 2009) that require certain entities to notify affected individuals, regulatory bodies and the media of "unsecured protected health information". The new breach provisions affect all entities that deal with protected health information, whether previously covered by HIPAA or not.

  The wide-ranging provisions include the appointment of a National Coordinator for Health Information Technology, who will "[ensure] security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable or indecipherable."

- **Family Educational Rights and Privacy Act of 1974 (FERPA)**
  The Family Educational Rights and Privacy Act of 1974, which is focused on protecting the privacy of students' education records, includes provisions for how states can transmit data to Federal entities.

The Emerging Trend to Implement Authentication Designed Exclusively for Your Own Environment

Although there is some commonality among organizations that use email, file systems, Web 2.0 applications and other tools that require authentication, most organizations have specialized and unique requirements that differentiate them from even seemingly similar companies of the same size or that operate in the same industry. Factors that differentiate organizations from one another include things like:

- **Business drivers**
  These might include things that are unique to an organization based on its ownership, history, specific customer requirements and corporate culture, among other factors.

- **Users' requirements for the usability of various systems**
  A company that gives users access only to corporate email and file systems will have different authentication requirements than one that allows access to a wide variety of external capabilities like Twitter, Facebook, personal Webmail systems, corporate Webmail systems, CRM systems like Salesforce.com or Constant Contact, etc.

- **The number and variety of applications used**
  Contributing to an organization's uniqueness is the specific mix of applications in use across the organization and by specific departments or functions. Many organizations will allow individuals or departments to implement specific applications that are sometimes limited in their deployment, but that sometimes will spread virally across an enterprise.

- **Government compliance regulations that apply to specific industries or geographies**
  For example, a financial services company will be subject to specific requirements from the Securities and Exchange Commission; a multi-national company will be subject to the specific data protection requirements in each country in which it operates; companies that operate in Nevada or Massachusetts will face stricter data protection requirements than those that do not; companies with customers in California will be subject to strict data protection laws for these individuals.

- **Characteristics of the user base**
  The number of remote or otherwise off-site users; the number of external users, such as customers, partners or consultants; and the number of branch offices all contribute to the uniqueness of an organization and the complexity of managing authentication mechanisms. For example, the authentication trends survey that we conducted for this white paper found that while employees are the most common individuals who access corporate systems, 7% are external business partners and 9% are consultants or others.

- **Organizational demographics**
  These factors include the size of the business, the industry in which it operates, the mix of products that it offers, etc.

- **The control that the IT department exercises**
  A key factor that contributes to the uniqueness of an organization is the level of control that IT exercises over use of approved and non-approved systems. For example, IT decision makers may consider a particular application not to be legitimate for use in a business context, but they might or might not disallow its use. In a major study of email, instant messaging and Web practices conducted by Osterman Research in April 2009, for example, it was discovered that only 28% of IT departments consider Facebook to be a legitimate application for use in business, but 50% permit its use. Similarly, while only 47% of organizations consider consumer-grade Webmail to be a legitimate application, 79% permit its use.

- **Authentication methods currently in place**
  The authentication trends survey found that there is a variety of sign-on methods currently in use. For example, 26% of the organizations surveyed are using a single sign-on system, 34% use a reduced sign-on system, while 40% require a unique sign-on for each system that users access.

Current Authentication Methods

WHAT AUTHENTICATION METHODS ARE CURRENTLY AVAILABLE?

There are a variety of authentication methods available, some more secure than others, some easier to use than others:

- **Username/password**
  This is the most commonly used authentication method and the one with which users are most familiar and comfortable. It has the advantages of familiarity and ease of use, but it has a number of disadvantages, including the ability for hackers to relatively easily guess users' passwords and the use of the same password to access multiple systems. This form of authentication is acceptable for information assets that are not critical to an organization.

- **Challenge question and response**
  This form of authentication requires an individual to answer questions that have previously been populated into an authentication system. For example, US Bank requires account holders to a) enter their username, b) answer one of three to five questions that the account holder has entered into the system previously (city of birth, city of marriage, street lived on as a child, etc.), and c) their password. 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 answer questions to which hackers and other unauthorized parties should not have ready access. It is not entirely secure, however, because those other than an authorized party could still guess or otherwise determine responses to the challenge questions.

- **Images or patterns**
  Some sites 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[1], can prevent robots or automated dictionary attacks from penetrating a system.

- **Seals**
  Another form of authentication, used by some banking sites, employs an image presented to the user, allowing the server to provide its identity. This gives users the

[1] Completely Automated Public Turing Test to Tell Computers and Humans Apart

confidence that the site asking for their credentials is not a rogue, impostor Web site. This form of two-way authentication will be a key area of authentication in the future.

- **One-time password tokens**
  One-time passwords (OTPs) are a more secure form of authentication in which a password is continually changed, each password being available for only one access attempt. OTPs can be delivered via SMS on a mobile phone, on a flash drive or via some other physical method. This method is much more secure than traditional authentication systems, but can be vulnerable to phishing attacks.

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

- **OpenID**
  This is an open source authentication mechanism developed in 2005. It has the advantages of being free, allowing the use of a single ID to access multiple content sources, and it is widely used. OpenID is similar in some ways to Security Assertion Markup Language (SAML), but the latter is focused more on end-user privacy considerations than OpenID.

- **Kerberos**
  Kerberos, developed by the Massachusetts Institute of Technology, is a popular authentication mechanism that allows mutual authentication between a user and a server over a non-secure network. If an organization has deployed Microsoft Active Directory, they it already has a built-in Kerberos infrastructure available to it.

- **Smart cards**
  A smart card is a (usually) credit card-sized token that contains circuitry and non-volatile memory allowing it, in some cases, to actually store information. This form of authentication provides a robust security mechanism and has been in use more than 25 years. The Common Access Card used by the US government for both military and civilian personnel, which doubles as a photo ID, is perhaps the most well known implementation of a smart card. The smart card approach has the disadvantage of being lost and thereby preventing access to secure systems.

- **Out-of-band authentication**
  Out-of-band (OOB) systems use two separate networks to authenticate users, such as a computer network that a user is trying to access and a telephone or mobile phone network to which the user has access. HSBC, for example, uses OOB to require users to transmit authentication information via a telephone when they attempt to access their accounts via the HSBC Web site. OOB is a fairly strong form of authentication, since an unauthorized user would require access to both networks in order to hack into an account. It has the disadvantage of being more cumbersome for users.

- **Biometric authentication**
  Biometric methods use a scan of an authorized user's fingerprint, iris, face, finger length or some other unique, biological characteristic of an individual authorized to access a system. Biometric methods can also use an individual's voice or typing rhythm. These systems have the distinct advantage of being very difficult to spoof by unauthorized parties, but they can result in false rejections. For example, a user that has cut his or her finger and then attempts to access a system via a fingerprint scan can be rejected. A user who is more stressed than when they provided their voiceprint might similarly be rejected. A user whose typing rhythm is being checked might have a different rhythm while holding a cup of coffee. Also, if a user's password changes, the old baselines may no longer be usable, and so the user would need to go through the fingerprint, voice, etc. scanning process again.

- **Multiple-factor authentication methods**
  There are also authentication methods that use a combination of some of the methods described above, such as username/password combination employed in conjunction with a smart card. Using multiple authentication factors can provide additional security beyond that provided by the use of a single method, but adding factors to the authentication process can be more difficult for authorized users. Tokens and smart cards are typically used as part of a two-factor or multi-factor authentication system. This form of authentication has the disadvantage of higher initial and ongoing administration costs, and a physical component of the authentication (e.g., a smart card) can be lost by end users.

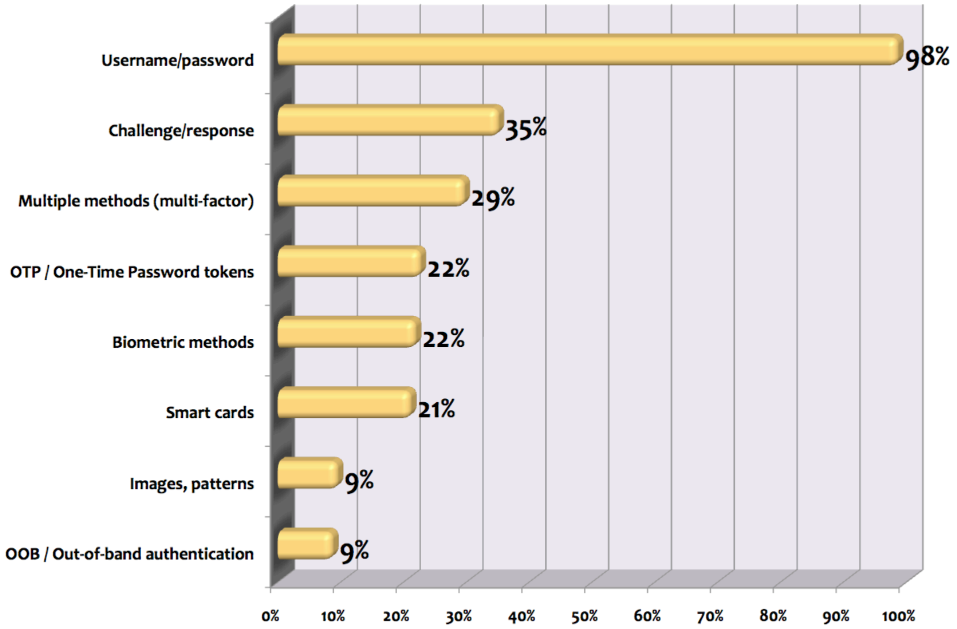
SOPHISTICATED AUTHENTICATION METHODS HAVE DRAWBACKS

More sophisticated authentication methods also have their drawbacks. For example, a two-factor authentication system using a smart card or token can be more cumbersome for users to employ, particularly for those that lose the physical component of this authentication mechanism. Biometric authentication can be troublesome because it can result in a high number of false rejections. Very strong passwords can also be troublesome because they are more difficult to remember, and so users will have a tendency to write them down, negating the benefit of using a difficult-to-guess password.

WHICH METHODS ARE MOST USED?

The authentication trends survey paper asked individuals in organizations of varying sizes about the authentication methods that they currently use. We found, as shown in the following figure, that username/password authentication is the dominant form of authentication, followed by challenge/response in a distant second place and multi-factor authentication.

Authentication Methods in Use



Projections on Future Authentication Trends

Organizations must improve the security of their system access methods for a variety of reasons, including the greater proportion of business records, confidential information and otherwise sensitive content that is stored electronically; the growth in the sheer volume of this information; and the greater threat from hackers and others that are attempting to gain access to this information, often for financial gain.

Some decision makers are beginning to realize their need for better authentication. For example, in the authentication trends survey, only 24% of respondents indicated that they currently have "very strong" authentication capabilities for their organizations' corporate data and access to systems, whereas 63% indicated their authentication is good but could be more robust. However, 13% told us that their authentication mechanisms are weak and need to be improved significantly.

Among the trends that will occur are the following:

- **Much more activity from hackers and malware developers**
  We expect continued and dramatic increases in the number of attacks directed against corporate sites and individuals by hackers and others intent on penetrating authentication mechanisms. For example, the Anti-Phishing Working Group (APWG) found that the number of individual malware instances designed to intercept login

credentials increased 827% from January to December 2008[2].

- **More Web 2.0-related attacks**
  While email continues to provide an inroad for viruses and Trojans, increasingly organizations are finding the Web to be a major source of malware. Security threats that Web 2.0 applications pose for the enterprise include insufficient authentication control that enables cyber-criminals to crack administrative accounts in order to gain access to sensitive information. Further, with Cross Site Request Forgery (CSRF) attacks, innocent-looking Web sites generate requests to different sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors.

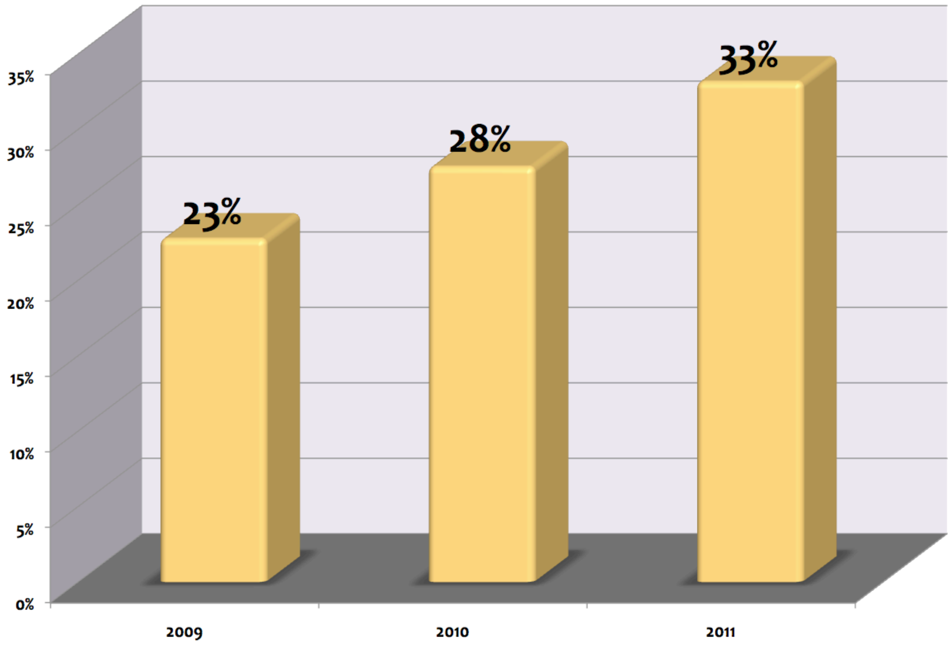
- **Greater use of multiple-factor authentication methods**
  While there will be continued use of simple username/password combinations for access to less critical systems and data stores, more sensitive content will be protected using multiple factors of authentication in order to prevent hackers and others from accessing it.

- **Greater use of SaaS / cloud-based services**
  Osterman Research anticipates much greater use of cloud-based services for a variety of capabilities, including messaging, customer relationship management, collaboration, encryption, archiving, security and a host of other corporate functions that today are normally managed using on-premise systems. Complicating the issue will be growth in the use of hybrid systems, in which both on-premises systems and cloud-based services are used, such as the former for a large headquarters operation and the latter for field offices.

- **More mobile security and authentication**
  The use of mobile devices is increasing at a steady pace, as shown in the next figure, and these devices are becoming an important computing platform for many corporate users. As a result, decision makers will need to focus on mobile security and authentication moving forward. This is particularly relevant given that in a June 2009 Osterman Research survey on mobile messaging in mid-sized and large organizations, 39% of organizations reported that the accessing corporate data repositories from a mobile device is one of the top five problems that they face in managing their mobile messaging infrastructure.

[2] APWG Phishing Activity Trends Report

Workforce That Uses Company-Supplied and Company-Funded Mobile Devices 2009-2011



- **Need for mutual authentication**
  Increasing levels of phishing, spearfishing, whaling and other social engineering attempts to penetrate individual or corporate systems will place greater emphasis on mutual authentication mechanisms. For example, some US government agencies now require all emails to be digitally signed to help combat email-based phishing attempts. A recipient can be assured that if the email purporting to be from the government is not signed, it is not from a trusted source.

- **Less use of a "one-size-fits-all" approach**
  We also expect to see less reliance on a single approach to managing authentication. Expect organizations to establish multiple methods of authentication for access to different systems based on the sensitivity of the information contained within them, the risks that they face from unauthorized access to sensitive content, and government regulations that require protection of personal information. Organizations will increasingly use authentication that is adapted to their unique requirements.

  The importance of these types of tailored authentication solutions should not be underestimated. They allow an organization to maximize the security of access to its systems and data, while at the same time imposing the minimum impact on users' productivity and the IT staff time required to manage access to corporate systems.

Summary

Organizations maintain a variety of systems and stores of sensitive content, each of which has some level of authentication required for users to access them. However, most organizations admit that their authentication mechanisms could use improvement, and that authentication must be more robust and more difficult to hack than the simple usernames and passwords that today are the most common methods of access.

There are a number of authentication mechanisms available, each of which has advantages and disadvantages. For example, an access method that uses user-defined usernames and passwords without any requirement for even strong passwords is simple for users and inexpensive to administer, but it is easily hacked. A smart card, on the other hand, provides much greater security, but is more expensive to deploy and manage on an ongoing basis.

Future trends in authentication will be driven by the growing quantity of electronic content that organizations possess, the growing number of systems that they maintain, more government regulations focused on the protection of data, and increasing attempts by hackers and others to gain access to content through social engineering and other means. We expect organizations to improve their authentication mechanisms by developing capabilities that are unique to their specific requirements, driven by factors like the types of data they maintain, the geographic distribution of their users, their corporate culture, specific requirements of the industry in which they operate, the mobility of their workforce and other factors.

About PistolStar

PistolStar, Inc. specializes in tailored authentication, providing software products and services that fit with the customer's environment, as well as optimize authentication processes and address requirements for enhanced usability, security, auditing and compliance. With its comprehensive solution set, PistolStar responds to an organization's need to secure access to information and ensure regulatory compliance, while simplifying the login process and reducing the IT staff's burden of managing passwords and tracking login threats. Launched in 1999, PistolStar is a pioneer in enabling authentication via Microsoft Active Directory and is an authority on authentication using Active Directory and Kerberos.

PistolStar offers several authentication solutions:

- **PortalGuard** is a password authentication and security solution that allows end-users to authenticate and manage a portal password directly from a Web browser, while providing administrators with functionality to meet or exceed their security objectives. With PortalGuard, administrators can implement best practices for ensuring stronger and consistently secure authentication.

- **Password Power** is a comprehensive set of authentication solutions addressing organizations' requirements for increasing usability while enhancing security and ensuring compliance. It supports a wide range of platforms, including SharePoint, Active

Directory, BlackBerry, Websphere Portal, SAP, Notes, Domino, Quickr and Sametime. It also supports many authentication mechanisms, including Kerberos, CAC, X.509 and smart cards, among others.

- **Web Set Password** is an authentication solution providing simplified, yet controlled access and enhanced security and compliance for Lotus Domino, Microsoft SharePoint, and IBM WebSphere Portal. Key features of the solution include stronger authentication through the use of challenge questions in addition to usernames and passwords, integration with Active Directory that allows organizations to reduce the number of passwords required, self-service password recovery, and end-user login auditing, among other features.

More than 400 organizations worldwide have selected PistolStar's authentication security and management solutions to simplify authentication, secure enterprise access, reduce the potential for IT risks, and ensure compliance. Most of PistolStar's customers are Global 2000 companies in a wide range of industries, although the company's solutions can also be used by small and mid-sized businesses. Approximately 70% of PistolStar's customers are based in the United States.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statue, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.