

Strategy Session

Presented in conjunction with

SECURITY
darkREADING
Protect The Business  Enable Access

Proof of Identity

How to Choose Multifactor Authentication

User names and passwords are no longer sufficient authentication. In a time when so much business depends on the Internet, security requirements and regulatory mandates are putting pressure on business to adopt strong, multifactor authentication methods. In this Tech Center report, we explain how to weigh cost vs. risk to select the Web authentication method for your high-risk applications.

By **Michael Cobb**



Strategy Session



T A B L E O F
CONTENTS

- 3 Author's Bio
- 4 Executive Summary
- 5 Understanding Strong Authentication
- 5 Figure 1: Comparing Two-factor Authentication Options
- 6 Solution Assessment Criteria
- 7 Figure 2: Authentication Methods and Effectiveness
- 8 Client-based Authentication Options
- 10 Authentication-as-a-Service
- 10 Figure 3: How Man-in-the-Middle Malware Defeats Two-factor Authentication
- 11 Weighing the Business Impact
- 12 Focus on High-Value Transactions
- 12 Risk vs. Cost vs. Benefit
- 13 Look at the Big Picture

ABOUT US | *InformationWeek Analytics*' experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at awittmann@techweb.com, executive editor **Lorna Garey** at lgarey@techweb.com and research managing editor **Heather Vallis** at hvallis@techweb.com. Find all of our reports at www.analytics.informationweek.com.



S t r a t e g y S e s s i o n



Michael Cobb
Cobweb Applications



Michael Cobb, CISSP-ISSAP, CLAS, is a renowned security author with more than 15 years of experience in the IT industry. He is the founder and managing director of Cobweb Applications, a consultancy that provides data security services. He co-authored the book *IIS Security* and has written numerous technical articles for leading IT publications. Michael is also a Microsoft Certified Database Administrator.



Executive Summary

To control access to your Web-based applications, you need to identify and authenticate anyone wishing to use them—that is, verify that they are who they say they are. Only after successful authentication can they be assigned access rights and be authorized to perform certain actions. Authentication is the key to who gets to do what. But why do you need to implement strong or two-factor authentication for your Web applications?

First, lawmakers have pushed security to the top of the agenda, and strong authentication is part of that agenda. Laws such as Sarbanes-Oxley and requirements such as PCI-DSS mean that single-factor authentication is no longer adequate for protecting access to high-value or personally identifiable information and providing reliable audit trails.

Second, any organization that sees customer trust as a business priority needs to provide secure authentication, and the password approach doesn't do that. Many organizations, though, are wary of implementing strong authentication due to its perceived cost. However, managing passwords can be expensive too. They provide too low a level of trust to be considered a viable option where assets of any value are involved. Also the situation's getting worse. The growing use of the number-crunching power of modern graphics cards to carry out brute-force attacks will soon make it trivial for hackers to crack strong passwords.

Adding a second factor credential to the authentication process provides additional security as well as a higher level of trust between a user and an application. In this report, we'll look at the various options for authenticating users to Web applications and whether a single authentication strategy can be developed to serve a wide variety of Web users (see Figure 1, "Comparing Two-factor Authentication Options," page 5).









Understanding Strong Authentication

Strong authentication requires two independent ways to establish an identity. It's normally implemented as a combination of any two of the following:

- Something you know, such as a user name, password or PIN
- Something you have, such as a token, card or key
- Something you are, such as a fingerprint or written signature, i.e., biometric

Figure 1

Comparison of Two-Factor Authentication Solutions

Solution	Ease of Use ¹	Security ²	Cost ³		User Type
			Support	Per Unit	
Soft Digital Certificate	*		\$ \$ \$ \$	\$ \$ \$	Employee Partner Government
Hard Digital Certificate	* *		\$ \$ \$	\$ \$ \$	Employee Partner Government
Grid Card	* * * *		\$	\$	Employee Consumers
OTP Token	* * *		\$ \$	\$ \$	Consumers Employee Partner Government
SMS OTP	* *		\$	\$	Consumers
Transaction Signing	*		\$ \$ \$	\$ \$ \$	Consumers
	¹ Scale 1 ((difficult) to 4 (easy)	² Scale: 1 (weak security) to 4 (strong) security	³ Scale: 1 (low) to 4 (high) cost		



It's not possible to prove an identity beyond doubt, but combining two of these factors achieves better identity assurance than just a username and password—they're both things you know. A smart card on its own doesn't provide strong authentication either—it could have been stolen—so strong authentication requires it to be combined with a password or signature.

The technologies for implementing strong Web authentication are:

- Soft or hard digital certificates
- One-time passwords (OTP)
- Challenge-response
- Authentication-as-a-service (AaaS)

Management is going to want a solution that's effective, flexible and scalable, and can be implemented with minimum disruption and cost. Your customers, on the other hand, will want a solution that not only offers increased security but is easy to use.

You'll note that we haven't included biometrics in the above list. Biometrics isn't really an option for Web-based applications. Yes, each user has a unique fingerprint, and they're not going to lose it like they might a smart card, but the big drawback is the cost and inconvenience of the enrollment process. Customers aren't going to queue at your offices to be fingerprinted, and remote enrollment can't be trusted.

Solution Assessment Criteria

There are three key issues when assessing a strong authentication solution:

Time. This refers to the additional time it will take your users to complete authentication. If they can't see any point in the extra time and inconvenience of your authentication process they won't use it. Completing a complex authentication process just to check an account balance will turn users away, as the information doesn't warrant that level of protection and the time it takes to access it.

A simpler logon would be more appropriate followed by more rigorous re-authentication should they wish to make a payment or transfer as this then matches the level of trust with the



type of action or asset being accessed. Users engaged in high-value transactions are likely to be more willing to put up with any extra time and inconvenience your system requires.

Risk. The issues of risk and cost are very closely related. What is the risk to your organization if you don't have strong authentication? What would be the cost to the organization if data was stolen—the cost to its reputation? What if the organization was shown to be out of compliance with laws, regulations and standards? The magnitude and possibility of these costs directly affect the ROI and cost benefit of a solution.

But the risks can change depending on who accesses the data or how it is accessed. The risk of not authenticating an employee accessing a Web application internally is quite different com-

Figure 2

Authentication Methods and Effectiveness

Option	Applicability Against Common Threats				
	Credential Theft	Weak Passwords	Password Reuse	Session based Attacks	Malware Attacks
Username & Password	V	RM ¹	V	V	V
Hard Digital Certificate	P	P	V	V	V
Grid Cards	P	P	RM ²	P	V
OTP Tokens	P	P	P	P	V
SMS OTP	P	P	P	P	RM ³
Transaction Signing	P	P	P	P	P

Key: V = Vulnerable, P = Protected, RM = Requires Mitigation

¹ Requires enforced strong password policy

² Requires large or regularly changed grid

³ Requires transaction confirmation e.g. Transfer \$5,000 from ABC Bank to John Doe Autos?



pared with the risk of not authenticating a customer accessing the same application via the Internet. So time and risk combine with the “who” and the “how” to determine what type of authentication you need and how much you can afford to spend on it.

Cost. The costs you’re going to have to consider include:

- Implementation
- Hardware, such as cards and readers
- Enrollment
- User management

The costs of user management are often overlooked, as they are not directly related to the cost of the authentication infrastructure, but relate instead to the support, education and maintenance of users, which can greatly increase the total cost per user. In fact, the problem of user management greatly limits the suitability of digital certificates as an authentication solution.

Client-based Authentication Options

Not long ago, client-side certificates and PKI were hailed as the solution to authentication (see Figure 2, “Authentication Methods and Effectiveness,” page 7). They not only authenticate people, but can be used to digitally sign and encrypt documents. They’re also inexpensive to issue, as they’re digital.

Sadly, they have proven to be a nightmare to manage when a large number of non-technical users are involved. One global bank found that although digital certificates were spectacularly successful in reducing fraud levels, they created an unbearable overload on their support centers. Also, customers were tied to using a specific PC, since exporting the certificate to another PC was a non-starter for the average user. This is even more of an issue now because of the proliferation of portable devices such as iPads and netbooks.

An alternative to soft certificates is connected hard certificates; here we’re talking about smart devices such as USB keys, where the digital certificate is stored on the device. There’s no tricky installation process for the user; the certificate is stored more securely and requires



S t r a t e g y S e s s i o n

a password to access it. It's mobile, and as soon as the smart device is removed, the user is logged out. These benefits make hard certificates more attractive but like soft certificates, they do not protect users from session riding and cross-site scripting attacks. This is why one-time passwords (OTP) are fast becoming the strong authentication method of choice with many banks.

Like hard certificates, OTP requires the issuance of a smart device—the OTP device generating unique passwords that are only valid for a short period of time. But in contrast to static authentication methods, they are not vulnerable to replay attacks. Here's what one bank had to say about OTP: "The main benefits of OTP devices over digital certificates are a simplified activation process, enhanced access as the user can log in from any computer with Internet access, and improved security as each security number is valid for a limited time only."

There are, of course, replacement costs to consider for any smart device as people lose and break things all the time. Overall, though, they're proving successful for large user bases, such as online banking, as are challenge-response tokens. These work by presenting a question, the challenge and the person you are authenticating providing a valid answer, the response. A common implementation is a series of rows and columns of letters and/or numbers typically printed on credit card-sized cards that the user consults to respond to challenges from the authentication system. Known as grid cards, they can be easily carried in user's wallets or be printed on the back of employee access badges. They're a cheap, relatively convenient alternative to OTP while still preventing password replay attacks.

An SMS-based challenge-response solution can work if a high percentage of your users have mobile phones, using them as an authentication token. When an authentication or transaction signing is required, the application sends the user a transaction number to their mobile phone along with a reference ID of the transaction to verify what is being signed. This type of out-of-band authentication solution can counter the threat of man-in-the-middle attacks, which token-based solutions are unable to do. SMS simplifies deployment, as it removes the need for proprietary hardware token devices, but suffers from recurring costs of the messaging and reliability of the messages sent. If you know your user base has java-enabled smart phones or PDAs then Mobile-OTP (<http://motp.sourceforge.net/>) may be an option. It's a free, open-source solution based on time-synchronous one-time passwords. Alternatively, Microsoft provides all the source code for an OTP solution via its MSDN Magazine (<http://msdn.microsoft.com/en-us/magazine/cc507635.aspx>).



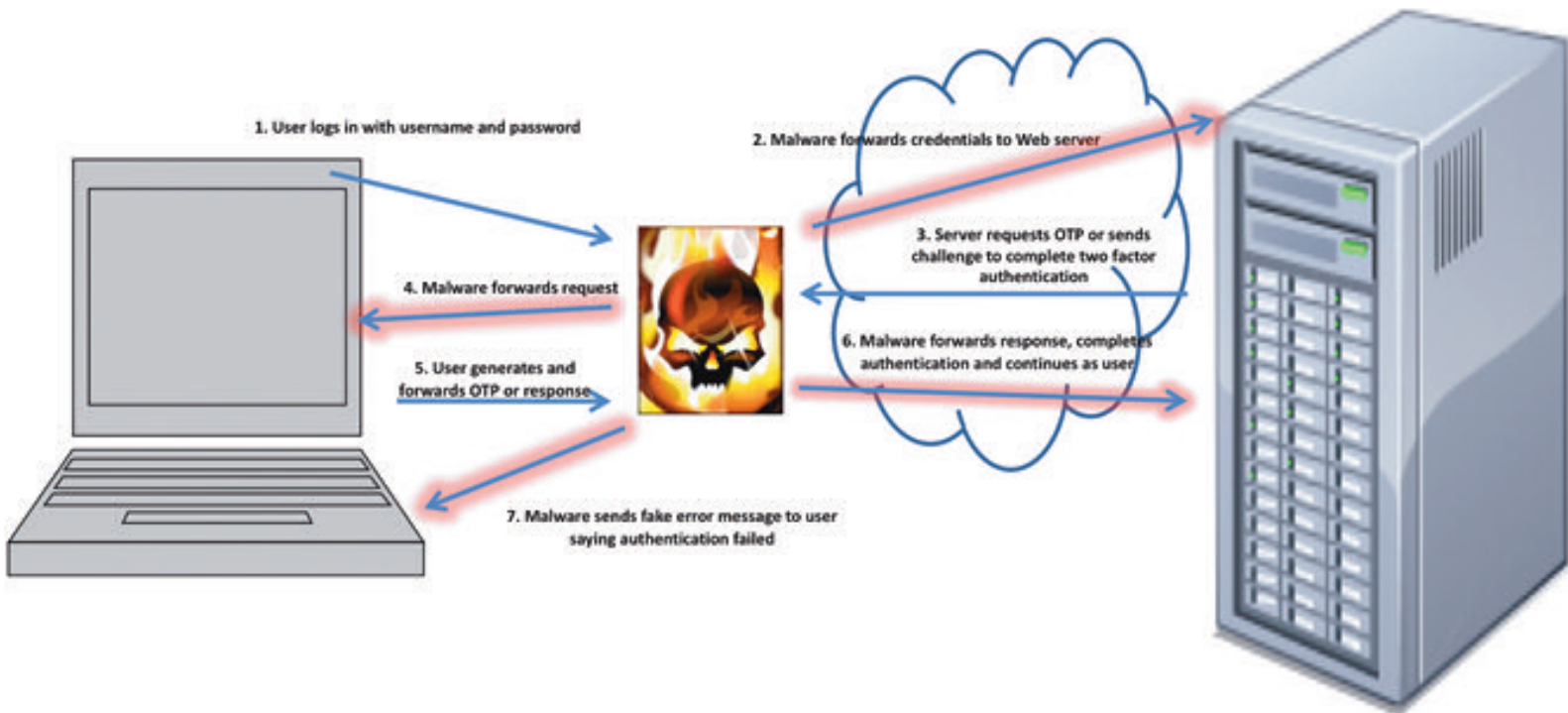
Authentication-as-a-Service

If you're not comfortable with building your own solution and have a limited capital or operations budget, a two-factor authentication solution you may find appealing is authentication-as-a-service (AaaS). AaaS is an Internet-based service that offers on-demand verification to seamlessly authenticate online users. AaaS can be more economically and operationally scalable than internally managed authentication, often with better reliability and response times.

To assess whether AaaS represents good value, you will need to compare the cost of procur-

Figure 3

How Man-in-the-Middle Malware Defeats Two-factor Authentication



Although OTP and challenge/response authentication are able to protect against phishing, pharming, replay, and other password related attacks they are still prone to the man-in-the-middle type of attacks. These attacks are by no means simple and require the attacker to install malware on the victim's PC.



ing and operating authentication systems in-house versus using AaaS. In-house costs include licenses, maintenance, operations, hardware and all costs around managing tokens such as procurement, provisioning, distribution and exception process management. AaaS costs include the initial setup, integration and fixed monthly fees, as well as per-authentication transaction costs.

If the figures stack up, then AaaS is a viable solution to your authentication problem as long as you are happy with the SLA, the level of customer privacy offered and the reputation of the service provider. Look for a provider that uses open standard technologies such as SAML, RADIUS and OATH, so that you are not locked into a specific provider. Examples of these services are myOneLogin provided by TriCipher and Signify's Secure Authentication Service.

Weighing the Business Impact

When assessing the pros and cons of introducing strong authentication, you need to take into account other potential benefits. Token-based solutions not only defend your data and systems but differentiate you from your competitors. Your choice of authentication will not only affect your company technically, it will impact your customers' perception of how well you're protecting their assets. Authentication methods directly influence customers' perception of trust. The more secure your users feel, the more online services they are willing to use; that equates to more transactions and increased profitability. Up-selling to customers is a great way to increase revenues, and if you can convince more of them to move to online transactions, you'll save money too.

But let's not get carried away. Strong authentication that can provide an acceptable user experience isn't a panacea to protect from every possible attack. Every solution can suffer from infected user machines or poor security practices that are outside of your control. Real-time man-in-the-middle attacks, where the attacker stands in the middle of the transaction stream between the user and your application, either using malware or a phishing site, can defeat the protection provided by hardware tokens and one-time passwords (see Figure 3, "How Man-in-the-Middle Malware Defeats Two-factor Authentication," page 10).

Also the deployment of hardware tokens is a logistical challenge. They can get damaged or lost, and the associated costs of re-issuance can mount up with a large user base. Smart cards require a reader, which is an extra expense and another device your users have to have plugged



in to their machine, although some laptops now ship with an embedded smart card reader. USB ports are standard on today's computers but a USB token can't fit in a wallet (though, it can easily be attached to a key ring).

Also, can all your users utilize a small device? Could a partially sighted user be able to read the tiny characters? Issues such as these will mean that you may well require an alternative authentication process, but you should always aim to keep the user experience consistent across all contact points. You can't expect users to provide different PINs or use different grid cards, for example, when authenticating to a telephone-based support desk.

Focus on High-Value Transactions

For high-value services, concentrate your resources on authenticating transactions more than users, as many attacks rely on poorly implemented user authentication schemes. Transaction signing is performed by offline challenge-response calculators. The user is presented with various items to enter into the calculator, which then calculates a response based on these inputs. This is the strongest form of authentication, as the user has to enter the transaction details; any other transaction will fail to produce a suitable response. This type of authentication is robust against man-in-the-middle attacks, cannot be replayed and has strong non-repudiation properties as well.

The downside is that each transaction involves several keystrokes and takes time to complete. Also, the calculators are larger than other smart tokens and are more easily lost or stolen. As always, it's a case of matching the level of trust with the type of action or asset being accessed. One major bank, for example, provides transaction signing for its commercial customers but not private ones. The average size of transactions made by its commercial customers means that the business case for strong authentication stacked up for commercial but not personal accounts. In fact, the bank finds it cheaper to refund the amount of any unauthorized transaction conducted online than support transaction signing for this segment of its user base.

Risk vs. Cost vs. Benefit

Choosing high-end authentication for high-value transactions is a good example of where a careful analysis of risks, costs and benefits before deploying a solution led to a decision not to deploy a single authentication strategy. In order to accurately establish the risks to your appli-



ation you need to classify the data it handles. By classifying data with respect to its level of confidentiality and how it's used, you can see where strong authentication may be justified.

For example, a username and password is still suitable for low-value systems such as blogs and forums. OTP or challenge-response is suitable for low-value e-commerce systems, while transaction signing is more suited to high-value systems, such as banking and trading systems. In the end, you have to make a measured assessment of the level of risk versus the impact on user experience and then make a pragmatic business choice.

Your final decision may come down to the cost difference between providing hardware tokens to everyone or only to a select group. One way to defray the costs and help change your customers' acceptance of a lengthier or more onerous authentication process is to give them the option of not using it on the understanding that they will bear more risk if their accounts are then breached.

Look at the Big Picture

To try to future-proof your decision, look to technologies that are standards-based, scalable and require the minimum amount of client software. This will reduce the headaches and costs of version control and updates. For example, why not double up your employees' ID cards, which they are probably required to carry, as a smart card for computer login? Using the same card provides enforcement of access policies for both physical and logical resources and ties the two very tightly together.

Over the last few years, supporting infrastructures such as Microsoft Active Directory have made it easier to tie in strong user authentication to new applications. So, if you haven't looked at the marketplace recently, now is the time to do so. New technologies are emerging, such as Cellular Authentication Token (CAT), providing a wider choice of options that may fit your particular requirements.

Don't forget, though, that authentication is just one aspect of a secure system. It must be combined with access control and event logging. You will also need a robust and trusted enrollment path to ensure that the authentication system itself is "strong." Simply sending any user who asks for an account a token or certificate provides no certainty that the user is who they say they are. User education must also feature in your plans in order to combat



phishing attacks, which can undermine your strongest security controls.

Strong authentication raises the bar, making it more difficult for hackers to successfully attack your application and system infrastructure. A well-implemented solution will reduce your risks and help avoid the costs associated with a data break-in. It will also stand in you good stead in a court case if you can show you performed your duty of care to current best practices. The human brain realizes the importance of being able to identify friend or foe, so too should your online applications.