UBM
TechWeb

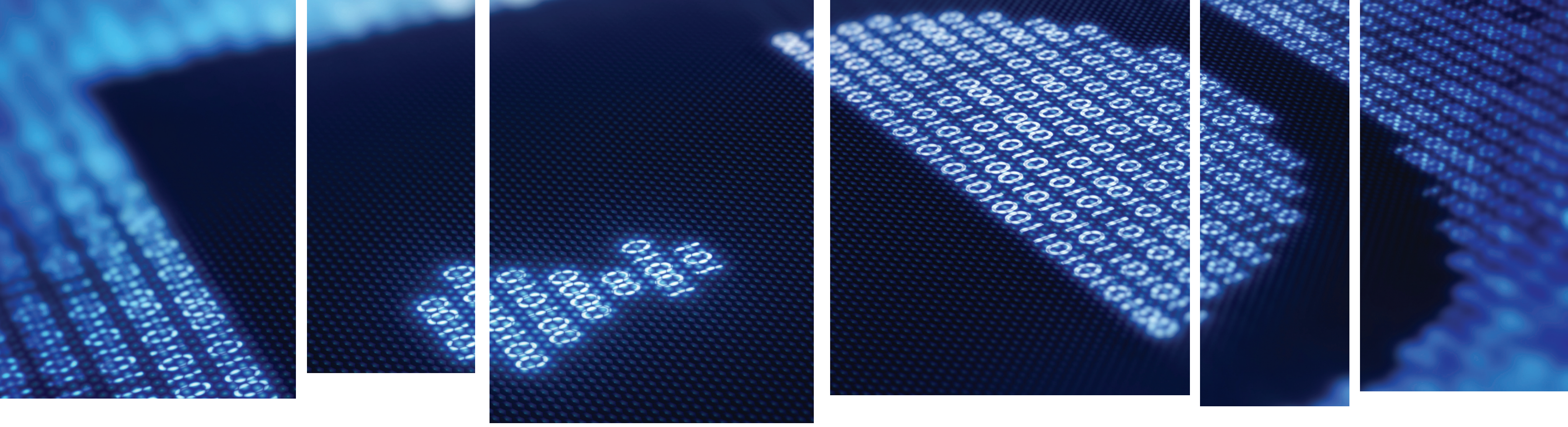
A UBM TECHWEB WHITE PAPER
AUGUST 2012

Software-Based Authentication Delivers More Reliable and Less Costly Security

With the adoption of mobility and cloud computing, coupled with an increasingly stringent regulatory environment, more workers than ever need secure remote access to corporate information. Learn how software-based authentication can simplify access and mitigate risks.

Brought to you by

SyferLock™



Software-Based Authentication Delivers More Reliable and Less Costly Security

With the adoption of mobility and cloud computing, coupled with an increasingly stringent regulatory environment, more workers than ever need secure remote access to corporate information. Learn how software-based authentication can simplify access and mitigate risks.

Information security has never been a bigger challenge for organizations, given the emergence of trends such as cloud computing and virtualization, the increase in the need for remote access, the proliferation of mobile technologies and the increased use of social networking.

In many industries, it's more difficult than ever for IT and security executives to ensure that all of the organization's information assets are protected.

Many companies today rely on hardware-based authentication for security. While these methods of authentication have some merit, they are flawed in a number of ways. Modern software-based authentication solutions provide far more cost-effective ways to ensure strong authentication/two-factor authentication across a range of use cases.

This white paper describes some of the security challenges businesses are facing today, and why software-based authentication makes sense in today's highly connected environment.

The Security Conundrum

Creating a highly secure IT infrastructure has become a major challenge for organizations. Megatrends such as the emergence of cloud computing, server and desktop virtualization, the proliferation of mobile technologies and employees' devices in the workplace, the increase in employees requiring remote access, and the greater use of social networking in the work environment have created new vulnerabilities and risks for companies.

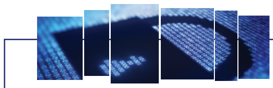
Users expect to be able to access information from virtually anywhere via the Internet and through mobile devices such as smartphones and tablets, and that means it is harder than ever for IT and security executives to ensure that all the organization's information assets are protected.

Recent industry research and high-profile security incidents show how companies are vulnerable to increasingly sophisticated threats such as malware and hacker intrusions, and many organizations are subject to threats.

For example, according to the Deloitte 2011 TMT Global Security Survey, which queried 138 companies in the technology, media and telecommunications industries about information security, information security breaches were reported by 75 percent of the global organizations. Mobile devices are considered the No. 1 security threat for 2012, according to nearly 40 percent of the survey respondents. That was followed by security breaches involving third parties, employee errors and omissions, faster adoption of emerging technologies, and employee abuse of IT systems and information.

One of the biggest concerns regarding security is unauthenticated access to systems and information. Given the proliferation of employees working remotely and the use of mobile devices, and the potential threat that represents for corporate networks, authentication should be an even higher priority than it has been for enterprises.

Hardware-based authentication solutions have



> **Mobile devices are the No. 1 security threat for 2012, according to nearly 40 percent of the survey respondents.**
>
> **— Deloitte 2011 TMT Global Security Survey**

been around for years, and many companies rely on these products as part of their security strategy. These tools can provide some benefits in terms of authenticating users, but they are flawed in a number of ways.

For example, hardware solutions such as security tokens can be lost or stolen, and they can also break. In addition, they can be costly, not only for the initial purchase but also for ongoing maintenance and administration of the physical devices. And while hardware authentication solutions provide a layer of security, they are not impenetrable — as was highlighted by recent high-profile security breaches. Furthermore, many of today's emerging use cases for online access are not conducive to hardware-based solutions, such as tokens, for strong authentication.

As a result of these and other drawbacks, many organizations today are looking to replace these legacy authentication products with solutions that are more effective and less costly.

Some organizations have deployed biometric systems for authentication purposes. But these technologies have their own drawbacks, such as high implementation costs and issues related to user privacy.

In some industries such as health care and financial services, the emergence or evolution of regulatory requirements is forcing even more stringent needs for strong authentication.

For instance, health care organizations must be compliant with the Health Insurance Portability and Accountability Act (HIPAA). Relying solely on usernames and passwords will no longer be sufficient for secure access to data, particularly sensitive information such as patient records.

Organizations such as large hospitals have to rethink their authentication strategies to ensure that they are compliant with the latest regulatory requirements.

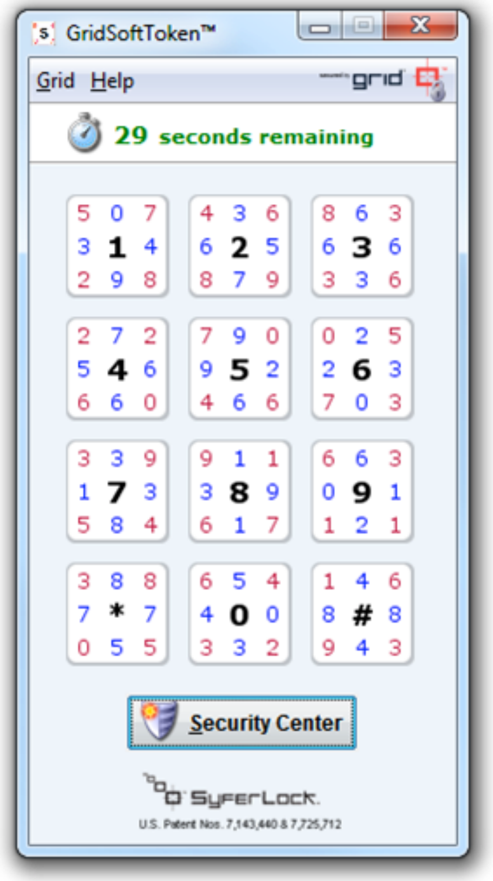
An Effective Alternative

There are software-based, strong authentication solutions available on the market that address the concerns and challenges companies face and provide an alternative to hardware-based authentication products. These software-based solutions can also help companies meet their regulatory requirements for greater security.

Some innovative software-based solutions deliver the level of authentication that companies need today, but at a much lower cost than hardware-based products such as tokens, smart cards, biometrics and other authentication offerings available.

Flexible, adaptable, software-based authentication solutions enable companies to address strong authentication and two-factor authentication across a range of use cases. By adopting these solutions, organizations can help eliminate hardware tokens and reduce the total cost of authentication, while at the same time ensuring that they are protected against current and emerging security threats.

Some of the software-based solutions available on the market deliver enhanced single-factor,

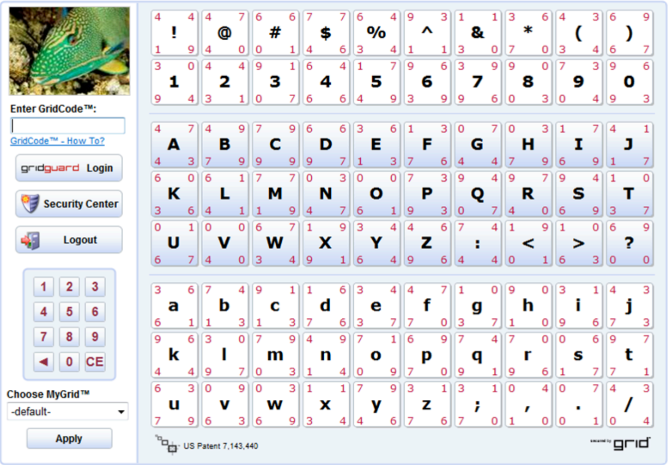


29 seconds remaining

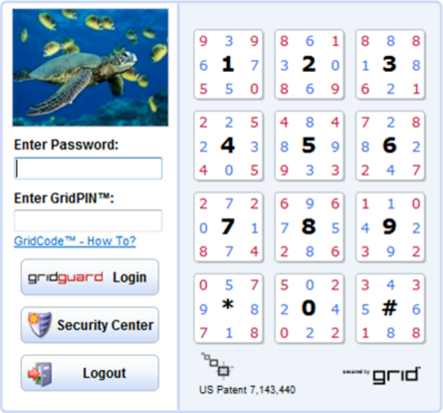
5 0 7 3 **1** 4 2 9 8	4 3 6 6 **2** 5 8 7 9	8 6 3 6 **3** 6 3 3 6
2 7 2 5 **4** 6 6 6 0	7 9 0 9 **5** 2 4 6 6	0 2 5 2 **6** 3 7 0 3
3 3 9 1 **7** 3 5 8 4	9 1 1 3 **8** 9 6 1 7	6 6 3 0 **9** 1 1 2 1
3 8 8 7 ***** 7 0 5 5	6 5 4 4 **0** 0 3 3 2	1 4 6 8 **#** 8 9 4 3

U.S. Patent Nos. 7,143,440 & 7,725,712

Figure 1: The user is presented with SyferLock GridSoftToken when requesting authentication. The password, or in this case PIN, is not presented to the user in the clear. Only the authorized user can input the PIN using SyferLock.



4 4 ! 1 9	4 7 @ 4 0	6 6 # 0 1	7 7 $ 4 6	6 4 % 3 4	9 3 ^ 1 1	1 1 & 3 0	3 6 * 7 0	4 3 (3 4	6 9) 6 7
3 0 1 9 4	4 4 2 3 1	9 1 3 0 7	6 4 4 6 6	1 7 5 4 9	9 6 6 3 9	3 9 7 9 6	9 0 8 0 3	7 3 9 0 4	9 6 0 9 3
4 7 A 4 3	4 9 B 7 9	7 9 C 9 9	6 6 D 9 7	3 6 E 1 3	1 3 F 7 6	0 7 G 4 4	0 3 H 7 9	1 7 I 6 9	4 1 J 1 7
6 0 K 3 6	6 1 L 4 1	7 7 M 1 9	0 3 N 4 7	0 0 O 6 1	7 3 P 9 3	9 4 Q 0 7	9 7 R 4 0	9 4 S 6 9	1 0 T 3 7
0 1 U 6 7	0 0 V 4 0	6 7 W 3 4	1 9 X 9 1	3 4 Y 6 4	4 6 Z 9 6	7 4 : 4 4	1 9 < 0 1	1 0 > 6 3	6 9 ? 0 0
3 6 a 6 1	7 4 b 1 3	9 1 c 1 3	1 6 d 7 6	3 4 e 3 7	4 7 f 7 0	1 0 g 3 7	9 0 h 1 0	3 1 i 9 6	4 3 j 7 3
9 6 k 4 4	3 0 l 9 7	7 9 m 0 3	4 9 n 1 4	7 1 o 0 9	6 9 p 7 0	7 4 q 9 1	7 0 r 9 6	0 6 s 1 7	9 7 t 7 1
6 3 u 7 9	0 9 v 6 3	0 3 w 6 9	1 1 x 3 4	7 9 y 4 6	3 1 z 7 6	3 1 ; 7 0	0 4 , 1 0	0 7 . 0 1	4 3 / 0 4



9 3 9
6 1 7
5 5 0
	8 6 1
	3 2 0
	8 6 9
		8 8 8
		1 3 8
		6 2 1

2 2 5
2 4 3
4 0 5
	4 8 4
	8 5 9
	9 3 3
		7 2 8
		8 6 2
		2 4 7

2 7 2
0 7 1
8 7 4
	6 9 6
	7 8 5
	2 8 6
		1 1 0
		4 9 2
		3 9 2

0 5 7
9 * 8
7 1 8
	5 0 2
	2 0 4
	0 2 2
		3 4 3
		5 # 6
		1 8 8

The SyferLock user interface can be a simple numeric pad or an advanced layout. It is completely customizable — allowing a variety of layouts, designs, colors, languages and character sets.

two-factor and multifactor authentication, using one-time passwords (OTPs) or PINs. Because these solutions provide device-less OTPs, they offer a simple, more secure way to access information while leveraging users' existing passwords and an organization's password infrastructure.

It is estimated that 99 percent of all authentications use static passwords or PINs, and another estimate shows that 95 percent of all authentications use only the first factor of static passwords/PINs. Organizations with the latest software-based authentication solutions can take the familiarity of static passwords and allow users to continue leveraging them, but convert these static passwords into dynamic OTPs that consist of a randomly changing string of numbers with every log-in.

These software-based solutions address the weaknesses of the traditional password without the need for any additional hardware, providing enhanced security no matter where users log in.

Some of these software-based authentication solutions can be applied to every access point, including virtual private networks (VPNs), Web portals, cloud environments, mobile devices such as tablet computers, personal computers, storage devices, ATMs and other physical devices.

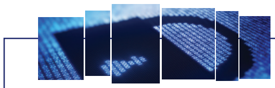
The software installation and registration process for software-based authentication provides organizations with a solution that is minimally intrusive, self-service and easy to operate. These software-based solutions are also scalable and deployable in a high-availability cluster. Such solutions also provide a cost-effective way to comply with authentication regulations and guidelines, both U.S. and international (FFIEC, SOX, GLB, HIPAA, FISMA, PIPEDA, 21 CFR Part 11, Annex 11, BASEL II, European and Japanese data protection directives).

Organizations that have moved away from hardware-based authentication products to software-based solutions are seeing positive results. For example, one company in the energy services field had been using hardware tokens to enable thousands of users to access its nuclear power plant.

The energy company moved to a software-based solution to reduce costs and improve secure access to the plant. It has renewed its subscription to the authentication software for the fourth year and is expanding implementation of the solution into domain/machine authentication, as well as helping to secure several legacy applications.

"Our requirement was a cost savings initiative without sacrificing the strength and security of the password system," an IT executive at the company says. The company chose the software solution for the convenience of a device-less OTP system coupled with attractive pricing and savings.

Another business in the biopharmaceutical industry also moved from hardware- to software-based authentication. The company now uses the solution to provide authentication for 5,000 users, and is considering expanding the implementation of the solution to 80,000 users across its parent company. A security project manager at the firm calls it "a great solution for our company, where the cost and complexity of the hardware token-based system we had previously deployed all goes away.”



Software-based authentication addresses the weaknesses of the traditional password without the need for any additional hardware, providing enhanced security no matter where users log in.

Plan of Action

Information security is a high priority for businesses, and having an effective authentication process in place is essential in today’s environment. Never before have so many users needed access to corporate networks and data from remote locations — and never before have the security threats been greater. A username and static password alone are not enough to ensure secure access.

Older, hardware-based authentication products such as tokens are not cost-effective, and they are subject to a number of drawbacks that can jeopardize the security of information.

By leveraging more modern, software-based authentication solutions, companies can provide superior authentication and security, and improved user experience, at a greatly reduced total cost of ownership (TCO). They no longer have to deal with the expense of tokens and token administration.

Some of these software-based authentication solutions can eliminate or mitigate many different types of attacks, including key logging, brute force, dictionary, sniffing, interception, stored browser passwords, shoulder-surfing and replay.

As more users conduct business and access data from remote locations, the need for reliable and secure application access is essential, but software-based authentication solutions can provide the reliability, security and cost-effectiveness that organizations require. IT and security executives should explore the available alternatives for authentication so they can best protect their organizations. ■

ABOUT SYFERLOCK TECHNOLOGY CORPORATION

SyferLock is an innovative provider of next-generation identity and access management solutions. SyferLock’s patented, software-based authentication, security and single sign-on (SSO) solutions enable enterprises, governments and users to secure every access point, including computers, networks, online access and mobile devices, across a range of applications, such as proprietary networks, cloud computing and mobile. SyferLock’s software-based solutions deliver enhanced single-factor, two-factor and multi-factor authentication through one-time passwords or PINs without the need for any additional hardware or tokens, providing a superior alternative to static passwords along with greatly reduced TCO. SyferLock’s flexible methodology is highly scalable, extremely lightweight and allows for rapid mass deployment.

SyferLock’s system and method is U.S. and foreign patented with additional foreign patents pending. Learn more at www.syferlock.com or contact us at info@syferlock.com.

© 2012 UBM TechWeb, a division of UBM LLC. All Rights Reserved.