

www.securecomputing.com

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.



Mobile Workforce Productivity

Securing Mobile Connectivity with Two-Factor Authentication

Table of Contents

Executive Summary	2
Working Remotely, Then and Now	2
User Identity Gets Lost in Translation	2
Remote Access Requires Stronger Security	3
Strong Authentication for the Mobile Workforce	3
SafeWord MobilePass – An Alternative Software-Based Authenticator	4
Key Benefits of Token-Based and Software-Based Authentication.....	4
Conclusion	5

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

Berkshire, UK
Tel +44.0.870.460.4766

Asia/Pac Headquarters

Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel +81.3.5339.6310

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

© 2007 Secure Computing Corporation. All Rights Reserved. IAM-MobileWk-Nov07Vf, Bess, enterprise strong, IronMail, IronIM, MobilePass, PremierAccess, SafeWord, Secure Computing, SecureOS, SecureSupport, Sidewinder G2, SmartFilter, SoftToken, Strikeback, Type Enforcement, CyberGuard, and Webwasher are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. Application Defenses, Secure Computing Edge, G2 Enterprise Manager, IronNet, On-Box, Power-i-Call, Radar, RemoteAccess, SecureWire, SmartReporter, SnapClear, Total Stream Protection, TrustedSource, and ZAP are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.

Executive Summary

Enterprises are increasingly opening up their networks to a greater constituency of remote users, but they often do not take into consideration the protection of user identity as a critical component of their strategy. The mobile workforce can now work productively from a remote location such as a home office, the airport, a hotel, or a customer site. Organizations must now implement a secure user authentication system, which includes two-factor authentication, as a means to secure these remote connections to sensitive network resources and applications. Moreover, the ubiquitous nature of mobile phones has now given rise to a new, convenient form factor for two-factor authentication—the software-based authenticator that resides right on the mobile device that everyone carries with them.

Working Remotely, Then and Now

It was not so long ago that working remotely and being productive were phrases not often used in the same sentence. Working from home was a luxury for the few, and it was often beset by slow access speeds and limited access to critical business applications. Physical presence in the office was inherently necessary to get any meaningful work done. For employees that traveled or were based in the field, work piled up as they spent long hours in airport lounges, hotels, taxis, and at customer locations.

With the broad adoption of remote access technologies, this scenario has changed. Today, workers outside the office have same level of access to applications, data and computing infrastructure as inside. Thanks to improvements in access technologies, corporations have thrown open the gates to their networks to empower their employees.

The economics of working from home or while on the move are attractive to both the employee and the corporation. To the employee it means a flexible work schedule and the ability to stabilize an otherwise inconsistent work schedule in a global business environment where an individual's responsibilities may span several time zones and countries. To the employer it means more productive employees and higher morale. Companies in a wide range of industries are seeing a growing number of employees who conduct business remotely. Remote access software and hardware markets have experienced tremendous growth as organizations extend the availability of critical applications and data.

Remote workers in a growing number of roles need access to email, files and critical business applications in order to perform day to day activities. Similarly, partners and even customers often need to have access to certain applications and data residing on an enterprise network. The growing number of users that need access to the network is matched only by the growing amounts of data that is available in the corporate datacenters.

User Identity Gets Lost in Translation

Enterprises have clearly created mechanisms and adopted technologies that open up enterprise networks and business applications to the outside world. The level of access control to these networks that was considered adequate within the confines of the office buildings is no longer acceptable. The prospect of a hacker gaining access to enterprise systems claiming to be an employee is enough to make even the most experienced IT administrators queasy.

Moreover, the concepts of managing user identity, in most cases the primary element to controlling the “keys to the kingdom,” have been relatively overlooked, much to the detriment of unsuspecting organizations. Most companies have implemented strong security measures to protect physical access to their facilities. And access to the network from inside the perimeter is often seen as a priority. Nonetheless, it is remote access security that often gets overlooked. User authentication with passwords has served as a means of establishing user identities since the beginning. The system worked fine when the community accessing information did so when inside the secured physical boundary of the organization.

Over the years, increasingly sensitive data on networks has been exposed to more users, attracting more hackers to break into enterprise network environments. Access by a large user community leaves enterprises even more vulnerable to hackers since security of the system is now dependent on the strength of the weakest password in a large group of passwords.

Remote Access Requires Stronger Security

Remote access gateways such as VPNs, Citrix, and Outlook Web Access all create secure tunnels over the Internet. These gateways provide a convenient and secure remote link to network resources. However, relying on simple usernames and passwords to access the entrances to these secure gateways is similar to leaving the front door to your house unlocked, or using a lock that can be easily picked. Static passwords are an unreliable mechanism for guarding the entrance to your trusted systems, applications, and networks. Many passwords can be easily guessed, hacked, or compromised by brute force attacks.

Even complex password policies present problems for end users and IT departments. Changing passwords every 30 days, not allowing users to repeat a password over a given time period and requiring multiple special characters in passwords adds significant complexity. Users may simply forget their password, requiring a call to the help desk to reset the password and driving up the overall cost of IT support and lost productivity, to say nothing of diminished user convenience.

The vulnerabilities of static passwords as an identity mechanism have been well-documented, raising the need for stronger methods of user authentication. Companies with mobile workforces need strong authentication solutions that not only provide reliable security, but that are also easy to install and deploy, simple to manage, and able to grow with their needs.

Strong Authentication for the Mobile Workforce

Clearly, organizations with valuable information must choose something stronger than passwords to protect their resources. Strong authentication—also known as two-factor authentication—refers to systems that require multiple factors for authentication and use advanced technology, such as secret keys and encryption, to verify a user's identity. The simplest example of strong authentication is your ATM card. This requires something you have (your card), and something you know (your PIN). Most people wouldn't want their bank to allow access to their checking account with just one factor. Yet many organizations allow entrance to their valuable VPN, Citrix, and Outlook Web Access resources (often much more valuable than a single personal checking account) with only one factor—a weak password!

Strong authentication solutions such as SafeWord® from Secure Computing® provides proof-positive user identity for users of VPNs, Citrix applications, Webmail, Outlook Web Access and other remote access gateways. SafeWord products positively identify users through strong authentication to assure that only the right people can make connections to trusted applications and networks.

Two factor authentication solutions deliver security through one-time passcode-generating hardware tokens <see figure 1 > combined with the user's PIN. The user simply pushes the button on the token, generating a single-use passcode (via a unique secret key and an advanced encryption algorithm that is contained inside). The user enters the passcode, followed by the user's unique PIN, to gain access. After one use, the passcode is thrown away by the system. If someone attempts to re-use a passcode, access is denied by the authentication server.



Figure 1: Hardware tokens

For employees who make a living on the road, SafeWord provides the vital “lock and key” mechanism to protect the login from almost any location. Road warriors frequently work from the airport lounge, at the hotel, on the train, or from a client's office. Access to the datacenter for these workers—who include sales reps, business consultants, marketing professionals, and other mobile professions—is a lifeline to their success.

SafeWord MobilePass – An Alternative Software-Based Authenticator

According to an analyst study, there are going to be 180.2 million Smartphones in use by 2009. A large percentage of these Smartphones will end up in the hands of business users. The bottom line is that mobile devices are now an integral part of our lives, both from a professional and personal perspective. Now these devices can be leveraged to perform additional activities that heretofore were dependent on other accessories.

Hardware tokens like SafeWord have been the chosen form factor for companies large and small. They are easy to use and easy to carry. But there are many cases where the end user may prefer an alternative, both in terms of carrying convenience and administrative rollout.

With the mobile phone, along with the laptop computer, becoming the ubiquitous mobile toolkit, it makes sense to leverage its presence for two-factor authentication. SafeWord MobilePass® is a software based authentication solution that generates one-time passcodes on a variety of popular mobile phone platforms, including Palm, BlackBerry, Windows Mobile, and J2ME-enabled devices. MobilePass is also available for Windows Desktops, where you can retrieve your one-time passcode from your laptop or desktop PC.

MobilePass combines the ubiquity of mobile devices, such as cell phones and handhelds, with proven strong authentication algorithms to generate one time passcodes right on the mobile device. Mobile devices such as BlackBerries and Palm-based mobile phones are fast becoming an indispensable tool for mobile workforce productivity. They keep us in touch and are always with us. SafeWord MobilePass combines the security of proven two-factor authentication with the convenience of one-time passcodes generated right on your personal mobile device or PC.

Software authenticators like MobilePass make two-factor authentication easier than ever, combining proven security with user convenience. Just quick-launch the MobilePass application from the mobile device to retrieve a one-time passcode for secure remote access logins.

MobilePass allows users to use their mobile phones to generate their secure one-time passcodes—just like a hardware token. It works by using a small software program that is easily downloaded onto users' mobile devices. And it works with any BlackBerry, Palm, J2ME- or Windows Mobile-enabled mobile phones. Users simply activate the application with a single touch of a button, and their one-time passcodes are generated right on the device's screen—just like pushing the button on hardware token. The user then enters that passcode onto their computer, along with their personal PIN, to log into the organization's secure network.



Mobile authentication solutions can reduce costs, such as those associated with deploying remote access and user authentication systems, and provide a very low total cost of ownership. Further, once the software-based authenticator is deployed, it will not expire and never needs to be replaced. And, since it can be used by users' mobile devices, it provides a new level of convenience and usability.

Key Benefits of Token-Based and Software-Based Authentication

1. Tokens that never expire

SafeWord provides the lowest total cost of ownership providing tokens that never expire. Competing authentication solutions require you to repurchase tokens every three years. Their tokens are programmed to expire at the end of that period. Additional costs are incurred not only purchasing replacement tokens, but also re-deploying those tokens to the user base. SafeWord tokens never expire, giving you compelling cost of ownership value.

2. Easy to install, easy to use

SafeWord products are designed to be easily and cost-effectively managed by administrators of remote access solutions. Independent industry product audits have confirmed that SafeWord is one of the easiest products to implement and administer, especially for Microsoft environments.

Installation is lightning-fast. Competing solutions can take hours or days to install and configure properly. Often, systems engineers must be scheduled from the vendor to install the software correctly. Security policies must be mapped out. Ports must be opened, or closed, or both. But with SafeWord, the wizard-driven installation leads you through the process in as little as 15 minutes. In many cases, a separate server is not even needed. SafeWord solutions can install easily on your Active Directory domain controller.

Administrators can manage all user information from the Microsoft tools they already know and use with Active Directory. Other solutions use a proprietary user database which must be managed separately. SafeWord offers true Active Directory integration. The Microsoft Management Console in Active Directory ties the SafeWord tokens directly to your Active Directory users, so there's just one place to manage users and tokens. SafeWord also includes a convenient, web-based user self-enrollment capability. With user self-enrollment, administrators don't have to match each user to their correct token or assign tokens users can simply enroll themselves online.

3. Powerful Remote Access Authentication for VPNs, Citrix, Outlook Web Access (OWA)

SafeWord adds critical strong authentication to positively identify a user before an encrypted VPN gateway is established—an essential component of any secure VPN solution. SafeWord offers robust and scalable solutions that work with all major VPN vendors including, Cisco, Citrix, Check Point, Microsoft, Nortel Networks, Juniper, Aventail, and F5.

Conclusion

The global workforce is going mobile. Employees from all walks of life are proving the value of working remotely. As any road warrior will attest, staying connected to email, core applications, and customer data is critical to job performance and productivity. Two-factor authentication solutions like SafeWord and MobilePass offer a much-needed lock and key mechanism to protect user identity for remote access logins. Securing the remote access connection has never been easier.