maverick™

2-Factor and 4-Factor Authentication Scenario*

LEGAL APPLICATION

*Scenario is for illustrative purposes only. This is not a case study.

IBM Business Partner

maverick™

TOLL FREE / 888-266-1678 **WEB /** www.MaverickSecure.com

Hello and thank you for your interest in Maverick Secure.

In establishing Maverick I had a vision to build a company that everyone could be proud to work for, be associated with, and would want to conduct business. I believe we have achieved that goal and continue to aspire everyday to make that an on-going reality of continuous improvement. Here at Maverick Secure we are building a company that is run with integrity. Our ethos: SECURITY IS EVERYTHING. Our products, our service, and our mission will not be compromised. Our mission is to provide the most secure authentication process available on the market, and match that with the most affordable price point in the market.

The Maverick family is founded on several core principles:

- To stay ahead of hackers and rogue elements by providing the strongest, most secure, highly innovative and patented authentication processes available;
- To provide a great product at a reasonable price;
- To be responsible to our customers: your success is our success;
- To be responsible to our employees: we all work hard and so we should all share in our collective successes.
- To be responsible to this land that we all share: make every effort to create a sustainable product that will contribute to the health, vitality and industry of this planet;
- To invest in solutions that will enable the business community to grow and develop: businesses of all sizesare the backbone of our communities, our culture and our country.

Maverick Secure is fully invested in developing and protecting a work environment that rewards integrity and embraces diversity. We believe in quality service and support this with a strong work ethic. Here at Maverick Secure, we will not compromise integrity for profit. We will not discriminate on the basis of race, ethnicity, religious preference, sexual orientation or gender – rather, we will truly endeavor to embrace and elevate individuals who deliver on our core values. It's simple really: your success is our success. We believe in good honest work, and we will work hard to produce the tools, the solutions, and resources that make your task easier, more efficient, more profitable and most importantly, MORE SECURE.

On behalf of the Maverick family, I welcome you to learn more about our family of products, and to become our next Maverick Secure satisfied customer.

Thank you.

Patrick McNicholas
Managing Partner

Contents

Introduction

In the legal profession, the principle of attorney-client privilege is held as one of the oldest privileges for confidentiality encouraging clients to make "full and frank" disclosures, which then enable attorneys to provide better advice.

The Need for a Strong 2-Factor Authentication

Nowadays, such solutions must have a low total cost of ownership.

Case Scenario

A small group of lawyers decided to partner in establishing a full service collection law firm both taking on legal and agency collection work. They had already signed qualified support staff onboard, like secretaries, paralegals and collectors.

Key Requirements

Strongly protect confidential data by moving from traditional username-password authentication.

Results

The new system provided employees with a more secure access.

Maverick Solution

Maverick 2-F™ perfectly fitted the key requirements.

About Maverick Secure LLC

Maverick allowed more secure, faster remote access to client records and collection cases and follow-up of collections and payments, enhancing productivity.

Court records are public records. Attorneys' communications with their clients are confidential. Both must be protected from tampering and illegal access.

At-A-Glance

Key Requirements

- Strong two-factor authentication system for remote access.
- Smooth integration.
- Versatile.

Solution

- A strong token access system featuring exceptional two-factor authentication.

Results

- More secure, faster remote access to client records and collection cases.
- Secure and faster follow-up of collections and payments, enhancing productivity.

Introduction

In the legal profession, the principle of attorney-client privilege is held as one of the oldest privileges for confidentiality-encouraging clients to make "full and frank" disclosures, which then enable attorneys to provide better advice and more effective representation at court. A client's safety and well-being depends on effective protection of the confidentiality of communication and pertinent documents or evidences he or she shares with his attorney. Consequently there is no better source of sensitive information than the legal profession. This makes legal data attractive for malicious attacks. Clients expect their disclosures to remain confidential and secure. Consequently, protecting the confidentiality of attorney- client communications especially in the age of electronic snooping is paramount. Even when all evidences have been turned into court records after a trial, the court records, if digitized, should also be secured from unlawful access and tampering to protect their integrity. Therefore, not only attorneys but courts of law should make it their duty to safeguard their records from electronic intrusion.

The Need for Better Authentication and Secure Digital Protection of Lawyer-Client Data

Attorney-Client Privilege does not protect confidential electronic data or evidence from being accessed surreptitiously, stolen, or tampered with. Strong security systems should therefore be put in place so that 1) data will not be accessed easily and 2) even if malicious parties get hold of the data, they won't be able to use it because of strong encryption (although this does not protect the data from copying and deletion). In some countries, encryption of data to be used as evidence in court is mandated by law (e.g. UK Data Protection Act of 1998 and the EU Data Protection Directive).

Strong encryption algorithms, like the Advanced Encryption Standard (AES), are well-documented and can easily be implemented for electronic documents without much expenditure and effort on an attorney's part. All he or she has to do is to select an encryption software system and devote enough time to this activity (it would take some time to encrypt records spanning years of law practice), also providing for secure backups and offsite storage.

The 'layers' are usually the Factors of Authentication, which are traditionally three:

1. Something you know – e.g., username, password and bits of personal information.
2. Something you have – security token, smart card, USB dongle. Requiring both 'something you know' and 'something you have' is two-factor authentication. ATM transactions, for example, cannot succeed without both the PIN and the ATM card.
3. Something you are – voice, fingerprints, iris or retina scan, DNA or even brainwave patterns.

Securing remote electronic access to the data, however, requires expert systems best left to vendors with years of experience in the field. Systems are available that put layers of protection between the data and attackers. Some systems even have the capability to monitor and audit who accesses the data and, by means of carefully designed policies, are able to determine whether the nature of such access is illegal, and also able to prevent illegal copying, printing and deleting of said data. However, the first thing to be done with confidential data is to prevent unauthorized access. As mentioned, a layered approach to user authentication and access is the best approach to weed out unauthorized users from the authorized ones. Other layers of security can be added but they are not authentication factors as such but limit the window of opportunity for malicious attackers to operate e.g., access can only be performed at a certain time, or the user's geographical location and position should fall in the list of allowed places some say "somewhere you are" is the fourth factor but the fact remains that location alone cannot be used as authentication and that makes such claims tenuous. By design, two-factor authentication schemes are: Flexible and scalable – They can be used and tailored for small organizations or very large corporations with sites around the world.

Easy to use and deploy– All you need is to insert a security token (smartcard, USB dongle, etc.) into the appropriate slot and the system grants you access after you give the username, password, or additionally, the one-time password (OTP). Since the concept is simple, deployment of security tokens all throughout an organization is faster and there are no steep learning curves. This means workflows are not impacted much, if at all. Cost effective – Ease of use and fast deployment and management (either centrally or distributed) and ubiquity allow greater savings in management, administration and system upkeep, helps realize greater returns on investment. Three-factor authentications (those that require the third factor) do not have these advantages, and are generally used only for the highest access to data and controls that involve the fate of a mega corporation, or national security.

Key Requirements

Remote access through two-factor authentication. Authentication system should be simple to use and integrate smoothly with the firm's existing data protection system to lessen impact on work performance. System should be able to work with different operating systems, requiring no installation on the remote clients' side.

Results

Maverick 2-F and 4-F security tokens were given to staff and clients, depending on staff position and client value and access needs. Those with simpler access needs were given 2-F tokens, those with higher clearances and bigger accounts were given 4-F (capable of storing and verifying digital certificates) for extra security.

Deployment took 3 man weeks. Clients had no major issues and both clients and staff expressed satisfaction with the new system, knowing that securely expediting their accounts was available anywhere there was web access, thanks to Maverick's strong two-factor authentication system.

Case Scenario

A small group of lawyers decides to partner in establishing a full service collection law firm both taking on legal and agency collection work. They had already signed qualified support staff onboard, like secretaries, paralegals and collectors. The firm was headquartered in a restored Victorian house which was a landmark of the locality. They had already installed the data processing and storage systems like client session and recording (even calls made by collectors); automated collection system; telephone services with an automated contacts dialling system; and imaging storage and query systems all tied together by Interactive Voice Response. To secure onsite data, the firm crafted a security policy compliant with various data protection and confidentiality legislation and standards (like HIPAA). They also installed an intrusion detection system with security cameras that would deter any unauthorized entry.

Entry to the premises (and time keeping) was also regulated by a fingerprint recognition system. System access was through username and password that's changed every two months. They hired a provider that monitored and maintained their computer systems. The firm now desired to give an even more enhanced service by allowing their clients and staff to be able to remotely access the firm's client accounts and records database. Clients had limited access, while the staff, depending on position, had different levels of access and permissions based on existing security policies.

Maverick Solution

After reviewing solutions offered by several vendors, the firm identified Maverick Secure LLC's 2-F security token solutions to be ideal for the firm's needs. The security tokens featured a military-grade two-factor authentication via the Maverick 2-F™ or 4-F™ tokens while staying simple, secure and affordable to be used by small organizations but robust enough for deployment by multinational corporations. The tokens generated a one-time password (OTP) that changed every 60 seconds at the touch of a button.

The OTP could be easily read from the security token even in low light conditions. The token easily fit into existing USB slots on the user's computer system and didn't require installation on the user's part. The authentication system was flexible enough to integrate into the firm's data protection system, with convenient web-based remote central management and configuration, allowing user synchronization and authentication from a variety of operating systems and also was able to accommodate various authentication access points and options. The new authentication system not only made the firm's data secure but also allowed the firm to realize savings that would have been otherwise used in intensive training and system installation.

About Maverick Secure LLC

Maverick provides multi-factor authentication solutions to safeguard confidential digital records and data. It is applicable to industries including technology, Internet, healthcare, education, financial services, government, military and subscription services. Maverick's strong multi-factor authentication processes are your solution when passwords just aren't enough to protect your sensitive data from unauthorized users and hackers.

The Maverick brand is dedicated to providing the business community with a high quality and affordable alternative to the pre-existing/overpriced offerings currently available in the market. By providing user-friendly, scalable and seamless compatible technologies, our products match and very often exceed our competitors' products while remaining price sensitive, affordable and much greater offering value for money.

Maverick offers stronger security by leveraging the industry's leading multi-factor authentication processes in very unique and efficient out-of-band channel methods. By living up to its name, Maverick takes a unique "out of the box" strategic perspective in protecting our clients from the threats that surround us in this constantly evolving security-vulnerable world. Maverick provides an easy-to-use approach for users while providing the highest level of security as an overlay to existing business applications and systems.

The Maverick brand started out as Maverick Computers and was named as "One of the fastest growing computer companies in North America," "#1 Solution Provider" and the "#1 System Builder in North America based on growth (2004)," and "Server Innovation Award" by CRN Magazine for developing a virtually indestructible server. The company then launched a new sister company called Maverick Communications which was awarded "2005 North American System Builder Association – Business Innovation of the Year" for creating an integrated array of video, voice and data services that included what was then the world's fastest Internet access for consumers at 45mbps. Over the past five years a new division of the Maverick brand, Maverick Secure LLC., was launched to combat the ever-evolving and tenacious attacks of hackers such unauthorized access of data and the multitude of other security breaches have caused serious turmoil within the computer and associated industries. In 2009 Maverick partnered with IBM, the number one server company in the world for enterprise users, to develop the "Maverick SMART Server Powered by IBM." By utilizing the award winning hardware of Maverick Computers, the industry's leading authentication process of Maverick Secure and the online and business applications of IBM, Maverick is now positioned to deliver end-to-end solutions for businesses small and large. We believe we have brought together the perfect harmony of leading technologies to offer one of the most secure solutions that addresses issues related to password authentication.t

Contact Us

To learn more about how 2-Factor and 4-Factor Authentication products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller.

Patrick McNicholas
President
Maverick Secure, LLC.
Patrick@MaverickSecure.com
www.MaverickSecure.com
772-216-9535 (Cell)
888-266-1678 (Toll-Free)
305-600-0772 (Miami)
917-470-9469 (New York)
415-424-4245 (San Francisco)
020-337-174-11 (London)
888-219-0113 (Fax)
GoToMaverick (SKYPE)

Maverick helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.