maverick™

2-Factor Authentication Scenario*
BANKING TRANSACTIONS

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

IBM Business Partner

maverick™

TOLL FREE / 888-266-1678 WEB / www.MavericksSecure.com

Hello and thank you for your interest in Maverick Secure.

Years ago we set out to build a company that we could all be proud to be a part of; and that is exactly what we are doing. Here at Maverick Secure we are building a company that is run with integrity. Our basic working model is this: SECURITY IS EVERYTHING. Here at Maverick Secure, our product, our service, and our mission will not be compromised. Our mission is to provide the most secure authentication process available at the most affordable prices on the market.

The Maverick family is founded on several simple principles:

- Stay ahead of the hackers and bad elements in the world by providing the strongest, most secure, highly innovative and patented process available.
- Provide a great product at a reasonable price: we endeavor to produce the best possible products with the highest possible standards at a particularly affordable price.
- Be responsible to our customers: your success is our success.
- Be responsible to our employees: we all work hard and so we all should share in any success.
- 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.
- Invest in solutions that will enable the small business community to grow and develop: small businesses are 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, that embraces diversity, that believes in quality service and support, and that recognizes 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 those individuals who deliver the kind of service small businesses deserve and who extend the kind of effort that our small business requires. It's simple really: your success is our success. We believe in hard, honest work and we will work hard to produce the tools, solutions, and resources that make your hard work 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

Banking industry experts are facing the realisation that just one form of customer authentication is not reliable or strong enough to provide proper security for customers, and adequate protection to the banks' finances and their reputation.

Key Requirements

Secure, reliable, easy to use (for customers) and easy to manage (for administrators) with uninterrupted service availability providing continuity during unscheduled downtimes.

Maverick Solution

Utilising the Maverick 2-F™ (Two Factor) authentication solution.

Results

The bank's position after implementing the Maverick security solution.

- Benefit 1 - Increased customer confidence and satisfaction
- Benefit 2 - Reduced costs
- Benefit 3 - Comprehensive secure online transactions
- Benefit 4 - Increased staff confidence in the system
- Benefit 5 - Number of unwarranted errors reduced

Summary

Adopting the scalable Maverick 2-F™ solution enables the bank to achieve its objectives and at the same time reduce its costs and realize a much better return on investment.

Bank Eliminates end-user complexity, Increases level of security, with Maverick™ Two-factor Authentication

At-A-Glance

The Challenge
The Bank needed a robust security system which provided easy secure accessibility but also combined with ease of use.

Key Requirements
The system had to be: Secure, reliable, easy to use (for customers), easy to manage (for administrators) and also gave uninterrupted service availability during unscheduled downtimes.

Solution
Implement the Maverick 2-F™ Authentication Solution One-time password Time-based password generation technology. Having a large LCD screen also made reading the numeric digits easier.

Results
Customer's confidence and satisfaction / Reduced costs / Secure online transactions.

Introduction
It is estimated that two out of three Americans perform online banking transactions at least once a week. This rapid expansion of Internet Banking in recent years has given rise to a generation of technologically savvy fraudsters who utilize increasingly sophisticated techniques of gaining unauthorized access to the accounts and funds of unsuspecting bank customers. Some of these hacking methods have reached a level of sophistication whereby they even manage to thwart strong preventive measures and authentication systems that have been put in place. This results in millions of dollars lost to electronic hackers who transfer victims' funds to untraceable accounts in countries that are outside of enforceable jurisdictional authority. In recognition of this ever increasing threat to banks, the U.S. Federal Financial Institutions Examination Council (FFIEC) recently released a new set of guidelines entitled "Supplement to Authentication in an Internet Banking Environment" to improve current online authentication procedures. Banking industry experts now realize that just one form of customer authentication is not sufficiently reliable to provide the necessary layer of security for customers, and to also protect the banks' finances and reputation. Consequently, layered (or multi-factor) authentication is now increasingly being recognised as the way forward for authenticating such online banking transactions. Implementing a primary requirement of the banks in utilizing these layered security authentications was to ensure its ease of use and simplicity. The winning solution had to be a combination of state-of-the-art authentication systems which was easy to use and implement, but also coupled with unbreakable security layered protection. For some financial institutions, the addition of another security factor could simply be restricting the time of day a customer could make a transaction, or in creating a 'white-list' of fund transfer recipients. Another secure way was to place a two-factor security control into banking transactions which used an additional "out-of–band" authentication (using a different channel or device than the one used for inputting the password). For most online banking customers, this means they used the Internet for putting in the password and further verification of their identity was provided through telephone or another communication device.

One-time passwords (OTP)

OTP have given good protection against malware such as "keyloggers"(software or hardware that record an intended victim's keystrokes)especially the key strokes for user names and passwords. OTPs become invalid after use, so in general, they are safe to use for accessing one's online account even on a public computer.

Security tokens

In case a key logging attack becomes successful [e.g. prior to the introduction of OTPs], using security tokens (smart cards, key fobs, dongles and other portable hardware) can improve security because even if the attacker had the password, they still would not be able to access an account without the token and vice-versa. Security tokens with the ability to generate OTPs create a strong two-factor authentication layer.

Case Scenario: Commercial Bank

A fifteen year old domestic commercial bank experienced rapid growth due to the high quality of service it provided both to local businesses and to local communities. With the advent of online banking the bank's senior management recognized that for them to continue delivering efficient and innovative services, they had to encourage more customers (especially their larger corporate accounts) to use online banking systems. In order to realise this aim it was important to generate a very secure, but also easy to use online environment. They had already created a very robust website with one of the most convenient e-banking experiences (as determined by several detailed customer surveys). The only piece missing was having a proven robust online security system. The challenge for the bank was to install a strong security system capable of thwarting phishing, malware, web attacks and other similar threats which, at the same time, was extremely easy to use.

Key Requirements

Online banking meant dealing with money as data. Every second lost in downtime was revenue lost to the bank. As such, any banking security system, ideally, should not cause any unreasonable downtime, or be resilient enough to prevent such downtimes in the first place. In the case of the particular bank in question, they needed a strong authentication system that met these key requirements that would not affect their day-to-day operations.

Secure Reliable Easy to Use (for customers) Easy to manage (for administrators) Uninterrupted continuity and provisioning during Downtimes. Notably, such a security system should protect against increasingly sophisticated variants of sniffing, keylogging, shoulder-surfing, cracking of saved passwords, and replay attacks. The best defences against any of these attack methods would be the use of one-time passwords and security tokens (see side bar).

For the IT administrator, the Maverick 2-F™ offered the convenient features:

- Web-based management interface for remote management
- Central authentication for networks or computer operating systems
- Provision of full configuration and management tool set
- Easy and fast integration in both centralized and distributed topologies
- Compliant with OATH TOTP algorithm
- Seamless integration with 3rd-party systems
- Support for a wide range of authentication and access gateway solutions to protect important information
- Certified with CE and FCC

And when it comes to support, the Maverick 2-F™ also comes with advanced pre-sales and after-sales services at reasonable rates.

The Maverick 2-F™ has proven effective against:

- Simple phishing attacks
- Real-Time phishing attacks
- Brute-Force attacks
- Chosen-Plaintext attacks
- Replay attacks
- Shoulder surfing and snooping

Maverick Secure Solution and Implementation

After reviewing several different online security strategies, the bank decided to install a second layer of security via two-factor authentication by providing security tokens with OTP capabilities to their customers. Out of many solutions considered, the bank chose the 2-F™ from Maverick Secure LLC with its time-based password generation and synchronization.

At the push of a button, the Maverick 2-F™ generated and displayed a secure OTP every 60 seconds (optionally every 30 seconds) which ensured proper identification and allowed only authenticated users with authorized access to critical applications and sensitive data. In addition, the unit's large LCD screen made it easier to read the numeric digits. This worked well even in low light conditions and was a must for users with aging eyes or defective/impaired vision. The Maverick 2-F™ also came with an added timer indicator that showed the time interval left before the next OTP generation. This made the Maverick 2-F™ very easy and convenient to use. The Maverick 2-F™ can be used with various operating systems Windows™, OS-X™, and Linux with no special installation required, ensuring the widest range of computer users could use the technology.

Results

Maverick Secure LLC's simple yet sophisticated solution met the full requirement. It worked smoothly with the bank's existing systems and they were able to complete the security token and intial product rollout within 90 days. No tangible adoption issues were encountered. Even with the additional authentication step, the customers realized the benefit of the bank's new security authentication system. The Maverick 2-F™ solution increased customer confidence in using the bank's website for online banking, especially those with corporate accounts. Adopting the scalable Maverick 2-F™ solution enabled the bank to achieve its security objectives, and at the same time, make sizeable reduction to costs and also realize a good return on investment.

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.

Contact Us

To learn more about how 2-Factor Authentication products, services, and solutions help solve your business and IT challenges please 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.