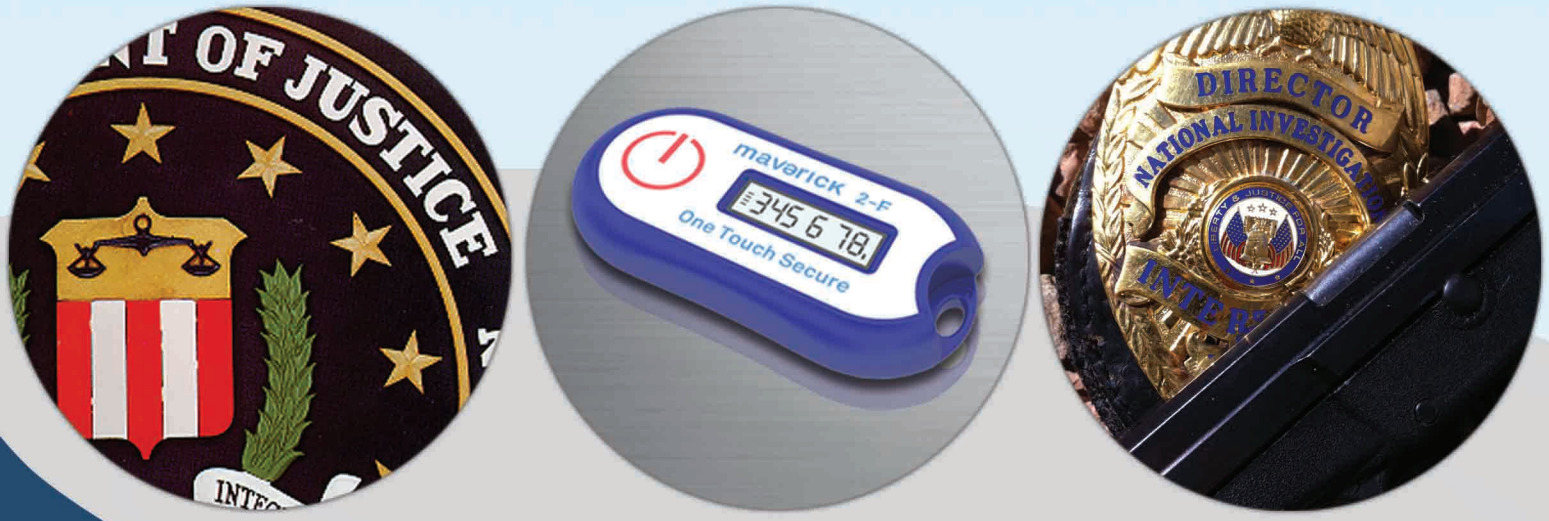
maverick™

2-Factor Authentication Scenario*

FEDERAL-STATE CRIMINAL INVESTIGATION



*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
Investigation and solution of crimes requires quick and secure cooperation between state and federal government agencies.

The Need for a Strong 2-Factor Authentication
To keep up with the need of the times, online data security systems i.e., authentication, should be flexible enough to adjust to an organization of any size.

Case Scenario
The investigative arm of a U.S. State was keen on tapping into the FBI's state-of-the-art real-time criminal-justice records system via its local Criminal Justice Information Services.

Key Requirements
Users must be able to authenticate via the secure layer provided by a two-factor authentication system.

Challenges
The new system had to be affordable enough to fit to a tight state budget.

Maverick Solution
After reviewing several options offered by different vendors, state officials opted for the solution with the best possible combination of flexibility, scalability, security and cost effectiveness found in the Maverick Secure LLC's Maverick 2-F™ token system.

Results
The new system provided employees with a more secure access combined with unparalleled scalability and simplicity.

About Maverick Secure LLC
- Fast, secure real-time state access to the FBI services.
- State investigators were able to do their work better and faster than before.
- State realized better and faster ROI compared to the old system.

Access to state and federal criminal investigation systems secured and protected by strong two-factor authentication

At-A-Glance

Key Requirements

- Authenticate via a two-factor authentication system.
- Easy to learn and deploy.
- Flexible and multi-user authentication system.

Solution

- A strong token access system featuring exceptionally resilient two-factor authentication.

Results

- Fast, secure real-time state access to the FBI services.
- State investigators were able to do their work faster and more securely than before.
- Great savings realized compared to the old system.

Introduction

Investigation and solution of crimes requires quick and secure cooperation between state and federal government agencies for fast exchange of information that can lead to prevention or solution of a crime. Hence, a secure fast and cost effective method of shared access to criminal investigative portals and resources is a must in today's increasingly online and interactive way of life. In addition, crime is increasingly becoming more sophisticated and is getting online savvy. Governments should therefore also become online aware as well in order to be one step ahead of criminal elements, to protect itself against criminal attacks and beat crime at its own game.

A simple username and password access to a dumb terminal connected by a leased line to a central criminal-justice records system is an inefficient, insecure and expensive way to conduct criminal investigations. A stronger, efficient and cost-effective means of authenticating online criminal investigations should replace the old methodology.

The Need for a Strong 2-Factor Authentication

To keep up with the need of the times, online data security systems i.e., authentication should be flexible enough to adjust to an organization of any size, adopt a wide variety of authentication options, secure, and have a low total cost of ownership to optimize return on investment. Two factor authentication meets these requirements. Not only do two-factor authentication schemes make it hard for attackers to steal a user's online credentials, it also requires the attacker to possess the actual physical security token in order for his or her attack to work. Secure two-factor systems make it very hard for malicious perpetrators online to duplicate the physical security tokens. These systems also generate time-based one-time passwords (OTPs) that are valid only for a certain number of seconds and are invalid after use.

Key Requirements

- Users had to be able to authenticate via the secure layer provided by a two-factor authentication system.
- The system had to be easy to use and deploy in a lot of situations to minimize workflow disruptions and implementation costs.
- More than one user had to be able to access the system at a time to facilitate fast and efficient collaboration leading to crimes being solved and prosecuted at a faster rate.

Challenges

- Since state computer systems could not all be upgraded in a short time, the new solution had to be more flexible enough to accommodate a wide variety of system configurations, including aging systems. This was coupled with a dual purpose role whereby the state was in the process of improving its electronic communications infrastructure.
- Different state personnel had varied security access needs.
- The new system had to be able to scale to these needs. The new system also had to be affordable enough to fit into a tight state budget.

By design, 2-Factor authentication systems 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 the security token (smartcard, USB dongle, etc) into the appropriate reader and the system grants you access after you provide the correct password. Since the concept is simple, deployment of security tokens all throughout the 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, thereby realizing greater returns on investment.
- Secure fast and easy systems make it easier for state criminal-investigation employees to concentrate on what they do best fighting and preventing crime.

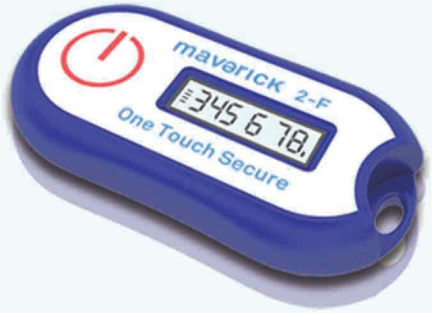
Without modern and robust security systems in place, governments cannot function very well and will always be at the heels of criminal elements.

Case Scenario

The investigative arm of a U.S. State was keen on tapping into the FBI's state-of-the-art real-time criminal-justice records database via its local Criminal Justice Information Services system. This was in order for state investigators to effectively follow-up and solve crimes by having secure access to records on registered offenders and convicts including current intelligence and fingerprints. The problem with the old state online investigation system was that it was not real-time, slow (using a dumb terminal), allowed only one person at a time, expensive (more than $10,000 per leased line per county) and was not flexible enough to allow various features (like video-conferencing). A flexible alternative to the old Criminal Justice Information Services system had to be found one that met the state's needs to connect into the federal system with the least amount of hassle, effort and cost but with the greatest security and feature benefits.

Results

- State forces now had real-time access to the FBI's information resources in a secure, multi-user manner.
- Secure two-factor authentication in an easy-to-use, easy to deploy, easy to administer and manage combination was a winner with state investigators.
- The projected savings (more than $2 million annually) was also an unexpected bonus ROI for state accountants.



Maverick Solution

After reviewing several options offered by vendors, state officials opted for the solution with the best possible combination of flexibility, scalability, security and cost effectiveness found in the Maverick Secure LLC's Maverick 2-F™ token system. By design, the Maverick 2-F™ system was secure enough to meet the needs of even the military through its simple two-factor authentication via the Maverick 2-F™ tokens while maintaining simplicity, security and affordability to be employed by even the smallest of organizations at the shortest possible deployment time. Inputting the second factor a one-time password (OTP) that changed every 60-seconds that was push-button generated and easily read from the security token even in low light conditions was a cinch. The token easily fitted into the existing USB slots of the state's computer systems and required no installation on the user's part. Managing and administering the new system was also flexible enough to easily integrate into existing state security access systems, provided web-based remote central management, configuration, user synchronization and authentication, worked with a lot of popular operating systems, and provided connectivity with a wide variety of authentication access options.

This convenience and flexibility of use and simplified management also resulted into greater state savings by replacing the expensive dedicated per-county leased lines and used the state's existing web-connected LAN which boosted its security in the process. Now, state investigators were strongly protected via two-factor authentication while they connected to the vast array of information resources at the FBI's disposal in an interactive mode. The new Maverick 2-F system also protected state employees against malicious online attacks like simple phishing, real-time phishing, brute-force attacks, chosen-plaintext and replay attacks, snooping and shoulder surfing.

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.