Implementing Strong Authentication Best Practices

By Stuart Rauch

Recently, challenges to Internet security have become far more sophisticated and organized. In the past, hackers weren't looking to make a profit, while today, cyber-crooks from around the world are looking to take advantage of any opportunity that will provide them financial gain. A corporation's data is the "crème-de-la-crème" sought after by hackers, who seek to gain insider information to try and manipulate a stock deal or steal sensitive customer information such as social security numbers to wreck havoc on a person's hard earned credit identity. Hackers also try social engineering techniques to bluff passwords out of unsuspecting employees. Should any security breeches occur, companies and their executives face strict financial and legal penalties, not to mention the negative ramifications from customers and the media. Our financial system, the stock market and our economy depend on the trust that corporations strive to maintain when they manage sensitive information. When the market loses that trust, the results can be disastrous, for corporations, their stockholders and customers. Fortunately, there are steps that can be taken to help safeguard a company's network and their data to help prevent such devastating thefts. This article will discuss some effective and reliable best practices that can be implemented.

WHAT MEASURES SHOULD BUSINESSES TAKE TO ENSURE THEIR DATA AS WELL AS THEIR CUSTOMERS ARE SAFEGUARDED?

One of the first steps a company needs to take to safeguard its customers' personal information is to create proper procedures for routine processes. In order to make sure that sensitive data such as customer bank account details or financial history is safe, the employees running day-to-day operations should all be following a strict set of guidelines. Having strict procedures in place helps ensure the security measures that a company creates to keep valuable data in the right hands are being followed. It's typical that companies allow information access to many third- party individuals and corporations, including partners, financial institutions and clearing houses, which are often necessary to carry out day-to-day operations. But do you know who is accessing your company's data? Are the security protocols in place to ensure that those who access the data are authorized to do so? How do you make sure that the information isn't compromised by someone who happened to get a hold of an employee's password that was under their keyboard or posted somewhere on a sticky-note?

Two-factor authentication and single-use passcodes allow companies to meet this data access challenge head-on.

While two-factor authentication is not a new technology to many IT professionals, there are some things to keep in mind when you are ready to implement your network and data-access protection strategy. Do you know that industry experts estimate that 30 to 40 percent of network passwords can be hacked within five minutes? The problem with reusable passwords is that criminals can reuse them too. "Low-hanging fruit," as it's known in the hacker community, refers to password-only security that is viewed as an easy target. Fixed passwords in the wrong hands can cost a company millions in losses, not to mention a potential legal and public relations nightmare—all because an easy to guess password was used. Most of the vulnerabilities of fixed passwords (stealing, sniffing, guessing, hacking, etc.) can be eliminated if users constantly change their passwords - not every 30 days, but every single time they log into the system. This is not a practical strategy since most users have a hard time switching passwords every few months, let alone every time they login. The solution to password vulnerabilities is two-factor authentication. Think of two-factor authentication tokens as you would an ATM card; two-factor authentication requires something a user has (the ATM card) and something a user knows (the pin).

A token (the ATM card in our example) generates and displays single-use passwords (the pin) on demand via a unique secret key and an advanced encryption algorithm that is contained inside. A server is linked to the token and uses the same secret key with an event counter to confirm the authenticity of each password presented by each user. After being used once, a token-generated password is useless and is thrown away by the system. If someone steals the used password, it is useless—which virtually eliminates threats from outsiders stealing, copying or reusing passwords. Next time you activate the token you generate a new, unique password thwarting the fundamental vulnerability of fixed-passwords.

When you're selecting an authentication system, it is easy to get confused by the numerous issues and variables involved. One thing to remember is that not all tokens are created equal—there are advantages and disadvantages of each. You might be thinking—isn't a token just a token? In fact this is not the case at all. You should care about the basic functionality of the token system you choose because the type of token you launch can dramatically affect the success or failure of your project. The choice you make can determine which applications can be protected and the level of security obtained. It can have a big impact on down-the-road admin costs that some people don't think about up front. For example, some expire in two or three years and must be replaced, substantially raising help desk costs. Others get out of time-synch easily due to failing battery life and result in frustrated end-user experiences.

Most importantly, authentication will be one of the most visible and tangible components of your security strategy. The success of your authentication strategy will largely depend on how well users accept the device and how easy it is for administrators to get the device into the hands of the end users. You might also be surprised about the lifespan of authentication systems. Most organizations that installed them more than 10 years ago still have them in place—and once a particular system is in place, it is fairly difficult to change, so you're making a decision that could impact a lot of people for many years.

What are the key characteristics you should consider when you are ready to implement your company's security policy?

- Token Security
- Compatibility
- Ease of Use
- Administration Costs
- Total Cost of Ownership
- One in a Million

Token Security—What token provides the necessary security? This should be your first and foremost consideration when selecting your authentication solution and the strength of your token may depend on the sensitivity of the data you want to protect. There are vast differences in security among various types of tokens. Understanding the differences will help you select the token that meets your specific needs.

Compatibility—Which applications can be protected? If an authenticator won't work with all of your applications, then no other characteristic matters. It is extremely important to select authenticators that are compatible with your existing administrative systems, like Microsoft's widely deployed Active Directory. Since you may not know what systems you will use in the future, you should look for systems that are flexible and adaptable. Another point to keep in mind is compatibility with your end users' systems—tokens can be used anywhere, while smart cards and biometrics are tied to a single machine and may require special hardware or software.

Ease of Use—Some tokens require a significantly larger number of key strokes and steps in order to perform authentication. Some require users to perform an extra step to resynchronize tokens with a server clock. Some require users to wait up to 60 seconds before obtaining a password, which all translates into lost productivity. How much is a minute worth? If an organization has 10,000 users, and if each month they need to wait on average just two times for a password, the costs can be more then you think! If the average annual compensation is $75,000 per user, the costs in productivity can be over $12,000 per month—and that is just waiting two times during the month! Imagine how much it would cost if a user had to wait every single time they logged in?

Administration Costs—These costs include deploying the tokens and replacing them down the road if necessary. It also includes costs to support token users, filed with things such as forgotten PINS, broken tokens and re-synchronization issues. Determining which token requires the least amount of support is a frequently overlooked cost.

Total Cost of Ownership—Adding up all of your costs, from the initial purchase costs to ongoing support fees determines the total cost of ownership. Tokens that use time-synchronous technology are always on, and they can rapidly diminish battery life. These tokens must be replaced after merely two or three years, significantly impacting your total cost of ownership. Determining what this cost is and calculating it before making a purchase decision is key.

One in a Million Security—How secure is that token? All tokens are more secure then just a fixed password—however the level of security a token provides varies tremendously based on the type of technology standards built into it. The banking industry established a standard for authentication security that can be followed to avoid most liability called ANSI X9.9. What this means in essence is that the odds of a successful attack on an individual account must be no greater than one in a million. In other words, the password criteria must allow for there to be one million possible legitimate passwords that can be used to protect the account. Unless the attacker can obtain the secret key, he has to guess which password is correct out of at least one million possibilities, so the odds are only about one in a million. Memorized passwords made up of English words don't meet these standards since the average adult vocabulary is 80,000 words, an attacker has a 1 in 80,000 chance of guessing the word—and even better odds; for example in a recent company password audit—22 percent of passwords were vanity words such as "stud," "goddess," or just the simple "password"—which most users thought were very clever.

SO WHAT CAN BUSINESSES DO TO IMPLEMENT STRONG AUTHENTICATION BEST PRACTICES?

First, there needs to be top-down commitment to IT security in the organization, starting with the CEO. Security needs to be built into the business plan of an organization; it can't be just another line-item IT project into which managers throw money. Next, the company needs to carry out a thorough risk assessment to define and understand the threats to their infrastructure by bringing in outside experts, if needed. From this, they should develop a comprehensive security policy, working closely with all of the departments in the company. Only after a company has gone through a thorough evaluation and operations assessment process should they think about products. You can view an unbiased, detailed explanation of various strong authentication technologies at www.securecomputing.com/index.cfm?skey=969.

As director of product marketing, authentication, NaSPA member Stuart Rauch is responsible for driving marketing strategy, positioning, and programs for Secure Computing's Strong Authentication product line. Mr. Rauch has over 14 years of product and corporate marketing experience in the high-tech industry. Prior to joining Secure Computing, he was director of marketing for PeopleSoft Inc., where he was responsible for creating and evangelizing corporate brand and positioning platforms. Mr. Rauch also held a wide range of product marketing positions at Oracle Corporation, most recently as principal product marketing manager for the Small and Midsize Business (SMB) group and supply chain management product team. He holds a BA degree in Linguistics and Spanish from the University of California, Berkeley.