

Technology secures remote access

By Diana Kelley

Access Control & Security Systems, Mar 1, 2002

Many enterprises are realizing the need to provide their users, partners and customers with remote access to their internal network or Web servers. Allowing access to valuable data is a business requirement, but it is also a risk. To prevent theft, enterprises need to complete risk analysis assessments to determine the value of the data. Modeling various risk scenarios enables firms to match the security requirements and costs involved with protecting an asset to the asset's value. Addressing all the points in a network where data must be protected ensures the security at both the transport and application layers. This article will cover questions and issues organizations need to address when creating secure remote access authentication solutions.

Is authentication necessary?

When designing a remote access solution, a company should answer several business questions:

- How will the enterprise monitor and audit remote access?
- What are the skill levels and patience of the remote users?
- Which servers and areas of the network do these users need access to?
- What is the cost associated with potential data loss?

The answers to these questions will guide the organization to the best technology solution for the business.

The foundation for any successful remote access solution is easy-to-use, strong authentication. Authentication is the process of providing and proving identifying credentials. Just as a traveler needs reliable proof of identity (a passport) to enter a foreign country, so too does a remote user need reliable proof of identity to enter a network or server. Once a user has been authenticated, his activities on the network can be monitored and controlled to prevent data loss and harm to internal systems.

Where to authenticate?

Remote access is usually provided at a couple of access points or gateways. To decide where to allow access, companies must consider the business' purpose.

In the case of a trading exchange, in which a company needs to provide access only to one or two internal databases from a Web server, it may make sense to keep the databases in a protected zone, put the application server in a DMZ or lobby zone, and request the user authentication credentials at the application server. For organizations that are supporting a large, mobile workforce, the point of remote access may well be a firewall, VPN, or other access gateway. In this case, the organization should put the authentication check at the point of remote access.

How to authenticate?

Enterprises must decide which type of authentication is best for their secure remote access solution. Identification and authentication (I&A) require a user or system to provide proof of identity in order to be authenticated. These proof points, or credentials, can be presented alone or in combinations to provide single or multi-factor authentication. Types of credentials include, “what you know,” such as a PIN or password; “what you have,” such as an ATM or credit card; and “what you are,” such as a fingerprint or voice scan. Traditionally, two-factor authentication is stronger but more costly to deploy than single factor. For access to low-value data, single-factor authentication may be sufficient. When protecting more valuable data, however, enterprises may consider the available multi-factor authentication solutions.

Single-factor authentication

Traditional single-factor authentication is well-deployed in the familiar manner of user ID and password. While there is nothing inherently wrong with user IDs and passwords, they should not be used as the only form of authentication. Passwords that can be re-used can also be stolen and used by attackers.

Two-factor authentication

There are four common methods of two-factor authentication.

- *eTokens and smart cards.* Both eTokens and smart cards can provide a second factor of authentication that makes them stronger than standard user IDs and passwords. However, both of these solutions require additional hardware. Additional hardware can be expensive to purchase and maintain, thus increasing the overall cost of the solution.
- *PKI and digital certificates.* Digital certificates, as part of an overall public key infrastructure (PKI) solution, can provide a second factor of authentication. Unfortunately, deploying a PKI is costly. Additionally, there is significant overhead involved because the user must keep possession of his/her private key in order to authenticate — leading to high technical support costs and administrative overhead.
- *biometrics.* Biometrics can include scans of body parts such as fingerprints or retina information. Biometrics also includes voice-print matching and measuring typing rates and patterns. Biometric readers can be costly and not completely reliable. For most consumer and enterprise remote access solutions, they are not yet a viable financial alternative.
- *hardware fingerprints.* Taking a digital fingerprint of a user's hardware and linking that to a password is another way to achieve two-factor authentication. This solution requires no additional hardware or steps for the end-user and is generally less expensive than other forms of two-factor authentication. It must be noted, however, that it works best in mobile work force deployments, where users are linked to a specific piece of hardware.

What to look for in a secure remote access authentication solution

There are three concepts most important to installing a secure remote access authentication solution.

- *monitoring and auditing.* The basis for any monitoring system requires knowing who or what to track. Strong authentication is the foundation for reliable monitoring and auditing information because it allows organizations to know exactly who is accessing their networks' Web site. Enterprises should look for products that provide detailed logging and reporting that can be used both to audit system usage and as a forensics tool.
- *protection of assets.* In the digital age, information is the key asset of most companies. Making sure that only pre-approved, authorized users have access to the information is critical. By protecting access to Web servers and networks with strong authentication, unauthorized users are prevented from stealing valuable data assets.
- *ease of use.* From the client perspective, a secure remote access solution must be easy to use. If it is not, users will find a way to circumvent it, thus eliminating all the security measures taken. Systems that provide strong authentication but do not require new hardware or tokens for users to carry are preferable.

Selecting the appropriate remote access authentication solution will provide the right level of security without making it difficult for the end-user. When all of these pieces fall together, secure remote access authentication will complement an overall data theft prevention strategy.

For the record About the author

Diana Kelley is vice president, security technology, at Safe3w Inc., a provider of strong two-factor authentication solutions for secure on-line access, payments and transactions.

About the company

Founded in 1999, Safe3w, Inc. provides strong two-factor authentication solutions for secure on-line access, payments, and transactions. The company's IDshield™ and FraudNet solutions require no hardware tokens or readers and are transparent to end-users. Safe3w, Inc. has corporate headquarters in the U.S. and a research and development center in Israel. The company has strong strategic alliances and has received investment capital in the U.S., Israel, Spain, China, Japan, Argentina, and throughout Europe. Current customers include enterprises that focus on e-payments, financial services/banking, B2B, and gaming, and corporate enterprises and governments focused on secure remote access. Safe3w, Inc. is a member of the Verified by VISA and MasterCard SPA secure payment programs.

For more information, go to Safe3w's web site at <http://www.safe3w.com> or contact William Sussman at 516-222-1580.

© 2002, PRIMEDIA Business Magazines & Media Inc. All rights reserved. This article is protected by United States copyright and other intellectual property laws and may not be reproduced, rewritten, distributed, disseminated, transmitted, displayed, published or broadcast, directly or indirectly, in any medium without the prior written permission of PRIMEDIA Business Corp.