

GuardID's Authentication Method May Have Wider Uses

Ant Allan

The new ID Vault offers two-factor authentication directly to consumers. But GuardID Systems' emphasis on this feature may obscure the product's value as a "caller ID" service to authenticate Web sites.

NEWS ANALYSIS

Event

On 7 February 2006, GuardID introduced ID Vault, a product designed to offer consumers secure online access to banks and other financial institutions. ID Vault, which Guard ID describes as a two-factor authentication system, uses a smart card — enabled with a personal identification number — that connects to a computer's USB (Universal Serial Bus) port, holds passwords for various Web sites and automatically forwards the appropriate password to each Web site by injecting it directly into the outgoing data stream.

Analysis

Most financial institutions and other companies doing business online recognize that password authentication alone does not deliver adequate security. Passwords leave businesses and users vulnerable to attack methods such as social engineering, spyware-based password theft and "phishing" (identity theft via e-mail). It is not yet clear what method of authentication will replace passwords, delivering the critical balance of strong security, cost and ease of use. However, a great deal of attention is being paid to so-called "two-factor" authentication, which combines something the user *knows* (such as a password or personal identification number) with something he or she *possesses* (such as a token or smart card).

GuardID seeks to place two-factor authentication directly in the consumer's hands for the first time. But this approach may obscure ID Vault's real benefits. ID Vault provides two-factor protection for stored passwords — but it is still the passwords alone that authenticate the user to the Web sites, so they remain vulnerable to social engineering. ID Vault also provides protection against simple password-stealing spyware, such as key loggers. However, because the passwords are sent using a Web browser and operating system that may not be secure, they remain vulnerable to more sophisticated spyware. Other vendors will target consumers with stronger authentication methods that mitigate both types of threat.

However, GuardID provides a service, embedded within ID Vault, that checks sign-in request against a database of thousands of online financial sites every time ID Vault is used to sign in. This can block phishing and "pharming" — attempts to take the user to a fake Web site — in a more proactive way than browser plug-ins and enhancements. This simple "whitelisting" service may represent ID Vault's real value. Gartner believes GuardID could best leverage this approach by offering a value-added caller ID service for Web sites, complementing other vendors' consumer authentication methods.

Recommendations for banks and other financial institutions

- Recognize that strong authentication is not yet a commodity that can be left to consumer choice. Consumers are less able than you to evaluate the benefits, and limitations, of stronger authentication methods.
- Seek to implement stronger consumer authentication methods or complementary safeguards by the end of 2007.
- Educate your customers about online security, especially by participating in industry initiatives such as Get Safe Online (www.getsafeonline.org).

Analytical Source: Ant Allan, Gartner Research

Recommended Reading and Related Research

- "Regulators Tell U.S. Banks to Adopt Stronger Risk-Based Authentication" — Regulatory guidance will spur most U.S. banks to move beyond password-based authentication by the end of 2006. **By Avivah Litan**
- "Caller ID Would Enable a Reliable, Trustable Internet" — Caller ID functionality must be added to e-mail and Web browsers to prevent fraud. **By John Pescatore**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509