Strikeforce's ProtectID Technology Boosts Identity Security with Phone Call

EWEEK, August 5, 2004
By Mark Hachman

Two-factor security aims to boost user identification beyond the simple password. However, StrikeForce Technologies Inc. offers a twist to this greater level of security: a verification technique that uses a wired or wireless phone.

StrikeForce Technologies recently re-branded its authentication technology. Previously called COBAS (Centralized Out-of-Band Authentication Software) will now be know as ProtectID, company officials said. The technology can reinforce a password with some other form of identification that uniquely identifies a user, such as forms of biometric identification. The company is also developing additional means of verifying identities, such as keyboard-level encryption.

StrikeForce's ProtectID VBVoice scheme adds an additional "out-of-band" layer of security, without undue hassle, the company said. After logging into a ProtectID-secured Web site, the user is asked to enter his or her username. The server then dials a specified phone number—usually an office phone or cell phone—and asks the user to input the password into the phone, and then hang up. Within a second or two, the login proceeds.

According to security researchers, there are several ways a security system can verify that someone is an authorized user. Most systems use a unique code that supposedly only the user knows, such as a password, possibly backed up a unique, hardware security token assigned to each user—something unique. More complex systems can also use some form of biometric identification, such as a fingerprint or retinal scan, to provide additional security.

Click here to Microsoft and RSA's vision for a token-based service called SecurID.

Taken individually, each form of security is defeatable. Together, the combination becomes more secure. However, one problem is that as security becomes more complex it places more of a burden on a user.

For example, in an April study of 5,000 e-commerce users, analyst Gartner Inc. found that requiring the use of an additional security device, such as a smart card, was the least desirable alternative toward enhancing e-commerce security, said Avivah Litan, the analyst responsible for the survey.

StrikeForce executives argue that a password tied to a somewhat personal device such as an office phone or mobile phone is more secure than a bare password, and less hassle than a dedicated token—although the ProtectID can be used with a token, as well.

"The goal is that it doesn't go out and force people to buy something new," said George Waller, executive vice president of StrikeForce, headquartered in Edison, N.J.

eWEEK.com Special Report: Cyber-Crime

Cloning a mobile phone won't necessarily defeat the system, either, he pointed out. "Are you going to approve a transaction you didn't authorize?" Waller said.

For insights on security coverage around the Web, check out eWEEK.com Security Center Editor Larry Seltzer's Weblog.

The software can also be configured to ring a second phone, such as a bank manager needed to authorize a large wire transfer.

Typically, the password entered through a phone's keypad will be a number, Waller said, a less-secure password than a one with different numbers and characters entered on a keyboard.

The ProtectID systems can also train a user to repeat back a unique password delivered over the phone, Waller said. The software is trained to identify the way in which a user not only repeats a number, but the rising and falling cadences a user uses when beginning and ending a series of numbers. This biometric identification can be used to prevent "shoulder surfing" a password, Waller said.

The "out-of-band" technique tries to ensure that if one means of communicating with the StrikeForce server over the network is compromised, another means—a phone—can be used as well. If responding to a phone becomes too onerous, StrikeForce said it is in the final phases of testing a technique to push a 128-bit SSL channel down to the keyboard level via a second out-of-band server. The keyboard encryption, enabled by a small client application, is designed to defeat keyboard loggers by encrypting the information, Waller said.

The third piece of the puzzle is a technology that StrikeForce calls "VerifyID". Based on a database of information that StrikeForce has acquired from third-party vendors and public records, the software can ask a user a series of multiple-choice questions based on personal history, something that only the user should know the answer to. Sample questions might ask for the color of a car the user previously owned, or the street address of a former home, Waller said.

StrikeForce's approach has won over at least one customer, myVirtualCard.com, a Montreal-based e-commerce company with 33,000 electronic transactions to date. It uses Panasonic as an ASP (authentication services provider). Japan's KDDI has also signed on as an ASP provider, Waller said.

"We took their technology and developed it further," said Howard Cohen, myVirtualCard.com's chief executive. "They came to us with their verification technology, and we developed the middleware for their e-commerce world. We haven't had an easy shot with it; some people like it, some people don't. It's not an easy sell."

That market resistance is partly because U.S. customers haven't accepted

supplementary security devices such as the smart cards used overseas, Gartner's Litan said. "They're ahead of the market," she said. "In terms of the market for out-of-band authentication, there's probably more of a market in the U.K. than the U.S."

In addition, U.S. banks are very reluctant to adopt another form of authentication, according to Litan.

Moreover, most confidential information isn't captured in transit to and from the bank, but on the bank's servers. "The rest of the market needs it more than banks do," she said.