

ZDNet

David Berlind's Reality Check



Is that a biometric device in your pocket?

By [David Berlind](#)

May 20, 2003

With cyber-terrorism such a hot topic these days, a lot of IT managers are looking into strengthening the security of their networks and applications by adding the oft-hailed third factor.

The first factor of security is what you know (i.e.: usernames or pin codes), the second factor is what you have (e.g.: an ATM card), and the third factor most often relies on biometrics to determine who you are.

Three-factor security is widely considered to be an important step for most if not all IT shops to take sooner or later. For many shops, the biggest challenge will be to determine which of the various biometric platforms can be easily and cost effectively deployed to everyone. After stumbling upon Strikeforce Technologies, I may have the answer for you.

Strikeforce asks a simple question. Instead of setting your budget back by buying dedicated biometric devices or computers with biometrics built-in, why not use a biometric device that virtually everyone already has--the telephone? It could be any phone-- the one on a user's desk, or the one in their pocket. That's right: Strikeforce CEO George Waller suggests that you use one of the most widely deployed platforms in the world to attain three-factor security. Furthermore, Waller claims that Strikeforce's out-of-band methodology for authentication adds a layer of security to any two- or three-factor system. "We actually make RSA security more secure than it is now," says Waller.

Waller and Strikeforce CTO Ram Pemmaraju, inventor of the company's Centralized Out-of-Band Authentication Server (COBAS), trace the origins of the company's methodology to the phone phreaking days of the '70s.

"Back in those days," says Pemmaraju, "phone phreaks had no trouble hacking into the telephone network because the voice and phone signaling were being carried in the same band. The minute AT&T switched to out-of-band signaling, where the signals are carried on a separate band than the voice, that type of hacking stopped overnight."

"In the same way that AT&T split the voice and the signaling, we went out-of-band on the authentication and essentially split the logical and physical pathway for supplying username and authentication" says Waller.

Nothing can describe the elegance of Strikeforce's solution as well as the demonstration I received from Verizon representatives at RIM's recent Wireless Enterprise Symposium. Verizon and Strikeforce are contemplating a deal that would make Strikeforce's Technology available to Verizon's customers.

The way it works is simple. Imagine many of the login screens you see today for Web-based applications, virtual

private networks (VPNs), or network logons (e.g.: a Windows domain). Instead being asked for your username and password, you only get to supply your username. Within a couple of seconds of supplying a username, your telephone rings. If the two-factor (what you know and what you have) version of COBAS is deployed, you're asked to use the telephone to key in your password. (The password is what you know. The phone, like the ATM card, is what you have.) In the same way that your bank account is only accessible with specific ATM cards, this form of authentication only works on one phone---the phone that COBAS is programmed to call for you. For the three-factor version that guarantees who you are, you must speak into the phone so the system can perform a biometric-based voice authentication.

Once you authenticate yourself via the telephone--with a password, your voice, or both-- the original application that asked for your username springs to life as though you had just entered your password with the keyboard or authenticated with local biometrics. The reason this is called out-of-band authentication is that the authentication data --- whether it was your password or your biometric information --- takes a different network path (or band) to the authentication server than does the username. The username goes over the Internet or a local area network, while the authentication data passes over the public telephone system. Waller claims that this sort of out-of-band authentication is much more secure than other forms where both the username and authentication data are essentially packaged together and travel across the same network.

Are telephones required? Not necessarily. Strikeforce has a proprietary instant messaging agent that's installed on the client device and that serves as the client side of a secondary band for carrying authentication data of any type. This agent can work with something as simple as a password, or with one of RSA's technologies, a Smart Card, a USB-based token, or a local biometric device of your choosing.

Authentication data is transmitted to your authentication server via the instant messaging mechanism, which serves as the "band" that's separate from the one carrying the username. According to Waller, the company is working on using Yahoo! Instant Messenger, AOL Instant Messenger, and MSN Messenger as alternative bands to Strikeforce's proprietary technology.

Another scenario where Strikeforce's out-of-band authentication comes in handy, according to Waller, is workflow situations in which approvals have to be escalated up the chain of authority.

"Picture a situation," says Waller, "where a bank employee has the privileges to authorize wire transfers up to \$25,000. When a request to wire more than that comes in, COBAS first does an out-of-band authorization with the bank employee, and then when the application sees that the wire threshold has been exceeded, it automatically does another out-of-band authorization with the person that has the privileges to authorize the requested amount."

This interception of business logic is evidence of the Switzerland-like role that Strikeforce is trying to play. COBAS can be used to intercept the authentication process for Windows domains, Web-based applications, RADIUS (AAA) servers, Citrix servers, Web services processes, and an agent for Solaris is under development. Also under development is an e-commerce solution: COBAS intercepts the credit card authorization process so that an out-of-band authentication is required before a credit card transaction will be processed. This could be especially useful for Web transactions.

Perhaps what's best about the solution is its cost. For the first 24 users, a COBAS server costs about \$2,700. The cost ranges from \$100 to \$125 per additional user, depending on the total number of users, and there is an additional per user fee depending on the types of authentication. PIN-based (two-factor) authentication is \$40 per

user and voice biometric (three factor) is \$60 per user. The company isn't offering a hosted model, where it makes the infrastructure available through an API or Web services interface, but Waller says he can envision a carrier getting into that business.