



IMMEDIATE RELEASE

New Weapon in Cyber-Security Has Roots in 70's Phone Phreaking

Cap'n Crunch Giveaway Leads to Second Revolution in Security

Edison , New Jersey – October 6, 2003 – As IT managers struggle to sure up and integrate security of their networks and applications, one company is offering a new security platform that traces its origins to the successful model the phone company used to stop hacking in the 1970s. In the same way that AT&T split the pathways that carried its voice and signaling data to stop phone phreaking 30 years ago, the new model takes the authentication step of security out-of-band -- splitting the physical pathways that carry usernames and authentication data.

The proprietary out-of-band methodology, known as C.O.B.A.S. (Centralized Out-of-Band Authentication Solution) was developed by StrikeForce Technology. It is recognized as the world's only universal authentication platform to solve the underlying fatal flaw of computer security – packaged credentials.

Phreaking – The Original Hacking

According to hacking lore, in 1971 a Vietnam vet named John Draper discovered that the giveaway whistle in Cap'n Crunch cereal boxes perfectly reproduced a 2600 Hertz tone that, when blown into the receiver, would trigger a free call from AT&T. His published underground newsletters started a nation-wide hacking movement called Phreaking. When AT&T switched to out-of-band signaling, where the signals are carried on a separate band than the voice, the phone hacking was eliminated overnight.

In the COBAS model, a user's credentials (password, biometrics or layered combination) are routed over a private one-way outbound server, away from the client network and out of reach from hackers or intruders. Out-of-band authentication has proven to be exponentially more secure than other forms of security, where both the username and authentication data are packaged together and travel across the same network.

“COBAS represents the second revolution in security in a complex and fragmented industry,” said George Waller, Vice President of Sales for StrikeForce. “Usernames and passwords have been traveling on the same vulnerable pathways since IBM programmers first started using computer passwords in the 1950s. COBAS not only changes the game for hackers, it gives IT managers a flexible and robust solution that achieves higher levels of security at 25 % to 50% of the cost, said Waller.”



StrikeForce Page 2.

COBAS – How it Works

To understand how COBAS works, one must understand the fundamental fatal flaw in existing computer security -- the inextricable pairing of usernames with credentials sent over vulnerable networked pathways. Regardless of the password scheme or device, tying a username to authentication acceptance makes hacking possible. Once a hacker has one piece of the security equation, it is only a matter of time before he gets the other.

COBAS creates a separate pathway for authenticating a user's credentials using existing platforms that nearly everyone already has access to -- phones or instant messaging. Its distinction is obvious at login. Instead of being asked for a username and password, a user is only asked to supply a username. Within two seconds of supplying a username, the user's telephone rings (a single cell or desk phone programmed to be called for that user). For two-factor authentication (what you know and what you have), the user is asked to enter a password on the phone keys. (The password is what you know. The phone is what you have.) For the three-factor authentication, that guarantees a user's identity, a biometric-based voice authentication can be performed over the same phone.

Once the authentication is complete, the original application that asked for the username springs to life as though the user had just entered a password with the keyboard or authenticated with local biometrics.

Is that a biometric in your pocket?

Instant messaging devices can replace phones to perform a similar two-factor authentication. The company's proprietary instant messaging agent, installed on the client device, 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 a finger print reader, a Smart Card, a USB-based token, or any number of local biometric devices for two-factor, three-factor -- or unlimited-factor authentication.

The Switzerland of Security

The company's out-of-network model easily integrates with all current and emerging authentication products -- biometrics, tokens and Smart Cards -- and tied with a password, is the only single product to achieve tri-factor authentication. Its out-of-band model adds a critical measure of security to all platforms -- extending functionality and eliminating the need for costly middleware.

Its "clientless" status gives it an immediate ability to layer all biometric devices over any combination of operating systems including, Microsoft, Linux, SUN, Unix, Novell or Mainframe. By partnering with best-of-breed service providers and manufacturers, the company's COBAS model is fast becoming the recognized standard authentication platform for today's smart networks, access scenarios and enterprises.



StrikeForce – Page 3.

Synchronized Secure Approval Chains

COBAS can also be applied to workflow or process authentication situations in which approvals have to be escalated up the chain of authority.

For example, when a bank employee with the privileges to authorize wire transfers up to \$25,000 needs to exceed that threshold amount, COBAS automatically does another out-of-band authentication with a second user to authorize the requested amount."

About StrikeForce Technologies

StrikeForce Technologies is an identity solutions firm that has developed a revolutionary new security platform providing unprecedented levels of security, interoperability, and usability -- in seamless cost-effective designs.

The company's award-winning distinction is a patent-pending technology, called COBAS, for (Centralized Out-of-Band Authentication Solution). COBAS creates a separate "out-of-band" pathway for authenticating a user's credentials, away from the client network and out of reach from hackers. The open, out-of-band server allows easy integration and layering with today's security devices (tokens, Smart Cards and biometrics) – and tied with a password, is the only product to achieve tri-factor authentication.

Headquartered in Edison, NJ, the company was established through the merger of two companies in December 2002. Predecessor companies were Netlabs.com, formed in May 1999 and Strike Force Technical Services, Inc. (SFT), formed in August 2001.

Partnering with best-of-breed service providers and manufacturers, the company's COBAS model is fast becoming the recognized standard authentication platform for today's smart networks, access scenarios and enterprises.