



The Fundamental Shortcoming in Current Cybersecurity

The fundamental shortcoming of cybersecurity is the fact that *a secure link is missing between the authentication of a valid user, and the authorization of an action.* The authorization of an action could be the execution of a financial transaction from Bob's bank account, a stock trade in Mary's brokerage account or access to important data on a private network such as SIPRnet (e.g. WikiLeaks). The authorization of an action typically occurs through the web browser since the browser presents a convenient interface for a person, but here is where this important connection between authentication of a user, and authorization of an action is broken.

On current systems the user authenticates on the host domain machine (e.g. mobile phone, laptop or PC). Then the same host domain machine also authorizes (and may also execute) the action. Since the host domain machine can be hacked, the lack of a secure and direct link between these two events breaches the security of user authorization.

Part of this shortcoming occurs because biometric authentication is typically and naively represented as an on/off switch – if in fact the system even relies on biometric authentication. In the same way, if this on/off implementation occurs in an untrusted computing environment, then outstanding biometric algorithms and sensor(s) become irrelevant because the biometric authentication can be circumvented between the user authentication and the authorization or confidentiality part of the security system.

The use of biometrics is, however, critical for proper security because it is the best way to know who is actually initiating a transaction. We further emphasize that *even with the use of biometrics, if the handling of the biometric information, storage of the biometric data, or control of actions based on a biometric verification is done on an unsecured host, the value of the biometrics is greatly reduced or nullified.* Biogy's secure module design and implementation securely binds biometric authentication to authorization of an

action, all within the secure module. As a consequence, the Biogy secure module solution addresses this common biometric authentication weakness.

An additional aspect of this weakness is that the action can be hijacked – for example, by executing a Trojan attack on the host machine. In other words, *a valid, authorized user cannot be certain that the action he or she is trying to execute is what is actually being done*. A concrete example of this weakness is the *untrusted browser attack* used to steal money from a person’s bank account: Mary’s web browser is telling her that she is about to send \$500 to Bob’s account, but in reality her untrusted browser will send \$50,000 to another account.

Since the web browser is executed on the host domain computer, the browser cannot be trusted even when using PKI and one-time passcodes! A recent *untrusted browser attack* on the gold standard of security, RSA SecurID, demonstrates this surprising fact. The consequences of this particular cyberattack were that \$447,000 was stolen from a company bank account in a matter of minutes, even though the valid user was using one-time passcodes to make the transaction more secure. The details of this cyberattack are shown below in a recent MIT Technology Review article.

<http://www.technologyreview.com/computing/23488/?a=f>



The screenshot shows the top portion of a web article. At the top left is the 'Technology Review' logo, with 'PUBLISHED BY MIT' in smaller text. To the right is a small image of a person wearing glasses. Below the logo is a navigation bar with links: HOME | VIDEOS | BLOGS | COMMUNITY | MAGAZINE | MIT NEWS | NEWSLETTERS | EVENTS | RESOURCES. The main navigation bar is dark with white text: Computing | Web | Communications | Energy | Materials | Biomedicine | Business. The article title is 'Real-Time Hackers Foil Two-Factor Security' in a large, bold font. Below the title is the subtitle 'One-time passwords are vulnerable to new hacking techniques.' and the author 'By Robert Lemos'. The date is 'FRIDAY, SEPTEMBER 18, 2009'. There are social media sharing icons for E-mail, Audio, Print, Favorite, and Share. The main text begins with 'In mid-July, an account manager at Ferma, a construction firm in Mountain View, CA, logged in to the company's bank account to pay bills, using a one-time password to make the transactions more secure.' Below this is a small image of a computer monitor displaying a security interface. To the right of the image is a text block: 'Yet the manager's computer had a hitchhiker. A forensic analysis performed later would reveal that an earlier visit to another website had allowed a malicious program to invade his computer. While the manager issued legitimate payments, the program initiated 27 transactions to various bank accounts, siphoning off \$447,000 in a matter of minutes. "They not only got into my system here, they were able to ascertain how much they could draw, so they drew the limit," says