



Two-Factor Authentication: Too Little, Too Late

Two-factor authentication isn't our savior. It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had 10 years ago, not the security problems we have today.

The problem with passwords is that it is too easy to lose control of them. People give their passwords to other people. People write them down, and other people read them. People send them in email, and that email is intercepted. People use them to log into remote servers, and their communications are eavesdropped on. Passwords are also easy to guess. And once any of that happens, the password no longer works as an authentication token because you can never be sure who is typing in that password.

Two-factor authentication mitigates this problem. If your password includes a number that changes every minute, or a unique reply to a random challenge, then it's difficult for someone else to intercept. You can't write down the ever-changing part. An intercepted password won't be usable the next time it's needed. And a two-factor password is more difficult to guess. Sure, someone can always give his password and token to his secretary, but no solution is foolproof.

These tokens have been around for at least two decades, but it's only recently that they have received mass-market attention. AOL is rolling them out. Some banks are issuing them to customers, and even more are talking about doing it. It seems that corporations are finally recognizing the fact that passwords don't provide adequate security, and are hoping that two-factor authentication will fix their problems.

Unfortunately, the nature of attacks has changed over those two decades. Back then, the threats were all passive: eavesdropping and offline password guessing. Today, the threats are more active: phishing and Trojan horses. Two two new active attacks we're starting to see include:

Man-in-the-Middle Attack. An attacker puts up fake bank Web site and entices a user to that Web site. The user types in his password, and the attacker in turn uses it to access the bank's real Web site. Done correctly, the user will never realize that he isn't at the bank's Web site. Then the attacker either disconnects

the user and makes any fraudulent transactions he wants, or passes along the user's banking transactions while making his own transactions at the same time.

Trojan Attack. An attacker gets the Trojan installed on a user's computer. When the user logs into his bank's Web site, the attacker piggybacks on that session via the Trojan to make any fraudulent transaction he wants.

See how two-factor authentication doesn't solve anything? In the first case, the attacker can pass the ever-changing part of the password to the bank along with the never-changing part. And in the second case, the attacker is relying on the user to log in.

The real threat is fraud due to impersonation, and the tactics of impersonation will change in response to the defenses. Two-factor authentication will force criminals to modify their tactics, that's all.

Recently, I've seen examples of two-factor authentication using two different communications paths: call it "two-channel authentication." One bank sends a challenge to the user's cell phone via SMS and expects a reply via SMS. If you assume that all the bank's customers have cell phones, then this results in a two-factor authentication process without extra hardware. And even better, the second authentication piece goes over a different communications channel than the first; eavesdropping is *much* more difficult.

But in this new world of active attacks, no one cares. An attacker using a man-in-the-middle attack is happy to have the user deal with the SMS portion of the log-in, since he can't do it himself. And a Trojan attacker doesn't care, because he's relying on the user to log in anyway.

Two-factor authentication is not useless. It works for local log-in, and it works within some corporate networks. But it won't work for remote authentication over the Internet. I predict that banks and other financial institutions will spend millions of dollars outfitting their users with two-factor authentication tokens. Early adopters of this technology may very well experience a significant drop in fraud for a while as attackers move to easier targets, but in the end there will be a negligible drop in the amount of fraud and identity theft. ■

BRUCE SCHNEIER is the CTO of Counterpane Internet Security, Inc., and the author of *Beyond Fear: Thinking Sensibly in an Uncertain World*. More of his security writings are available at www.schneier.com.

