Security
April 24, 2009 12:15 AM PDT

Device identification in online banking is privacy threat, expert says

by Elinor Mills

SAN FRANCISCO--A widely used technology to authenticate users when they log in for online banking may help reduce fraud, but it does so at the expense of consumer privacy, a civil liberties attorney said during a panel at the RSA security conference on Thursday.

When logging into bank Web sites, users are typically asked for their user name and password. But that's not all that is happening. Behind the scenes, the server is taking measures to identify the device being used in an attempt to verify that the person logging in is the person whose account is being accessed under the assumption that most people use the same computer for banking.

Wachovia, which recently merged with Wells Fargo, tags the consumer's computer with a unique identifier, said Chris Mathes, an information technology specialist in online customer protection at the bank.

The technology not only can be used to allow legitimate customers into Web sites, but also to block computers that have been targeted as "bad actors," said Todd Inskeep, a senior vice president for the Center for the Future of Banking at Bank of America.

Another device fingerprinting technology provided by **41st Parameter** is similar but doesn't tag the computer. Instead, the technology figures out the degree of probability that the computer accessing the site is the one that should be accessing it by querying the computer for things like time zone, language, browser type, Flash ID, cookie ID and IP address, said Ori Eisen, founder of the company. If enough of the answers match, the account can be accessed.

The 41st Parameter technology is being used by 120 large e-commerce companies, including the top five banks in the U.S., USAirways and Continental Airline, Eisen said in an interview.

Even though none of the information gathered during a log-in is personally identifiable, the bank shouldn't have to collect regular data on when, how often and from where a consumer accesses a bank account, said Jennifer Granick of the **Electronic Frontier Foundation**. Such information can be compiled with other more sensitive information to create profiles and cross referenced to learn more about consumers, she said.

For instance, the bank could learn who a consumer's roommate is if the same computer is used regularly to access different accounts, Granick said. Consumers also could be deemed suspicious for breaking with their patterns on deposits or withdrawals or the information could be sold to advertisers, she added.

"There is very little privacy protection in the U.S. for this type of information," Granick said. "We don't want it shared with affiliates that do advertising." There should be restrictions on how long the bank will keep the data, who it can share it with and for what purposes, she added.

Eisen said his technique was more "privacy friendly" because it doesn't assign identification numbers to devices. The questions posed to computers by his technology are akin to what WebTrends and Google Analytics find out from computers for Web analytics purposes, he said.

Granick wasn't convinced, noting that even without a unique device identifier, the bank is still able to monitor consumer transactional patterns.

Right as the session was ending, Louie Gasparini jumped from his seat in the audience to make a comment at a microphone set up for the question-and-answer session.

"The privacy issue is encumbering banks," who have a fiduciary obligation to prevent fraud, said Gasparini, who said he used to work in Internet banking at Wells Fargo and helped create Device ID at RSA, the security division of EMC.

Another attendee had a different perspective.

"The concerns are not overstated. There are fundamental deficiencies in privacy law," said Andrea Matwyshyn, assistant professor of legal studies and business ethics at the University of Pennsylvania's Wharton School. "If an end user license agreement contractually reserves the right of a company to collect data for fraud prevention purposes and if this data is then sold as a secondary revenue stream, a privacy concern would clearly exist."

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Privacy & data protection**

Tags: **RSA 2009**, **online banking**, **device identification**, **fingerprinting**, **EFF**, **41st Parameter**

Related

From CNET

Microsoft unleashes another 'laptop hunter' ad

U.S. offers peek at proposed copyright treaty

Taking your health records online

From around the web

Let The Bonus Stalking Begin

Gadgetwise: Mac Security III: The Rise o... The New York Times