Challenge/Response
Security & privacy for e-commerce

955 Massachusetts Ave, Suite 130, Cambridge, MA 02139
+1 617 606 5990 • fax: +1 617 848 0626

FOR IMMEDIATE RELEASE
OCTOBER 30, 2007 12:30EDT

First live SiteKey exploit seen in operation

An active exploit of the SiteKey security system used by Bank of America and other financial institutions, employing the man-in-the-middle attack described by Challenge/Response Labs in our white papers of July 2006 and in subsequent work by other researchers, has been observed in a live phishing attack. We believe this is the first time a live, man-in-the-middle attack against SiteKey has been seen in the wild.

The fraudulent site displays valid SiteKey images and text phrases to potential fraud victims. It apparently became active in the early morning of Oct. 30, 2007 (EDT) and was still active at 12:30 EDT Oct. 30, 2007.

We have tested the fraudulent site using the credentials for both a non-existent and an actual account. The site successfully retrieved and displayed a correct SiteKey image for the valid account when given the correct answer to one security question. It also successfully detected and recovered from the error sent back from Bank of America's servers when we used a nonexistent account ID.

The attack appears to use PHP scripts to relay a victim's login credentials to the attacking site, and to relay a victim's SiteKey image and phrase from Bank of America's servers back to the victim.

Firefox's built-in "Tell me if the site I'm using is a suspected forgery" feature, using a downloaded list of suspected sites, does correctly flag the fraudulent site, and warns the user away.

Why today's development is significant:

• Now that the supporting software ("scripts") has been written and debugged, the code can be expected to circulate to other attackers, so that even those lacking the skill to devise this type of attack on their own can create fake banking sites that interact fully with SiteKey.

• Customers of all financial institutions that use SiteKey-style security are vulnerable to this class of attack.

• Nothing more can be done to "fix" SiteKey to stop the attack, compared to what can be done about any phishing exploit (that is, banks must contact ISPs and server operators to attempt to shut the servers down).

• A potential risk we noted in July 2006, and subsequently studied in depth by other researchers, is now an actual risk. Bank of America's statement that "If you recognize your SiteKey image, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey image is also how you'll know that it's safe to enter your Passcode." may create a false sense of security, increasing the likelihood that a customer could be persuaded to enter his or her password into a fraudulent web site, when that fraudulent site shows their SiteKey image and phrase - exactly as occurs in this attack.

• Because the exploit was launched through a compromised BlogSpot blog page, it was propagated by Google Alerts and potentially by RSS feeds, and may have circulated widely without requiring a mass e-mailing.

NOTES AND CONTACT INFORMATION

Challenge/Response LLC is a Cambridge, MA provider of collaborative, p2p security and e-commerce technologies that bring together the online and offline worlds.

Contact: Jim Youll, jim@cr-labs.com

(continued on next page)

The 2006 Challenge/Response Labs publications, "Fraud Vulnerabilities in SiteKey Security at Bank of America" and "Why SiteKey Can't Save You", as well as this report, are available at: http://cr-labs.com/publications/

The NIST Vulnerability Summary for this issue is CVE-2006-7201, available at http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-7201

See also: The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies, by Stuart Schechter, Rachna Dhamija, and Andy Ozment, available at: http://usablesecurity.org/emperor/

The exploit was observed and recorded by Challenge/Response, LLC on Oct. 30, 2007, 0908 to 1012 EDT.