# Why SiteKey Can't Save You

Jim Youll <jim@cr-labs.com>
CTO, Challenge/Response, LLC
Cambridge, MA

This version: August 24, 2006

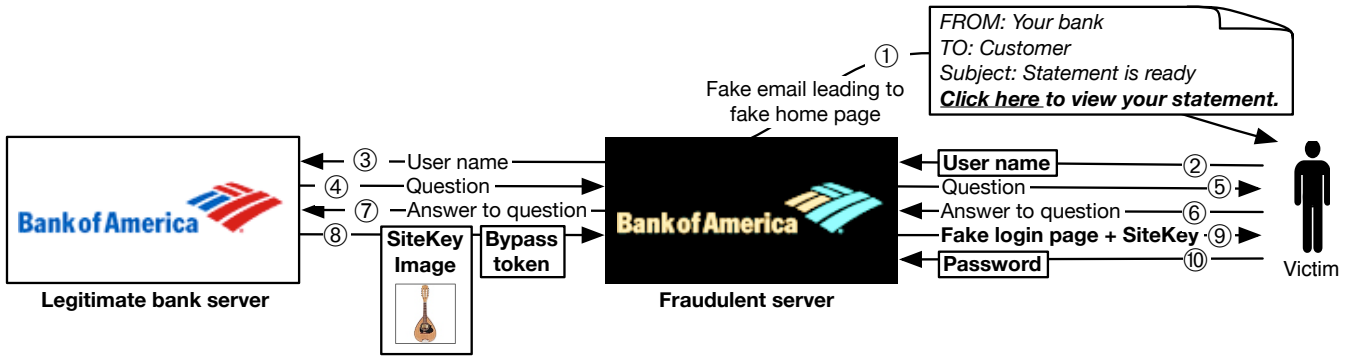
*This overview of "Fraud Vulnerabilities in SiteKey Security at Bank of America" is written for a non-technical audience. Some details have been greatly simplified, and some new material is presented. Readers seeking more depth of coverage should consult the original paper, available at http://cr-labs.com/publications/.*

Although this report discusses SiteKey℠ at Bank of America Corporation, the general risks discussed here apply to all SiteKey sites including ING Direct and Vanguard.com, and they apply even more generally to any security method that relies solely on server-side interventions to detect and stop online fraud.

## The product and the problem


SiteKey shows web banking customers a "secret image" – a little icon of a mandolin or a coffee mug or something else – that only the customer and the bank are supposed to know. Customers of SiteKey-using banks are told that if their correct secret image appears on a purported bank web page, they can be sure that they are connected to the bank's real web site, and can safely enter passwords and other secrets. Nobody could guess a person's secret icon chosen from a pool of hundreds of images, right?

Bad guys – unless they're psychic – definitely cannot guess secret pictures with the accuracy needed to pull off phishing frauds. Unfortunately, the design of SiteKey means they don't have to guess. Rather than guessing, a scammer can carry out a "man in the middle" attack in which an innocent person's true SiteKey image is retrieved directly from the bank's own servers, then displayed to the victim on a fake web site. Criminals who can write simple server software, or who hire someone to write such software, can create fake bank web sites that look just like the real thing, and that display correct, "secret" SiteKey images to unsuspecting victims.




*Defeating SiteKey in a ten step man-in-the-middle attack: in the end, the fraudulent server has the victim's user name, password, question-bypassing token and SiteKey image, allowing unlimited access to the account.*

## What this means for online banking customers

Even if you see your personal, "secret" SiteKey image on a web page, the page may not be legitimate. When entering your password or answering a security question, picture or not, you could be giving away secrets to an overseas crime ring, rather than logging on to a bank account.

Some SiteKey installations strongly promote the safety of SiteKey. For example, Bank of America tells customers:

> *"If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the Sign In button."*

But that statement is not true all the time. It's true most of the time, because most of the time a bank's customers are not looking at fraudulent web pages. But "most of the time" is of little use when trying to detect the one instance out of a thousand when it really is a bad guy, and not the bank, at the other end of the connection. SiteKey can't always do that, and the process of creating a fake SiteKey page is fairly trivial.

Some people may be worse off with SiteKey than without it. Marketing language like "...if you recognize your SiteKey... you'll know that it's safe to enter your Passcode" could unintentionally help criminals by persuading security-conscious customers that the presence of the SiteKey image is absolute proof of the safety of a web page.

An additional problem is that the things SiteKey protects – user names and passwords – aren't very good security devices. In particular, they can be reused by a bad guy in a "replay attack," which means simply that once stolen, they can be used over and over to access a victim's account.

Although some security systems resist replay attacks, few online services offer replay-protected authentication, so this vulnerability isn't special. But Bank of America says SiteKey does guard against replays by requiring customers to save and answer personal "challenge questions" such as "What was the name of your first pet?"

This sounds fairly safe: a bad guy holding someone's user name and password is not likely to guess the name of the victim's first pet before the system locks him out for making too many incorrect guesses.

But a bad guy who has stolen a user name and password using a real SiteKey image – via the method described in the full paper – doesn't have to answer challenge questions. When an attacker fools a victim into making a single login to his or her account though a fake site, SiteKey issues a "bypass token" – a code that turns off challenge questions altogether. The token can be copied and shared among many computers.

Thus, by tricking a victim just once, an attacker picks up a victim's user name, password, SiteKey image and bypass token, granting unlimited access to the victim's account even though the attacker cannot answer the remaining challenge questions that should still guard it. Challenge questions provide little added protection against future access to an online account, and are compromised right along with the user name and password during man-in-the-middle attacks.

### Limitations of single-ended security

Security methods that try to protect everyone from the server's end of a connection are popular right now. Customers don't have to be involved, and it is presumed, wrongly in my view, that they cannot or will not participate in their own protection beyond looking at pictures in web browsers. SiteKey *appears* to involve both ends of the connection, but as explained here, when a SiteKey image is sent blindly toward an apparently customer-controlled computer, there is no assurance that the image has reached an actual customer, or that it has done so so free of "man in the middle" tampering.

Server-side security does stop some attacks, and makes others difficult. But the approach has gaps that cannot be filled by adding more server-side security. Security is a *process* issue more than a technology issue. Fixing half a process is a bad idea generally, and it's a terrible approach to high-stakes security.

Just as a landline phone call doesn't travel over a private wire between two phones, there are no direct connections on the Internet. A web page sent from your bank's web server to your browser is turned into "packets" that pass through many unrelated points along the way. A bank can't lock down the path those packets travel between itself and you, because it doesn't control the whole path from end to end. And some indirection in online communications is perfectly normal, so it can be difficult or impossible to tease out rare cases of malicious indirection.

A bank's web server also cannot control exactly what's displayed on your computer screen. Web browsers are not televisions that show exactly what was sent: they *interpret* web pages and display them a bit differently on every computer. Something could be changed en route – such as when an attacker drops a real SiteKey image onto a fake web page – and the bank probably will not know anything about it.

If a victim is led far astray – say, to a fake web page that does not involve a bank's servers at all – the bank cannot detect or interrupt the fraud. SiteKey helps with this scenario, by forcing fraudsters to retrieve a victim's SiteKey image from their bank's real servers. If too many inquiries were to come to those servers from one place, alarms could be raised. However, such monitoring can be foiled with "bot nets" – clusters of thousands of Internet-connected home and office computers that have been taken over by criminals without their owners' knowledge. Fraud-related connections made through such bot nets would not come constantly from one busy server, but would arrive a few at a time from many different computers, interfering with this sort of detection.

Customers of SiteKey-protected banks are also apparently still falling victim to frauds that don't even attempt to show SiteKey images. Customers need more basic assistance in detecting those occasions when a bank's servers are completely uninvolved in a fraud.

### What can customers do to be safe? Can anything more be done by banks?

Keep in mind that a bank using SiteKey is no less secure than any other online bank – it's just not appreciably *more* secure than the others. Never let your guard down just because you see your correct, personal SiteKey image.

The best tactic is to observe the same safety tips that apply to all other e-commerce:
• Never click links in e-mail messages
• Always type the URL of your bank's home page into the browser, or save the bank's login page as a bookmark
• Remember that banks and e-commerce vendors don't send alarmist "your account will be closed" messages
• The Federal Trade Commission offers more tips at: http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

Although the connection between a bank and its customers cannot be made completely safe with security that's added only at the bank's end, this does not mean that frauds cannot be stopped. If fraud-stopping processes are engineered properly, frauds can not only be detected, but could made a virtual non-issue in everyday e-commerce.

Challenge/Response and other companies are working on end-to-end security methods that make e-commerce sites and their customers partners in safe online commerce. Customers should encourage their banks and other online trading partners to let them take an active role in their personal protection by using tools like these.

### Making SiteKey less risky

A few changes could make SiteKey installations less risky for customers. Among our suggestions are these:

1. Financial institutions must never claim that a security system will provide absolute security. Customers need and deserve frank information about risks in the security provided by the companies they do business with.

2. Customers should be given more control over the "bypass tokens" that disable challenge questions. For example, a customer should be able to tell SiteKey to invalidate all the tokens ever issued for his or her account. Then no computer would be able to access that customer's account without a fresh, complete theft of the customer's secrets.

3. The Federal Trade Commission recommends that banks use SSL for all web pages. SSL encrypts the data between a bank and a customer, and activates the "lock" icon in browsers. SSL *does not* prove that a web page is legitimate. However, fraudsters move their fake sites constantly as their servers are discovered and taken offline, and SSL servers are difficult to move around. For that reason, most online frauds do not use SSL and probably will not use it in the future. A missing lock symbol on a page that *should* be secure would definitely signal trouble if banks always used SSL. But despite the FTC's guidance, most banks still don't use SSL for all their web pages, so the presence or absence of the lock symbol does not help customers discover frauds by this simple method.

4. Banks may have to stop e-mailing their customers with messages that include links back to the banks' web pages. Fake e-mails outnumber real ones by a big margin, and it is hard to tell a real e-mail message from a fake.

### Notes

• SiteKey began as a product of Menlo Park, California-based PassMark Security. Passmark Security was acquired by RSA Security in April, 2006. As of July 2006, RSA was in the process of acquisition by EMC, Inc.

• The information needed to understand SiteKey or to perpetrate frauds against its users can be acquired with little more than a web browser and an HTTP or TCP monitor such as tcpdump, or from the traffic logs of a web proxy such as Squid. No privileged access to servers or other devices is needed.

### About the author

Jim Youll is CTO of Challenge/Response, LLC, a Cambridge, MA startup creating security tools for fraud prevention, online security and new forms of electronic commerce. He holds a B.S. in Computer Science from Bowling Green (Ohio) State University, and an S.M. from MIT, where he was a research assistant studying e-commerce, distributed market systems, location technologies and wireless. He is also founder of the non-profit Voting Transparency Project, and a fellow of the Stanford Center for Internet and Society.

### Acknowledgments

Thanks to the reviewers for their efforts in fact checking, reading drafts, and suggesting improvements, and to the Stanford Center for Internet and Society.

## Abstract

This overview of "Fraud Vulnerabilities in SiteKey Security at Bank of America" is written for a non-technical audience. Some details have been simplified, and some new material is presented.

SiteKey shows web banking customers a "secret image" – a little icon of a mandolin or a coffee mug or something else – that only the customer and the bank are supposed to know. Customers of SiteKey-using banks are told that if their correct secret image appears on a purported bank web page, they can be sure that they are connected to the bank's real web site, and can safely enter passwords and other secrets.

However, criminals who can write simple server software, or who hire someone to write such software, can create fake bank web sites that look just like the real thing, and that display correct, "secret" SiteKey images to unsuspecting victims.

If you are an online banking customer, this means that even if you see your personal SiteKey image on a web page, the page may not be legitimate. When entering your password or answering a security question, picture or not, you could be giving away secrets to an overseas crime ring, rather than logging on to a bank account. A bank using SiteKey is no less secure than any other online bank – it's just not appreciably *more* secure than the others. Never let your guard down just because you see your correct, personal SiteKey image.

## Location

This document and other publications are available from Challenge/Response, LLC Labs at http://cr-labs.com/publications/.