

# **Solving Online Security Problems for E-Commerce by SiteKey**

Hongwei Du<sup>\*</sup>

*Along with the popularity of E-Commerce increasing the online security concerns grow as well. Online crimes such as phishing target more and more customers compromising brands, undermining customer trust in institutions. Online banking is especially affected, and banks are under constant pressure from customers, government, and whole society to take adequate measures to defend client from online criminals. This paper focus on how Bank of America, one of leading brands in the bank industry, try to enhance security by implementing SiteKey technology. By considering pros and cons of the SiteKey implementation, the paper tries to look through several possibilities to enhance security protection. It is important to consider SiteKey as a part of layered security system because neither of components alone is able to prevent phishing or other online frauds. Only collaborative effort on each level, client, server, and enterprise make the online system adequately protected.*

**Field of Research:** Online Security, E-Commerce, SiteKey

## **1. Introduction**

It is hard to deal with frustration about spending all day going from one store to another trying to buy the item that fits one's needs and expectations. It is very tempting to forget about mailing payments by traditional check-envelop-mailbox way. Emerging E-Commerce exactly answered the needs of millions of customers. A lot of businesses now take the E-commerce form. Many traditionally brick and mortar businesses are now using Internet for advertising, order placement, deliveries, transactions, tracking, and customer service. E-commerce represents completely different business model, where there is much less need to have physical facility spread all over the place to grow. Retailers, financial institutions, government agencies, and other industrial sectors found online communication to be quick, less expensive, flexible, and convenient way to deliver products or services to customers. More and more people find it much more convenient to shop, study, and manage accounts online. However, convenience has its cost. Not always online business can guarantee absolutely safe online communication.

Unfortunately, often the temptation to try online service ends up with the new frustration. Online communication is not safe. The numerous online crimes are a huge restricting factor not allowing e-commerce becomes the prevailing business model. For example, one of the big concerns for E-banking is Phishing. Phishing

---

<sup>\*</sup>Hongwei Du, Department of Management, College of Business and Economics, California State University, East Bay, Email: Hongwei.du@csueastbay.edu

## Du

frauds compromise online banking in several ways. Both clients and banks are losing money due to unauthorized transactions. Customers are losing trust in online banking.

Online threats, competition, and government regulations make safety a top priority for business planning. Security is also one of the most costly components of successful e-business. Constant E-commerce security development allows company to remain on competitive edge and adequately respond to development of malicious technologies victimizing e-business and online consumers.

Bank of America and its online banking system are known as security award winning leader in the industry. SiteKey is one of the really interesting solutions implemented by bank's security team. The pioneering effort of the company attracted increased attention of IT security specialists, researchers scrutinizing new technology. They point on positive and negative aspects of SiteKey. Main questions are whether SiteKey solution was feasible, what are the main flaws of the system, and what additional security measures needs to be considered.

To be effective, online security should be considered as a multi layered system. E-Commerce digest website considers following four principles as a necessary components of such system as privacy, integrity, authentication, and non-repudiation (Ecommerce Security Issues, 2009). Build for E-Commerce systems should take care about clients' privacy. No customer would want to buy product or service online, if he/she is not guaranteed that the personal information is reasonably secure. Secondly, such system needs to be designed with consideration of possibilities of unauthorized external code or data modifications. For example SQL injections could modify transaction information so that allowing future illegal activity. Next, it is very important to include the elaborate authentication mechanism, so that not only company could identify a legitimate client, but also a client could verify that he/she is communicating with the real, not fake, server. For example, guidance for online banking specifically highlights the bank's responsibility to have reliable authentication in place. Finally, non-repudiation has to deal with client or company refusing admits transaction made. In such cases online systems need to consider functionality, which would verify the delivery of the message to the recipient. For example, in the case of transferring funds in amount exceeding some limit, bank can call or message the client.

SiteKey and similar solutions work well as a segment in the bigger system. They are helpful for preventing phishing frauds as long as the company does not neglect taking other security measures, as long as customers are aware of the treat and are adequately educated.

## 2. Phishing Frauds

### *What are Phishing Frauds*

Phishing takes name from "fishing" and "phreaking" - term used by earlier hackers. Like fisherman mislead fish to swallow the hook, attacker tries to lure user to disclose confidential information, which could be used for fraudulent activity. Anti-Phishing Work Group organization in the Q2 2008 Report defines phishing as "a

## Du

criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials"(Phishing Activity Trends Report, 2008).

Phishing attacks employing social engineering involve several steps:

- 1) User receives a fake e-mail, which masquerades like it came from legitimate source such as bank. E-mail encourage user to click on a link (See Appendix A for illustration).
- 2) By clicking on such link, victim gets into the fake site, which looks like legitimate one.
- 3) On the fake site user prompted to enter confidential information such as user name, password, credit card, or social security number.
- 4) Fraudster uses retrieved information to read e-mail, transfer funds, modify order, or to do other criminal activity.

The part of the technical –subterfuge mechanism is implanting Spyware to the victim's machine. Some attacks are conducted by creating proxies, which enable phisher extract user information from client PC. Phishing Activity Trends Report call such schemes technical-subterfuge (2008).

During the last several years the number of phishing attacks substantially increased. These frauds impact the victims more severely. The confidence of the customer in the online communication suffers. Also the number of ways this attacks are organized and carried over keep growing.

Only in June 2008 APWG received 28,151 reports of unique phishing emails and 18,509 reports of unique phishing web sites (see Appendix B for more statistics). If at the very beginning phishing was mostly conducted by the people who wanted to full around and prove yourself, now it associated with organized crime. Fraudsters carefully target their victims. For example, they might obtain customer e-mails data from targeted brands, such as banks, and communicate with customers pretending to be legitimate. Fake sites are often created with superior quality, which make it extremely hard for ordinary user to recognize a trick. Whole criminal organizations operate to produce bogus sites, send bogus e-mails, and attack multiple users at once.

There are several known ways phishing crime could be carried over including man-in-the-middle attacks, cross-site scripting, URL obfuscation, etc. The Professional Services Director Gunter Ollmann wrote, "Using a multitude of attack vectors ranging from man-in-the middle attacks and key loggers, through to complete recreation of a corporate website, Phishers can easily fool customers into submitting personal, financial and password data"(2004, A 21<sup>st</sup> Century Scam, para. 4). Some phishing attacks use the mixture of approaches. Understanding what are vulnerabilities and how criminals can used them is very useful for creating better E-Commerce systems.

### *Man-in-the-Middle Attacks*

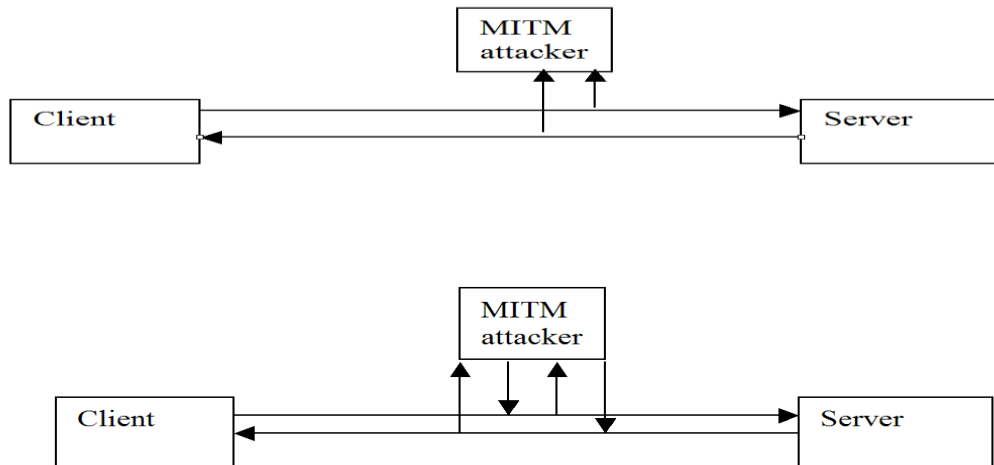
Man-in-the-Middle (MITM) Attacks took it name from the general approach fraudsters take: interfering Client-Server communication. Neither client nor server is aware of

## Du

the intruder presence. All possible scenarios of such attack could be categorized onto two main groups (See Figure 1):

- 1) Attacker uses eavesdropping to sniff confidential information
- 2) Attacker manipulate data client and server exchange

**Figure 1. Man-in-the-middle attack scenarios.**



Gunter Ollmann points on several ways man-in-the-middle attacker can force network traffic to go through malicious proxy server:

- Transparent Proxies
- DNS Cache Poisoning
- URL Obfuscation
- Browser Proxy Configuration (2004, p.10)

### *Transparent Proxies*

Transparent Proxies are used widely in networking and not only by phishers. These proxies conveniently increase network performance. Client IP address is open. Such proxies do not need special HTTP configuration. SOCKS and Squid are examples of proxy servers, which enable transparency of network communication, and are among favorite among the hackers. Phishers establish a secure connection with victim location by capturing requests to be redirected to attacker server. Then they rout all request to real server through proxy host, where sensitive user information could be captured.

### *DNS Cache Poisoning*

The system host files contain domain match information. System sends a request to DNS to get an IP of the particular domain. Finally request is sent to the server with given IP . DNS Cache Poisoning modifies IP addresses and redirect user to attacker server instead.

## Du

### *URL Obfuscation*

In other cases client might be tricked to click on the link, which closely resembles the official domain name, but have added part. Sometimes such “suffixes” or “prefixes” to the real address are encrypted and gives no clue where information would go.

The minor variations of URLs do not attract customer attention, and as a result victim become connected to the proxy server instead of the real one. For example, for the real URL such as <http://real.companyname.com> obfuscated URLs could be similar to:

<http://companyname.real.com>

<http://real.campanyname.com>

<http://real.companyname.com:ebanking@phishersite.com>

<http://real.companyname.com@252.123.12.35/login.htm>

<http://real.companyname.com/%25%35%u01Fc>

Often fraudsters use resources directly from the imitated websites. For example, they can modify the image passes so that they contain the full path URLs. Another trick is when real company placed as an image on the top of attacker address in the URL field. In such case user might see the image with text <https://bankofamerica.com:ebanking> and does not know that image hide the real <http://phishersite.com> address. Similarly padlock icon could be only an image placed by phisher to mislead victim about SSL connection present.

### *Browser Proxy Configuration*

In this case attacker acts in advance. Before sending a fake e-mail, it infect user machine with some malicious software, which is able to modify browser proxy settings. When victim click the link, browser already presented to rout traffic to attacker proxy server.

## **3. Preventing Phishing Frauds**

Phishing Fraud became a great concern for users of online services because the most private information could be relatively easily stolen. The providers of the online services are suffering from the lost related with fake transactions and from the lost of clients trust. Such organizations as Anti-Phishing Working Group (APWG) and OnGuard online coordinate the effort to prevent Phishing Fraud. Governmental organizations such as Federal Trade Commissions develop set of recommendations and regulations encouraging the E-Commerce companies to be very serious about online security. Mentioned organizations provide useful tips for users how to recognize and deal with online fraud. Many believe that e-business especially online banking have to carry responsibility for consumers' online safety. The representative of California's branch of APWG Peter Cassidy said, “Scammers target the industry's biggest brand names... and 92 percent of phishing e-mails target banks”(as cited by Stech, 2006).

## Du

Before offering online service such institutions need to take care about deploying sophisticated security measures. Especially this applies to online banking where financial loss of the victims might be extremely painful.

In 2005 Federal Financial Institutions Examination Council published the bulletin on “Authentication in an Internet Banking Environment” where it not only direct Financial institutions to take security measures while providing online service, but specifically say that such measures have to be adequate, “ Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks”(Authentication, 2005).

Under single factor authentication online security specialists understand security measures such as using user name and password. Such data could be easily stolen either by phishers or directly from the company database using insiders’ help. Multifactor authentication includes usage of at least two authentication methods from three groups. These groups are: what customer know, what customer has and what customer is (Authentication, 2005).

Customer know the user name, customer ID, PIN, the answer to security question, etc. Customer could have physical thing such as plastic card or digital password generator. Finally, biometric characteristics and PC “fingerprints” are uniquely identified customer or customer machine.

**Figure 2. Security Layers**

<b>Client Side Security</b>
<b>Server Side Security</b>
<b>Enterprise Level</b>

The key component of the client side security is awareness. However, having in mind growing sophistication of phishing attacks, even knowledgeable user could be vulnerable. To enhance client side security several technical solutions are available including anti-virus and anti-Spam, and anti-spy software, firewall, monitoring solutions, digital signing, and browser settings (Ollmann, 2004).

Still average user might be unaware of the ways online frauds including phishing are conducted. It is very important that companies, which provide service over Internet, supplied necessary warnings to customers. While designing secure system, company specialists must consider what are the possible vulnerable components and make sure that appropriate authentication is used. Using simple naming convention (straight forward URLs for example) also help to make server side more secure.

On enterprise level company could develop a policy of never asking for social security number in e-mails, implement sophisticated online monitoring systems, use encrypted SSI/TLS link, using digital signatures, add gateway protection, and buy multiple domain name, representing minor variations of officially used name.

E-Commerce actively uses third party solutions to increase security measures and prevent online frauds such as phishing. In 2005 Bank of America trailed in several its branches the product of the PassMark Security SiteKey. Later bank made SiteKey the part of online security system for all branches. Yahoo, Vanguard, and some other companies use similar to solutions.

### 4. Sitekey

Back in 2004-2005 the Bank of America started to consider cardinal changes for its online security system. According to Katy Stech, "The Anti-Phishing Working Group, a technology advocacy group, estimates that this type of fraud cost banks about \$2 billion [in 2006]"(Stech, 2006). Yet even bigger problem was not that the Bank of America was victimized by phishing attacks a lot, but that bank was losing opportunities because customers were reluctant to use online banking. "Nearly 30 percent of the online bankers say that online attacks have influenced their online banking activities. Over three-quarters of this group log in less frequently, and nearly 14 percent of them have stopped paying bills via online banking", said Avivah Litan, the VP and Distinguished Analyst in Gartner Research (as cited in "Consumers losing confidence in online commerce, banking, 2005). Yet another side of the problem was that customers were losing trust in online correspondence from the bank. Litan gave an example, "A bill sent electronically costs about half of what a bill costs when sent through regular mail"(Consumers, 2005). By Turban, Aronson, and Liang, "For banks [electronic banking] offers an inexpensive alternative to branch banking (e.g., about 2 cents cost per transaction vs. \$1.07 at a physical branch)" (2005, Cyberbanking, p.762). Because customers were concerned about online security, bank could not explore the full potential of this cost-effective option. This problem remains true.

In 2005 the Bank of America implemented the SiteKey solution, the system created by PassMark Security later acquired by RSA Security and now belonging to EMC Inc. In 2005 IT society admitted that the SiteKey was the best security solution of the year. Many also applauded to the bank for voluntarily implementing the solution.

#### *SiteKey Implementation*

The main feature of the SiteKey is that it allows not only bank server to recognize the legitimate user, but also allows user to verify that he or she is actually communicating with the Bank of America's server. By Trevor Zion Bauknight, the web designer and writer, "PassMark calls its system a "Two-Factor Two-Way Authentication"(TM) system"( Bauknight, 2009, What Is SiteKey, para.1). Two-Way authentication is about both client and server side ability to authenticate legitimacy of each other. SiteKey product could be considered a two-factor system because it uses what user knows and what user is to authenticate communication. User knows login name, password, image, phrase, and the answers to security questions. SiteKey system allows server to identify the user's machine, thus by PassMark claim it can verify who user is. Bauknight clarifies, "Two-Factor: first factor – password; second factor – 'unique' 'fingerprint' of the machine, consisting of things like HTTP headers, the IP-address, software configurations and even its geographic location (based on IP-address geomapping)"( Bauknight, 2009, What Is SiteKey, para.2).

## Du

The basic login process for online banking with BofA implementing the SiteKey is following:

- 1) User enters the login name.
- 2) User verifies image authenticating site
- 3) User enters password

According to the Bank of America official site, SiteKey consist of three parts:

- 1) A unique image chosen by customer
- 2) The complimentary image title created by customer
- 3) Three challenge questions, answer to which will help BofA to recognize user if he/she sin in from the computer different from “the computer [user] told us to recognize” (SiteKey at Bank of America, 2009).

Storing browser cookies or Flash objects is a part of the SiteKey service.

### *Similar to SiteKey Solutions Implementations*

Vanguard and Yahoo are the most known companies implementing solutions similar to SiteKey. Vanguard uses enhanced logon to protect their online customers from phishing fraud. Yahoo also uses site-authentication images. Similar to BofA’s SiteKey Vanguard and Yahoo solutions placing cookies and Macromedia flash objects as the second factor of authentication.

The login order for Vanguard is almost identical to SiteKey. Vanguard online security center instruct users, “When you sign up for account access, you’ll select and name a security image, known only to you. When you log on, we’ll show you this image so you know you’re accessing Vanguard.com, not an impostor site”(Enhanced logon FAQs, 2009). Vanguard security team believes that enhanced logon is reliable system because if someone will succeed in stealing the user name and password of the client, it is very unlikely that this person will try to access account from the client machine. Because server won’t recognize the machine unique token, only one why will be able to answer the security questions will get an access to the account.

Vanguard enhanced logon system will put the cookie containing a randomly generated unique number. On the next logon from the same machine Vanguard website will recognize the number, and no question answering would be necessary. In case user deleted cookies, Vanguard website will use Flash object. If user does not have flash installed the security question will help to identify user.

Sign-in seal on Yahoo works slightly differently. Image is associated with computer not user account, and user can choose custom image (Vanguard, for example require to choose image from it’s db). When user send a request to the Yahoo server to display a login page, depending on the machine, which is recognized by server, sign-in seal – site authentication image – appear in the right top corner. User enters login name and password on the same page if he or she sees the proper image. As opposite as it works for SiteKey or Enhanced Logon, Yahoo’s sign-in seal would be the same for every yahoo users on the machine. For example if a student using computer lab to access an account, the image displayed might be chosen by administrator and would be the same for every student using this machine.

Similarly to the SiteKey and Enhanced Logon the sign-in seal “tells you that you’re seeing a genuine Yahoo! Site, not a phishing site” as stated on Yahoo! Sign-In Seal FAQ page (2009).

### 5. Bank Of America’s Sitekey Limitations

SiteKey or similar site-image authentication solutions brings user an additional layer of protection; however, they cannot guarantee safety if implemented alone without considering other approaches of online security. Online fraudsters still able to full Bank of America’s online clients because of several factors:

- Not every BofA web pages use SSL connection
- SiteKey might create false sense of security
- SiteKey cannot prevent real-time man-in-the-middle attacks using proxy
- SiteKey second authentication factor is questionable
- SiteKey stores images, names, and password in bank’s database
- SiteKey is not a guarantee of human rationality

#### *Inconsistent use of Secure Socket Layer connection*

Until recently not every page of Bank of America web site including home page was created using Secure Socket Layer (SSL) connection. For example [http://newsroom.bankofamerica.com/index.php?s=press\\_releases&item=7872](http://newsroom.bankofamerica.com/index.php?s=press_releases&item=7872) Inconsistent usage of SSL encryption affects user awareness. The research performed by the group of researchers from Harvard and Massachusetts Institute of Technology revealed that the majority of users ignore absence of SSL connection indicators such as https (not http) URL prefix or “padlock” icon (Schechter, Dhamija, Ozment & Fische, 2007).

#### *False sense of security*

The fact that the majority of the studied group of users ignored the fact that they were presented with http connection instead of https does not itself suggest that it was the SiteKey flaw. However, authors of the study believe that “customers may be less likely to pay attention to HTTPS indicators when instructed to focus on their site-authentication images”(The Emperor’s, 2007, p. 9). Such conclusion was reached based on explanations users who ignored HTTPS indicators gave to researchers.

Bank of America and other institutions implementing solutions similar to SiteKey may help to create the false sense of security in customers by ensuring them that when correct site-authentication image is displayed it is safe to enter a password. For example, Bank of America, tells its 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” (As cited by Stone, 2007).

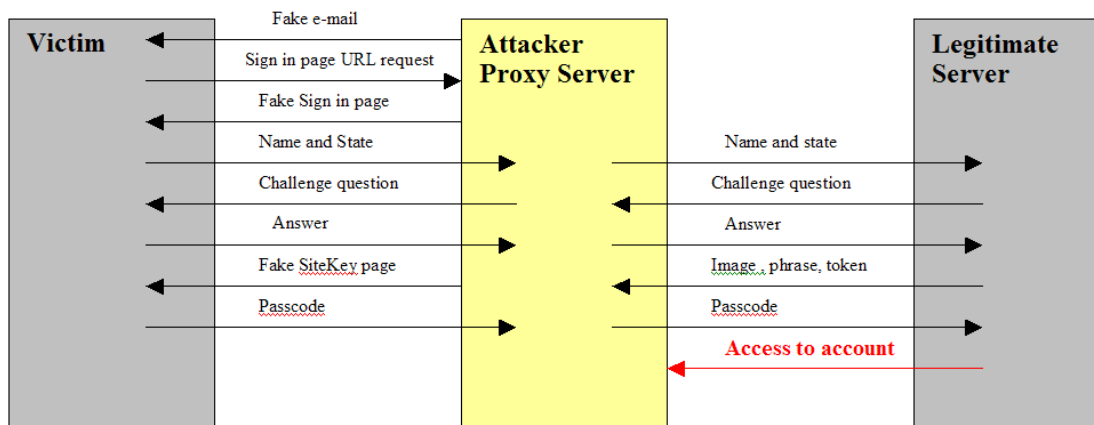
#### *Site Key and Man-in-the-Middle Attacks*

The presence of the SiteKey works well preventing user to enter password to static phishing site. However, real-time MITM attacks still could be conducted using proxy server. One of the several scenarios for such attack could be the following:

## Du

- 1) User is linked to the fake BofA site and prompted to enter login name and state.
- 2) Proxy server capture user input and transfer it to a legitimate site
- 3) Since SiteKey does not recognize the machine, it sends the challenge question to user
- 4) Proxy server capture the challenge question and transfer it to victim
- 5) Victim submit answer to the question
- 6) Proxy server capture the answer and pass it to SiteKey
- 7) SiteKey create bypass token on the machine attack was conducted from and sent SiteKey image and phrase.
- 8) Proxy capture token, image, and phrase and generate bogus SiteKey page
- 9) User disclose passcode to the attacker
- 10) Attacker has full access to user account

**Figure 3. MITM Attack on the Site Using SiteKey (Youll, 2006).**



Here again the presence of the SiteKey only creates false confidence that communication goes from client to legitimate server where as, according to IT Security Architect Doug Ross, “The zombie PC could present a false BofA store-front to the victim and proxy login information from the user to the bank and any resulting pages and images from the bank to the victim” (as cited by Bauknight, 2009, Sounds Great. What’s Wrong With it?).

### *Advantages and disadvantages of using challenge bypass token*

Cookies and Macromedia Flash shared object creation makes it harder for phisher to trick its victims while making legitimate user experience easier. Cautious user might notice that challenge question was presented while it was not suppose to. Such situation could indicate that the server did not recognize the machine “fingerprint”. Thus the phishing attempt could fail at the very beginning. Alternatively, if server recognized the user machine, user will be able to skip extra validation steps.

Internet Browsers and Flash Players have security features preventing web sites from accessing files stored on a local system. This makes getting secret token a harder quest for online fraudsters. They would have to get it in real time.

## Du

Some aspects of using challenge bypass token might generate problems. Problems are related with token itself, the way it is used, and with irrationality of users. Talking about SiteKey, Jim Youll believes, "Reasons for its vulnerabilities, the risks posed by its design and by its persistent storage of a security-weakening token"(2006, Abstract). The biggest question among online security specialists remain on whether created by SiteKey unique "fingerprint" of the user's machine is rally a second authentication factor.

In order to get victims digital code generator or card criminal has to have physical access to that person. SiteKey uses cookies and Flash objects, but fraudster does not need to have access to user to get it; tokens could be stolen over the Internet. Even though such tokens are called the machine "fingerprint" they could be copied and used by phisher. For example, if user's machine is infected by a spyware, criminals could get the token.

Users might not necessarily know that they are not suppose to be prompted to answer a challenge question once server stored token on the machine. Customers might not be cautious enough to pay attention to whether question should be asked or not. Also, In case the customer is using public computer challenge question won't look suspicious at all. Though it is very unlikely, that phisher will use the same machine as legitimate customer, theoretically such scenario is possible. Finally, online attackers could successfully set proxy to run from the victim machine.

### *Personal Information Storage*

Trevor Zion Bauknight has more concerns regarding using SiteKey solution, "In addition, and this is probably the most worrying caveat, given the recent rash of massive security breaches at large storehouses of personal information, the SiteKey approach still relies on the storage of images and so on in your personal records on the merchant's database"(Bauknight).

Having in mind the trend toward phishing fraud being more organized and targeted, images, phrases, security questions might be as vulnerable as plane combination of user name and password. Thus question is whether SiteKey solution is really feasible.

### *SiteKey and Human Rationality*

Researchers from Harward and MIT observed a group of 67 users and found out that many of them entered their password even when SiteKey image was absent. They also ignored the warning given by the browser, that server was unknown. No matter how good the security technology is, it can't rely on assumption that humans will behave rationally.

## **6. How Bank Of America Can Enhance Online Security**

Back in 2005 the Bank of America voluntarily decided to implement SiteKey solution to make online banking safer experience for it's clients. This was a plausible step, which helped the bank to stay on competitive edge in the industry. In spite of multiple publications ranging from calling SiteKey the waste of money to blaming the

## Du

solution for implicitly helping the phishing attacks, bank security team is confident that implementing the SiteKey was the right thing to do.

According to representatives of Bank of America's online security team, SiteKey proved to be an effective measure, which helps to reduce the static phishing attacks and monitor real-time man-in-the-middle attacks. The representatives of the bank highlight that SiteKey is only one part of the multi layered security system protecting bank and its customers. The major aim of the SiteKey is to "thwart large-scale phishing that might injure many customers at once"(As cited by Youll, 2006, Comments from Bank of America and RSA Security).

### *SSL Digital Security Certificates*

First of all, using Secure Socket Layer connection and digital certificates is a good weapon against phishers for two reasons, encryption and difficulty to obtain such certificate. It requires much more knowledge and effort to get or insert information from or to the encrypted page. Stand alone phishers generally unable to get a certificate. Suppose malicious web site was created by the organization, which already owns such certificate. However, as soon as such site would be spotted, it will be shut down. There would be no mean for a phisher to obtain a new one quickly. Also the process of obtaining the digital security certificate is such that companies should go through several steps to get one.

To obtain a digital security certificate the business or organization need first to submit a Certificate Signing Request (CSR) form to one of the Certificate Authorities (CA) companies. Thawte and VeriSign are two of the most trusted companies. Next, Certificate Authorities companies will verify the company information such as legitimacy of domain and approve request. After that business will have to install the certificate.

Digital certificates are not free. For example a "128-bit Extended Validation SSL" certificate valid during one year would cost \$1,499 if obtained from VeriSign ("Secure Site Pro with EV", 2009). SSL Web Server Certificates with EV from Thawte will cost \$599.00 for one year. There are different versions of SSL Certificates with different features, which determine the price. For example, the Extended Validation (EV) will display address bar in green in the latest browsers (Figure 11.) Both, Bank of America and Vanguard sites sign in pages use certificates from VeriSign, Inc. that display such bar.

SSL certificates authenticate server to the client. If a certificate received is on the list of trusted domains, client machine will generate an encryption key, which will be known to server, so secure communication could be established (See Appendix C for process details).

It is worth of noticing that SSL certification has its own flaws. The international group of researchers, studying "vulnerability in the MD5 algorithm, one of the standard cryptographic functions used to check that SSL certificates" discovered one of such flaws (Stray, 2008). It turns out that if SSL certificate uses MD5, it opens a "back door" for ones, who might want to create a forge certificate. The representatives of VeriSign claim that they stopped using MD5, "We went into our systems and

## Du

removed the MD5 algorithm and replaced it with SHA-1 (Secure Hashing Algorithm)"(As cited by Stray, 2008). However, According to Stray, about 30 or 35 percent of Certificate Authority organizations are still using mentioned algorithm (2008).

### *Using Browser Build in Security Features*

The web browser, which is configured having security in mind, can be a substantial part of online security system. Gunter Ollmann suggest to use following measures to prevent a majority of the Phishing attacks:

- "Disable all window pop-up functionality
- Disable Java runtime support
- Disable ActiveX support
- Disable all multimedia and auto-play/auto-execute extensions
- Prevent the storage of non-secure cookies
- Ensure that any downloads cannot be automatically run from the browser, and must instead be downloaded into a directory for anti-virus inspection" (2004).

Unfortunately these and other web browser "nice to have" features create additional vulnerabilities, which could be exploited to conduct a phishing attack. Microsoft Internet Explorer web browser has a lot of functionalities, which makes it one of the most vulnerable. Firefox Mozilla is considered to be a safer browser.

To help fight Phishing special plug-ins were developed. For example, plug-in can verify that URL of the site is not on the list of discovered Phishing sites. Also some web browser could issue warning messages if there are suspicions that trying to establish connection server is not legitimate.

Some of the browser's characteristics actually help SiteKey to do its job. For example there is no mean for a phisher to download or change secure cookies stored on a local system through the web browser. Browsers prevent applications from access to the local system. Thus, unless user's PC is infected with SpyWare the challenge bypass token is relatively safe.

### *Considering vulnerabilities*

E-Commerce applications are complex and should be designed with security concerns in mind. There are several well-known vulnerabilities of online systems, which allow conducting attacks. K.K. Mookhey in his article "Common Security Vulnerabilities in e-commerce Systems" listed several of such vulnerabilities:

- "SQL Injection
- Price Manipulation
- Buffer overflows
- Cross-site scripting
- Remote command execution
- Weak Authentication and Authorization" (2004).

Designing every component of the system architects might have a choice of the tools to use. For example, there could be options on whether to use Oracle or MS SQL Server for the database. From the security point of view Oracle would be more

## Du

preferable because it is less susceptible to the SQL Injection solution. Including in the system such enhancements as SiteKey will allow strengthening Authentication and Authorization process.

### *Bank of America's SafePass*

In 2007 BofA, the bank with the history of implementing innovative security solutions, introduced, SafePass technology developed by VeriSign. By the official announcement on the Bank of America press release site, "Latest innovation provides two-factor authentication via one-time password delivered to a mobile phone or from a wallet-sized card Combination of SiteKey™ and SafePass provides consumers with a new level of security when banking online"( "Bank of America Introduces SafePass™ for Safer Online Banking", 2007). Provided service is optional and aim is to make such online operations as "transferring money for amounts over current limits", "Authorizing new payees in bill pay", "Adding new accounts for online transfers", "Signing in from a computer not recognized by SiteKey" much safer (Bank of America, 2007).

The delivery of the one-time code via a mobile phone service is free. Customer can subscribe for SafePass online. During the initiation process customer enter one or two the mobile phone numbers SafePass would use to authenticate an activity (See Appendix D for illustrations). Later, when customer will need to add payee, transfer large amount of money, or logon from the machine not recognized by SiteKey, SafePass will send a six-digit randomly generated number via mobile phone, and user will be allowed to proceed only if he/she enter the correct code. Generated code expires either right after use or in ten minutes after it was requested.

SafePass card is also an option for the user but it cost \$19.99, which is not much for the value its provide. It sized to fit valet for convenience. To request bank to generate a one-time code customer need to push a button on the card.

It is very unlikely that fraudster will be able to obtain login information and SafePass. To do that one would need physical access either to the mobile phone or card. Thus combination of the SiteKey with the SafePass provides the higher level of protection.

### *Monitoring*

Even the most elaborate and sophisticated online security system won't prevent every Phishing attack. Thus layered security system for E-Commerce will have to use different monitoring techniques such as Domain monitoring and active Web Monitoring to make sure that measures taken are up to date.

Businesses providing online services usually spend a lot of moneys to buy domain names similar to the key corporate domain. Thus Bank of America would probably own several hundreds of domain names close to bankofamerica.com such as bofa.com, thebankofamerica.com, bankofamerica.net, etc. These domain-monitoring measures not only protect a trademark of the company, but also prevent fraudsters from using brand names to trick online customers.

## Du

E-Commerce could use intelligent agents to monitor who is accessing server. Such agent could catch up if account activity performed from suspicious machine, could catch an unusual transaction activity. In such case Bank of America, for example, will call a client to verify the transaction. Another case is when multiple accounts are accessed from the same machine. Intelligent agent will report such activities so that suspicious servers would be banned from accessing information, reported to anti-phishing agency. Next Web Monitoring might notice that a particular server is unusually active in retrieving companies' resources. It is a good practice from security point of view to have a "white list" of authorized users of logo, trademark, and unique web content to the service provider"(Ollmann, 2004, p.40). In the case unauthorized site try to display image, user will get a warning message such as displayed on the Figure 4.

### *Other Security Features offered by BoA*

Bank of America online banking security system widely accepted as one of the best in the industry. Bank lists following features as additionally available aids for online customers:

- Automatic e-alerts help customers detect potential fraud on their Bank of America accounts.
- ShopSafe® lets Bank of America card customers create a unique, temporary account number for online purchases.
- The bank's Zero Liability Guarantee protects customers from unauthorized transaction on their online accounts.
- The Bank of America Toolbar, powered by EarthLink and available to consumers for free at bankofamerica.com, helps identify fraudulent Web sites and includes a pop-up blocker.
- Up to a 50 percent discount of the full retail price on Norton Internet security 2007. (Bank of America, 2007)

By being proactive and innovative in creating the reliable online security System Bank of America lead competition in online banking and is a good example for other E-Commerce companies.

Figure 4. Swapping Out The Real Image With The Warning (Krebs, 2006).



### *Educating customers*

It is in the interest of the e-commerce companies to educate customers along with adding more and more layers of security. On one hand online customers want to feel secure. On the other hand their experience should not be overloaded with extra security features. It is very important that clients understood, that their machine, their online habits, and their cautiousness are the huge part of any online security. The Comptroller of the Currency Administrator of National Banks Interagency Guidance states, “[C]ustomer awareness is a key defense against fraud and identity theft” (2005). It is does not matter how elaborate is the SiteKey or other techniques are if customer would ignore the absence of the SiteKey Image or any other warning sings. Schechter, Dhamija, Ozment, and Fischer observed behavior of 67 online customers when https indicator was removed, site-authentication image was removed, and special warnings were presented. They discovered that 63 out of 67 customers overlooked the absence of SSL certificate, 58 out of 60 users ignored the absence of image, and 30 out of 57 participants proceeded with logon process in spite of the warning “There is a problem with this website’s security certificate”(2007, p.6).

There exist multiple sources where online customers can learn more about security. Governmental organizations and different online security groups like OnGuard, APWG publish a lot of useful information and tips on how protect one from online frauds such as phishing (See Appendix F for user tips). Below are some of such information sources:

## Du

Anti-Phishing Working Group <http://www.antiphishing.org/>

Federal Trade Commission <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>

OnGuard Online: Your safety net <http://www.onguardonline.gov/topics/phishing.aspx>

Governmental organizations also issues the Regulations for E-Commerce operations including Online Banking, which require banks to take measures to educate customers. It is also important do not mislead customers on a level of safety. For example, it is positive thing that Bank of America's customer have zero-percent liability insurance, but it is unfortunate that they can get a false confidence, which leads to ignoring security warning signs.

### *E-Commerce Security Systems' Future Study*

As computer technology advances, more solutions become available for E-Commerce to fight online fraudulent activity. Unfortunately, this fight is also a race with cyber criminals, who invent new ways of conducting attacks. This is why it is so important for the Computer Information System specialists to learn the best security design practices, conduct constant monitoring of the internal and external for the system situation, be informed about recent technology development. It is very important to learn well what are the known E-Commerce vulnerabilities and what are the ways used by online fraudsters to foresee the problems. Future security systems should be more preventive mechanism than treating.

## 7. Conclusion

SiteKey is a very important part of the Bank of America system. It works well in preventing attacks where multiple customers are victims though it is not flawless. Maybe even more important benefit from the SiteKey solution implementation is that its brought customers back to online banking, increased they confidence, demonstrated bank's good will to exploit wide range of available security solutions to protect customers from the unpleasant experience. Thus the implementation was also a great marketing step for the bank. SiteKey is only one of the many solutions offered on IT market. There is a huge field of study in this area. Learning more about phishing and other online frauds, being aware of vulnerabilities, and taking a complex approach to protective/preventive solution will benefit to any E-commerce organization. Balanced "layered" security system could be considered a competitive advantage for the E-business.

## References

"Authentication in an Internet Banking Environment", 2005. Comptroller of the Currency Administrator of National Banks. Interagency Guidance. OOC Bulletin. Retrieved from [http://www.ffiec.gov/ffiecinfobase/resources/info\\_sec/2006/occ-bul\\_2005-35.pdf](http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/occ-bul_2005-35.pdf)

Bandar, Ehab, 2007. "Test driving Bank of America's SafePass". Banking Unwired. Retrieved from <http://www.bankingunwired.com/2007/12/05/test-driving-bank-of-americas-safepass/>

"Bank of America Introduces SafePass™ for Safer Online Banking". 2007. Bank of America. Newsroom. Retrieved from [http://newsroom.bankofamerica.com/index.php?s=press\\_releases&item=7872](http://newsroom.bankofamerica.com/index.php?s=press_releases&item=7872)

## Du

- "Bank Of America – 'Online Banking Alert (Change of Email Address)'"'. 2005. Anti-Phishing Working Group. Retrieved from [http://www.antiphishing.org/phishing\\_archive/04-19-05\\_BOA/04-19-05\\_BOA.html](http://www.antiphishing.org/phishing_archive/04-19-05_BOA/04-19-05_BOA.html)
- Bauknight, T.Z., 2009. "PassMark's SiteKey – answering the wrong Question". Cafeid create your identity. Retrieved from <http://www.cafeid.com/art-sitekey.shtml>
- Bruene, Jim. 2007. "Bank of America launches SafePass, but you'd never know from its website". Netbanker.com Retrieved from [http://www.netbanker.com/2007/09/bank\\_of\\_america\\_launches\\_safepass\\_but\\_not\\_mentioned\\_on\\_website.html](http://www.netbanker.com/2007/09/bank_of_america_launches_safepass_but_not_mentioned_on_website.html)
- "Buy thawte SSL Certificates". 2009. Thawte. Retrieved from <https://www.thawte.com/ssl-digital-certificates/buy-ssl-certificates/?click=buyssl-buttonsleft>
- "Consumers losing confidence in online commerce, banking". 2005. Consumer Affairs website. Retrieved from <http://www.consumeraffairs.com/news04/2005/gartner.html>
- "Ecommerce Security Issues". 2009. Ecommerce Digest. Retrieved from <http://www.ecommerce-digest.com/ecommerce-security-issues.html>
- "Enhanced logon FAQs". 2009. Vanguard. Security Center. Retrieved from <https://personal.vanguard.com/us/help/SecurityLogonFAQsContent.jsp>
- "How not to get hooked by a 'phishing' scam, 2006. Federal Trade Commission Retrieved from <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>
- "Internet security". 2008. Access eCommerce. University of Minnesota Extension. Retrieved from <http://www.access-ecom.info/article.cfm?id=60&xid=MN>
- Jakobsson, Markus & Soghoian, Christopher, 2007. "A Deceit-Augmented Man In The Middle Attack Against Bank of America's SiteKey Service". <http://paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html>
- Krebs, Brian. 2006. "Using Images to Fight Phishing". The Washington Post. Retrieved from [http://blog.washingtonpost.com/securityfix/2006/08/using\\_images\\_to\\_fight\\_phishing.html](http://blog.washingtonpost.com/securityfix/2006/08/using_images_to_fight_phishing.html)
- Mookhey, K.K., 2004. "Common security vulnerabilities in e-commerce systems". SecurityFocus. Retrieved from <http://www.securityfocus.com/infocus/1775>
- "Network security". 2005. CICS Transaction Gateway V6.0.1. IBM. Retrieved from <http://publib.boulder.ibm.com/infocenter/cicstg/v6r0m0/index.jsp?topic=/com.ibm.cicstg600.doc/ccllai0210.htm>
- Ollmann, Gunter. 2004. "The phishing guide: understanding & preventing phishing attacks". Next Generation Security Software Ltd. Retrieved from <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>
- "Phishing Activity Trends Report", 2008. APWG. Retrieved from [http://www.antiphishing.org/reports/apwg\\_report\\_Q2\\_2008.pdf](http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf).
- Schechter, Stuart E., Dhamija, Rachna, Ozment, Andy, and Fischer, 2007. "The Emperor's New Security Indicators: The 2007 IEEE Symposium on Security and Privacy. Retrieved from <http://www.usablesecurity.org/emperor/emperor.pdf>
- "Secure Site Pro with EV". 2009. VeriSign. Retrieved from <http://www.verisign.com/ssl/buy-ssl-certificates/extended-validation-pro-ssl-certificates/index.html>
- "SiteKey at Bank of America". 2009. Bank of America website. Retrieved from <http://www.bankofamerica.com/privacy/sitekey/>
- Stech, Katy. 2006. The Post and Courier. Charleston, S.C. pg. A.1. ProQuest Research Library.

## Du

- Stone, Brad. 2007. "Study Finds Web Antifraud Measure Ineffective". The New York Times. Technology. Retrieved from [http://www.nytimes.com/2007/02/05/technology/05secure.html?\\_r=2&th&emc=th](http://www.nytimes.com/2007/02/05/technology/05secure.html?_r=2&th&emc=th)
- Stray, Jonathan. 2008. "Web browser flaw could put e-commerce security at risk". CNET. Retrieved from [http://news.cnet.com/8301-1009\\_3-10129693-83.html?subj=news&tag=2547-1\\_3-0-20&part=sphere](http://news.cnet.com/8301-1009_3-10129693-83.html?subj=news&tag=2547-1_3-0-20&part=sphere)
- "Yahoo! Sign-In Seal FAQ". 2009. Yahoo. Retrieved from [https://protect.login.yahoo.com/login/set\\_pref?.intl=us&faq=1#faq2](https://protect.login.yahoo.com/login/set_pref?.intl=us&faq=1#faq2)
- Youll, Jim. 2006. "Fraud vulnerabilities in SiteKey security at Bank of America". Challenge/Response LABS. Security & privacy for e-commerce. Retrieved from <http://cr-labs.com/publications/SiteKey-20060718.pdf>