Global Information Assurance Certification Paper

What Users Should Know About Online Banking Security
William Lassiter
GSEC 1.4b

Introduction

The purpose of this paper is to educate the typical user who wants to use the internet to pay bills, transfer funds, or just review account activity through his/her bank's online banking service. Online banking has quickly become one of the most popular activities on the internet. Currently there are approximately 22 million households using online banking. This number is predicted to increase to over 35 million households by the year 2005.[6] After all, who would not agree that it's much easier to sit on the couch in your pajamas and do your banking than having to drive to the local bank and wait in long lines? The same things that used to take hours to do in person at the bank now take just a few minutes to do online. With this being the case, why would anyone want to stand in lines again, just to transfer money, or manage his/her accounts? Well, there are still people out there that are skeptical about entering personal information into a computer and sending it over the internet. Most of the people who are skeptical about doing their banking over the internet would probably feel more at ease if someone would educate them more about it.

Online Banking Overview

Chances are your bank has some type of Online Banking that gives you the ability to pay bills, transfer funds, access checking and savings accounts, etc. When you sign up with your bank, you will have to set up an online account that you will use to access checking and/or savings accounts over the internet. When setting up this account, you will have to create a password that will be used to access your account. Once the online account is setup and the password is chosen, it may take several minutes before the bank synchronizes your new online account information. After synchronization has taken place you will then be able open your internet browser and attempt to log into your banks web server. When you enter your username and password, the bank validates the account information which allows the banking session to continue. This seems relatively simple but let's get into a little more detail on exactly how all of this actually works.

Risks

Along with any type of ecommerce that takes place on the internet comes a certain amount of risk. Over the years, both banks and users have suffered through growing pains related to internet banking. These growing pains are unfortunate but have proven to be essential in order for the ecommerce experience to have advanced to what it has become today. While Online Banking has come a long way and many banks have taken many of the necessary precautions to create a secure internet experience, not all institutions have done

[6] "Banks compete for online customers"

enough. Banks are under a lot of pressure to provide users with this type of service and unfortunately take short cuts around security in order to save time. You should always be aware of how your banking institution mitigates the risk of the various types of vulnerabilities associated with ecommerce. Yes, the host of the internet banking web site has a lot of responsibility, but what most users are not aware of is how much of the responsibility they actually have while using these services. Online Banking sessions are vulnerable to several forms of attacks where either someone hacks into the banking institution's web site or assumes the users identity in order to gain access to his/her account. Therefore, it becomes very apparent that depending on how banks and users protect against these vulnerabilities will determine how safe it is to do online banking. It is important that Online Banking users are aware of what the risks are and what they can do at home to make the online banking experience a safer one.

Bank's Responsibility

In order for a bank to properly protect their services from being attacked, there are certain things that they need to be concerned with such as the way they issue Account Identifiers, the method in which they store a user's information, Session Identifiers, and encryption levels relating to the Secure Sockets Layer. Being familiar with what the banks responsibilities are will allow you to know what questions to ask when deciding whether you want to use your banks online services or not.

1) Account Identification and Storage

Depending on how the bank is securing your information, both during and after the session has a tremendous impact on the level of security. When the bank issues you an Account Identifier (ID), they should use a unique string of characters and numbers that would be of little use to an attacker should they gain access to it. There have actually been reports in the past where banks were using credit and debit card numbers as the users Account ID.[1] If someone were to gain access to you Account ID in this case, the risk would be similar to someone stealing your wallet and using your credit cards to make purchases. Even if the account ID is unique and well designed, the bank should never allow users to store their account information and password on their computer. This offers a small convenience for users by allowing them to log in without having to go through the normal authentication steps. The amount of risk that goes along with this type of convenience is not worth it. If this account information is saved to the local hard drive it will allow a hacker to view this information in clear text should that system become compromised.

2) Session IDs

When you log into your banking institution, there are two authentication tokens that are exchanged. One is the user identifier, and the other is the user password. These two items are generated into an authentication string called a

[1] "Bank One Online Puts Customer Account Information at Risk"

session ID. A session ID is an identification string that is used to associate site specific web page activity with a specific user. This session ID allows you to maintain the same state throughout your session without having to be authenticated over and over again. Because the session ID now makes up the authentication mechanism for you as you browse from page to page within the site, it becomes just as important as the actual username and password. Session IDs are usually long random alphanumeric strings that are usually transmitted within the Unique Resource Locator (URL). A URL is the address that users type in the address bar within their web browser to access a particular site. Being that this alphanumeric string is usually randomly generated, it may be difficult to be guessed and may force a hacker to use some type of brute force to obtain a user's identity. Brute force is a trial and error process typically used by a hacking application that is designed to decode encrypted items like passwords or other user data.[4] While most sites will use an account lockout policy to protect against someone trying to guess usernames and passwords, there are many that do not protect against someone guessing session IDs. An attacker could possibly try thousands of Session IDs within a short amount of time and the site would never see it as an attack. Therefore it is important that the site is equipped to look for this type of activity and be alerted when it happens. It is very important that sites use a random, complex algorithm to generate the session IDs. The session ID should be randomly generated and should never contain user sensitive information such as username, password, or social security numbers.

Another way that Session IDs are transmitted and stored, are within cookies. A cookie is what a web site uses to store information on your hard drive so that it can remember personal information about you for future visits to that web site. When Session IDs are stored in a cookie, the cookie is normally held by the browser, and should be set to expire once the browser is closed. This type of cookie is called a session cookie. Another type of cookie is called a persistent cookie, which does not expire upon closing the browser. A persistent cookie is the result of a user selecting for the web site to remember his username or password. Being that persistent cookies do not expire, they create a huge security risk and may allow a hacker to gain easy access to users accounts.

The length of the session ID is extremely important and should be as long as possible. If the string is short, it makes the password easier to crack for the attacker through guessing or the use of brute force. Even if the encryption algorithm is strong, a short session ID becomes very easy to crack. Session IDs should typically range between forty and fifty characters based on the level of security that the bank is practicing.

Let's look at an example of what happens during a typical session. A user named Jim will open his browser and type the URL of his bank. At which time he will be prompted to enter his user identification and password. After the bank has authenticated him, the bank will generate a session ID and transport him to a secure page which will be discussed later when we talk about Secure Sockets

[4] Endler, David. "Brute Force Exploitation of Web Application Session IDs"

Layer. After the initial log in process has taken place, Jim may see something similar to the URL listed below.
https://www.bank.com/2y56HnfU489imNcsw084Qclp8w44uwiBvda215wrP78hrvd/1/btfa/ik/IAS/presentation
In this example the Session ID is "2y56HnfU489imNcsw084Qclp8w44uwiBvda215wrP78hrvd". Notice that the session ID is very long (48 characters) and appears to be randomly generated. This session ID is now used as Jim navigates through the banking session, instead of him having to be re-authenticated each time he goes to a different page.

Session IDs should always have an expiration time associated with them. They should be set to expire on the web server when the session is terminated or timeout after a period of inactivity by the user. If the session ID does not have a timeout value associated with it, a hacker could break into a user's computer and capture cookies or search log files to gain access to active session IDs. If a hacker can gain access to an active session ID, he can use it to gain access to a user's account.

3) Secure Sockets Layer

Another key security feature is the level of encryption that the institution is using to transmit and receive data. Encryption is accomplished through a protocol called Secure Sockets Layer (SSL). SSL is a security protocol that protects data that is sent between your web browser and the distant web server that resides on the internet. SSL gives you confidence that the web server that you are communicating with is legitimate. SSL is also responsible for making sure that the data being sent has not been tampered with while it was in route to its destination. The easiest way to determine if your browser is communicating with SSL is to look at the web site address. If the address starts with "https", the session is secure and the browser is using SSL. In most cases you will see a small padlock at the bottom of the browser window that will give additional assurance that the connection is using SSL. If you double click the padlock, you will be able to view the certificate that you were issued in order for you to be able to communicate with the web server.[2]

Authentication is what initiates the communication between you and the banking institution that you are trying to communicate with. While it is necessary for you to authenticate with the bank, it is also necessary for the bank to authenticate with you. For example, in the world we live in, when you write a check at the grocery store, the clerk typically asks for your identification. This identification may be in the form of a driver's license or some other picture ID. This verifies that you are who you say you are. When it comes to computers, the same is true, but instead of having to show your driver's license, identification is handled with digital certificates. There are two types of certificates- server and client. Server certificates are used to verify that the web server you are talking to is what it says it is. Likewise, a client certificate is to authenticate the identity of the user. Certificates are made up of both public and private keys. A public key is provided by a trusted authority as a form of encryption that, combined with a

[2] "Secure Sockets Layer"

private key that is derived from the public key, can be used to effectively encrypt messages. A private key is a form of encryption that is known only by the parties that exchange secret messages. Before a web site can start using a secure web server that uses SSL, they must register with a trusted authority and be issued a public key certificate. This certificate provides verification to anyone wishing to communicate with the web server that it has been validated by a trusted source. Here is an example of how SSL works.[7]

1) John opens his browser and enters the web site address, https://usersbank.com and tries to connect.
2) The usersbank.com web server realizes that John's browser wishes to make a secure connection and starts a negotiation process typically referred to as a handshake.
3) The usersbank.com web server will now present its public key certificate to the user's web browser.
4) The web server lets the user's browser know the encryption level that will be used for this session. Note: If the user's browser is not capable of the level of encryption that the server is requiring, the session cannot take place and an error will most likely be displayed to the client.
5) The user's browser authenticates the certificate (agrees that the web server is really usersbank.com).
6) The user's browser then generates a random session key that is used to encrypt data traveling between his browser and the bank's web server. This session key is encrypted using the bank's public key and sent back to the server.
7) The bank decrypts this message using its private key and then uses the session key for the remainder of the communication.

The level of encryption is of great importance. Encryption is the conversion of plain text into a format called cipher text so that it cannot be understood by people that are unauthorized to read it. In order for someone to read the data that is encrypted, he must have the decryption key. Decryption simply takes the encrypted data and converts it back into plain text. While encryption and decryption seems relatively secure, there are computer programs that can be used to try and break the encryption. The more complex the encryption algorithm, the harder it is to break. There are typically two types of encryption that are commonly used on the internet today. The two types are high and standard. The difference between these types of encryption is the strength of capability. A High encryption (128-bit) is much more powerful than a Standard encryption (40 bit). In today's society, all banks should be using, at a minimum, 128-bit encryption. Most online banking websites will give recommendations as to what browsers to use that will give the level of encryption needed to do business with them.

Even though SSL is considered highly secure, and will prevent attacks in most cases, there are still vulnerabilities that you should be aware of. One of the most common vulnerabilities is called a "Man in the Middle" attack. This type of attack

[7] "How SSL works"

is where the attacker intercepts data in a public key exchange and forwards it to the intended party. By doing this, it allows the attacker to substitute his public key for the requested one. This creates the illusion for the parties participating in the exchange and it will seem like they are actually talking to their intended party directly. Once the attacker has accomplished the "Man in the Middle" attack, he can view all messages in plain text and choose whether to forward the original data or modify it before sending.[5] A properly configured web browser will typically alert you if a certificate have expired, not recognized by a trusted authority, or the name registered on the certificate does not match the DNS name for that server. For this reason, you should never use public terminals in places like airports or libraries for any type of credit card purchases or online banking. These terminals are susceptible to attacks since an attacker can physically configure the computer to trust his certificate. By doing this, the public computer will see the attacker's machine as a trusted server and not issue any kind of alert to you. Once you log onto the public terminal that has been compromised, you will provide the attacker all the information that he needs to steal your identity.

User's Responsibility

While a lot of responsibility falls on the banking institution to make everything as safe as possible, there are several things that users must do at their end. You must review your account statements on a regular basis to make sure that no unexpected activity has occurred with your accounts. If any unexpected activity is found, you should contact the bank immediately and bring it to their attention. Most banks will offer some sort of reimbursement if the incident was brought to their attention within a certain amount of time.[3] As stated before, you must never use public computers to do any type of ecommerce since there is no way to know if that computer is secure. You should make sure that you are using good practices when using the internet from home by properly configuring your web browser, running some form of virus protection, properly securing passwords, and by using a firewall.

1) Web Browser Practices

Proper use and configuration of your web browser is of great importance. Users should never leave your computer while they are logged into an online banking session. Leaving a session unattended is very dangerous because anyone that sits down at the computer that you were using will have full access to your account information. When you have finished and wish to exit, you should always properly terminate the online session by properly logging off and then closing the browser. One reason for closing the web browser is if it is not configured correctly, browsers will temporarily store secure pages in the computer's memory. This is referred to a caching and it will allow someone to access the session by simply selecting the "Back" button within the browser. Even though you have terminated the session by logging off, there remains the danger of an

[5] Burkholder, Peter. "SSL Man-in-the-Middle Attacks"
[3] "Online Banking Guarantee"

attacker obtaining information such as the Session ID and any personal information being shown in the browser. The procedure to disable the caching of secure web pages is listed below:

a) Open Internet Explorer, select the "Tools" menu, and select "Internet Options"
b) Select the "Advanced" tab and scroll down to the "Security" section
c) Select the "Do not save encrypted pages to disk" checkbox and select "OK" to save the selection

Even if the browser is configured as noted above, it is always a good practice to log out after the banking session is over and close the browser. This will clear any cached information that may have been stored in memory.

2) Passwords

When you set up your online banking account, you will need to assign the account a password. This password should be complex and should be changed on a regular basis. While using simple passwords makes things easy for you to remember, it also makes it easy for an attacker to guess in order to obtain access to your account. A complex password consists of between six and eight characters and should consist of uppercase, lowercase, numeric, and special symbols. Passwords are very personal and should be kept private. At times while on the internet, you may be asked whether you want the computer to remember your account information. You should never let your browser store and save username and passwords. If your computer is either stolen or hacked into, things like saved usernames and passwords will allow easy access to your personal information.

3) Virus Protection

You should make sure that your computer is protected against viruses and malicious programs. Some viruses and malicious programs have the capability to capture keyboard strokes and send the results to someone on the outside. If your computer is infected with a virus with this capability, when you log into your bank or use your credit card online, the hacker will have captured privileged information and could begin to impersonate you on the internet. Depending on how long it takes for you to realize that your account has been tampered with, the attacker has probably covered his tracks and cannot be caught. This becomes a nightmare for you because now you have to prove to the bank that you did not make the purchases or transfer money from your account. A good virus program will help to prevent common viruses and will provide periodic definition updates for new viruses that happen to be going around the internet. It is imperative that you verify that the latest virus definitions are being downloaded and that they are actually being applied to your computer on a regular basis.

4) Personal Firewalls

A properly configured personal firewall can greatly enhance the security posture of your home network. A personal firewall allows you to provide a layer of protection to your internal network. By placing a firewall between the incoming

connection from your Internet Service Provider (ISP) and your computer, it helps you in preventing unauthorized access from intruders. Depending on the type of internet access you have will determine how much time and energy is necessary to keep intruders off of your computer. There are two types of personal firewalls that are commonly used- Intrusion Detection Software and Routers.

Intrusion Detection Software

In the past, the most common internet connection was accomplished with a dial-up modem that was attached to the home's phone system. With this type of connection, you are only vulnerable while you are actually dialed into your ISP. In this case, you should probably be using intrusion detection software to alert you if someone is trying to gain access to your system. This software constantly watches your computer activity and will block an attackers attempt to launch an attack by email or instant messaging, and it protects the system while you are web browsing.[8]

Routers

With high speed cable modems and DSL connections becoming more and more popular a need for a more complex firewall is a necessity. The reason for this is because dial-up connections are only connected to the internet when they are dialed up to their ISP. High speed internet such as cable modems are connected to the internet twenty-four hours a day. For connections of this type, you should invest in a hardware device called a router. The router's job is to act as the middle man and route information from your private network to the rest of the internet. Basically, a router separates your internal computers from the rest of the internet and an attacker must get through the router before he can access the computers on your internal network. This provides an additional layer of protection and can be used in combination with intrusion detection software if so desired. There are many types of routers available, and the majority routers that are going to be used for home use are fairly inexpensive and pretty easy to set up. Routers give you a lot of flexibility in that you can choose to configure things such as port access, filtering, port forwarding, and numerous other advanced items. Taking advantage of items like port access and filtering will allow you to block any ports that are not typically used as well as selecting which computers on your internal network will have internet access through the router. Please note that while the default configuration has some basic security benefits, and is better than nothing at all, additional configuration is required to acquire a more secure environment. Procedures are normally available on the vendor's web site to assist users with the configuration of the router.

While personal firewall manufacturers strive to produce a product that has no vulnerabilities, the constantly changing nature of the internet makes this virtually impossible. Typically, when the manufacturer finds out that their product has a vulnerability that needs to be fixed; they will produce updates and provide them for download from their web site so that the users can download them. Depending on the manufacturer, step by step procedures are normally provided to make applying the updates as painless as possible. You should always

[8] "BlackICE™ PC Protection"

monitor the manufacturer's website for updates to the firmware for your specific personal firewall.

Just about any type of personal firewall, provided that it is properly configured, will make being connected to the internet a lot safer. For users that do not wish to take the time to configure and manage their personal firewalls, there are many companies that will do this for a small fee. The price that you will pay someone to correctly setup your firewall is a small price to pay for the protection of your identity.

Conclusion

In summary, we have discussed how online banking sessions are vulnerable to several forms of attacks. It becomes very apparent that depending on how the bank protects against these vulnerabilities determines how safe it is to do online banking with them. You should always be aware of how your banking institution handles the various types of vulnerabilities that currently exist on the internet today. Before attempting to do your banking online you should use the information put forth in this paper to verify that your bank is taking all the necessary precautions to keep your personal information secure. If your bank is doing their part to mitigate the amount of risk involved with ecommerce, they will be happy to answer all your questions. You have very right to ask these questions and if you do not get the answers you are looking for, do your online banking at another institution. As an internet user you should always strive to make accessing your home network as difficult as possible for an attacker. Taking the necessary security precautions now may prevent you from having to go through the nightmare of restoring your identity and your credibility later.

References

1. "Bank One Online Puts Customer Account Information at Risk", Interhack Corporation, 10/25/2000, Revision 1.0
URL: http://www.interhack.net/pubs/bankone-online/

2. "Secure Sockets Layer", Computerworld, 3/01/2003, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,43518,00.html

3. "Online Banking Guarantee", Bank of America, 3/14/2003, URL: http://www.bankofamerica.com/onlinebanking/index.cfm?template=security

4. Endler, David. "Brute Force Exploitation of Web Application Session IDs", iDefense, 11/01/2001, URL: http://www.blackhat.com/presentations/bh-usa-02/endler/iDEFENSE%20SessionIDs.pdf

5. Burkholder, Peter. "SSL Man-in-the-Middle Attacks", 2/01/2002, URL: http://www.sans.org/rr/threats/man_in_the_middle.php

6. “Banks compete for online customers”, The Mercury News, 9/22/2002,
URL: http://www.philly.com/mld/philly/business/technology/4175612.htm

7. “How SSL works”, Netscape, 2/22/2002,
URL: http://developer.netscape.com/tech/security/ssl/howitworks.html

8. “BlackICE™ PC Protection”, BlackIce Product Page, 5/5/2003,
URL: http://blackice.iss.net/product_pc_protection.php