Hacking Online Banking and Credit Card Transactions – And How to Prevent It

del.icio.us

Discuss in Forums {mos_smf_discuss:Hoffman}

By Daniel V. Hoffman, CISSP, CWNA, CEH

Dan is at it again. His very popular column on wireless hacking and how to prevent it is generating a lot of interest with over 125,000 page views and counting. Paraphrased comments on digg.com have ranged from 'Fantastic' and 'Awesome' to 'That's not really hacking' and 'Where's the beef.' Well... just remember that you asked for it!

The Scenario

You go to a coffee shop for a cup of coffee and to utilize the shop’s Wi-Fi HotSpot to surf the web. You connect to the hotspot network and decide to perform some online banking or to purchase something online. By the way, this could happen to you at home, as well. As an end-user, you feel quite secure, as you see the lock in the bottom corner of your Internet browser, symbolizing that the online banking or online credit card transaction is safe from prying eyes. Your data, including username, password, credit card info, etc. will be encrypted with 128-bit encryption. So it's secure, right?

It is not uncommon to perform banking and to purchase products online with your credit card. It is also a common thought that doing so is secure, as this is done via SSL. For the most part, this is true and the sessions are secure. Discover Card, for example, posts the following statement on their website:

Figure 1

The problem is that it is not “virtually impossible” for someone else to see your data, such as login information or credit card numbers. It can actually be relatively easy, as you’ll see, if you as an end-user are not knowledgeable about how you can be exploited and know the signs that this is occurring.

Figure 2 (Indicates a Secure SSL Session)

Continuing with the scenario, what you didn’t realize is that a hacker has intercepted your Online Banking login credentials and credit card information and can now log into your Online Banking Website or purchase items with your credit card. How is this possible, since SSL was used and is hard to break? The answer is that you made a fatal mistake that subjected you to an SSL Man-in-the-Middle (MITM) attack.

The Attack

The fatal flaw that enabled the sensitive information to be stolen is possible when an end-user is not properly educated on an easy to do and well-known SSL exploit – SSL MITM.

Here’s how it’s done:

The hacker goes to coffee shop and connects to the same Wi-Fi network you are connected to. He runs a series of utilities to redirect other user’s data through his machine. He runs a number of other utilities to sniff the data, act as an SSL Certificate Server and to be the Man-the-Middle. The following diagram shows a very simplified graphic of how your SSL Banking session should work under normal conditions, then how it would work during an attack:

Figure 3

Figure 4

An important concept to grasp here is that a certificate is used to establish the secure SSL connection. This is a good thing, if you have a good certificate and are connecting directly to the website to which you intended to use. Then all your

data is encrypted from your browser to the SSL website where the bank’s website will use the information from the certificate it gave you to decrypt your data/credentials. If that is truly the case, then it is pretty darn hard for a hacker to decrypt the data/credentials being transmitted, even if he is able to sniff your data.

This is a bad thing if you have a “Fake” certificate being sent from the hacker, and you are actually connecting to his machine, not directly to the bank’s website. In this case, your credentials are being transmitted between your browser and the hacker’s machine. The hacker is able to grab that traffic, and, because he gave you the certificate to encrypt the data/credentials, he can use that same certificate to decrypt your data/credentials.

Here are the exact steps a hacker could use to perform this attack:

The first thing he would do is turn on Fragrouter, so that his machine can perform IP forwarding

Figure 5

After that, he’ll want to direct your Wi-Fi network traffic to his machine instead of your data traffic going directly to the Internet. This enables him to be the “Man-in-the-Middle” between your machine and the Internet. Using Arpspoof, a real easy way to do this, he determines your IP address is 192.168.1.15 and the Default Gateway of the Wi-Fi network is 192.168.1.1:

Figure 6

The next step is to enable DNS Spoofing via DNSSpoof:

Figure 7

Since he will be replacing the Bank's or Online Store’s valid certificate with his own fake one, he will need to turn on the utility to enable his system to be the Man-in-the-Middle for web sessions and to handle certificates. This is done via webmitm:

Figure 8

At this point, he is setup and ready to go, he now needs to begin actively sniffing your data passing through his machine including your login information and credit card info. He opts to do this with Ethereal, then saves his capture:

Figure 9

He now has the data, but it is still encrypted with 128-bit SSL. No problem, since he has the key. What he simply needs to do now is decrypt the data using the certificate that he gave you. He does this with SSL Dump:

Figure 10

The data is now decrypted and he runs a Cat command to view the now decrypted SSL information. Note that the username is “Bankusername” and the password is “BankPassword”. Conveniently, this dump also shows that the Banking site as National City. FYI, the better, more secure banking and online store websites will have you first connect to another, preceeding page via SSL, prior to connecting to the page where you enter the sensitive information such as bank login credentials or credit card numbers. The reason for this is to stop the MITM-type attack. How this helps is that if you were to access this preceeding page first with a "fake" certificate and then proceeded to the next page where you were to enter the sensitve information, that page where you would enter the sensitive information would not display. That is because the page gathering the sensitive information would be expecting a valid certificate, which it would not receive because of the Man-in-the-Middle. While some online banks and stores do implement this extra step/page for security reasons, the real flaw in this attack is the uneducated end-user, as you'll soon see:

Figure 11

With this information, he can now log into your Online Banking Account with the same access and privileges as you. He could transfer money, view account data, etc.

Below is an example of a sniffed SSL credit card purchase/transaction. You can see that Elvis Presley was attempting to make a purchase with his credit card 5440123412341234 with an expiration date of 5/06 and the billing address of Graceland in Memphis, TN (He is alive!). If this was your information, the hacker could easily make online purchases with your card.

Figure 12

Also Real Bad News for SSL VPN Admins

This type of attack could be particularly bad for corporations. The reason for this is that Corporate SSL VPN solutions are

also vulnerable to this type of attack. Corporate SSL VPN solutions will often authenticate against Active Directory, the NT Domain, LDAP or some other centralized credentials data store. Sniffing the SSL VPN login then gives an attacker valid credentials to the corporate network and other systems.

What an End-User Needs To Know

There’s a big step and end-user can take to prevent this from taking place. When the MITM Hacker uses the “bad” certificate instead of the “good”, valid certificate, the end-user is actually alerted to this. The problem is that most end-users don’t understand what this means and will unknowingly agree to use the fake certificate. Below is an example of the Security Alert an end-user would receive. Most uneducated end-users would simply click “Yes”… and this is the fatal flaw:

Figure 13

By clicking “Yes”, they have set themselves up to be hacked. By clicking the “View Certificate” button, the end-user would easily see that there is a problem. Below are examples of the various certificate views/tabs that show a good certificate compared to the bad certificate:

Figure 14

(Good Certificate) (Bad Certificate)

Figure 15

(Good Certificate) (Bad Certificate)

Figure 16

(Good Certificate) (Bad Certificate)

How an End-User Can Prevent This

-

Again, the simple act of viewing the certificate and clicking “No” would have prevented this from happening.

-

Education is the key for an end-user. If you see this message, take the time to view the certificate. As you can see from the examples above, you can tell when something doesn’t look right. If you can’t tell, err on the side of

caution and call your Online Bank or the Online store.

-

Take the time to read and understand all security messages you receive. Don’t just randomly click yes out of convenience.

How a Corporation Can Prevent This

-

Educate the end-user on the Security Alert and how to react to it.

-

Utilize One Time Passwords, such as RSA Tokens, to prevent the reuse of sniffed credentials.

-

When using SSL VPN, utilize mature products with advanced features, such as Juniper’s Secure Application Manager or Network Connect functionality.

Conclusion

This type of attack is relatively easy to do in a public Wi-Fi hotspot environment. It could also easily happen on a home Wi-Fi network, if that Wi-Fi network isn’t properly configured and allows a hacker to connect to that home network (See Essential Wireless Hacking Tools for more info on securing your home network). An educated end-user and sound security practices by corporations can protect your valuable data.