8-1-2008

Safer Practices in Financial Transactions on the Internet

Jeffrey Barlow
Pacific University

Follow this and additional works at: http://commons.pacificu.edu/inter08

Recommended Citation

This Editorial is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 8 (2008) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Safer Practices in Financial Transactions on the Internet

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: http://commons.pacificu.edu/inter08/22
Safer Practices in Financial Transactions on the Internet

Editorial by Jeffrey Barlow

Introduction

We have often addressed issues relative to financial transactions on the Internet. [1] So far as the impact of the Internet is concerned, on-line financial security should, surely, have long since become a topic on which very little remains to be said. Unfortunately this is not true, but there is much information available to help us guard ourselves against electronic mishaps. Here we address an important new study on safe web practices for both financial institutions and their customers.

Most of us are now so accustomed to electronic transactions, whether through E-bay or Amazon.com or the thousands of other possibilities that we tend to think little about them. We are often amused by obvious phishing scams [2] though, incredibly, many still fall victim to them.

Yet the losses to various forms of electronic fraud continue to mount annually. [3] It was once possible to easily find annual estimates of such losses. We are now well beyond any simple accounting. The schemes have become so varied and so common that no satisfactory estimate is possible.

However, there are many signs that electronic fraud, despite all precautions, is probably many times more costly than ever before. One such index is the number of attempts at such fraud. If the industry were not paying, it would die out. Rather it has become steadily more pervasive and more sophisticated. So have the counter-measures, ranging from simple insurance offers to elaborate electronic protection software and sites. Our vocabularies have enlarged to include new meanings for such terms as "virus" and "worm" and new words like
malware and keyloggers. Surely almost all of us have met or read about a victim of identity theft.

Yet, while our awareness has surely increased so has our reliance upon electronic transactions. I recently had the experience of opening with my daughter a new account at a local bank into which I will make electronic deposits from Oregon, while she later will enthusiastically make withdrawals from Beijing. I asked the very efficient and knowledgeable bank officer about security in such transactions. And of course, we weren’t discussing transactions between two New York banks, but one between perhaps one of the least sophisticated nodes of the banking industry, small town Oregon, and the home of many of the world’s most sophisticated hackers, China. "Oh, no problem," the officer assured me.

We eventually completed our transactions, somewhat slowly because the entire computer system of this nation-wide bank was down and data had to be hand-written onto forms for later entry.

An Important Recent Study: Following our transactions, I returned to my office at Pacific University's Berglund Center for Internet Studies to find an e-mail from Ben Elliott, our former Systems Manager, calling my attention to a sophisticated new study of security design flaws on financial websites. This study is the centerpiece for this editorial. [4]

The study has been widely reported upon, by the usual pointing-with-alarm journalists, and by those hoping to sell us relief for such fears. The paper is a carefully nuanced one and its conclusions are, I feel, often overstated in the subsequent reports on its appearance. One such alarmist notice, for example, shouts "75 Percent of Banking Websites Vulnerable To Cyber Thieves Study Shows" while hawking software and services. [5]

In fact, what the paper seems to me to tell us is not that these banks (The authors studied the electronic sites of 214 U.S. financial institutions!) are necessarily vulnerable, but that flaws in their page designs make it
difficult or impossible for even sophisticated users to judge whether or
not they are vulnerable.

This conclusion, embedded as it is in an excellent analysis, is actually
more valuable to us than would be the extremist views of its findings.
None of us wants to lose our ability to use sites such as those at financial
institutions. We all, however, should want to become more sophisticated
users of such sites.

While the study is at points pretty heavy going, it can certainly be
recommended for anyone wanting to better understand best practices in
financial sites, and to better understand safe use of such sites. It will also
be of great interest to anyone capable of reading source code with some
awareness, meaning anyone who has made a web page.

The Study's Conclusions: I shall try to boil down some of the study’s
conclusions for nonprogrammers, a group to which I regretfully belong.
We are not by any means suggesting that the following discussion will
make you safe on the Internet nor that you should use it for a primer
with which to berate your banking officers. Reading it will make you a
more secure Internet user.

A preliminary discussion of the study's methodology is in order because
it reveals some of the limitations of the study. The authors used a
combination of software to automatically scan and save the pages easily
accessible at financial institutions. They then used other software to
identify potential weaknesses in such sites. They tried throughout to
draw only very conservative conclusions, and gave the benefit of the
doubt to many apparently flawed pages.

However, their purpose was not to specifically identify vulnerabilities
open to hackers, but to find badly designed sites that would prevent
concerned users from assessing the relative security of such pages. In
short, the authors believe that good design should let consumers make
reasoned judgments about security. Bad design then, is not necessarily
indicative of vulnerabilities, but it erodes, or should erode, a user’s trust in such sites.

The authors repeatedly state that pages with design flaws are an indication that the flaws are not well understood by those responsible for security. [6] And, if we are to draw an extremist conclusion of our own from the study, we will go farther to say that this lack of awareness makes us at least question the designers’ knowledge of security in general. It may be that underlying security devices not immediately accessible to the study team or to the wary user are robust, even bullet-proof, but to fail to follow best practices in design may well be an indication of additional potentially compromising flaws in security itself.

The Importance of a Chain of Trust: What then, are best practices, either for financial institutions or for users? First, users must have a complete "chain of trust." [7] Simply put, this means that pages that are secured according to best practices must be easily distinguishable as such. This means for us, at a minimum, that the site should use "SSL-protected pages" (Secure Socket Layer) or some variant upon them. Such pages are on an authenticated server: the user knows with a high level of confidence that the server is what and where it claims to be. It is this protocol that produces the often tiresome "Warning you are leaving a Secure environment for an insecure environment. Do you wish to do so?" or its equivalent. At the very least, if we leave an SSL protected page in a financial site for an unprotected one, we should be warned.

It is not unusual for financial sites to fail to provide this level of warning. In fact, the study contends, 30% of financial sites break the chain of trust. Most commonly this consists of sending the user from a secured page on an authenticated server to an insecure page on the same server.

The problem is that this insecure page is much more easily accessible to a determined hacker (or to an insider) who may change data on the page to direct a user to another site with evil intentions, or perhaps may introduce malware to capture data, or may not properly encrypt data
moving from that page to other Internet sites. So, as a general principle, a user should never leave an SSL (there are variations on this protocol which are also secure) environment without being warned.

Even worse, not infrequently the user may be directed from the authenticated server to a server controlled by others, most probably by a firm offering additional services to the institution. We cannot know that the new destination is insecure; but we can state that we should have been warned that we were leaving so that we could choose to examine that new server’s authenticity by looking at its certificate. Often, that certificate will show ownership not by the financial institution or the company providing the services, but perhaps by a third party which owns the second company. Our “chain of trust” is now properly somewhat attenuated.

How can we know that we have fallen afoul of any of these problems? Most basically, the URL throughout our journey in a financial site should always read HTTPS, meaning that it uses SSL protocols or one of the several common variations of it. On many pages we may also find a graphic representation of a lock and a statement that the page follows certain practices.

I suggest that to get an idea of how your own financial institution works, you go to its main page and carefully read all the information on security. Note that the main or welcome page is probably not SSL protected. But once you enter your user name and password you should be in HTTPS designated pages, or at least warned you are not. At my bank’s site I was directed to an unsecured page without warning, but I was also kicked out of my personal site and had to log back in if I wanted to work with my accounts. This is probably less than ideal security as it did expose me briefly to an unsecured page, but I was, as best I am capable of determining, at least in the bank’s sites throughout.

This is important because SSL requires that our server examine the site’s certificate and affirms to our server and then to our browser that the site is what and where it purports to be. It also means that the data being
transferred is properly encrypted and is much less vulnerable to interception in route between the server and our browser. [8] This is, of course, emphatically not total security. Much can go wrong, particularly at our end, but it means that the site is doing its best, given current practices.

Secure Login: The second issue that should cause the aware reader concern is the security of login options. This is particularly problematic. My own bank places my user name login options on an unsecured page. This is probably because they want as much information as possible available to a user with a minimum of hassles. It is, however, not a best practice according to authors Falk, Prakash, and Borders in their study. The bank does not give me a password option until I am in an SSL environment so it is probably still quite secure. Some banks, however, at least at the time the study was done, do not. This means that it is possible that an entire page has been spoofed or altered specifically to misdirect the user into harm’s way.

An aware user should probably check his or her bank’s pages and at least have a chat with an officer in the local branch if it provides both login and password in an insecure environment as indicated by the lack of an HTTPS url. The local officer will probably have to make some phone calls, but you will perhaps learn a bit more about your own security, and your bank may well learn something too, perhaps that many customers now care about such arcane issues.

Contact/Security Information on Insecure Pages: There are other issues that must be considered as part of login practices. Does your institution provide its security information on secure pages? Mine does not. In theory, as the authors point out, this means that such pages could be more easily spoofed (perhaps a phishing attack directs me to a phony page with a dire warning) and then asks me to change my password? Or I am directed to call a given phone number for some necessary procedure which results in me giving up personal data? If the security pages are in a secure environment I am less likely to have been fooled, and the page highly unlikely to have been spoofed.
Inadequate Policies for User IDS and Passwords: None of us like unwieldy passwords or IDS. Few of us change them regularly. The worst practices here are easily summarized:

- Your institution should not permit you to use social security numbers or email addresses as user ids or passwords.

Social Security numbers and email addresses are terribly easy to collect. If you are in any way identifiable as someone likely to have even moderate resources, it is worth the time of a criminal to collect such data on you, perhaps by purchasing it from yet other thieves. Alternatively, you may simply be unlucky enough to be included in one of the many massive thefts of unencrypted data as per any number of recent cases. If your institution lets you use either of these identifiers, change them immediately on that institution’s site, and at the first opportunity chide them for the practice.

Why should we be concerned about the institution’ practices once we have protected ourselves against them? I was once studying the Nigerian email scams (See references at note 1 below.) and asked my bank for permission to open a false account and to place a minimal amount of money in it so that I could follow up the chain of the scam. I offered to do anything reasonable to indemnify the bank, to produce my bona fides, to get the FBI involved from the beginning, etc.

I was quickly referred to a very alarmed security officer at the home office. This person could barely speak of the sophistication of hackers, Dutch, Russian, Nigerian, unknowns, all manner of lurking threats, without sobbing. I was told that if such master criminals got one valid account number, which I proposed to give them of course, as part of my study, they would then be able to identify nearby accounts in the numbered sequence with more certainty, and perhaps hack into them. So none of us want any accounts in our institutions to be vulnerable; one security hole may well open others.
Email Security: Worst of all possible bad practices by financial institutions or by any user, is to move critical information by email. Your email is not secure, no matter where it is stored or how it is sent. One very sophisticated user recently told me that storing email in one of the currently popular free email services on the web was equivalent to leaving it in a public restroom, and the archives were about as difficult to rummage through.

Conclusion: This editorial has not been a light-hearted romp, either to write, or, I am sure, to read. It is dismaying to think that we as individuals should bear so much responsibility for protecting ourselves in environments that, after all, we are paying no small amount of our limited resources to enter. But, sadly, this is the fact. Educate yourself. Save yourself and others. Lobby for best practices, including web site design that permits you to make reasoned judgments about the level of security it provides.

[1] While many of these issues are so familiar to even unsophisticated users of the Internet as to have become common knowledge, surprisingly, all of them still present dangers to the unwary.


Although many of the problems discussed in these pieces are now at least 6 years old, little progress has been made in solving them.
[2] It is hard to imagine a reader who is at all interested in Interface and also is unfamiliar with this term, but it is a generic name for attempts to inveigle a user into providing information or better, money, to an online criminal. Usually these are some variant on either promising something for nothing, or, ironically, to providing data to protect yourself against other schemes: "You need to reregister your user name/password/social security number/other valuable data to continue using your bank/E-Bay", etc.

[3] To see the endless creativity of these attempts, and the clever way in which they often establish trust by tying into recent events, such as rebate checks, see the FBI site at: http://www.fbi.gov/cyberinvest/escams.htm


The study can be downloaded in PDF from:
http://www.eecs.umich.edu/~aprakash/ See references at "Some Sampling of My Research"

[5] See report at:


[7] As the PDF is not paginated we resort here to citing sections of the study, here, for example section 3.1.

[8] I have found the materials at PCmag.com useful in understanding these issues.
See:
http://www.pcmag.com/encyclopedia_term/0,2542,t=SSL&i=51944,00.asp

See also Bank of America's statements about security found at: https://www.bankofamerica.com/privacy/Control.do?body=privacysecu_bankofamerica for an example of very thorough explanations.