4-1-2006

CYBERJACKED! Again... and Again...

Jeffrey Barlow
Pacific University

Follow this and additional works at: http://commons.pacificu.edu/inter06

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 6 (2006) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
CYBERJACKED! Again... and Again...

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: http://commons.pacificu.edu/inter06/16
We last wrote about cyberjacking, the general category of crimes (at least we hope that somewhere in the world they are crimes) of misusing another’s World Wide Web site for your own purposes, in the spring of 2004. [1] The fact that we have not mentioned the topic in almost two years is not due to the fact that there have not been additional incidents. Rather, like everyone who manages a large web presence, we have come to accept a certain low level of incidents as “normal.” We also assumed that there was not much to be learned from additional incidents, as they tended to be similar to previous ones. However, the situation has changed rather dramatically. Here we discuss a new wrinkle, having one’s electronic files totally downloaded to another’s server, in one example below, the server of the Iranian Ministry of Science.

After the incidents we discussed in 2004, we altered our security practices so as to minimize problems. This has had mixed consequences; problems have become less frequent. But unfortunately, nearly all such procedures amount to some form or other of restricting access.
In some cases, the loss to learning and research has been significant, we feel. Our Berglund Center real-time internet-protocol courses with China, for example, have produced a wealth of interaction between American students and instructors and their Chinese counterparts. [2] Our Fall 2005 class, “Love and Modernity” had thousands of electronic bulletin board messages (BBS) in which Chinese and American college students earnestly discussed the advantages and disadvantages of their own courting and marriage rituals, not to mention issues of gender and sexuality.

I recently read a book mss on related topics which was submitted for possible publication at a large commercial publisher. This miss was based on a good deal less information on contemporary Chinese practices and beliefs than we had available on the web for more than six months, open to any researcher.

.03 The Introduction of Pornographic or Inappropriate Content (return to index)

Unfortunately, the information on Chinese social practices was also open to any pornographer or spammer. These send out “Spiders” or “Bots” to search the Internet endlessly for unprotected BBS postings. These lower forms of life (Here we refer to both electronic and organic forms.) were posting into our application advertisements for sexually oriented webcams, graphic graphics, etc.

We had no choice but to remove the materials, either that or comb through thousands of postings looking for links to such sites. And now such links can be embedded in any number of ways so that they are not always immediately discoverable.

.04 Loss of Access (return to index)

The approved way to avoid such problems, of course, is to make the BBS accessible only by password. However, in order to provide real security, these protocols have to be quite rigid. Too, the registration procedures are clumsy and time-consuming.

Having now had experience with several different such applications, we have seen that a percentage of users will be frustrated by some element of the registration and simply give up. Board managers must examine each and every application for registration. Often this means tracking down the electronic origins of such applications and then refusing to permit registration for those which seem not to be valid.

In addition to requiring that access to potentially useful materials must be restricted, there are other consequences to cyberjacking. One of the many good points made in the book Cyber Alert by Warren and Streeter reviewed in this issue (http://bcis.pacificu.edu/journal/2006/02/warren.php) is that various exploitations of the Internet such as cyberjacking not only threaten the immediate victim, they also threaten general confidence in the Internet itself. Such lack of consumer confidence in financial transactions, for
example, is a costly obstacle to electronic commerce.

We have had two noteworthy incidents in the last several months that were not solved by our own attempt at careful digital hygiene (another lovely term from Warren and Streeter’s work). In one case we were notified by the publisher of quite a large digital encyclopedia, and one with a very high level of authority, that he was being forced to take down one of our sites due to embedded links to pornographic sites. These apparently masqueraded as real links in our site, but when clicked upon took the unwary consumer of information in a scholarly article on traditional Vietnam martial arts to quite a different level of content. As here is considerable cachet in having one’s site referenced by such an encyclopedia, we took immediate action. But we could not locate any such links.

Going back to the email which reported the problem, we noticed that yes, it was our material. But it was not on our site. It had been “mirrored” or downloaded into to a martial arts supply house which was presumably using it to attract customers. But this entrepreneur then had his corporate server hacked and pornographic links inserted. We envisioned a very expensive legal process, but the encyclopedia, when we pointed out the actual situation, simply solved the problem by deleting the link to the bogus mirror and going directly to our site.

This incident gave us a new perspective on having our material “borrowed” by other sites. In our own sites, we are very careful never to copy more than a few sentences from other sites without getting permission, never to copy graphics without permission and require strict citations even for legal or “fair use” of others’ content. And never would we download an article or directory to our own site.

However, there is invariably a sort of compliment implied when one’s own content is downloaded to another site. Not only does it usually seem harmless, it may even, depending on the nature of the links in the materials, enhance our own traffic. But now we were suffering from a sort of second-level cyberjacking.

.05 Controversial Mirrors (return to index)

Then several weeks ago, quite a different and much more complicated situation developed. As this situation is as yet unresolved, let me lead the reader through the actual discovery process so as to better illustrate the issues. A student in one of my classes forgot the link to the class web site and knowing that the pages could be found through my own home page, ran a Google search on “Barlow, Jeffrey”: this will take you to such a search:


Go ahead and click on it, preferably in a second window.

Now, in your second window, you are in the familiar Google listings page. But before clicking on
the blue link, please look carefully at the fourth line down where the full server address, on my browser, appears in green:

journals.iranscience.net:800/mcel.pacificu.edu/mcel.pacificu.edu/as/faculty/barlow.html

Now click on the blue anchor and go, after a relay through an older page, to:

http://journals.iranscience.net:800/mcel.pacificu.edu/mcel.pacificu.edu/history/dept/barlow.html

Hopefully by now you have noticed that you are not, in fact, any longer in the Berglund/MCEL servers, but in the portal of the Iranian Ministry of Science! To clarify what has happened, still in your second window, go to: http://journals.iranscience.net/ this is the index page for the directory which incorporated some of our content, including my home page.

This situation requires additional explanation: There are applications available that will permit a user to download an entire site or part of a site from the Internet to their own computer. The user can set the level of the process so that it will download associated content one click deep, two clicks deep, down presumably to the Nth level. This has happened to our site, in, apparently, an attempt to quickly build a reputable portal on computing at the Iranian Ministry of Science. Observe the link “Journal of AHC” in the left hand column of the two-column list. This Journal, of which I am the founding editor, is on our MCEL server at Pacific University. It is the first, and to our knowledge, only peer reviewed e-journal in the fields of history and computing on the WWW. This was apparently the target of the borrowing process but it scooped up many of our related pages, including my own home page.

If this were just a simple mirror or a legitimate copy of our site, no real harm would have been done. However—and here we are now in the realm of speculation—we believe that the Iranian techs also “Googlebombed”—that is, they manipulated the Google search process to quickly raise their own directories to the top of the Google listings. Thus, a search on my name takes the querent to a directory in Iran with the “borrowed” pages on it.

Other than the obvious political issues involved in having one’s content borrowed by a potentially contentious site, such as the Iranian Ministry of Science, there are additional problems. The Persian techs did not take all the directories and applications on our servers. A reader or a student cannot, for example, now get from my syllabus pages to the BBS associated with that class on the Persian copy, presumably because the Iranians do not run PHP-based apps on their server. Neither are the pages they downloaded usually the most updated version of the pages found; these are on our own servers but will not be found by a Google search, because that search will send you on the manipulated search path.

We have been through a number of channels to find out more about this particular example of cyberjacking. We find it a fascinating one for a variety of reasons. The incident seems to be almost a text book example of the difficulties encountered when local practices, beliefs, and electronic content are suddenly “globalized.” We wish we could tell you how to either prevent or solve this problem, but we cannot yet do so. All we can say at this point is that the Internet has
become a labyrinthine environment. We will report back as soon as we have additional information.

0.06 Notes (return to index)


This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3238].

2 THOUGHTS ON “CYBERJACKED! AGAIN... AND AGAIN...”

nigeria
on February 3, 2014 at 1:40 AM said:

Whats up. Incredibly nice internet site!! Guy .. Beautiful .. Incredible .. I am going to bookmark your website and take in the feeds additionally...I am satisfied to uncover plenty of helpful details right here from the article. Thanks for sharing...

nigeria entertainment news
on February 4, 2014 at 10:42 AM said:

Awesome talk! Thank you so much for hosting Great.