Chapter 91
URL Manipulation and the Slippery Slope:
The Case of the Harvard 119 Revisited

Michael E. Whitman
Coles College of Business, Kennesaw State University, USA

Humayun Zafar
Coles College of Business, Kennesaw State University, USA

ABSTRACT

While computer ethics and information security courses try to teach computer misuse and unauthorized access as clear black and white examples, when examining the use and potentially misuse of URLs the discussion becomes less clear. This paper examines a number of computer use ethical scenarios focusing on the modification of URLs within Web browsers. Using the documented case of applicants to several Ivy-league schools as a discussion point, this paper presents a survey of U.S. students enrolled in information security and computer ethics classes, asking at what point does modifying the URL become hacking, and at what point does it become unethical. The findings of this study are discussed.

INTRODUCTION

In March 2005, Harvard University made headline news by summarily rejecting the applications of 119 admissions candidates who allegedly accessed an unauthorized section of ApplyYourself's website, gaining access to their own admissions reviews. ApplyYourself is an application offered by Hobsons, a student recruitment, enrollment and retention management company. At other universities including MIT's Sloan School of Management, Stanford's Graduate School of Business, Duke's Fuqua School of Business, and Dartmouth's Tuck School of Business, an undisclosed number of additional students performed the same actions, and were either denied admission or not, depending on the particular institution's perspective on the applicants' actions. While the vulnerabilities that allowed those students to access the unauthorized material have long been resolved, academic classrooms are still visiting and revisiting the ethical and legal implications of these student's action.

Harvard University's Business School Dean labeled the applicants' actions as "unethical at best

DOI: 10.4018/978-1-4666-6433-3.ch091

-- a serious breach of trust that cannot be countered by rationalization" (Weisman, 2005). While the university stopped short of calling the applicants hackers, the issue raises the question – 'At what point does URL manipulation become hacking?'

URL MANIPULATION

The Uniform Resource Locator (URL), better known as a Web address, has become integral to modern organizations. Some organizations even use their URL as their company name and identity. Web site file names, just as with any manmade document, are subject to typographical errors; and Web site source code is subject to the same programmer errors as other applications. However, the global access to Web site content creates a dramatically increased potential for intentional and unintentional modification and exploitation. With an estimated 2.4 billion Internet users worldwide, the risk of misuse and abuse of Web site content involving the URL has increased almost 700 percent since 2000 (Internet World Stats, 2012).

URL manipulation, also known as HTTP manipulation, is a set of attacks against Web based systems specifically focusing on attempts to gain access to unauthorized information based on a direct manipulation of the URL. URL manipulation attacks are part of a larger group of application-oriented attacks which include cross-site scripting attacks and SQL injection attacks. However, while there is a great deal of previous work on examining Web application vulnerabilities, buffer overflow attacks and protection against SQL injections and cross-site scripting, there is a conspicuous lack of research examining general URL manipulation.

PREVIOUS WORK

Past research in this area has predominantly revolved around ethics in IS (Banerjee, Cronan, & Jones, 1998; S. Harrington, 1996; Leonard & Cronan, 2001). Ethics according to these studies refers to informal norms and behaviors that may help deal with situations for which there are no formal rules or policies (Dhillon & Backhouse, 2000). A limitation in this line of research is that there is a general difficulty in classifying behaviors as being ethical or unethical. It is not always straightforward. According to prior studies (Calluzzo & Cante, 2004), some undesirable behaviors related to use of organizational IT property were viewed as being neither ethical nor unethical. An example of such behaviors is downloading files at the workplace or at an educational institution from the Internet for personal use.

Some work has investigated the issue of training employees on how to integrate ethics into decision making and behavior related to the recommended use of computers (Harrington & McCollum, 1990). Anderson et al. (1993) focused on the practical implications of the ACM code of ethics, with a number of illustrative case studies. There has also been some extensive research done in the area of computer and cyber-crime (Cymru, 2006; Kshetri, 2006; Tavani, 2000). Braunfeld and Wells (2001) provide a concise introduction to issues such as copyrights, patents, and trademarks. Digital Millennium Copyright Act and Digital Rights Management, alongside their legal ramifications have also been discussed (Camp, 2003; Gibbs, 2000; Liu, Safavi-Naini, & Sheppard, 2003).

METHODOLOGY

In order to better understand contemporary perspectives on URL manipulation, a survey was created to examine a spectrum of possible URL manipulation situations. In these scenarios, situations involving the modification of a university's URL were presented allowing the respondent to indicate two perspectives:

1. Whether the activity presented was viewed as ethical or unethical – as measured on a 5 point