

Term Paper Proposal - Firesheep

By Girum Ibssa

CSC 300: Professional Responsibilities

Dr. Clark Turner

April 16, 2013

Abstract

Firesheep is an extension for the Firefox web browser that wraps session hijacking logic in a simple GUI. Created by Eric Butler and Ian Gallagher, Firesheep's motivation was described by its creators: "We're bringing up this tired issue to remind people of the risks they face, especially when on open WiFi networks, and to remind companies that they have a responsibility to protect their users. To drive this point home, we are releasing an open source tool at ToorCon 12 which shows you a 'buddy list' of people's online accounts being used around you, and lets you simply double-click to hijack them" [5].

Was it ethical to release this software? The Association for Computer Machinery defines a Code of Ethics stating that "software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession" [4]. Firesheep is built specifically to allow untrained users to hijack browser sessions from unsuspecting victims [2], which directly contradicts Section 1.03 of the Code of Ethics: "1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good." [4]. However, Firesheep's release prompted many large software companies to quickly fix the security holes that Firesheep was designed to expose [6]; the companies were slow to fix it before Firesheep's release [6]. Firesheep was detrimental to public welfare in the short term, yet its long term benefit to the community outweighed its initial detriment enough to make it an ethical product.

1 Facts

Eric Butler describes in his blog: “When logging into a website you usually start by submitting your username and password. The server then checks to see if an account matching this information exists and if so, replies back to you with a ‘cookie’ which is used by your browser for all subsequent requests [2].

“It’s extremely common for websites to protect your password by encrypting the initial login, but surprisingly uncommon for websites to encrypt everything else. This leaves the cookie (and the user) vulnerable. HTTP session hijacking (sometimes called “sidejacking”) is when an attacker gets a hold of a user’s cookie, allowing them to do anything the user can do on a particular website. On an open wireless network, cookies are basically shouted through the air, making these attacks extremely easy” [2]. Butler continues with his description of the “problem that has been talked about to death” and how it remains to be solved [2].

At its time of release, Firesheep worked on the following sites: Amazon, Basecamp, bit.ly, Enom, Facebook, FourSquare, Github, Google, Hacker News, Harvest, The New York Times, Pivotal Tracker, Twitter, ToorCon: San Diego, Evernote, Dropbox, Windows Live, Cisco, Slicehost, Gowalla, Flickr and Yahoo [1].

Known facts that are not disputed that lead to your question. Do not judge these facts or make anything like an argument for an answer in here. Just note the facts that give us the general background and end them with the facts leading to the controversy you are interested in. The reader should naturally be asking the question you’ll be asking by that point in your paper. In general, attach your facts to a specific case, the more specific and detailed the facts, the better for your analysis. Cite all facts to their sources. [?]

2 Research Question

Your research question – this is the ethical question you are interested in answering. It should be one simple sentence and lead to a yes/no answer. It needs to be very narrowly focused, specific, and not abstract at all. It’s best to question a detailed case in the general area of your interest. Open ended questions are very hard to answer. [?]

3 Extant arguments

Extant arguments – this is where you gather the arguments made by others interested in the same question. No judgments, just repeat their arguments for the answer in the best possible light from the arguer’s perspective. Cover both sides of your question (the “yes” side and the “no” side) to get a complete picture of how others are thinking about it. Do not include any general ethical principles in here unless they are explicitly written up in the arguments. Cite all arguments to their sources. [?]

4 Applicable analytic principles

Applicable analytic principles – give a list of the basic ethical (and other) principles you’ll rely on to come up with your analysis, include several explicit principles from the SE Code of Ethics, deontological principles, utilitarianism (rule-utilitarianism) as well as others that will aid you. Indicate generally how they apply to your specific case. Cite any additional facts or principles you’ll need. Cite to sources for the principles you list. [?]

5 Abstract of Expected Analysis

Give a short abstract of the basics you expect to analyze and present in your paper. Divide it into sections that make sense for your work.

One way would be to: a) start with deontological perspectives as a section where you analyze those arguments based on the inherent ethics of the act itself rather than the results or trade-offs; then, b) use a utilitarian perspective and list the appropriate analyses of the trade-offs and stakeholders to define the most desired results and how to get them. Be explicit about the trade-offs (what value is balanced against what other value, which stakeholders win, which stakeholders lose...) What is the “utility” in “utilitarian” in your case – what value do you want to advance the most (derived from the general utilitarian “happiness”)? How do you maximize (or optimize) it?

Note that the SE Code should be the center of your ethical analysis (and remember that it includes both deontological and utilitarian [and more] principles you can utilize). Estimate where you’ll end up for your answer (you can change your mind in the final paper!). Keep referencing sources for any additional facts, quotes, or other information you might use here. [?]

References

- [1] E. Butler, “Firesheep source code (github).” [Online]. Available: <https://github.com/codebutler/firesheep/wiki/Handlers>

Source code and documentation for Firesheep

- [2] —, “Firesheep,” October 2010. [Online]. Available: <http://codebutler.com/firesheep/?c=1>

Eric Butler’s personal blog post detailing Firesheep.

- [3] —, “Firesheep, three weeks later: Fallout,” November 2010. [Online]. Available: <http://codebutler.com/firesheep-three-weeks-later-fallout/>

Eric Butler’s personal blog post detailing the fallout of Firesheep

- [4] A. for Computing Machinery, “Software engineering code of ethics and professional practice.” [Online]. Available: <http://www.acm.org/about/se-code>

The ACM Code of Ethics that this paper uses to define ‘ethics’

- [5] S. Gibson, “Security now! episode 272 (transcript),” October 2010. [Online]. Available: <http://www.grc.com/sn/sn-272.htm>

Transcript of a podcast in which Leo Laporte and Steve Gibson discuss Firesheep.

- [6] B. Kennish, “Widgetjacking: Why more social widgets mean less secure wi-fi,” November 2011. [Online]. Available: <https://blog.disconnect.me/widgetjacking>

A blog discussing ”life after Firesheep”