Term Paper Proposal - Firesheep

By Girum Ibssa

CSC 300: Professional Responsibilities

Dr. Clark Turner

April 18, 2013

Abstract

Firesheep is an extension for the Firefox web browser that wraps Wireshark (an existing piece of session hijacking and packet sniffing software [1]) in a simple GUI [3]. 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" [9].

Was it ethical to release this software? Eric stated in his release of Firesheep that "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 is a widely known problem that has been talked about to death, yet very popular websites continue to fail at protecting their users" [4]. Yet the use of wire sheep may be illegal in the US and beyond [10]. I will show that Firesheep was indeed ethical to release due to SE Code 1.04, the requirement for Software Engineers to fully disclose any potential software danger to the public [8].

1 Facts

1.1 Description of Firesheep

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 [4].

"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" [4]. Butler continues with his description of the "problem that has been talked about to death" and how it remains to be solved [4].

Qualified hackers were already able to perform session hijacking like this well before the release of Firesheep, using the program 'Wireshark' (which Firesheep is built on top of). [1].

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 [3].

1.2 Definition of the ACM Code of Ethics

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" [8].

1.3 Firesheep's adherence to said Code of Ethics

Firesheep's release was intended to allow the general public perform session hijacking on suspecting or non-suspecting victims, with consequences that may not be "beneficial and respected." However, Firesheep's release prompted many large software companies to quickly fix the security holes that Firesheep was designed to expose [12]; the companies were slow to fix it before Firesheep's release [12]. From a strictly

objective point of view, Firesheep was detrimental to public welfare in the short term and was beneficial to public welfare in the long term.

2 Research Question

Was it ethical to release Firesheep to the public?

3 Extant arguments

3.1 In Favor of Firesheep's release

3.1.1 Eric Butler's argument

Eric Butler himself argues in favor of the release of Firesheep. In his article "Firesheep, a week later: Ethics and Legality", Butler states outright that "it is nobody's business telling you what software you can or cannot run on your own computer" [6]. He defends by saying that code is a form of free speech, and that we have a Constitutional right to free speech [6].

3.1.2 Mozilla's support of Firesheep

Mozilla themselves support Firesheep. Firefox (the browser for which Firesheep is an extension for) features an internal blacklist of extensions that it does not allow to work [2]. Mozilla, the creators of Firefox, specifically decided not to blacklist Firesheep [11]. Mike Beltzner, director of Firefox, praised its release: "[Firesheep] demonstrates a security weakness in a number of popular websites, but does not exploit any vulnerability in Firefox or other Web browsers" [11].

3.2 Against Firesheep's release

3.2.1 Real-world use of Firesheep may be illegal

The actual use of Firesheep, however, may be illegal [10]. Federal wiretapping laws state that it's not illegal "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public" [10]. However, Jonathan Gordan, partner at Los Angeles law firm Alson and Bird, states that "when people are accessing their social network [account], they have an expectation that whatever

they're doing is governed by the privacy settings in that network", and that a open Wi-fi network does not qualify as "readily accessible to the general public" [10].

3.2.2 Firesheep contradicts parts of the ACM Code of Ethics

Firesheep is built specifically to allow untrained users to hijack browser sessions from unsuspecting victims [4], 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" [8].

4 Applicable analytic principles

I will use SE principles 6.06, 1.04, 1.03, and 1.08 to show that Eric Butler was ethical to release Firesheep [8].

4.1 SE Principle 6.06

4.1.1 Definition

"6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest" [8].

4.1.2 Pertinence

Laws in the US, UK and beyond generally outlaw the use of Firesheep for most of its use cases [10] [14]. However, Firesheep's release managed to force software vendors to quickly fix the security holes that Firesheep was designed to expose [12]. These software vendors were notoriously slow to fix the security hole up until the release of Firesheep [12].

4.2 SE Principle 1.04

4.2.1 Definition

"1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents" [8].

4.2.2 Pertinence

Firesheep was released specifically with the intent to educate the general public of the security holes many major websites had concerning non-authenticated HTTP sessions [4].

4.3 SE Principle 1.03

4.3.1 Definition

"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" [8].

4.3.2 Pertinence

Firesheep's allows otherwise unqualified hackers to perform session hijacking on unsuspecting victims [4]. Increasing the size of the pool of people qualified to perform a crime clearly diminishes privacy and quality of life in the short term.

4.4 SE Principle 1.08

4.4.1 Definition

"1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline" [8].

4.4.2 Pertinence

Firesheep was developed in Eric Butler's free time, released in the hope that a simpler UI would give greater exposure to a long-known security vulnerability in several major websites [13]. It succeeded in this purpose [5].

5 Abstract of Expected Analysis

5.1 A Deontological Perspective

5.2 A Utilitarian Perspective

References

[1] "About wireshark." [Online]. Available: http://www.wireshark.org/about.html

Wireshark official website

[2] "Extensions.blocklist.enabled." [Online]. Available: http://kb.mozillazine.org/Extensions.blocklist.enabled

Firefox's own details of how its blacklist works, and what it was for.

[3] E. Butler, "Firesheep source code (github)." [Online]. Available: https://github.com/codebutler/firesheep/wiki/Handlers

Source code and documentation for Firesheep

[4] ——, "Firesheep," October 2010. [Online]. Available: http://codebutler.com/firesheep/?c=1

Eric Butler's personal blog post detailing Firesheep.

[5] ——, "Firesheep, a day later," October 2010. [Online]. Available: http://codebutler.com/firesheep-a-day-later/

Eric Butler's personal blog; his thoughts on Firesheep the day after release

[6] ——, "Firesheep, a week later: Ethics and legality," November 2010. [Online]. Available: http://codebutler.com/firesheep-a-week-later-ethics-and-legality/

Eric Butler's personal blog post detailing the ethics and legality of Firesheep

[7] ——, "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

[8] 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'

[9] 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.

[10] G. Keizer, "Is it legal to use firesheep at starbucks?" November 2010. [Online]. Available: http://www.computerworld.com/s/article/9194159/Is_it_legal_to_use_Firesheep_at_Starbucks_

Article on the legality of Firesheep

[11] ——, "Mozilla: No 'kill switch' for firesheep add-on," October 2010. [Online]. Available: http://www.computerworld.com/s/article/9193420/Mozilla_No_kill_switch_for_Firesheep_add_on?taxonomyId=17&pageNumber=1

Computerworld article detailing that Mozilla either can't or won't disable Firesheep from working in Firefox using Firefox's blacklist mechanism

[12] 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"

[13] S. J. Purewal, "Firesheep's a huge hit with amateur hackers," October 2010. [Online]. Available: http://www.pcworld.com/article/208773/Firesheeps_a_Huge_Hit_with_Amateur_Hackers.html

News post about Firesheep being popular among unqualified hackers

[14] TechnoLlama, "Is firesheep illegal?" November 2010. [Online]. Available: http://www.technollama.co.uk/is-firesheep-illegal

UK Article on the legality of Firesheep