Term Paper Short Draft

By Girum Ibssa

CSC 300: Professional Responsibilities

Dr. Clark Turner

May 21, 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 [4]. 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" [13].

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" [5]. Yet the use of wire sheep may be illegal in the US and beyond [15]. 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 [11].

Contents

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 [5].

“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” [5]. Butler continues with his description of the “problem that has been talked about to death” and how it remains to be solved [5].

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].

Firesheep works by allowing users to write custom ”handlers” for it to allow it to work on webpages of their choice. Firesheep’s source code currently includes ”handlers” for several popular websites including: 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 [4].

Some of those websites have quickly fixed the security hole (not using HTTPS) that Firesheep relies on to work [8]. However, a strong portion of websites simply didn’t fix the security flaw, weeks and months after the release of Firesheep [8].

2 Research Question

Was it ethical for Eric Butler to release Firesheep to the general public as a means of forcing websites to improve their flawed security?

2.1 Relevance

Firesheep can be downloaded today (May 21, 2013) from GitHub.com, a website hosting free open source programs [4]. At its time of release, several websites simply refused to implement HTTPS site-wide, allowing Firesheep to work on a large number of sites [5]. Today, Firesheep still works on a few sites that haven’t switched to using HTTPS site-wide, including the entire Stack Exchange network of websites [9].

Session hijacking allows users of Firesheep to impersonate ”logging in” as their victims on the sites that it works on [5]. The consequences of this can be anything from posting false Facebook status updates to outright deleting a person’s Stack Overflow profile. Eric Butler’s free software simplifies this process to the point where normally unqualified people may perform these acts, increasing the vulnerability of typical users worldwide.

3 Extant arguments

3.1 In Favor of Firesheep's release

3.1.1 Code as "free speech"

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" [7]. He defends by saying that code is a form of free speech, and that we have a Constitutional right to free speech [7].

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 [16]. 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" [16].

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 [15]. 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" [15]. 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" [15].

3.2.2 Firesheep desired to violate privacy

Firesheep is built specifically to allow untrained users to hijack browser sessions from unsuspecting victims [5], 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" [11].

4 Analysis

4.1 Why is the SE Code of Ethics applicable to this problem?

The Code defines software engineers as "those who contribute by direct participation to the...design, development...of software systems" [11]. Did Eric Butler contribute by "direct participation" to the design of some "software system"?

Firesheep is the name of software written in the C++ programming language that wraps existing packet sniffing software (Wireshark) in an easy to use, one-click GUI extension for the Firefox browser [**?**]. Firesheep is a software system directly written by Eric Butler, maintained on his open source GitHub account [4]. Eric Butler (the software engineer) has therefore contributed by direct participation (programming himself) in the design of a "software system" (Firesheep) [**?**].

Since he contributed by "direct participation" to "the design" of a "software system," Eric Butler is defined to be a "software engineer" under the ACM Code of Ethics, and therefore must follow the Code [11].

4.2 Argument 1: Disclosure

SE Code 1.04

Disclose to appropriate persons ... any actual or potential danger to the user, the public ... that they reasonably believe to be associated with software [11].

Eric Butler shall disclose to the general public

Eric Butler developed Firesheep as a concrete example of how serious the HTTPS problem was: "Today at Toorcon 12 I announced the release of Firesheep, a Firefox extension designed to demonstrate just how serious this problem is" [5]. That is to say, 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. The release of Firesheep can be seen as a programmer's attempt to 'show by doing'; Butler chose to release Firesheep as a catalyst for the seriousness of the HTTPS problem. Forcing websites to handle the HTTPS problem by openly catalyzing the problem is an excellent form of danger disclosure.

Session hijacking dangers

Session hijacking as a concept is simple: "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" [5].

This was already possible before the release of Firesheep through software such as Wireshark [1]. Firesheep's source code is written as an extension of Wireshark [4]. Firesheep was so significant simply because it offers a much simpler GUI than traditional session hijacking solutions.

Users of the affected websites

The victims of potential session hijacking are simply any users of the affected websites that are so unfortunate as to be physically near any session hijacking predators. The 'affected websites' to be spoken of at the time of release included websites as large as Google, Facebook and Yahoo! [4]. Google's Google+ social network has 343 million users [18], Yahoo's email service has 281 million users [19], and Facebook has over 1 billion users [3]. Even today, Firesheep works on sites like Stack Overflow, which over 2 million registered users at the time of writing [10]

Users logged into any one of these sites are 'affected' by these sites' inability to use site-wide HTTPS to prevent session hijacking.

Dangers associated with non-site-wide HTTPS authentication

Since Firesheep works by intercepting the "cookies [that] are basically shouted through the air" [5], any users who are on the same open WiFi network as Firesheep users are potential victims of the dangers associated with non-site-wide HTTPS authentication.

Substituted SE Code 1.04

SE Code 1.04

[Eric Butler shall] Disclose to the users ... any session hijacking dangers to the users ... that they reasonably believe to be associated with non-site-wide HTTPS authentication [11].

Argument 1 Analysis

SE Code 1.04 can be paraphrased as 'if there's serious danger going on with some software, you're morally obligated to tell the right person' [11]. In the blog post accompanying the release of Firesheep, Eric Butler made it very clear that he believed that non-HTTPS session hijacking was a serious problem: "This is a widely known problem that has been talked about to death, yet very popular websites continue to fail at protecting their users" [5].

Therefore, Eric Butler had an ethical responsibility, by SE Code 1.04, to create and release of Firesheep to the general public in order to disclose the dangers of session hijacking to the public.

4.3 Argument 2: Volunteer professional skills... contribute to public education concerning the discipline

SE Code 1.08

Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline [11].

4.4 Argument 3: Responsbility for detecting, correcting and reporting errors in software

SE Code 6.08

Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

4.5 Argument 4: Cooperate in efforts to address matters of grave public concern caused by software

SE Code 1.05

Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

5 Conclusion

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] "Facebook reports first quarter 2013 results," May 2013. [Online]. Available: http://investor.fb.com/releasedetail.cfm?ReleaseID=761090

Facebook's first quarter results

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

Source code and documentation for Firesheep

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

Eric Butler's personal blog post detailing Firesheep.

[6] ——, "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

[7] ——, "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

[8] ——, "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

[9] S. Exchange, "Why doesn't the stack overflow team fix the firesheep style cookie theft?" November 2010. [Online]. Available: http://meta.stackoverflow.com/questions/69171/why-doesnt-the-stack-overflow-team-fix-the-firesheep-style-cookie-theft

A post on Stack Exchange asking why they outright refuse to use HTTPS site-wide.

[10] ——, "Stack overflow users," May 2013. [Online]. Available: http://stackexchange.com/leagues/1/week/stackoverflow

Live query on Stack Overflow's current user base.

[11] 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'

[12] R. Garner, "Moral philosophy: A systematic introduction to normative ethics and meta-ethics."

[13] 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.

[14] R. Hursthouse, "Virtue ethics."

[15] 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

[16] ——, "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

[17] 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"

[18] M. McGee, "Report: Google+ now 2nd-biggest social network worldwide," 2012. [Online]. Available: http://marketingland.com/report-google-now-2nd-biggest-social-network-worldwide-31908

A post detailing Google's Google+ statistics

[19] R. Molla, “Gmail finally beats hotmail, according to third-party data [chart],” 2012. [Online]. Available: http://gigaom.com/2012/10/31/gmail-finally-beats-hotmail-according-to-third-party-data-chart/

A post on detailing the popularity of email clients

[20] 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

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

UK Article on the legality of Firesheep