Jeremy Hellmer
SE 4930
Article Review 2
1/11/12

The ability to keep track of past events could be considered one of the most desirable traits possessed by a human being. This allows a better organization and prioritization of future activities. After all, it would not be very desirable to pay a credit card bill twice. People are able to revisit events or activities that brought them joy and avoid those that have been deemed bad or a mistake. This is also a great time savor which is perhaps why it has been incorporated into the internet browsing experience.

To allow for the recall of past events on the internet, browsing history was put into place. This meant that a browser could remember where the user has been before and provide this information as user feedback. This was extremely important in the early days of the internet when it was used as a means to view static data. Since the data was unchanging, it was unnecessary to visit the same document on more than a single occurrence. The browser afforded the user this ability by varying the color of links to previously visited pages, an idea that has been adopted by the browsers of today's internet.

Websites began thinking of various uses of this browsing history. It could be used as a security threat detection system, alerting a user prior to entering login information that they had previously visited a known malicious website and their information may be vulnerable. It could also be used as a cookie by placing information into the history to identify a returning user. However, the reasons that history sniffing was actually occurring appeared to be selfish. It was being used to detect if a user had been to a competitor's page. It was also being used to tailor advertising packages to the specific users, making their website more relevant and desirable which as the article states is similar to the use of tracking cookies.

Automated history sniffing attacks could be implemented using three different techniques. A direct sniffing attack used JavaScript to identify the CSS values of links to determine if a link had been

visited. A sniff would then be performed on a visited link to see where the user went from there, allowing a user profile to be created. The second technique, indirect sniffing, would either change the size of page elements or the background styling of websites based on whether they had previously been visited. This would allow inspection of page elements other than links and allow a decision to be made based on how the page was rendered if it had previously been visited. The final technique is called a side channel. It involves passing information through an open channel intended for a different set of information. The most common side channel attack involved timing. A check would be performed on how long it took the user to obtain a source. If it arrived too soon, it would be an alert that the site was obtained from the cache meaning that it had been previously visited.

In 2010, however, David Baron of Mozilla developed a means of blocking all automated sniffing. A direct sniffing attack could be prevented by having the Document Object Model pretend that all of the links had a CSS styling that matched being unvisited. Indirect was prevented by limiting the changes CSS could make based on a visited/unvisited page. To block side channel, Baron allowed a history lookup only once per rule which is always done at the end to prevent timing differences. While automated attacks have been prevented, attacks involving user interaction are still possible. In all, the article was able to point to six sniffing techniques that remain possible even with Baron's defensive techniques. These included four user interaction and two using the webcam to detect color reflection. While it has been greatly improved, history sniffing is still possible and may always be possible without removing features from the internet browsing experience.

From this article, I learned that some of the features that make the internet and software user friendly are also areas for exploitation. In this case, there is no functional benefit to providing the user with feedback on previously visited site. It is simply a convenience type item that opens up a security risk that many people would not even realize is possible.

Works Cited

Weinberg, Zachary, Eric Y. Chen, Pavithra R. Jayaraman, and Collin Jackson. "I Still Know What You Visited Last Summer." *Browsing Security and Privacy*. Proc. of 2011 IEEE Symposium on Security and Privacy. 147-61. Web. 2012. <http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper010.pdf>.