Concordia Institute for Information System Engineering
(CIISE)

Concordia University

INSE 6150 – Security Methodology Evaluations

Assignment -2:

Submitted to:

Professor Jeremy Clark

Submitted By:

Nithish Reddy Yalaka - 40164619

(Question 1)

List seven core tasks that a typical user would want to perform using Privacy Badger. Describe each task briefly (maximum three sentences) and why it should be considered a core task:

What is Privacy Badger?

Privacy Badger is a browser extension or an add on that restricts advertisers and other third-party trackers from anonymously tracking where you browse and what kind of pages and data you visited at on the Internet. If an advertiser seems to be tracking you across numerous websites without your permission, Privacy Badger will automatically block that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly vanished or disappeared.

Seven Core Tasks:

1. **Fast and Secure Browsing: -** Protect the internet users from tracking using HTTPS everywhere and blocks ads

   Unnecessary advertisements and pop-ups make the browsing difficult and uncomfortable to the user. This add-on prevents it by blocking trackers and intrusive ads which decelerate the browsing. It is a core task because user always looks for the authentic and absolute information and is not interested in ads and pop-ups.

2. **Do not Track: -** User can send a request to not to track to the website.

   Privacy Badger sends a Do Not Track request to the websites. However, the data of the user depends on the website replying to the user's request. Most of the websites still collects the data and use it to improve security, content and services on their website and achieve reporting statistic.

3. **Leakage of Data and Search History: -** With DNT (with the installation privacy badger, it will automatically enable the DNT flag as clear signal for sites that internet users don't want to not being a part of online search and data tracking) and Privacy Badger, users have important new tools to block stealthy online browser tracking and the exploitation of their online browsing history and data.

4. **Acting as a Shield: -**

   Privacy Badger looks at any third-party domains that are loaded on a given site and regulates whether they appear to be tracking you (e.g., by setting cookies that could be used for tracking, or fingerprinting your browser). If the same third-party domain or website appears to be tracking you on more than 3 different multiple websites, Privacy Badger will finalize that this third-party domain is a

tracker and block future connections to it from your browsing.

For some reliable websites, if Privacy Badger were to restrict an embedded domain completely, it would break the site's most important functionality and the site will lose its main functionality.

5. **Color Coding Sliders for analyzing the website: -** Privacy Badger analyzes each third-party website's behavior over time, and picks what it thinks is the best setting for each domain, but you can modify the sliders if you wish.

   Green - It has been seen that there's a third-party domain or website, but it still hasn't yet been observed tracking your activities across multiple sites, so it might be incorrupt or clean.

   Yellow - It has seen that third party domain is trying to track you, but it is on Privacy Badger's cookie-blocking yellow list of third-party domains or websites that, when analyzed, seemed to be important for the functionality of the website. In that case, Privacy Badger will accept the website and load content from the domain but will try to remove third party cookies and references from it.

   Red - Privacy Badger has identified the third-party domain as a threat and it blocks the that content from this third-party tracker.

6. **Real Privacy:** - Protection from malicious sites and codes, cookie control, Browser Fingerprinting.

   Protects the users from Traffic analysis and Network Surveillance using DuckDuckGo and Tor. Privacy Badger provides the user additional privacy by linking private tab with Tor and private search engine DuckDuckGo which ensures that all the connections are encrypted, and it masks your location from the sites. It is a core task because user needs to increase the anonymity which ensures the real privacy.

7. **HTTPS Analyzing**: To ensure a secure connection to any website User can enable connections upgraded to HTTPS so that Privacy Badger redirects to HTTPS Version of any website if it is available on their sites. It is a core task because it provides a secure connection to any website that the user connects. Privacy Badger can detect if it was malicious site, and further blocks the site from popping infected buttons.

(Question 2)

Three Core Tasks of the Seven will be used for the Security Evaluation:

1. Acting as a Shield

2. Fast and Secure Browsing

3. Color Coding Sliders for analyzing the Website

The core tasks will be evaluated based on the below mentioned Guidelines/Heuristics:

Guideline 1. User should be aware of the steps they have to perform to complete a core task.

Guideline 2. User should be able to determine how to perform these steps

Guideline 3. User should know when they have successfully completed a core task.

Guideline 4. Users should be able to recognize, diagnose, and recover from non-critical errors.

Guideline 5. Users should not make dangerous errors from which they cannot recover.

Guideline 6. Users should be comfortable with the terminology used in any interface dialogues or documentation.

Guideline 7. Users should be always aware of the application's status.

Part-2 Security Evaluation:

Core Task-1:

Acting as a Shield:

It is the top priority of Privacy Badger which provides unparalleled security and privacy. Privacy Badger fights malware, cross-site scripting trackers, HTTPS Connections, throwing away cookies and making harder to recognize. User can customize these settings according to his requirement as per-site or globally.

G1. (Satisfies the guidelines) User need to install the Privacy Badger Extension as required to perform this core task. User can easily customize the settings according to his need by just switching it on.

G2. (Partially Satisfies the guidelines) User needs to carefully analyze and perform the steps he needs in order to get high end security and privacy.

G3. (Satisfies the guidelines) After enabling the Plugin, Privacy Badger displays statistics of how many ads blocked, scripts blocked, cookies controlled to the user.

G4. (Satisfies the guidelines) All the non-critical errors like scripts can be easily recognized, diagnosed and get recovered by encrypting the connections, blocking the scripts using Privacy Badger.

G5. (Partially Satisfies the guidelines) If user doesn't enable all the proper shielding settings of the Privacy Badger, then it might cause dangerous threats because online trackers can compromise the system by fingerprinting and cookie track.

G6. (Satisfies the guidelines) Terminology is simple and understandable to the user in both in documentation and interface dialogues. Privacy Badger is self-explanatory, by clicking on extension button user can easily understand the interface.

G7. (Satisfies the guidelines) All the subtasks in shielding like cookie control, fingerprinting etc. has separate set of status through which user can know the state of the shielding. Example for cookie control, 3rd party cookies blocked, Cookies blocked, All Cookies blocked is shown to the user. Also, the Color-coded sliders for understanding the severity.

Core Task-2:

Fast and Secure Browsing: This Privacy Badger blocks the trackers and intrusive ads that slows down the browsing by using along with free and private search engine DuckDuckGo and also saves the internet. It provides additional security and privacy by using HTTPS Everywhere and tracks Cookies and It makes the browser to load major sites 8 times faster than the browser without this extension.

G1. (Satisfies the guidelines) User need to install the Privacy Badger Extension as required to perform this core task. By default, once the privacy badger is enabled by the user, it will increase the speed and blocking trackers increases the security of the browser.

G2. (Satisfies the guidelines) User need not perform any steps since the Privacy Badger enables it by default. In case of extended security user can enable HTTPS Everywhere in the settings

G3. (Partially Satisfies the guidelines) when a user browse left of the web address contains status by which the user will be able to know the secure, not secure and dangerous sites. But user cannot know immediately as soon as the setting in privacy badger is enabled.

G4. (Satisfies the guidelines) All the non-critical errors are easily recognized, diagnosed and get recovered while blocking the trackers for online privacy using Privacy Badger.

G5. (Partially Satisfies the guidelines) If any user unblocks the blocked tracker mistakenly, Privacy Badger does not notify the user any warning. Therefore, once the personal information of the user is compromised it cannot be recovered which might be dangerous.

G6. (Satisfies the guidelines) The status and symbols provided are very simple and straightforward which user can understand very easily.

G7. (Satisfies the guidelines) To check a site's security, privacy badger provides three statuses on the extension with three colors stating the severity of the threats along with the detected potential trackers.

Core Task-3:

Color Coding Sliders for analyzing the Website: Privacy Badger evaluates each third-party domain's behavior over time, and prefers what is the right setting for each and every domain, but user can adjust the sliders accordingly.

Green – It has been seen that there's a third-party domain or website, but it still hasn't yet been observed tracking your activities across multiple sites, so it might be incorrupt or clean.

Yellow – It has seen that third party domain is trying to track you, but it is on Privacy Badger's cookie-blocking yellow list of third-party domains or websites that, when analyzed, seemed to be important for the functionality of the website. In that case, Privacy Badger will accept the website and load content from the domain but will try to remove third party cookies and references from it.

Red – Privacy Badger has identified the third-party domain as a threat and it blocks the that content from this third-party tracker.

G1. (Satisfies the guidelines) It is clearly visible when you click on the extension that there will be 3 different colors (green, yellow and red). User can clearly understand the severity later set automatic payments and many others to support the content creators.

G2. (Satisfies the guidelines) Browser can automatically distribute your contributions depending on the time user spends on each site. User can optionally choose to tip the sites directly or even often it monthly.

G3. (Satisfies the guidelines) User can clearly understands the successful output of the sliders as once he opens a website from the browser with enabled Privacy Badger. Privacy Badger will automatically divide the threats in color coded. It is clearly visible as task completion.

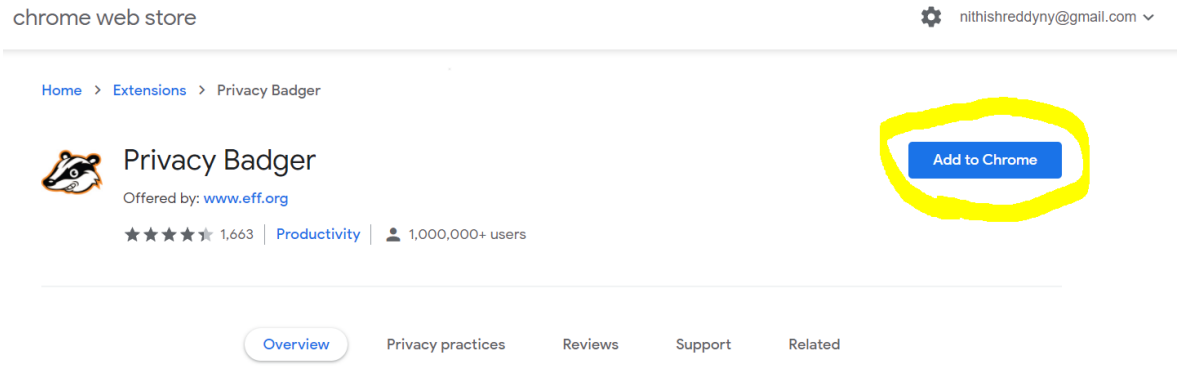
G4. (Satisfies the guidelines) Upon looking at the sliders and its corresponding tracking threats, User can recognize the severity, and he can wish to block them for good.

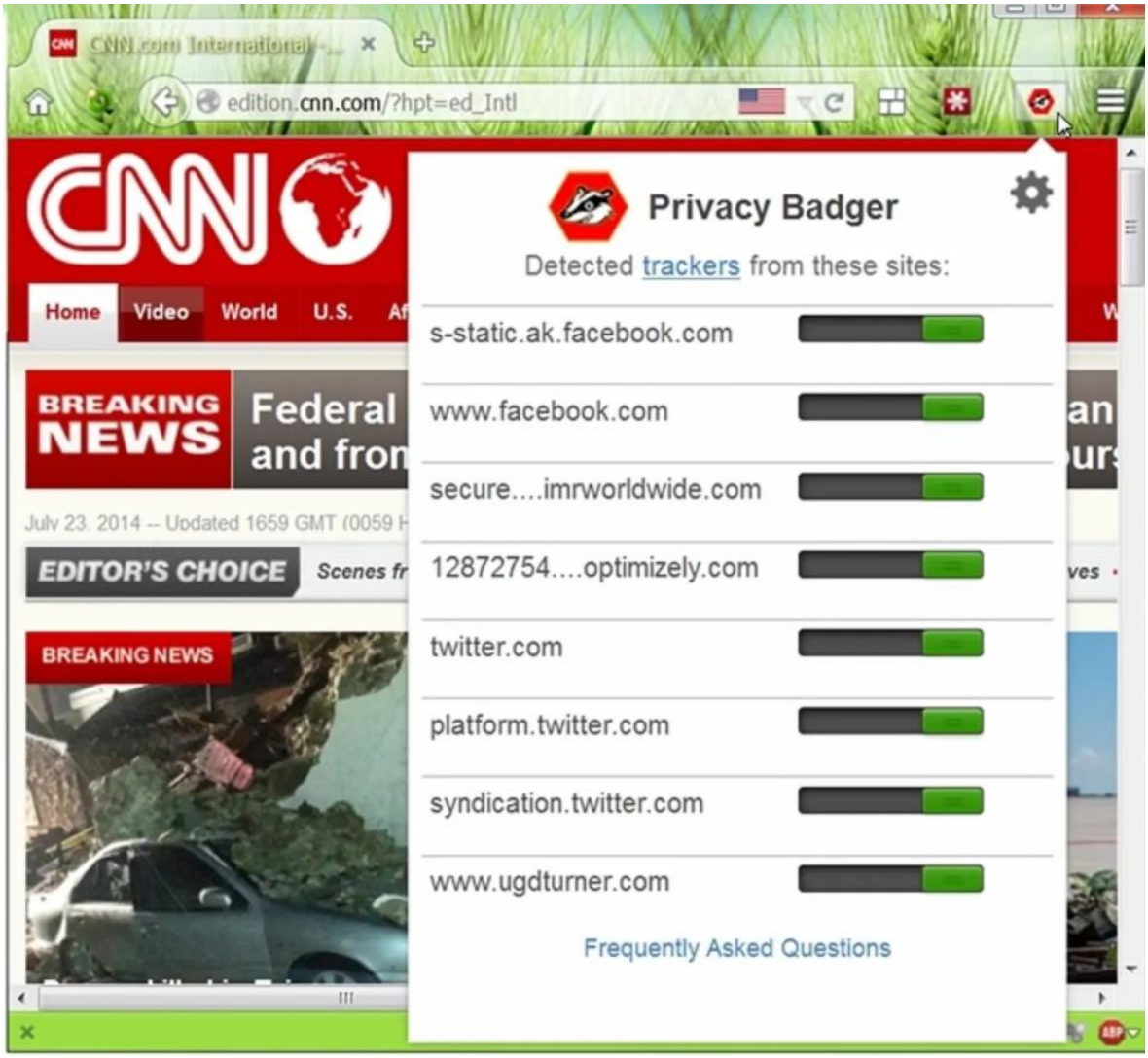
G5. (Partially Satisfies the guidelines) After the threats are segregated among the colors, user has to be very careful on which ads or pops to allow. He cannot just unblock a severe threat. Once he does that, he is vulnerable to attacks.

G6. (Satisfies the guidelines) By clicking on Color coded sliders, user can view the status of threats and tracks for a particular website and it is straightforward which user can understand very easily. You can also adjust the sliders as you wish in the settings.

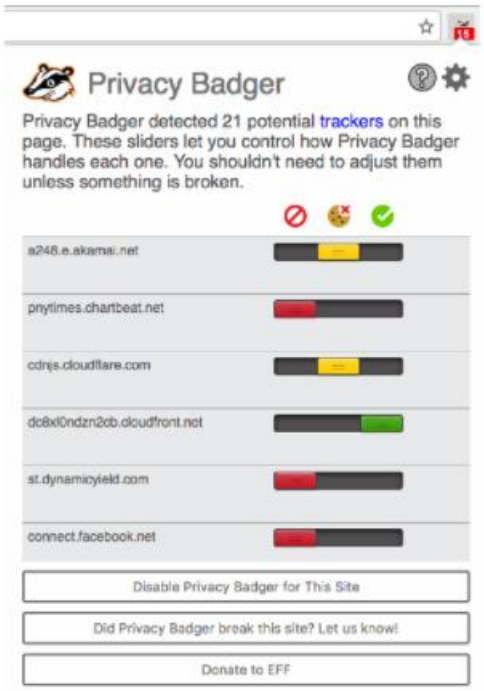
G7. (Satisfies the guidelines) User can know the status of the sliders by just clicking the extension tool and he can see the color-coded sliders with tracker information and severity.

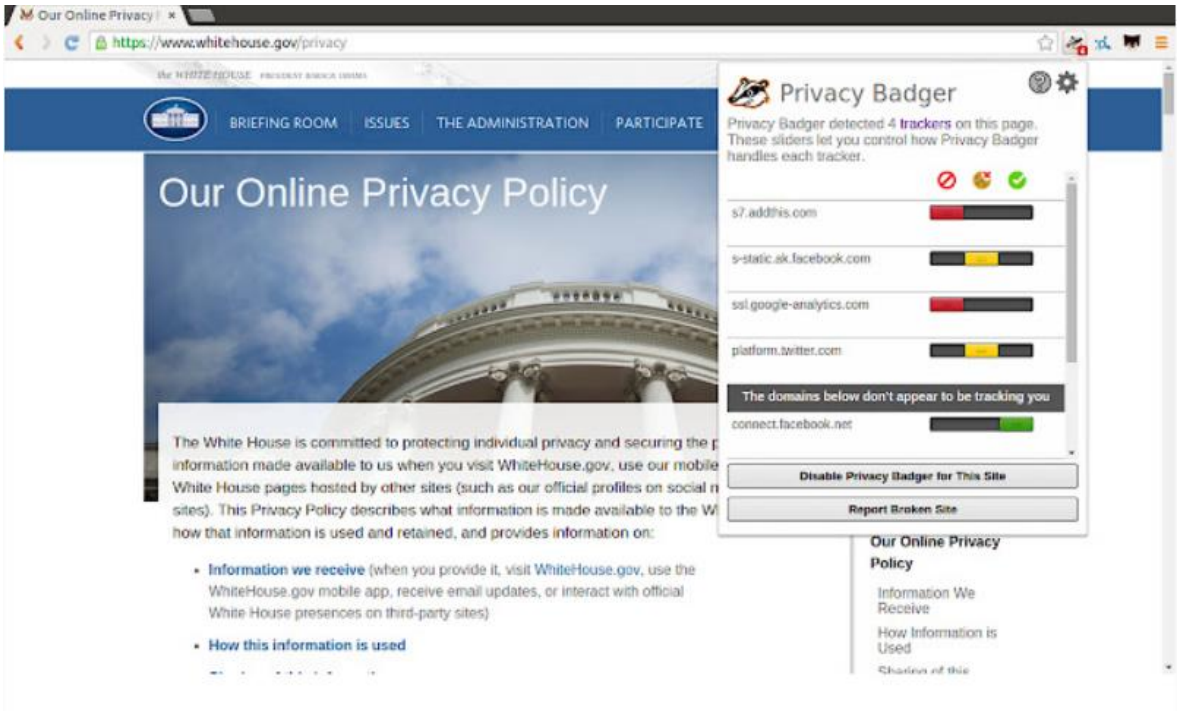
(Appendix):





Initially, once you visited, everything will be in green and Privacy Badger will evaluate the trackers and modify the colors according to the threats.





As you can see, colors have changed for several third-party domains as per their threat evaluation by Privacy Badger

(References):

1. https://www.eff.org/pages/privacy-badger
2. https://www.eff.org/deeplinks/2016/12/new-and-improved-privacy-badger-20-here
3. https://privacybadger.org/
4. https://users.encs.concordia.ca/~clark/courses/1603-6150/scribe/L07.pdf