Kenny Crowell

Computer Security

Final Project

December 12, 2014

Abstract

Over the past few years, Google Chrome has become one of the most popular web browsers throughout the world. Along with this came the emergence of developer apps and extension designed for this browser. These extensions can provide very useful services to the user. An example of this is perhaps the most popular extension, AdBlock. There are millions of extensions that can be found within the chrome store that people can download for free. However, many people do not realize the sort of data that these extensions can have access to. Virtually everything you do in your browser is fair game to many chrome extensions. While this does allow extensions to do many unique things, it can also be a serious security concern. In the future, users must be weary of the security risks of these extensions and proceed cautiously when downloading content for their browser.

Introduction

The availability of Google Chrome extensions rivals that of mobile apps through both Apple's App Store and the Google Play Store. Millions of apps are in each store mainly because of the ease of access developers have to such stores. From single individuals to multi-million dollar companies, apps can be added by anyone. This leads to a great concern about the security of these stores. If anyone can add their applications then there are bound to be many malicious

apps available at any given time. These applications can gain access to your personal data and either use that themselves, or sell it to companies that will pay for such information such as advertisement targeting agencies. Some extensions can have access to all of your web browser's data and history this can lead to a serious breach of privacy. For this reason it is important for user's to choose applications wisely and to be aware of the data that these extensions have access to.

To The Community

It is important that people know of the potential risks of chrome extensions because they are the ones that are able to stop the spread of malicious applications. By being aware of the permissions certain applications need and what these permissions imply, users can make a wise decision about whether an extension is malicious or not. For example, if an application requests permission to view all web browser data and there is no good reason for this then it is possible that this application is malicious and should not be installed. By being aware of what they are downloading, the community can avoid malicious extensions and ensure that their privacy is not breached.

How a Google Chrome Extension Works

"Extensions are extra features and functionality that you can easily add to Google Chrome. By using extensions, you can customize Google Chrome with features you like, while keeping your browser free of things that you don't use."[1] Extensions take data from websites that you are visiting or have previously visited and use this information in order to better the user

[1] About Extensions. (2014, January 1). Retrieved December 11, 2014, from https://support.google.com/chrome/answer/154007?hl=en

experience. Perhaps one of the most well know extensions, AdBlock Plus, has access to things such as your IP address, the web address accessed, the browser identifier, and the referring page. All of this data is stored in website logs, and while it is stated that none of this information is shared with third parties, it still could pose a security risk.[2] For example if someone were to attack AdBlock plus and gain access to its web logs than they would be able to see all of the information taken. Of course, security risks like these are hard to avoid and are often found to be worth the risk. In situations like this people often choose to trust the developers of the applications to ensure that they are as secure as possible. For this reason almost any extension on chrome is potentially harmful, but it is up to developers to secure information as much possible.

Security Risks

As mentioned above, almost any chrome extension can have a security risk based on how a developer chooses to secure information gathered through their extension. This is the case for many things in the world we live in today. For example, people trust stores and websites to store their credit card information every time they checkout. This has resulted in several major security breaches over the years resulting in many credit card numbers being leaked. Any chrome extension that stores any type of personal information of value carries this same risk.

Another way that this type of information can be leaked is through the use of third party applications. If an extension sends data to a third party app for either data storage or any other purpose there is a chance that this data can be leaked. For example, earlier this year a third party app that Snapchat (a mobile app) used for data storage was hacked which resulted in thousands of private photographs being leaked to the public. At this point it does not come down to just the

[2] Privacy Policy. (2014, January 1). Retrieved December 11, 2014, from https://adblockplus.org/en/privacy

developer of the application to ensure everything is secure, but rather that this developer know all of the implications of using this third party service as part of their application. However, users often never know whether or not the extensions that they are using actually send their data to third party applications. For this reason, many people are not even aware of what problems can arise from allowing applications to access all of their data.

Of course, on top of unintentional data loss, some apps could actually be selling information they gather to third parties. Many advertisement agencies will pay for information such as the users browsing history because this allows them to target the user with specific ads. In fact some extensions actually inject ads into the pages you visit.[3] For this reason, many chrome extensions do not give the user any privacy. In today's world it is becoming harder and harder to truly keep one's life private and Google Chrome extensions are just another privacy concern for the public.

Examples of Information Gathering

Chrome extensions make it unbelievably easy for one to access a user's private data. For example, the chrome.tabs API allows access to open tabs in Google Chrome. With this tool, the developer can get everything from the URL of a page (using the chrome.tabs.query method) to a screenshot of the page (using chrome.tabs.captureVisibleTab). These two things alone can be extremely invasive to a person's privacy. Would you use an extension if you knew that it could take screenshots of all of your browsing? You could be updating private information about yourself on Facebook and the extension could take a screenshot of everything you are doing. On

[3] Heddings, L. (2014, January 20). Warning: Your Browser Extensions are Spying on You. Retrieved December 11, 2014, from http://www.howtogeek.com/180175/warning-your-browser-extensions-are-spying-on-you/

top of this the chrome.tab API allows for the running of scripts on the tabs which can be used for malicious purposes. These scripts could be used to steal personal information that was input to the page. There is potential for things such as passwords of credit card numbers to be viewed this way.[4] Chrome.tabs is only one API available for use with chrome extensions and it can be used to invade the privacy of anyone who is using it. A very simple chrome extension I wrote called URL logger uses this API and outputs the URL of every open tab in the window into the console log. This takes almost no code and can potentially be breach the privacy of the user. Although my extension only outputs each URL to the console log, imagine if it instead saved this information into a database with a user ID. If this were the case the developer could track each user for his own uses or sell it to a third party for their use. Using other APIs Google Chrome extensions can gain access to much more information including the IP address of the host. Using all of the information available to them a developer can essentially discover the identity of the person using his or her extension. At this point the user has virtually no privacy as everything they do online is being watched.

Past Problems

An example of the malicious capabilities of Google Chrome extensions can be shown by an attack that happened in 2013. Users were prompted through a Facebook message or email to follow a link by saying that they had been tagged in a video. In order to watch this video they would have to install a Google Chrome extension to view it. However, there is no real video. Instead, users who downloaded the extension had installed a malware that was capable of taking

[4] Chrome.tabs. (2014, January 1). Retrieved December 11, 2014, from https://developer.chrome.com/extensions/tabs

over their Google Chrome browser. Considering many people allow Chrome to store their login credentials and other information such as addresses, this is a major problem. This attack affected over 80,000 chrome browsers when it was done which gives the attacker access to a huge amount of private data.[5] This is just one of several malicious Google Chrome extensions that have affected thousands of users. In this case it was phishing that caused users to download the extension but in others it is possible that the extension could be downloaded for a specific purpose. Some extensions may serve useful functions but in the background can be running malicious software. This is the type of malware that people need to be especially careful of. This example shows how easy it is for an attacker to retrieve a user's personal data and use that for their own good.

Defenses

The best defense in this situation is just to be smart about downloading an extension. Like in the previous case, you should not download an extension based on what a Facebook message or email tells you to do. It is also a good idea to research any potential extension that you are thinking of downloading. If there is very little information about it online it is probably not safe, or there is probably another extension that does something similar. It is also important to pay attention to the permissions that the extension will need. There are 10 permissions that an extension can have and these range from a low alert to a high alert. For example, one of these permissions gives the extension access to all data on your computer and the websites you visit. This permission is clearly a high alert as it gives access to all of your data. If an extension asks for this and it is unclear why it will need all this access it is probably safest to avoid it all

[5] Donohue, B. (2013, August 30). Faux-Facebook Notifications Lead to Browser Hijack Malware. Retrieved December 11, 2014, from http://threatpost.com/faux-facebook-notifications-lead-to-browser-hijack-malware/102150

together. Other lower permissions can give access to things such as your browsing history and data you copy and paste. While less harmful, these permissions can still be harmful as they can still access private information.[6] It is important to understand what each permission gives access to and to try to think of why the extension you are thinking of downloading may need these permissions. At this point it is up to you to trust this extension with your data.

Conclusion

I hope it is now clear that Google Chrome extensions pose some serious security risks. Along with simply taking away privacy, these extensions can gain access to a lot of useful data and take over your browser. Although many extensions are most likely safe to use and can provide useful services, one must be careful when downloading a new extension. The main thing to be aware of when downloading an extension is the permissions it requires to run. Even an extension that provides a useful service in the foreground could be malicious in the background. Another key point worth noting is that even if an extension has no malicious intent, it can still be prone to attackers who can steal the data that it collects. As the world changes and it gets exponentially harder to truly be private, it is sensible to put more effort into to securing ones data. For this reason, people must think twice about downloading Google Chrome extensions.

[6] Understand permissions requested by apps and extensions. (2014, January 1). Retrieved December 11, 2014, from https://support.google.com/chrome_webstore/answer/186213?hl=en&rd=1