2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) | 978-1-6654-3811-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAC3N53548.2021.9725431

Free Services - A Threat to Privacy: Ensuring a Safe Online Presence using Chrome Browser Extension

Krishan Bhadana
Department of Computer Science & Engineering
Faculty of Engineering and Technology
Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
bhadana.k11@gmail.com

Supriya P. Panda
Department of Computer Science & Engineering
Faculty of Engineering and Technology
Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
supriya.fet@mriu.edu.in

Abstract **- Internet users all across the world are concerned about the effects of free services on their privacy and security. The Internet is a vast collection of websites, the most of which are informative in nature while some are service-oriented. Paid services charge for their services, whereas others provide them for free. It may appear to be free, but there is always a catch. This paper discusses the fundamental differences between paid and free internet services, as well as the drawbacks of free services, how they can jeopardize a user's security/privacy (on occasion), and how a little bit of vigilance can shield users from prying eyes. Maintaining a balance between convenience and security goes a long way, it is understandable that removing some security walls and automating some tasks make everyday tasks easier but it is always a good habit to give preference to security. To tackle such threats, there must be a system that is looking out for user's security and privacy all the time, the system designed in this paper is a chrome browser extension that fulfills some of these tasks and ensures a better browsing experience.**

Keywords - Privacy, Security, Free services, User Profiling, Targeted advertising, Hidden cost of services, Browser extension, Site blocking, Trackers, digital footprint, Application Programming Interface(API), Google safe browsing, Malware.

I. INTRODUCTION

The lure of technology has trapped us in the modern world. Everyone requires the most up-to-date technology and functionality, with no regard for privacy or security.

In July 2020, Indian government banned 59 apps because those apps were engaged in questionable activities prejudicial to the sovereignty and integrity of India, defense of India, security of the state, and public order. This was accompanied by more apps ban in August 2020 and September 2020.

The PlayStore and AppStore contain millions of apps overall some of which secretly spies on the users and exploit data. This number grows exponentially when WebPages are are mentioned. All the apps that were banned were free of cost i.e., they were made to benefit themselves in ways that are secretive and probably unethical.

Nothing Comes for Free [1], even if the user is paying nothing. Their presence on the internet is enough for the company to make a profit.

If a company does not charge for its product that means its user is the product. Some might not notice, but it can often cost more than just money.

Since the industry is growing so fast and data processing is becoming easier each day, companies have started using user's data more than ever. Free services are good but because of some stumbling blocks, users prefer paid services.

Tracking a user can be a business model of a company and that is completely fine but when it is done in the background or without the user's consent, it drops many red flags.

Data harvesting is also not a bad practice but because of the reason mentioned above, companies prove themselves substandard. Full transparency is a requirement that every company should fulfill these days. The point is that the consumers have a right to know all that is shared with developers by them or their devices.When a person has an online presence, whatever is done leaves a digital footprint. That data created about the user's behaviour and preferences gradually turns into a profile and pattern. This profiling and pattern make it easier to guess the user's password.

II. LITERATURE REVIEW

Nothing Comes for Free: How Much Usability Can one Sacrifice for Security. "In this paper, authors discussed tradeoff between usability and security; they conducted a pilot user study among university students in the university elections setting, and quantitative analysis. They emphasize determining that to which extent a voter would sacrifice usability for security. Their findings revealed that voters would sacrifice approximately 26 points (scale 0-100) of usability given a system with higher security" [1].

A. Facebook: Threats to Privacy.

"In this paper, the authors examined how Facebook affect user's privacy, how users from different age group and category share their information on social media, and how the platforms are handling that data. The authors investigated the platform's privacy policy and found serious flaws in the system, they found out that Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook, they analyze the Facebook system in terms of Fair Information Practices as recommended by the Federal Trade Commission, they also made recommendations on how to address the issue" [2]. An Empirical Assessment of the Effectiveness of Deception for Cyber Defence."In this Dissertation, the author performed a network penetration test for over two days in which he controlled both the presence of and explicit mention of deceptive defensive techniques. He also investigated the effectiveness of decoy systems for cyber defence by comparing performance across all experimental

ISBN: 978-1-6654-3811-7/21/$31.00 ©2021 IEEE

conditions"[3]. Big Data for All: Privacy and User Control in the Age of Analytics "In this paper, the authors wrote about the fundamentals of big data and how it is affecting the privacy of many. The authors also shed light on the disadvantages of big data"[4]. The Price of Convenience: Privacy and Mobile Commerce "In this paper, the authors raised the topic of privacy and mobile commerce. How effective mobile commerce typically requires a system that maintains a detailed and dynamically updated profile of the individual user. While at the same time receiving aggregate information based on data transmitted by other users. Privacy is being exchanged for convenience" [5].

Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations. The Authors studied the work of Sicari et al and others who centered their work on the analysis of available solutions in the field of IoT security. Since IoT communication protocols and technologies differ from traditional IT realms, their security solutions ought to be different as well. The survey of a broad number of academic works led to the conclusion that despite numerous attempts in this field, many challenges and research questions remain open. In particular, the authors stressed the fact that a systematic and unified vision to guarantee IoT security is still lacking.

B. Privacy vs. Convenience

There are times when a user comes across a decision that makes him/her choose between privacy and convenience. A simple example of it is passwords; some people do not apply passwords on their devices just for the sake of convenience. Another example is people using the same password on all their accounts so that they don't need to remember too many passwords. As a result, this tendency of prioritising convenience over privacy has an impact on user's life on a larger scale. Here are some examples:

- *Example 1*: *Sharing contacts with Truecaller* Truecaller asks for contact access permission, and then only the user is allowed to use the caller ID feature. So, for the sake of convenience user grants permission and shares his/her family/friends' contact details with the app. Almost every app downloaded from Appstore or Playstore instantly requests permission to access the phone's contacts, storage, camera, etc. Sometimes even those apps which have nothing to do with contacts ask for contacts access permission.
- *Example 2: Sharing photos with Google photos:* Google photos user allows its users to backup unlimited photos to their cloud, This unlimited offer grabbed the attention of the world and almost everybody was uploading their entire library to the Google photos app. At that moment for many users convenience outweighed privacy. As discussed in the previous section the software license agreement does not cover one's privacy rights, it only covers intellectual property rights (IPR).
- *Example 3 : GPS Navigation:* A Global Positioning System (GPS) helps to locate one on the map by sending signals to multiple satellites. These technologies are mostly used to navigate but users often forget that they are constantly sharing their present location and there is a company that knows where its users are at each point in time.

III. SELF- PROTECTION & REAL-TIME THREAT ASSESSMENT

The privacy and security threats are all-time present, therefore there must be some precautionary measures that could be taken to avoid losses due to such threats. The first and foremost goal of these services is to keep the users engaged with their platform, the time spent on viewing each post and the watch time overall accounts for a lot.

There are so many algorithms (designed to keep up user engagement) trying every possible way to keep the user online, this brings up another issue with these free services which are an addiction. Social media addiction is one of the major issues in society, people have started feeling more comfortable in the virtual world rather than the real world.

Youtube and Facebook come in the top three most frequently visited websites. "These three free sites, Facebook, Google Sites, and Yahoo sites accounted for 16%, 11%, and 9% of time spent online, respectively ComScore.com 2011)"[6].

Many long sessions on these platforms accumulate a lot of data about users; similarly other millions of users give their information to these platforms easily. This all collected data is utilized for profit one way or other.

Big Data has come to refer to a constellation of phenomena having to do with the production, consumption, amassing and analysis of large data sets produced by a vast variety of sources in a very large number of formats, in unprecedented volumes and data flow velocities.

Big data is useful, it has solved many world problems but there are some downsides too. Data nowadays is collected irrelevant of its type, sensitivity, or knowing its use in hope of getting something out of it after analysis. Here are some downsides of big data. Some data may not be relevant unless cross-referenced with some other information. Most users are unaware about the fact that how much data is being collected from them. Automatic decision-making with the help of big data can lead to economic imbalance and capricious classification.

- *Example*: loan grant based on the future probability of repayment capability.

Data collection is done everywhere, sometimes it's given different names like a loyalty program, purchase history, etc but the goal is always the same. Taking an example of Facebook, 2 researchers proved in a week time that how easy it is to mine data from Facebook " we (two students) were able to data-mine the Facebook in a week, using the time allotted to us for one class is evidence that data-mining the Facebook is evidence that it is not only possible but easy"[2].

Facebook has it in its terms and service that it is forbidden to use its website for data harvesting purposes. It is not allowed to use automated scripts on their website although there is no recourse on the people who attempts to do so. "There are no provisions for the violation of the Terms of

Service, and the termination of the offending account would not be a sufficient deterrent for those determined to obtain and use this information"[3].

People lose access to their accounts, their social media platforms get compromised similarly there are many more consequences if a person doesn't take proactive measures.

Nowadays many countries along with India promote digital payments and because of this most of the capital of any individual is stored in the bank. If a person's life savings is just a password and OTP away, it becomes necessary to keep our sensitive data secure all the time. So, there is a need for proper guidelines to protect oneself and a smart way to assess security threats in real-time.

Cyber security has got the spotlight in recent years and terms like ethical hacking, a cyber security expert can be heard more often, this is because many major companies and governments have understood its importance.

Precautionary measures are also necessary because cyber attacks are increasing day by day. Even after these precautionary measures are implemented there is a need for Adaptive cyber defense, A system that can tackle such problems in real-time, "an intelligent system that can automatically react to malicious behaviour and evolve their defences over time as attacks change"[2].

People always get attracted to free services on the internet without realizing the tradeoff between security and privacy. Users are constantly giving away information like it's nothing and on the other end, that information is being collected and analyzed to form a digital version of the user which can emulate his/her every action and eventually even predict their actions. This a very scary situation that humankind is facing and 99% don't even realize it.

The control has shifted towards machine learning algorithms and AI Machines and the creators of the platform like Instagram and Facebook no longer have full control of what comes next to users' feed. It is clear that AI is taking over and the said services have expanded so much that the creators have opted for automation in their operational work.

IV. CHROME BROWSER EXTENSION

The extension is an add-on to the browser which adds some functionality to the browser without diving deeply into the native code. It can be created using few technologies like HTML, CSS, Javascript, JQuery. A Chrome extension has three modules namely, I Elements, Background scripts, and Content scripts. These three modules handle different tasks and can communicate with each other to exchange information.

The extension uses Google Safe Browsing. It is a Google cloud service which offers multiple products, one of which is Web Risk API. Web Risk is Google's new enterprise security product which allows an application to check URLs for threats. Uniform resource locator (URL), also referred to as web address is a reference to web resource that specifies the location on the web. The URLs are checked against Google's constantly updated list of unsafe web resources. These constantly updated lists can be searched for matching URL. Clients can either use Update API or Lookup API.

LOOKUP API : It allows applications to send web URLs to web risk server and get its risk status in return.

UPDATE API: It allows the application to download and store hashed version of web risk lists in the local storage/database and check them later on locally.

In the development of extension, Lookup API was used because of its simple method as compared to Update API and also it fulfills the objective.

To check whether the URL is on the web risk lists, the application sends an HTTP GET request using Uris.search method. The Lookup API can handle only one URL per request, If there is a need to check multiple URLs then multiple separate requests can be sent.

V. CONCLUSION

The developed browser extension can identify suspicious and fraudulent websites as soon as the website is loaded. The URL is sent via a GET request to the web risk server. The server matches the URL with the constantly updated lists, then in response to the request, the server returns whether the URL is safe or not.

The extension then gives an alert to the user that the website being visited is not safe. The alert view can be seen in Figure 1.

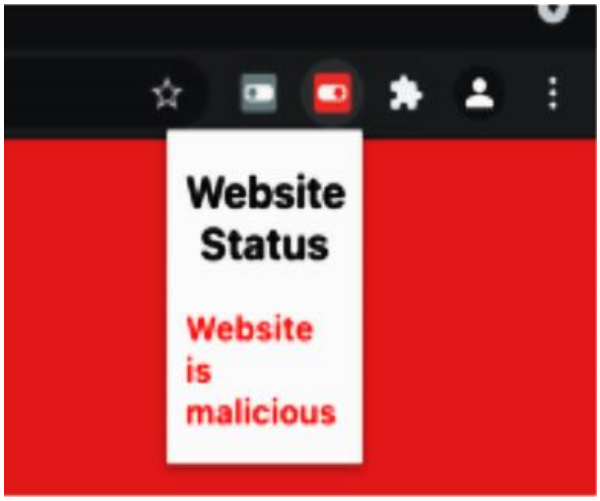

Fig.1 Site Blocking

VI. SCOPE

This work presented here can be further extended in various dimensions. Cyber security has a very big scope. This work includes detection of bad websites which have been detected by Google's services. There can be a system which proactively works in detecting such websites learning from secure browsing habits. Also, a system can be designed which focuses not only on websites but overall protection.

REFERENCES

[1] Kulyk, Oksana, et al. "Nothing comes for free: How much usability can you sacrifice for security?." IEEE Security & Privacy 15.3 (2017): pp. 24-29.

[2] Jones, Harvey, and José Hiram Soltren. "Facebook: Threats to privacy." Project MAC: MIT Project on Mathematics and Computing 1.01 (2005): pp. 4-6.

[3] Ferguson-Walter, Kimberly J. "An empirical assessment of the effectiveness of deception for cyber defense." (2020): pp. 7-9.
[4] Tene, Omer, and Jules Polonetsky. "Big data for all: Privacy and user control in the age of analytics." Nw. J. Tech. & Intell. Prop. 11 (2012): p 27.
[5] Ng-Kruelle, Grace, et al. "The price of convenience: Privacy and mobile commerce." Quarterly Journal of Electronic Commerce 3 (2002): p. 273-286.
[6] Brynjolfsson, Erik, and JooHee Oh. "The attention economy: Measuring the value of free digital services on the internet." (2012): pp 63-67.