Hare Hunting in the Wild Web: A Study of Web Security Threats and Solutions

Shital Patil

Kaitec Solutions Pvt Ltd, Pune, India

Email: kaitecsol@gmail.com

---***---

Abstract: *Over the past decade, web applications have undergone a transformation from a collection of static HTML web pages to complex applications containing dynamic code and rich user interfaces. As the supporting platform for such applications, web browsers execute and manage dynamic and potentially malicious code. However, lack of protection mechanisms in the execution environment provided by web browsers has made various attacks possible that can compromise the privacy and integrity of web applications. Various existing solutions are proposed to secure web applications.*

This work presents a survey of web application threats and countermeasures research which is the emerging domain. The goals of this research work are three-fold: i) serve as a guideline for researchers who are new to web security domain and want to contribute to this research area, ii) provide a guidelines for secure web applications, and iii) provides further research directions in the web application security domain.

Keywords: malicious JavaScript, web security, malicious web requests, malicious browser extensions, malicious advertising, web session integrity.

1. Introduction

Web browsers have been evolving from an application that displays simple static web pages into a complex environment that executes a myriad of content-rich web applications. Web application logic is divided into client-side components and server-side components. Web browsers provide the execution environment to client-side components of web applications. In addition, web browsers allow themselves to be extended by third-party code, such as browser extensions. It allows web browsers to test new functionality and enhance user experience and extend support of web browsers to new features. This increases the complexity of the browser execution environment. However, an important aspect of such complex execution environment has been largely overlooked: Security.

The execution environment provided by web browsers contains a set of trusted and untrusted components to process the web content and communicate with web servers. For example, the JavaScript engine executes code from various sources such as web page, extensions, etc. Browser extension enrich user experience by providing new functionalities such as, auto logged in users to web application, notify new emails, etc.

Therefore, existing state-of-the-art web security systems need to be examined from the perspective of attacks which can be reasonably expected against these systems. This research work studies existing systems.

2. Same-origin Policy (SoP)

To prevent data of one web application from being accessed by other web applications in execution environment, web browsers use the same-origin policy (SOP)[1]. For each web page, browsers create a separate environment and associate *origins* to web page objects. An origin is defined as the triple of *protocol*, *host*, and *port*. SOP allows a piece of code S to access an object O only if S and O are from the same origin. In effect, SOP partitions the web applications execution environment based on origins. Code from the origin of a partition is allowed to fully access web page data in the same partition, but code from other origins is not allowed to access objects in this partition. In essence, SOP ensures proper separation at document level.

Under SOP, all contents included in one web page are associated with the origin of the hosting web page. Hence, untrusted third-party code embedded in a web page, such as libraries and advertisement code, runs with the privileges of web application's origin even though it only needs limited access to resources in the origin. This could lead to compromise the integrity of web application sessions. For example, web applications to earn revenue could sell some region of their web pages to an advertising network. The advertising network takes advertisements from its client and displays them on the publisher's web pages. An attacker pretending as an advertiser to the advertisement network, by submitting the malicious code he could compromise integrity of the web applications, alter browser homepage, spawn pop-ups, or forge malicious requests to victim web application.

3. Observations

Current browsers do not provide necessary isolation on different components that can affect web sessions during runtime. JavaScript is the most widely used programming language in web based applications. It plays a key role in supporting dynamic and interactive features in the latest generation of web applications. It is also used as a platform-independent language to build browser components, such as browser extensions. However, attackers can use JavaScript as a tool to carry out attacks on user sessions.

4. Contributions

In summary, this research paper makes the following contributions:

- Classifies state-of-the-art research performed in the web security.
- Provides analysis of important aspects in preserving privacy and integrity of web applications.
- Provides guidelines and further research directions required in the web security area.

5. Literature Review

The growing ubiquity of untrusted third-party JavaScript in web applications offers attackers an opportunity to compromise the integrity of web applications and subvert the behavior of web applications. Patil et.al.[2] proposed that the root cause of the web session integrity problem is the lack of behavior control in the JavaScript environment. By offering the desired fine-grained access control mechanism in the JavaScript environment for JavaScript context, the proposed approach provides separated privilege and least privilege principle support within an origin.

Dong et.al [3] proposed a new behavior model for diagnosing attacks in Ajax applications, which abstracts both client-side state transitions as well as their communications to external servers. The proposed model articulates different states with the browser events or user actions that trigger state transitions. With a prototype implementation, the authors demonstrated that the proposed model is effective in attack diagnosis for real-world Ajax applications. Kailas Patil et.al[4, 5] reported a measurements on a large corpus of web applications to provide a key insight on the amount of efforts web developers required to adapt to CSP. The results also showed errors in CSP policies that are set by website developers on their websites. To address these issues and make adoption of CSP easier and error free, the authors implemented UserCSP a tool as a Firefox extension. The UserCSP uses dynamic analysis to automatically infer CSP policies, facilitates testing, and gives savvy users the authority to enforce client-side policies on websites.

Abhijeet et. al. [6] gives detailed survey of mobile health monitoring system and specially addresses the problem of obtaining confidentiality of client's data across untrustworthy environment such as cloud service provider. The paper discusses the uses of untrustworthy cloud service provider for health services poses serious risk on privacy of client's medical data and intellectual property of mobile health service provider. This risk may reduce adoption of mobile healthcare system.

Omanwar et.al. [7] proposed a novel network bandwidth conservative technique for personalize web access that reduces web latency on low network bandwidth devices or users. In particular, the proposed approach uses object reordering, priotarization and compression algorithm to reduce the web latency. The approach proposed by the authors allowed user to specify his preferences to improve browsing experience with filtering unnecessary advertisements and unwanted content on website and compress images and videos. Thus, low latency network user's perceived latency can be minimized and network bandwidth consumption can be reduced.

Vishal Meshram et.al [8] presented a survey of ubiquitous computing research which is the emerging domain that implements communication technologies into day-to-day life activities. It provided a classification of the research areas on the ubiquitous computing paradigm. The goals of the survey research work were three-fold: i) serve as a guideline for researchers who are new to ubiquitous computing and want to contribute to this research area, ii) provided a novel system architecture for ubiquitous computing system, and iii) provided further research directions required into quality-of-service assurance of ubiquitous computing.

Shekhar et.al.[9] showed in the survey that lot of research work have been focused to restrict android application permissions based on user profile. However there is lack of mechanism that can restrict Internet access on site basis similar to application layer firewall. This paper present comprehensive coverage of different techniques and apps available in Google Play store used to provide access control mechanism.

6. Research Questions

To solve research problems in the web security needs to address the research challenges in Javascript execution environment, safe inclusion of third party contents and regular audits of embedded contents in web applications. The need to the web security solutions generates a number of important research questions:

- How to automatically verify the integrity and behavior of the embedded contents in web applications?
- How to ensure privacy and integrity in the execution environment provided by web browsers?
- How to confine behaviors of browser extensions?
- How to perform regular audits of web applications?
- How to identify malicious contents run-time at client-side?

To achieve privacy and integrity in web execution environment, it is necessary to address above research questions.

7. Conclusion

We analyzed protection mechanisms available inside an origin, and the existing research efforts to protect a web application's session from malicious JavaScripts injected in webpages. We observed that there is a lack of behavior control mechanism in the JavaScript environment of web browsers. This allows attackers to compromise the privacy and integrity of web sessions. This research work serves as a guideline for researchers who are new to web security domain and want to contribute to this research area. In addition, it also provides further research directions in the web application security domain.

References

[1] Same-origin policy. Available [online]: https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

[2] Kailas Patil , Xinshu Dong , Xiaolei Li , Zhenkai Liang , Xuxian Jiang, Towards Fine-Grained Access Control in JavaScript Contexts, Proceedings of the 2011 31st International Conference on Distributed Computing Systems, p.720-729, June 20-24, 2011 [doi>10.1109/ICDCS.2011.87]

[3] X. Dong, K. Patil, J. Mao and Z. Liang, "A comprehensive client-side behavior model for diagnosing attacks in ajax applications", Proceedings of the 18th International Conference on Engineering of Complex Computer Systems (ICECCS), 2013.

[4] Kailas Patil and Braun Frederik, "A Measurement Study of the Content Security Policy on Real-World Applications", International Journal of Network Security, Vol. 18, No. 2, pp. 383-392, 2016.

[5] Kailas Patil, T. Vyas, F. Braun, M. Goodwin, and Z. Liang, "Poster: UserCSP-User Specified Content Security Policies", SOUPS, 2013.

[6] Abhijeet S. Kurle and Kailas Patil, "Survey on Privacy Preserving Mobile Health Monitoring System using Cloud Computing", International Journal of Electrical, Electronics and Computer Systems, IJEECS, Vol. 3, No. 4, pp. 31-36, 2015.

[7] S. S. Omanwar, K. Patil and P. N. P. Pathak, "Flexible and fine-grained optimal network bandwidth utilization using client side policy", Proceeding of the International Journal of Scientific and Engineering Research, IJSER, vol. 06, no. 07, pp. 692-698, 2015.

[8] Vishal Meshram, Vidula Meshram and Kailas Patil, "A SURVEY ON UBIQUITOUS COMPUTING", ICTACT JOURNAL ON SOFT COMPUTING, IJSC, vol.06, no.02, pp.1130-1135, 2016 .

[9] Shekhar Shende and Kailas Patil, "Survey on Access Control Mechanism in Android", International Journal of Electrical, Electronics and Computer Systems (IJEECS), Vol. 3, No. 4, pp. 22-26, 2015.

BIOGRAPHIES

Shital Patil is the security analyst in Kaitec Solutions pune, India. Her research interests include Cyber Security, Ubiquitous Computing, Internet of Things and Web Security.