Chapter 19
A Taxonomy of Browser Attacks

Anil Saini
Malaviya National Institute of Technology, India

Manoj Singh Gaur
Malaviya National Institute of Technology, India

Vijay Laxmi
Malaviya National Institute of Technology, India

ABSTRACT

Browser attacks over the years have stormed the Internet world with so many malicious activities. They provide unauthorized access and damage or disrupt user information within or outside the browser. This chapter focuses on the complete attack actions adopted by an attacker while crafting an attack on Web browser. The knowledge gained from the attacker's actions can be framed into a suitable taxonomy, which can then be used as a framework for examining the browser attack footprints, vulnerability in browser design, and helps one to understand the characteristics and nature of an attacker. This chapter presents a browser attack taxonomy that helps in combating new browser attacks and improving browser security.

INTRODUCTION

A Web browser is an important component of every computer system as it provides the interface to the Internet world. The browser allows users to view and interact with content on the web pages. It provides users the interface to perform wide range of activities, such as, personal financial management, online shopping, social networking and professional business. Hence, the web browsers are becoming an increasingly adequate and important platform for millions of Internet users. With the rapid increase in the number of users, browsers are becoming the potential source of attacks. The appearance of various browser attacks executed on web browsers cause real challenges to Internet user in protecting their information from an attacker. The browser attacks provide an unauthorized access, damage or disruption of the user information within or outside the browser. For example, suppose an attacker is able to inject malicious scripts that do not change the website's appearance, but silently redirect you to another web site controlled by an attacker without your notice. This redirected malicious web site may execute some malicious program to download a malicious file on your machine (Howes, 2004). The major goal of such attacks is to allow remote access of your machine to the attackers, and to capture personal information, often related to obtaining credit card, banking information and data used for identify theft.

DOI: 10.4018/978-1-4666-6324-4.ch019

Like other software, web browsers are vulnerable to attack and exploit if appropriate updates and security patches are not applied. Moreover, a fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins and add-ons are not fully patched. The plug-ins and add-ons are third party software used to enhance Browser functionality, but at the same time they are vulnerable to attacks. The vulnerabilities in Firefox extension system have been mentioned in the literature (Beaucamps, Reynaud & Loria-Nancy, 2008), where the risks associated with the Firefox extension have been explained. The plug-in and add-on softwares are not automatically patched with the Browser updates, instead they require some extra support from third party for updating their versions and patching vulnerabilities

Traditionally, browser-based attacks are commonly originated only from malicious web sites (Obied & Alhajj, 2009). However, the attackers have recently been introduced attacks which are beyond the malicious web sites. Over the years, the browser-based attacks are initiated different attack vectors apart from malicious web sites. The attacks may arises from trusted and legitimate web applications, since all web applications developers are not security experts and due to poor security coding the vulnerabilities occurs in these web applications. The attacker can exploit vulnerabilities present in trusted or legitimate web sites to deploy attacks. For instance, an attacker can take advantage of vulnerabilities within browser to run arbitrary code, which can steal user's sensitive information or install malware. Plug-in and extension vulnerabilities can also be exploited by an attacker to initiate browser-based attacks.

There are several questions, which could help to characterize an attacker: *Who is the attacker? What source an attacker used to enter into the system? What Vulnerabilities he exploited?* By answering these questions, we can get the clear picture of an attacker and what should be done next in order to protect the information. This chapter will cover a concise survey of browser-based attacks and how these attacks are initiated by an attacker. In addition to that, the chapter focuses on the complete attack process, which helps to understand the characteristics, and the nature of an attacker. The actions taken by an attacker to execute Browser-based attack have been represented in the form of taxonomy using example attack scenario. The proposed taxonomy consists of an attacker side dimension, or vulnerability model, classifying how an attacker is launching an attack, and Browser side dimension, or security model, classifying how the Browser is trying to protect the attack. With the help of this taxonomy, we are able to analyze different weak points with an attacker can exploit, and at the same time what action the Browser will take to provide security against these attacks. Our taxonomy tries to provide the details of Browser attacks and vulnerabilities exploited in different Browser components. Thus, our taxonomy is different from other previously mentioned taxonomies discussed in Section 2 in two ways: First it will explain the vulnerabilities present at different Browser components, and second it will classify different attacks on those components. In addition to that, we also classify the security model which plays an important role in securing web Browsers. In nutshell, this chapter surveys Browser attacks caused due to vulnerabilities exits in different components, and discuss the security model adopted by Browser in order to provide protection against these attacks.

The rest of the chapter is organized as follows: The section two contains the background study of Browsers evolution, and taxonomies adopted in the field of security and attacks. In section 3, an overview of Browser attacks is presented, to better understand the Browser-based attacks, a taxonomy of attack is presented in section 4. Section 5 will discuss the adoption of proposed taxonomy in the field of Browser research, and future direction. Finally, we conclude in section 6.