DOI:10.16002/j.cnki.10090312.2002.02.005

JavaScript 与客户端安全

张志远
(东莞市公安局计算机安全监察科, 广东东莞 523000)

摘 要 客户端安全是网络安全不可分割的一部分。随着 JavaScript 程序越来越多的被使用在各种场合,其带来的安全问题也日渐突出。本文探讨 JavaScript 影响客户端安全的主要途径和典型方式,并给出解决方法。

关键词 客户端;JavaScript;网络安全;解决方法
中图分类号 TP312JA; TP393

网络安全是最近几年最热门的 IT 话题之一。我们可以把网络简单理解为通过网络设备连接起来的服务器和客户机。客户机安全是整个网络安全不可分割的一部分。因为绝大多数的上网者是以客户端的身份出现在网络上,客户端安全也许离普通上网者的生活更贴近,也更现实。影响客户端安全的因素有很多,比如病毒的威胁、停电的威胁等。本文讨论的重点是 JavaScript 程序对客户端安全的威胁。

JavaScript 是一种具有面向对象、跨平台、结构化等特性的程序语言。经历几年发展,目前版本已非常成熟与强大,提供了许多安全保护措施,保护终端用户不受安全问题困扰,如利用签名脚本对程序员的权限进行限制。但对客户端控制的特性决定了 JavaScript 程序不可避免地成为客户端安全的隐患。随着 JavaScript 程序越来越多的被使用在各种场合,其带来的安全问题也日渐突出

1 JavaScript 程序对客户端安全的影响

以下讨论基于客户端的 JavaScript 处于启用状态。

JavaScript 程序对客户端安全的影响表现在以下两个方面:

1.1 网站管理员可以直接获取用户信息

通过简单的 JavaScript 命令,网站管理员就可获得客户端浏览器版本、操作平台、屏幕分辨率、用户所在国家、使用语言、用户的历史访问记录、IP 地址等敏感信息,网站管理员可以全面记录用户在网站的活动情况,细致到可以记录下用户鼠标的一举一动。更进一步,有心的网站管理员还可获取客户端的目录结构。获取这些信息并不需要利用系统漏洞,有些甚至是在用户不知情的情况下完成,而这些信息往往为黑客提供了进行攻击的突破口。

1.2 利用系统漏洞,通过 JavaScript 程序可获取客户文件,下载、安装恶意程序,直至完全掌握客户机

因为系统漏洞不同,客户端安全受威胁的方式和程度也不同,这里通过几个典型例子加以说明。

(1) 因为 JavaScript 程序在浏览器中运行,浏览器对整个系统安全具有特殊的意

收稿日期:2002-06-11
作者简介:张志远(1965-),男,广东东莞人,工程师。

义。JavaScript 程序可以利用浏览器中安全措施的漏洞进入文件系统。早期的 IE4.0 允许 JavaScript 程序在客户不知情的情况下用剪切和粘贴的方式获取文件并上传，现在 IE5.0以上版本则对此漏洞做了修补。

（2）与 Cookie 有关的漏洞。网站管理员在 Cookie 中写入特定的 JavaScript 程序，当 Cookie 被调用时，内嵌的 JavaScript 程序执行非授权操作以获取有关 HTML 文件。相应的例子和 JavaScript 程序可以在 Peacefire.org 的技术文档中找到。Netscape Communicator 4.x 受此漏洞影响。

（3）访问恶意网站时，网站管理员会利用 JavaScript 程序使客户端下载病毒、木马或其它恶意程序。

2001 年 8 月，日本政府信息技术促进局（IPA）通报一个案例，使用 IE 4.X 或 IE 5.X 的用户在登陆一个被黑客掌握的拍卖网站时，会自动下载一段恶意的 JavaScript 程序，该程序运行时会修改系统配置。

另一个典型代表是 Nimda 蠕虫病毒，传播方式之一是客户端访问受病毒感染的网站时，暗藏其中的 JavaScript 程序执行下载病毒到客户端。

既使是在客户端设置下载文件前要显示安全警告窗口，也未必能阻止这类恶意攻击。新的测试发现，JavaScript 程序可实现屏幕欺骗功能，别有用心的网站管理员可利用简单的 JavaScript 程序将安全警告窗改头换面，如改为链接指向之类的善意提示，并可屏蔽窗口的‘取消’按钮，使用户在不知不觉中执行下载命令。

（4）也许被访问的网站本身并没有攻击意向，但从网站下载的文件或通过网站收到的电子邮件却可能包含了恶意的 JavaScript 程序，一旦这些文件被调入浏览器中查阅，也会对客户端造成侵害。为保证安全，利用浏览器操作的电子邮箱系统对传输的文件进行 JavaScript 程序过滤，Hotmail.com 便是其中一个。但近期发现通过使用十六进制 ASCⅡ码，可以绕过 Hotmail 对 JavaScript 程序的过滤，这一安全漏洞使恶意的 JavaScript 程序可以在用户打开邮箱时显示一个欺骗的登陆界面，让用户输入密码并窃取它。

（5）安全设置不当的安全问题。随着浏览器版本的升级，其中关于安全性的设置也变得越来越繁多复杂。在与 JavaScript 有关的设置中，包含‘跨域浏览子框架’的选项，这个功能的启用可以使一个框架中的 JavaScript 程序捕捉另一框架从不同域服务器装入的信息，这种情况下，如果客户端一边网上购物，一边浏览其它网站，极有可能被心怀叵测的网络管理员读到用户的信用卡帐号、密码等信息。除非有特别需要，不要在客户端启用此项功能。

2　解决方法

防止 JavaScript 程序威胁客户端安全的方法并不复杂。JavaScript 程序作用于客户机的渠道可分为两类，一是客户端远程访问，包括浏览网页，使用浏览器打开异地文件等。二是 JavaScript 程序内嵌在某些文件中，通过客户端下载、邮件、文件交换等方式进入客户机，当该文件被调入浏览器时，内嵌的 JavaScript 程序被执行。因此，与 JavaScript 有关的安全问题最终可归结为防范恶意的 JavaScript 程序在客户浏览器上运行。第一，合理设置浏览器的安全级别。第二，不要访问不信任的网站，不要用浏览器打开远程不信任的文档。第三，对本机内的文件，如果对其安全性有怀疑，在调入浏览器之前，最好用编辑器等工具先检查一下是否内嵌有恶意的 JavaScript 程序。

参考文献

1 John P 美). JavaScript 编程起步,云巅工作室译. 北京:人民邮电出版社,2001

2 Martin W(美). JavaScript 示例导学. 聊宏斌译,北京科海培中技术有限责任公司, 2002

3 Allen W R,Jason D G,Charlton T. Pure JavaScript. USA Sams Publishing,1999

4 Microsoft Corporation. Microsoft Scripting Technologies. USA Microsoft corporation,1998

JavaScript Procedure and Client's Safety

Zhang Zhiyuan

(Public Security Bureau Dongguan City)

Abstract Client's safety is an inalienable part of network security. As JavaScript Procedure is used on various occasions more and more, the security problems caused by it are becoming outstanding day by day. This article points out the main and typical modes of JavaScript procedure to endanger the client's safety, and some countermeasures are introduced to solve these problems as well.

Keywords client's safety; JavaScript; network security; solution

(上接第19页)

The Development of the Infrared Remote Control Photoelectric Gun

Li Mingxu, Yu Cheng

(Dongguan University of Technology)

Abstract The co-authors have developed a new-type of infrared remote control photoelectric gun. In this paper, they introduce the operational principles, installation, adjustment and application of the infrared transmitting and receiving circuits based on the frequency division modulation infrared remote control technology and the calculating circuit.

Keywords infrared remote control; frequency division modulation; electronic toy