HTML5新特性安全研究综述

韩多成

（宁夏工商职业技术学院，宁夏 银川 750021）

摘 要： HTML5的推广与应用带给了浏览器更多功能，属于Web应用最新标准。但同时HTML5新特性存在安全隐患，由不同新特性安全问题构成。文章结合功能不同对HTML5标签和表单、通信、离线应用的问题探究，将HTML5安全问题总结为不同类型，指出了HTML5安全研究今后发展，即：新特性安全性、恶意检验、新安全应用等。

关键词： HTML5；新特性；安全

如今，Web成为人们生活、工作重要组成部分，例如网购、银行业务、新闻观看、社交等。伴随着人们需求的多元化，HTML5的出现有效满足了人们多元化的需求。尽管HTML5应用形式更为多样化，但其安全性也随之出现，以往Web安全问题在HTML5条件下形成了新的发展。同时，XML HttpRequest2，Web Storage等新API引进了新的跨源、标签通信风险[1]。HTML5安全问题与浏览器有着密切联系，因此，各国纷纷对HTML5新特性安全展开研究。

1 HTML5新特性安全研究

笔者结合新特性功能差异分析其安全现状。跨站点脚本因其普遍性，可以作为其他侵入的决定条件，因此进行单独分析。另一方面，分析确保其完整性以及HTML5有关安全问题。

1.1 标签和表单

安卓平台HTML5 APP发现了存在XSS供给。因此，也应列为今后研究课题之一，例如：HTML5在移动终端、WebTV等平台安全、隐私保护、恢复力。HTML5对HTML解析器进行规范，对其新的内容展开定义，例如音视频标签，MathML等。同时，丰富原有表单、内嵌窗口属性。其内容不仅带有跨站点脚本威胁外，也会带有其他风险。Iframe的sandbox属性可以设定是否允许内嵌窗口执行脚本，进而让攻击人员展开UI欺骗过程中越过FrameBusting检验。HTML5增加表单功能也带来了新的风险，例如：autocomplete属性提供自动完成功能，让Web结合表单ID把输入信息储存在文档中，为用户提供方便，也与同源策略背道而驰，容易导致表单隐私外泄。不过，研发人员依然要在服务器终端对输入展开认证，忽略造成的安全风险。Formaction属性涵盖了form的action属性，侵入者如果可以对表单输入其属性，就能够操作表单提供的地址。同时，因为并非脚本注入，因此不能受到CSP的保护[2]。

HTML5新标签丰富性造成的安全问题也是多元化的，为侵入者越过防御提供了条件，也容易导致研发者应用过程中出现新的问题，例如资料外泄、表单注入。现阶段，新标签安全性问题想要展开系统的研究，具有一定困难，需要以打补丁方式展开，有待进一步研究其安全问题。例如各终端浏览器中的不同展现方式。

1.2 通信功能

1.2.1 postMessage API

立足于安全性问题考量，运营在相同浏览器的窗口间、标签页的通信存在不同影响因素；实际合理需求使不同站点内容可以在浏览器中交互。HTML5为跨文档信息机制创造了postMessage API，进而达到窗口通信、标签页功能。利用响应事件接受信息，经过检查信息来源判断是否需要科学处理。对此，一些人进行了研究，发现新型浏览器在设置postMessage技术过程中客户端通信协议发生安全问题；具体origin源认证发生漏洞，给了侵入者可乘之机。针对这一问题，提供跨文档消息输送形式SafePM确保安全性。

1.2.2 XMLHttpRequest2

XMLHttpRequest2 API为Ajax技术的应用创造了条件，作为其修改后的版本，XHR2具有跨源与进度事件功能。跨源支持也为CSRE提供了条件，经过XHR2目标的setRequestHeader设定Content-type，multi/form-data，把属性WithCredentials设定true，进而实现cookie重放展开攻击。

现阶段，不同地区对postMessageAPI与WebSocket安全性展开研究，同时得到了推广与应用。其中，对postMessage的分析包括研发人员安全使用与浏览器bug，以及其他安全问题中的展现与新恶意使用形式。XHR2基于XHR下进行提升，分析集中于跨源新特性带来的风险。通信API包含客户端和服务端，分析服务端达到安全性问题，也是其今后发展主导。

1.3 离线使用和保存

1.3.1 本地储存API

WebStorage作为HTML新增的本地储存有效形式，相对于cookie，WebStorage降低了通信流量，减少了被监听的风险。WebStorage应用单一的字符串键值对本地储存信息，具有简单简便的特点。不过，针对较大结构化数据储存具有一定困难。IndexedDB可以在客户端储存较大的结构化数据，同时检索效果显著。

1.3.2 应用程序缓存

伴随着互联网的推广与应用，成为人们生活、工作重要组成部分。不过，在实际应用中偶尔出现网络中断问题；而通过HTML5引进应用程序缓存，防止程序加载过程中的正常网络请求。若缓存清单文件是最新的，浏览器则无需检验

作者简介： 韩多成（1978— ），男，甘肃民乐人，讲师，学士；研究方向：网络技术，有静态网页制作和服务器配置等。

气态资源是否为最新，这样一来能够节省带宽，快速进入页面，也降低服务器荷载。

2 HTML5新特性安全性划分

现阶段，安全界对HTML5安全性给予了高度重视，可以划分为2类。

（1）对某个特性展开分析，例如，发现新的恶意形式、API自身存在问题、应用漏洞等。其中，通信API与离线应用、储存关注较多，该方面是因为其特性自身复杂性，本地储存客户端的实现，应用程序缓存的长久性与时间机制全部引进了安全风险。一方面因为应用广泛性，例如：postMessage在应用对源验证漏洞。多媒体类特性也具有一定复杂性，包含到脚本接口和硬件连接特性，生成一些安全问题。属性和设备访问类特性因为自身特征，其研究集中于社会工程学的隐私泄露。标签和表单时常引入新的注入供给，供给思路固定，预防措施成熟受到了重视。

（2）主要是安全使用建议与整体安全分析、以往问题的总结、安全检测等。例如HTML5总体展开安全性研究，把HTML5安全问题划分成3类：HTML5安全泄漏、新型供给机制、新特性滥用。通过调查得出挖掘思路，基于漏洞出现原因分析能够把HTML5安全问题划分3类。①受传统因素影响，即Web供给思路延伸至HTML5应用，对原来预防制度造成影响。例如：新标签带来的XSS对黑名单过滤出现挑战，移动端HTML5 APP出现的XSS等。这种问题重点关注新供给和传统供给在思路上是否相同。②新功能的恶意使用，即：新特性在提供研发便利条件过程中，为攻击者提供了新的供给方法。③新特性错误出现漏洞，即：研发人员在应用新特性过程中因为对新功能缺少了解，未对安全漏洞有所重视。例如：应用CORS过程中缺乏对源的校正与数据检验[3]。

3 HTML5新特性安全展望

现阶段，HTML5标准体系趋于成熟，其安全性研究给予了大量投入，包含一些漏洞与研究成果。XML HttpRequest2，Web Storage等新API引进了新的跨源、标签通信风险。接下来，笔者就今后HTML5新特性安全研究展开分析。

3.1 新特性安全性

伴随着HTML5的规范化发展，安全性研究同步发展。不过，在其新特性自身研究上仍然存在诸多问题，集中于两点：（1）虽然研发人员对一些新特性展开研究。不过，在Web高速发展的同时新特性也有了新的发展；例如：W3C推出Web Storage第二版，持续推出的新特性具有适用性广与修补安全性，同时也出现了新的安全问题，有待优化。（2）一些特性的安全性缺少综合性考量，研究的特性不能规避其他恶意使用形式。例如：通信API服务端、多媒体API的底层兼容。

不同新特性应用在浏览器中逐渐趋于复杂性。因此，对不同特性隐藏的安全性问题依然是今后研究重点，其中包含隐私保护、新恶意使用形式、平台差异等。笔者建议通过差异化形式对新的安全问题进行研究。

3.2 恶意使用检测

现阶段，研究多集中于发现一个问题处理一个问题，具有局限性。一些研究注重现存在的漏洞检验，缺乏对HTML5恶意使用检验与预防措施，考量恶意行为建模研究、特征提取，设备学习等方法，依据入侵检验系统形式。

3.3 跨平台安全性

W3C集中于统一不同平台的Web标准，便于研发功能多样的Web应用流程。但是，各平台、终端有着不同的标准，进而埋下安全隐患。移动网络与物联网的快速发展让HTML5得到了应用，浏览器也趋于多样化，一些智能设备中也安装了Web程序。这样一来，一些智能设备也会存在安全问题，例如：设备访问API在各硬件特性平台中存在隐患[4]。现阶段，安卓平台HTML5 APP发现了存在XSS供给。因此，也应列为今后研究课题之一，例如：HTML5在移动终端和WebTV等平台安全、隐私保护、恢复力。

4 结语

总而言之，Web现已得到了广泛应用，对HTML5安全性有着重要作用与意义。笔者围绕HTML5新特性安全性，首先综合国内外研究分析，随后结合功能不同分析HTML5不同新特性安全漏洞。同时，将HTML5安全问题划分为不同类型。最后，进一步分析了其未来发展的安全问题。

[参考文献]

[1]张玉清，贾岩，雷柯楠，等.HTML5新特性安全研究综述[J].计算机研究与发展，2016（10）：2163-2172.

[2]赵学铭，王刚.基于HTML5的交互式移动学习平台研究[J].现代教育技术，2016（9）：106-112.

[3]王淑庆，韩勇，张小垒，等.基于HTML5的时空轨迹动态可视化方法[J].计算机工程与设计，2015（12）：15.

[4]徐久成，孔德宇，骆阳阳.基于HTML5的移动在线教育平台学习支持技术[J].河南师范大学学报（自然科学版），2015（3）：143-147.

Overview of HTML5 new features security study

Han Duocheng

（Ningxia Vocational Technical College of Industry and Commerce, Yinchuan 750021, China）

Abstract: The promotion and application of HTML5 bring more functions to the browser, which is the latest standard of Web application. But at the same time there are security risks in the new HTML5 features, which are made up of different new feature security issues. In this paper, the HTML5 tags and forms, communication and offline applications are explored based on different functions. The paper summarizes the HTML5 security issues as different types and points out the future development of HTML5 security research, namely, new features security, malicious inspection, new security applications and so on.

Key words: HTML5; new features; security