Kennesaw State University
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2016 KSU Conference on Cybersecurity Education, Research and Practice

Hands-on labs demonstrating HTML5 security Concerns

Mounika Vanamala
vanamala.mounika7@gmail.com

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp

Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Vanamala, Mounika, "Hands-on labs demonstrating HTML5 security Concerns" (2016). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 15.
https://digitalcommons.kennesaw.edu/ccerp/2016/Student/15

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract
The research is focused on the new features added in HTML5 standard that have strong implications towards the overall information security of a system that uses this implementation.A Hands-on Lab is developed to demonstrate how Web Storage and the Geo-location API of HTML5 can affect the privacy of the user.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

This event is available at DigitalCommons@Kennesaw State University: https://digitalcommons.kennesaw.edu/ccerp/2016/Student/15

SUMMARY

The research is focused on the new features added in HTML5 standard that have strong implications towards the overall information security of a system that uses this implementation. The built-in security support offered by features like Cross Origin Resource sharing, Web Storage (either Local Storage or session Storage), Geolocation, Web Sockets advantage over the capabilities offered by HTML4.

HTML5 provides new features to web applications but also introduces new security issues. Consequently, through adding those new features the evolution of the current web standards to HTML5 introduces also new security vulnerabilities and threats. New HTML5 features open innovative ways to attackers for launching their attacks. These new vulnerabilities, threats and attack possibilities are addressed in this paper. Every part of the specification has an own subsection dealing with security. This paper covers the points that need to be well thought-out when implementing the corresponding parts. The vulnerability which can result from this feature and how to securely implement it by the browser manufacturers is described.

A Hands-on Lab is developed to demonstrate how Web Storage and the Geolocation API of HTML5 can affect the privacy of the user. The main security concern with Local Storage is that the user is not aware of the kind of data that is stored in Local Storage. The user is not able to control storage respectively access to data stored in Local Storage. The new threats introduced by local storage like Disclosure of Confidential Data and User tracking are discusses in this paper.

The HTML5 Geolocation API provides the possibility of identifying the user's physical location based on GPS position. Prior to HTML5 it was only possible to determine the position of the user through plugins such as Java Applets. With the Geolocation API mainly privacy issues are associated. Every website is able to determine the position of the user which can be used by web application providers for user identification and tracking. This breaks the security requirement of Identity protection.