Smart XSS Attack Surveillance System for OSN in Virtualized Intelligence Network of Nodes of Fog Computing

Shashank Gupta, Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, 136119, India
B. B. Gupta, Department of Computer Engineering, National Institute of Technology Kurukshtra, Kurukshtra, India

ABSTRACT

This article introduces a distributed intelligence network of Fog computing nodes and Cloud data centres for smart devices against XSS vulnerabilities in Online Social Network (OSN). The cloud data centres compute the features of JavaScript, injects them in the form of comments and saved them in the script nodes of Document Object Model (DOM) tree. The network of Fog devices re-executes the feature computation and comment injection process in the HTTP response message and compares such comments with those calculated in the cloud data centres. Any divergence observed will simply alarm the signal of injection of XSS worms on the nodes of fog located at the edge of the network. The mitigation of such worms is done by executing the nested context-sensitive sanitization on the malicious variables of JavaScript code embedded in such worms. The prototype of the authors’ work was developed in Java development framework and installed on the virtual machines of Cloud data centres (typically located at the core of network) and the nodes of Fog devices (exclusively positioned at the edge of network). Vulnerable OSN-based web applications were utilized for evaluating the XSS worm detection capability of the authors’ framework and evaluation results revealed that their work detects the injection of XSS worms with high precision rate and less rate of false positives and false negatives.

KEYWORDS


1. INTRODUCTION

1.1. Fog Computing

A new virtualized platform (i.e. Fog Computing) is developed that outspreads the infrastructure of cloud platforms to the edge of the network (Bonomi et al., 2012). Fog computing performs the computation of resources in the edge of the network (very close to the ground). It generally performs its computation between the cloud data centres and the network of smart devices. Figure 1 highlights the three-way hierarchy, that clearly highlights the devices of fog computing will be act as an intermediary nodes between the cloud data centres and the network of end smart devices (Stojmenovic et al., 2014). The
1.2. Cross-Site Scripting (XSS) Attack

XSS vulnerabilities are considered to be the topmost threat that have turned out to be a plague for the modern web applications like facebook, twitter, linkedIn, etc. (Gupta et al., 2015a, 2015b, 2014). Such worms steal the sensitive credentials of the active users by injecting the malicious JavaScript code in the form of some posts on such web applications. The statistics of acunetix web application vulnerability report 2015 (Acunetix Web Application Vulnerability Report, 2015) clearly reveals that nearly 38% of web sites were vulnerable to XSS attacks and falls first in the list. In addition, the statistics of 2015 website security statistics report by white hat (Website Security Statistics Report, 2015) undoubtedly discloses that XSS was a significant issue across all platforms of diverse languages utilized by modern web applications. Figure 2 illustrates the simple scenario of exploitation of XSS attack on the web server installed on the backbone of Fog device.

Here, web server is deployed on the node of Fog computing, that acts as an intermediary between the data centres of cloud platforms and the network of smart end devices (placed at the edge of the network). The malicious smart devices can also inject the vulnerable JavaScript code on this Fog device that can also be replicated to the cloud data centres. Later on, such vulnerable piece of JavaScript code will get fetched by the smart devices network. The XSS attack will get exploited on the web browsers of smart devices on the execution of this suspicious JavaScript code (Gupta et al., 2017a, 2017b). The speciality of such vulnerable strings of JavaScript is that they simply replicate themselves onto the different adjacent nodes of Fog network and data centres of Cloud computing. Figure 3 highlights the detailed pattern of exploitation of XSS attack on the OSN web server deployed at the fog computing network. The exploitation of XSS attack will get executed on the web browser of smart devices and the credentials (cookies, password, etc.) of the victim are being re-directed to the attacker’s domain.

1.3. Our Contributions

The key contributions of our work are as follows:

- A novel XSS defensive model is introduced that executes in a distributed intelligence network of cloud data centres and fog computing for defending against XSS vulnerabilities on OSN;
Related Content

An Approach to Checking Compatibility of Service Contracts in Service-Oriented Applications
[www.igi-global.com/article/approach-checking-compatibility-service-contracts/4103?camid=4v1a](www.igi-global.com/article/approach-checking-compatibility-service-contracts/4103?camid=4v1a)

Selective Service Provenance in the VRESCo Runtime
[www.igi-global.com/chapter/selective-service-provenance-vresco-runtime/66968?camid=4v1a](www.igi-global.com/chapter/selective-service-provenance-vresco-runtime/66968?camid=4v1a)
On Feature Interactions Among Web Services
[www.igi-global.com/article/feature-interactions-among-web-services/3068?camid=4v1a](www.igi-global.com/article/feature-interactions-among-web-services/3068?camid=4v1a)

Service Class Driven Dynamic Data Source Discovery with DynaBot
[www.igi-global.com/article/service-class-driven-dynamic-data/3103?camid=4v1a](www.igi-global.com/article/service-class-driven-dynamic-data/3103?camid=4v1a)