

웹 표준으로 변경 시 발생하는 웹 페이지 보안 체크 모델 제안

원희연⁰, 김재웅^{**}, 이윤열^{*}, 채의근^{*}, 정영석^{*}

⁰공주대학교 컴퓨터공학과,

^{*}공주대학교 컴퓨터공학과,

^{**}공주대학교 소프트웨어학과

e-mail: why980909@gmail.com⁰, jwkim@kongju.ac.kr^{**}, {alphaone, ygchae, merope}@kongju.ac.kr^{*}

Proposal of a web page security inspection model that occurs when changing to a web standard

Hee-Yeon Won⁰, Jae-Woong Kim^{**}, Youn-Yeoul Lee^{*}, Yi-Geun Chae^{*}, Young-Suk Chung^{*}

⁰Dept. of Computer Engineering, Kongju National University,

^{*}Dept. of Computer Engineering, Kongju National University,

^{**}Dept. of Software, Kongju National University

● 요약 ●

ActiveX와 같은 플러그인으로 돌아갔었던 웹 페이지들은 보안 취약성과 인터넷 익스플로러(IE)의 서비스 종료로 인하여 많은 웹 브라우저들이 플러그인 제거 사업을 진행하였다. 하지만 웹 표준으로 전환하였을 때 생기는 웹 호환성과 보안 문제들이 발생하였다. 이를 해결하고자 호환성과 보안 문제를 혼린 시킨 클라우드 서버를 이용하여 미리 파악하고 진단할 수 있는 웹 페이지 보안 체크 모델을 제안한다. 본 논문에서 제안한 모델을 적용한다면, 웹의 표준 및 호환성과 보안 문제에 대해 더 빠르게 파악하는데 도움을 줄 수 있을 것이다.

키워드: 웹 표준, 웹 호환성, 웹 보안

I. Introduction

인터넷에 접속하여 웹에 있는 정보를 보기 위한 프로그램으로 웹 브라우저가 개발되었다. 웹 브라우저로서 점유율이 높았던 인터넷 익스플로러(Internet Explorer)의 서비스가 종료됨에 따라 확장프로그램으로 사용되던 ActiveX와 다양한 플러그인이 사용의 불편함과 악성코드에 취약점으로 더 이상 사용되지 않고 있다. 정부는 2018년부터 플러그인 제거 사업을 추진해 왔으며 그 결과 대부분의 플러그인 제거는 해결되었으며 ActiveX를 대체하기 위해 다양한 기능을 플러그인 없이 브라우저만으로 쉽게 사용할 수 있는 HTML5로 전환하였다.[1] 그러나 새롭게 추가된 기술들로 인해 웹 기반 취약점에 대한 공격 범위가 넓어지는 문제가 발생했다. 이러한 취약점인 보안 문제를 찾아내기 위한 웹 페이지 보안 체크 모델을 제안한다. 제안된 모델을 활용하면 보안에 대한 취약점을 찾는 데 도움이 될 것이다.

II. Preliminaries

1. Related works

1.1 웹 표준 HTML5

웹 표준은 웹 기술과 관련된 규약과 규칙의 집합으로 개발자들이 웹 페이지를 개발할 때 따라야하는 표준화된 규칙들을 의미한다. 2014년 W3C의 최종 웹 표준으로 채택된 HTML5는 신규 기능으로 Canvas, Cross-document messaging, Geolocation, Web storage, Web worker 등 다양한 멀티미디어 기능과 보안 기능을 사용할 수 있다.[2] 또한 HTML5은 강력한 이식성과 상호운용성을 기반으로 아직까지 쓰이고 있다. 하지만 신규 요소에 의한 보안 취약점, CORS 보안문제, Web Worker의 DDoS 공격 취약점, Web Storage 정보 탈취 문제점, Web Socket의 사설 네트워크 정보 유출 문제들이 발생한다.[3]

1.2 웹 호환성

웹 페이지가 다양한 웹 브라우저와 다양한 플랫폼에서 일관되게 작동하는 것을 의미한다. 각각의 브라우저마다 구현 방식이 다르거나

웹 표준을 지키지 않는 경우, 다양한 디바이스 및 환경에서의 차이로 인하여 문제가 발생한다[4].

향후 클라우드 서버에 웹 표준과 호환성에 대해서 어떻게 훈련을 시킬지 연구할 생각이다.

III. The Proposed Scheme

3.1 웹 페이지 보안 체크 모델 구성도

본 논문은 웹 표준으로 전환 시 발생하는 호환성 및 보안 문제 해결 모델로 웹 페이지 보안 체크 모델을 제안한다. 다음 Fig.1.은 제안하는 모델의 구성도이다.

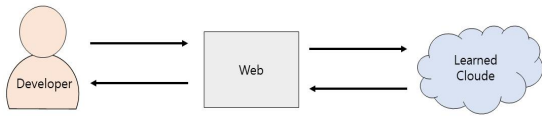
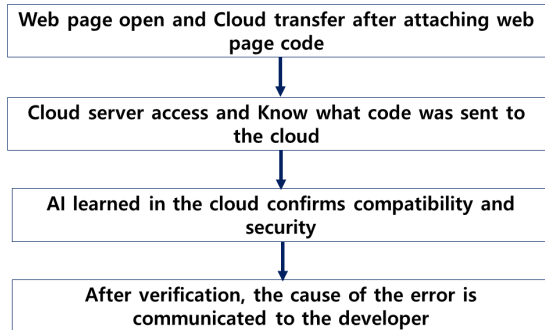


Fig. 1. Web page security check model

개발자는 프로그램 코드를 학습된 클라우드 서버가 있는 웹에 올리면 학습된 클라우드가 웹의 호환성과 보안성을 확인하고 다시 개발자에게 결과를 알려준다.

3.2 웹 페이지 보안 체크 모델 프로세스

다음 Fig.2.는 웹 페이지 보안 체크 모델의 프로세스이다.



첫 번째, 웹 페이지에 접속한 뒤 해당 웹 페이지에 코드를 첨부 후 클라우드에 전송한다.

두 번째, 클라우드 서버에 접속하면 클라우드는 전송된 코드를 파악한다.

세 번째, 클라우드에서 학습된 인공지능이 호환성과 보안성을 확인한다.

마지막으로 오류의 원인을 찾아내면 이를 개발자에게 전달한다.

IV. Conclusions

본 연구에서 웹 표준화 시 발생할 수 있는 웹 페이지 보안 체크 모델에서 발생하는 호환성과 보안 문제를 해결을 위한 모델로 “웹 페이지 보안 체크 모델” 제안하였다. 제안된 모델을 적용하면 호환성과 보안 문제를 좀 더 빨리 발견할 수 있을 것이다.

REFERENCES

- [1] Ministry of Public Administration and Security, <https://www.mois.go.kr/>
- [2] JaeKwon Kwak, "The risk of the HTML5 technology utilization for the realization of Web-based Non-ActiveX security", Korean Society of Information Science and Technology Academic Papers, pp.962-964 , 2015.
- [3] Kang Sok-Chul , Park Jeong-Seop, "Security issues in HTML5 next-generation web standard environment" , REVIEW OF KIISC24,4, pp.44-55, 2014. DOI: 10.13089 /JKIISC.2016.26.4.1025
- [4] Kim, Hye-ri, Lee, Sang-joon “A Study on Web Accessibility Evaluation of Public Agency Homepage”, IJIBC, Vol. 17, No. 4, pp.19-25, 2017. DOI : 10.7236/ IJIBC.2017.17.4.19