한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

무선공유기 웹 보안 설정 점검을 위한 모바일 앱 개발

윤희주*, 김지혜*, 이해영O
O*서울여자대학교 정보보호학과
e-mail: haelee@swu.ac.krO

Development of Mobile Apps for Checking Web Security Configurations of Wireless Access Points

Heeju Yoon*, Ji Hye Kim*, Hae Young LeeO
O*Dept. of Information Security, Seoul Women's University

● 요 약 ●

사물인터넷(Internet of Things)의 도래와 함께, 무선공유기(wireless access point)들의 보안이 심각한 문제로 대두되고 있다. 연구진은 대부분의 무선공유기들이 제공하는 웹 기반 관리 인터페이스들에 웹 어플리케이션 취약점(web application vulnerability)들이 존재할 수 있다는 점을 착안, 국내 주요 무선공유기들에 대한 웹 어플리케이션 취약점 점검을 수행하였으며, 악용이 가능한 여러 취약점들이 존재함을 확인하였다. 본 논문에서는 연구진이 무선공유기 대상 웹 어플리케이션 취약점 점검에 보조적으로 사용하기 위하여 개발한 3종의 모바일 앱(mobile app)들을 설명한다.

키워드: 웹 어플리케이션 취약점(web application vulnerabilities), 무선공유기(wireless access point), 정보보호(information security)

I. Introduction

무선공유기(wireless access point, 이하 공유기)들이 제공하는 웹 기반 관리자 인터페이스들에는 웹 어플리케이션 취약점(web application vulnerability, 이하 웹 취약점)들[1]이 존재할 수 있다. 이에 연구진은 국내 주요 공유기들에 대하여 웹 취약점 점검을 수행하였으며, 이를 통해 교차 사이트 스크립팅(cross-site scripting, 이하 XSS), 패스워드 평문 전송, 검증되지 않은 리다이렉트들(unvalidated redirects) 등의 취약점들이 존재함을 확인하였다[2-4].

본 논문에서는, 국내 주요 공유기들에 대한 웹 취약점 점검을 기반으로, 연구진이 개발한 3종의 모바일 앱(mobile app, 이하 앱)들을 설명한다. 개발 앱들에는 스마트폰 주위 공유기들의 정보를 수집하는 앱, ipTIME 공유기에 대해 모의 공격을 수행하는 앱 및 공유기의 XSS 취약점 대응책을 확인하는 앱을 포함한다. 개발한 앱들은 공유기들 대상 웹 취약점 점검에서 보조적으로 사용이 가능하다.

II. Security Configuration Checking Apps

1. App for Collecting Information on Neighboring Wireless Access Points

주변 공유기 정보 수집용 앱은 현재 스마트폰과 연결된 공유기 및 주위의 공유기들에 대한 정보를 수집하여 사용자에게 보여준다. 수집하는 정보에는, 각 공유기의 SSID(service set identifier), 암호화 방식, RSSI(received signal strength indication), 채널 번호 등이 포함된다. 본 앱은 주변 공유기들의 제조사들을 추측하는데 보조적으로 사용할 수 있다. 특정 공유기의 제조사를 추측할 수 있으면, 알려진 취약점들을 기반으로, 침투 테스트(penetration test) 등을 수행하거나, 적합한 보완책 제시 등을 할 수 있다.

2. App for Synthesizing Security Attacks on ipTIME Wireless Access Points

연구진은 국내 주요 공유기들에 대한 웹 취약점 점검에서 "ipTIME 공유기 XSS 취약점(15-342)"을 발견하여 한국인터넷진흥원(KISA)에 신고하였다. 15-342 취약점에서는, ipTIME 공유기와 연결된 클라이언트에서 악성 코드를 HTTP 요청의 "Referer" 헤더 내용에 포함시켜 송신(공유기 관리자 권한 불필요)하면, 관리자가 ipTIME 공유기의 로그 페이지를 열 때 해당 코드가 실행된다[3]. 해당 취약점은

ipTIME 공유기의 68개 모델들에서 발견되었으며, 현재는 패치가 발표된 상태이다. ipTIME 공유기 모의 공격용 앱은, 15-342 취약점을 기반으로, 현재 스마트폰과 연결된 ipTIME 공유기에 모의 공격용 코드를 삽입한다. 모의 공격용 코드는 자바스크립트(JavaScript) 경고창을 띄우는 코드, ipTIME 공유기의 로그 페이지에 아이프레임(iframe)을 삽입하는 코드 및 ipTIME 공유기의 관리자 페이지 메뉴를 조작하는 코드이다. 본 앱을 통하여 모의 공격을 수행함으로써, ipTIME 공유기들의 펌웨어(firmware) 업데이트 여부를 확인할 수 있다.

3. 공유기 보안 설정 확인 앱

XSS은 가장 널리 분포되어 있는 웹 취약점으로[1], 3개 제조사의 공유기들의 웹 인터페이스들에서도 발견되었다[2]. XSS에 대응하기 위한 가장 기초적인 방법들 중 하나는, HTTP 응답(response)에 "X-Frame-Options" 헤더를 설정하는 것이다. 해당 헤더는 HTTP 응답 페이지가 프레임이나 아이프레임 내에서 표시될 수 있는지 여부를 설정한다. 공격자는 "X-Frame-Options" 헤더가 설정되지 않은 페이지를 특정 사이트의 프레임 또는 아이프레임 내에서 표시되도록 함으로써, 공유기들의 정보를 얻거나, 설정을 변경할 수도 있다. 또 다른 기초 XSS 대응책으로는, HTTP 응답 중 "Set-Cookie" 헤더에 "HttpOnly"를 설정하는 것이다. 이는 클라이언트 측(client-side) 자바스크립트에서의 쿠키 접근을 방지한다. "HttpOnly" 설정이 XSS 자체에 대응하는 것은 아니지만, 공격자가 XSS으로 쿠키 정보를 획득, 세션을 탈취하는 등의 공격을 예방할 수 있다. 본 앱은 현재 개발 중으로, 연결된 공유기의 HTTP 응답을 관찰하여, "X-Frame-Options" 헤더 설정 여부 및 "Set-Cookie" 헤더에서의 "HttpOnly" 지정 여부를 확인하여 사용자에게 알려준다. 개방된 공유기에 접속하는 경우, 사용자는 본 앱을 사용하여 XSS 대응책 설정 여부를 먼저 확인함으로써, XSS으로 인한 침해 사고를 어느 정도 예방할 수 있을 것이다.

III. Conclusions and Future Work

본 논문에서는 공유기 웹 취약점 점검에서 보조적으로 사용할 수 있는 앱 3종을 설명하였다. 주변 공유기 정보 수집용 앱은 스마트폰 주위의 공유기들의 정보를 수집하며, 이를 통해 제조사들을 추측할 수 있다. ipTIME 공유기 모의 공격 앱은 스마트폰과 연결된 ipTIME 공유기에 모의 공격 코드를 삽입함으로써, 보안 설정을 확인할 수 있다. 현재 개발이 진행 중인 공유기 보안 설정 확인 앱은 스마트폰과 연결된 공유기의 HTTP 응답을 관찰하여, XSS 기초 대응책들이 갖추어져 있는지 확인한다. 향후 연구로는, 먼저 3종의 앱들을 통합 및 보완하여 취약점 점검 전문가용 앱으로 발전시킬 예정이며, 또한 보안 설정 확인 앱을 일반 사용자들이 "가볍게" 사용할 수 있는 앱으로 발전시킬 예정이다.

Acknowledgment

이 논문은 2015 년도 정부(교육부)의 재원으로 한국과학창의재단(대학단계프로그램(URP)지원사업)의 지원을 받아 수행된 연구임. 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (NRF-2013R1A1A1006542).

References

[1] OWASP, OWASP Top 10, 2013.

[2] J.H. Kim, H.J. Yoon, D.R. Park, H.Y. Lee, "XSS Vulnerabilities in Web Interfaces of Wireless Routers," KIPS Autumn Conference, Oct. 2015.

[3] H.J. Yoon, D.R. Park, J.H. Kim, H.Y. Lee, "Security Logging Might Be Exploited: A Case of a Wireless Router," RAID 2015, Nov. 2015.

[4] J.H. Kim, D.R. Park, H.J. Yoon, H.Y. Lee, "Web Application Vulnerabilities in Wireless Routers," AsiaSim 2015, Nov. 2015.