

추계학술 발표대회

2019.11.1(금)~2(토)

부경대학교 대연캠퍼스

주최 사단법인 한국인터넷정보학회

주관 부경대학교

후원 (주)카카오, (주)아이티센, LGCNS(주), (주)한스컴정보통신

www.ksii.or.kr



KOREAN SOCIETY FOR INTERNET INFORMATION

사단법인 한국인터넷정보학회

법인등록번호 101-86-11111



논문발표

11월 2일(토) 09:30~11:30(향파관 3층 309호)

세션 B. 인터넷보안

좌장 : 배인한 교수(대구가톨릭대)

- B-1 DLOTA2 기반의 안전한 펌웨어 업데이트 방안
이민경, 최슬기, 광진(아주대)
- B-2 **DCV 기반 공격기법 분석 및 대응방안**
정해선, 광진(아주대)
- B-3 유전 알고리즘을 이용한 컴파일러 분류
황철훈, 신건윤, 한명목(가천대)
- ☆ B-4 은닉형 안티포렌식 APK 분류기법에 관한 연구
김대규, 김창수(부경대)
- B-5 악성코드 프로파일 기반 유사 악성코드 검색 연구
강홍구, 최보민, 김경한, 박순태(KISA)
- B-6 완전동형암호를 이용한 Metropolis Hastings 샘플링 알고리즘에 관한 연구
유준수, 윤지원(고려대)
- B-7 완전 동형암호를 이용한 베이지안 선형 회귀분석
홍미연, 윤지원(고려대)
- B-8 안드로이드 취약점 기반 변종 랜섬웨어 동향 분석
박소희, 광진(아주대)
- B-9 암호화된 데이터상에서 영상처리를 위한 Gaussian 필터 구현
송백경, 윤지원(고려대)

11월 2일(토) 09:30~11:30(향파관 3층 304호)

세션 C. 인터넷통신

좌장: 김석훈 교수(순천향대)

- ☆ C-1 실시간 얼굴인식을 위한 분산 시스템
장종권, 범정현, 추현승(성균관대)
- C-2 Wi-Fi 기반 그룹 관리 MAC 프로토콜 구현
한명승, 장윤경, 유인태(경희대)
- C-3 무선 센서 네트워크에서 시간 효율적인 지연 제한 데이터 집계를 위한 제한 기법
Vo Van Vi, Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-4 듀티 사이클 센서 네트워크에서 구조 기반 데이터 집산 알고리즘에 대한 성능 평가
Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-5 WIT-tree 기반의 가중치 빈발패턴 마이닝 기법의 분석
임현근, 윤은일, 남효주, 백윤지, 김종성, 김현호(세종대)
- C-6 STPA 기반 무인기 조작 규정 안전 검증 새로운 방법
Xiaorui Shao, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-7 STPA 기반 무인기 시스템상의 컴포넌트 오류 및 불안정한 상호작용에 관한 연구
Palash Sontakke, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-8 복수의 SFC 환경에서 모니터링 에이전트 배치 최소화를 통한 시그널링 비용 감소 방안
이도경, 김문성, 사이드무함마드라자, 추현승(성균관대)

DCV 기반 공격기법 분석 및 대응방안

정해선*, 박진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *hsjeong.isaa@gmail.com, **security@ajou.ac.kr

Analysis and Countermeasures of DCV-based Attack Technique

Hae-Seon Jeong*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

WebView는 웹브라우저의 기능을 앱 내에서 사용할 수 있게 제공하는 모바일 앱의 UI 구성요소로써, iframe/popup 등의 기능을 제공한다. 웹브라우저에서 iframe/popup 기능을 악용할 경우 frame hijacking, clickhijacking 등의 보안 위협이 존재하며, 특히 안드로이드 WebView는 웹브라우저와 다른 UI, 프로그래밍 특징으로 인해 추가적인 보안 위협이 발생한다. 이와같이 안드로이드 WebView에서 발생하는 취약점을 DCV(Differential Context Vulnerability)라고 정의하며, 해당 취약점에 의해 개인정보 노출, 하드웨어 불법 접근 및 피싱 등의 공격이 발생할 수 있다. 이에 따라 본 논문에서는 DCV 기반 공격기법을 분석하고, 이에 대한 대응방안을 제안한다.

1. 서 론

WebView는 특정 웹페이지를 모바일 앱 내에서 보여주는 UI 구성요소로, WebView를 통해 앱 내에서 iframe/popup 등의 기능을 사용할 수 있다. 하지만 iframe/popup 기능을 악용할 경우에는 frame hijacking, clickhijacking 등의 보안 위협이 존재하여 웹브라우저에서는 이를 막기 위해 SOP(Same Origin Policy), HTML5 iframe sandbox, navigation 정책 등의 대응방안을 가지고 있다.

하지만 안드로이드 WebView의 경우 UI, 프로그래밍 특징으로 인해 웹브라우저의 대응방안으로 해결하기 어려운 iframe/popup 관련 취약점이 존재한다. 이와같이 안드로이드 WebView 환경에서 발생하는 iframe/popup관련 취약점을 DCV(Differential Context Vulnerability)라고 정의하며, DCV를 통한 공격으로 공격자는 사용자의 민감 정보에 접근하거나 피싱 공격을 수행할 수 있다[1]. 이에 따라 DCV에 대한 공격기법을 분석하고 대응방안을 도출할 필요가 있다.

본 논문의 구성은 다음과 같다. 2절의 관련 연구에서 DCV 취약점 및 공격 시나리오를 분석하고, 3절에서 DCV 공격에 대한 대응방안을 제안하며, 4절에서 결론을 맺는다.

2. 관련 연구

2.1 iframe/popup의 origin 유효성 검사 취약점

웹페이지를 통한 iframe/popup간에 통신 시, 웹페이지 전송자의 포트, 프로토콜, 도메인을 알 수 있는 'origin' 필드를 통해 상대방을 검증할 수 있다. 이때 loadData() api를 통해 웹페이지 내용을 가져올 경우 메인프레임은 'null' origin을 갖는다[2]. 하지만 이는 메인프레임 고유의 origin값이 아니기

때문에, 공격자가 메인프레임 내부에 'null' origin을 형성하면 공격을 수행할 수 있다.

공격자의 서브프레임에서 'null' origin을 갖는 서브프레임 $F_{\neq sted}$ 를 생성하고, $F_{\neq sted}$ 에 공격을 수행하는 코드를 넣는다. $F_{\neq sted}$ 는 'null' origin을 갖는 메인프레임, 서브프레임, 혹은 Webview에 대해 공격을 수행할 수 있다. 이때 피해자는 $F_{\neq sted}$ 의 'null' origin만 확인할 수 있기 때문에 메인프레임과 동일한 'null' origin을 가지는 $F_{\neq sted}$ 의 작업을 유효하다고 판단하므로 공격이 발생할 수 있다[1].

```
//웹메시지 핸들러
onmessage = function(e){
    //메인프레임의 origin이 "null"일 때 웹메시지 유효성 검사
    if(e.origin=="null"){
        //유효 작업 수행
    }
}
```

(그림 1) 웹메시지 유효성 검사 코드

2.2 WebView 이벤트 핸들러 취약점

이벤트 핸들러 onCreateWindow()는 새로 요청된 웹페이지 내용을 보여주기 위한 새로운 Webview를 생성한다. 하지만 onCreateWindow()는 웹페이지를 요청하는 자를 구분하지 못한다. 또한 이벤트 핸들러 onCloseWindow()는 기존의 WebView를 삭제하지만, 보여주는 WebView의 순서를 검사하지 않는다[3].

2.3 공격 시나리오

공격자가 WebView에 서브프레임 $F_{\neq sted}$ 를 생성할 수 있는 경우, 2.1절의 'null' origin 취약점을 이용하여 $F_{\neq sted}$ 는 메인프레임, 서브프레임 혹은 WebView에 직접적으로 DCV 공격을 수행할 수 있다. 가능한 공격 시나리오는 다음과 같다[1].

(표 1) DCV 공격 분석

공격명	공격 설명	공격 결과
Origin hiding	'null' origin을 갖는 경우 발생할 수 있는 공격	개인정보 탈취 및 하드웨어 접근 (예: 카메라, 마이크)
WUI redressing	onCreateWindow()와 onCloseWindow()의 작업을 수행하는 WebView에 순서가 없기 때문에 발생할 수 있는 공격	피싱 공격 수행
Mainframe privileged navigation	WebView 설정과 API간 충돌로 인해 발생할 수 있는 공격	

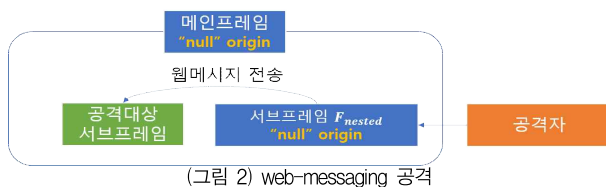
origin 사용으로 인한 DCV 공격에 대응할 수 있다.

서브프레임에서 http를 사용하는 경우, 공격자는 MITM 공격을 통해 서브프레임에 코드 인젝션을 수행하여 $F_{\neq std}$ 를 생성하여 DCV 공격을 수행할 수 있다. 또한 광고 도메인 등의 third-party 도메인을 공격자가 소유한 경우 공격자는 서브프레임 $F_{\neq std}$ 를 생성하여 DCV 공격을 수행할 수 있다. 가능한 DCV 공격으로는 Origin hiding, WUI(Webview UI) redressing, Mainframe privileged navigation 등이 있다[1].

2.4 DCV 공격 분석

□ Origin hiding

공격자는 'null' origin을 갖는 서브프레임을 이용하여 'null' origin을 갖는 메인프레임을 대상으로 web-messaging 공격을 수행하거나, web-mobile bridge에 접근하여 개인정보를 탈취 또는 하드웨어 자원을 이용할 수 있다.



□ WUI redressing

취약한 onCreateWindow()를 이용해 신뢰할 수 없는 웹내용을 기존 창 위에 띄우고(WUI overlap 공격), 추가로 취약한 onCloseWindow()를 이용해 기존 창을 삭제(WUI closure 공격)할 수 있다. WebView에는 주소창과 탭창이 없어 WUI의 순서를 조작하여 피싱 공격을 수행할 수 있다.

□ Mainframe privileged navigation

서브프레임에서 팝업을 생성하면 안드로이드는 팝업 내용을 보여줄 WebView를 선택한다. 팝업 생성이 비활성화되었을 때도 WebView 선택은 항상 일어난다. 팝업 생성이 비활성화되었을 경우에는 기존에 있는 WebView를 사용하여 팝업 내용을 보여준다. 즉, 메인프레임에 팝업에 들어가야 하는 웹내용이 포함되므로 메인프레임이 팝업으로 사용되고, WebView에는 주소창과 탭창이 없어 사용자에게 피싱 공격을 수행할 수 있다.

3. DCV 공격 대응방안

loadDataWithBaseURL(String baseUrl, String data, String mimeType, String encoding, String historyUrl) api에 유효한 baseUrl을 명시하여 웹페이지 내용을 가져오면 메인프레임은 'null'값이 아닌 고유한 origin을 생성할 수 있다. 따라서 'null'

또한 WebView에는 주소창과 탭창이 없기 때문에 DCV 공격을 수행하여 임의로 iframe/popup를 띄워도 사용자는 이를 알아차리지 못한다. 하지만 DCV 공격은 공격자의 익스플로잇 코드를 통해 사용자가 모바일 기기를 터치하지 않아도 iframe/popup를 생성한다. 따라서, 앱 터치 이벤트 없이 URL을 로드하여 iframe/popup를 생성한 경우, 로드된 URL을 화면에 별도로 표시하여 사용자가 웹 내용이 변경된 것을 볼 수 있도록 한다.

(표 2) DCV 공격 대응방안

No.	대응방안	Origin hiding	WUI redressing	Mainframe privileged navigation
1	메인프레임 생성 시 웹 내용을 가져올 때 loadDataWithBaseURL() 사용 화면 터치 없이 WebView에 웹내용이	O	O	O
2	포함된 경우 포함된 웹내용의 URL을 화면에 표시	-	O	O

4. 결론

WebView는 기존 웹브라우저와 다른 UI 구성과 프로그래밍 특징으로 인해 웹브라우저의 iframe/popup 기능 사용 시 발생하는 취약점과 다른 DCV 취약점이 WebView에서 발생한다. 해당 공격은 하나의 앱 내에서 발생하는 취약점으로, 공격자는 iframe/popup 생성으로 개인정보를 탈취하거나 하드웨어에 접근할 수 있다. 또한, 공격자는 DCV 공격을 통해 피싱 공격을 수행할 수 있다.

본 논문에서는 DCV 공격에 대응하는 방안을 제시하였다. 이를 통해 WebView를 사용하는 앱의 안전성을 향상시킬 수 있다.

참고문헌

- [1] GuangLiang Yang, Jeff Huang, and Guofei Gu, "Iframes/Popups Are Dangerous in Mobile WebView: Studying and Mitigating Differential Context Vulnerabilities", 28th USENIX Security Symposium, 2019
- [2] Android Developers Docs, [https://developer.android.com/reference/android/webkit/WebView.html#loadUrl\(java.lang.String\)](https://developer.android.com/reference/android/webkit/WebView.html#loadUrl(java.lang.String))
- [3] Android Developers Docs, <https://developer.android.com/reference/android/webkit/WebChromeClient>