Journal of The Korea Society of Computer and Information
Vol. 20, No. 6, June 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.6.037

모바일 환경에서 실시간 악성코드 URL 탐지 및 차단 연구

박 재 경*

A Study of Realtime Malware URL Detection & Prevention in Mobile Environment

Jae-Kyung Park*

요 약

본 논문에서는 악성코드에 대한 피해를 실시간으로 탐지하고 차단하기 위해 모바일 내부에 악성링크에 대한 데이터베이스를 저장하고 또한 악성링크 탐지 엔진을 통해 웹 서비스를 통제함으로 인해 보다 안전한 모바일 환경을 제공하고자 한다. 최근 모바일 환경에서의 악성코드는 PC 환경 못지않게 기승을 부리고 있으며 새로운 위협이 되고 있다. 특히 모바일 특성상 악성코드의 피해는 사용자의 금전적인 피해로 이어진다는 것이 더 중요한 이유이다. 이러한 사이버 범죄를 어떻게 예방하고 실시간으로 차단할 수 있을 것 인지에 대해 많은 연구가 진행되고 있지만 초보적인 수준에 불과한 실정이다. 추가적으로 SMS나 MMS를 통해 전달되는 스미싱도 탐지 및 차단할 수 있는 방안을 제안하고자 한다. 향후 모바일 사업자는 본 연구를 바탕으로 한 근본적인 대책을 수립하여 안전한 모바일 환경을 구축해야 할 것이다.

▸ Keywords : 모바일, 악성코드, 악성링크, 탐지, 차단, SMS

Abstract

In this paper, we propose malware database in mobile memory for realtime malware URL detection and we support realtime malware URL detection engine, that is control the web service for more secure mobile service. Recently, mobile malware is on the rise and to be new threat on mobile environment. In particular the mobile characteristics, the damage of malware is more important, because it leads to monetary damages for the user. There are many researches in cybercriminals prevention and malware detection, but it is still insufficient. Additionally we propose the method for prevention Smishing within SMS, MMS. In the near future, mobile venders must build the secure mobile environment with fundamental measures based on our research.

▸ Keywords : Mobile, Malware, Malware URL, Detection, Prevention, Crawling, SMS

• 제1저자 : 박재경, • • 교신저자 : 박재경
* 투고일 : 2015. 4. 23, 심사일 : 2015. 5. 7, 게재확정일 : 2015. 5. 29.
* 한국과학기술원 사이버보안연구센터(Cyber Security Research Center in KAIST)

I. 서 론

최근 스마트폰을 통한 모바일 환경의 진화와 기기의 발전에 따라 보안에 대한 위협도 늘어나고 있는 추세이다. 해커는 스마트폰에 설치된 악성코드를 통해 개인정보나 금전적인 이득을 취할 수 있다[9]. 이러한 환경에서 악의적인 앱 뿐만 아니라 웹 서비스를 통해서도 악성코드에 대한 URL을 통해 앱을 다운로드 받고 지속적인 해킹을 수행할 수 있다[13].

스마트폰 플랫폼 중 가장 많이 사용되는 안드로이드는 빠른 시장 확장을 위하여 공개 형태를 취했고 그 결과 과반 이상의 시장 점유율을 갖게 되었다[1]. 하지만 이러한 빠른 진화와는 달리 모바일 보안 솔루션은 아직 초기 단계에 머물러 있으며 그 피해도 날로 증가하고 있는 실정이다. 현재 모바일 보안 서비스는 매우 제한적으로 백신 정도만 보급되어 있지만 공격의 유형을 살펴보면 기기의 오작동, 정보 유출, 무작위 통신, 외부 모듈 다운로드, 백도어 설치, 모바일 내부에서 변형 등등의 매우 다양하고 치명적인 활동을 하고 있다[2][3].

트랜드마이크로 사에 보고에 따르면 현재까지 탐지된 악성코드 중에서 내부적으로 악성링크를 포함하고 있는 비율이 17%에 달하는 것으로 조사되었고 그 중 90% 이상은 매우 치명적인 내용으로 앱이 설치된 이후 URL을 통해 다른 앱을 다운로드 받거나 악성 컴포넌트를 다운받는 것으로 조사되었다[13]. 이러한 악성링크에 대한 대비책이 현재는 없으며 백신으로 해결할 수 있는 문제가 아니다. 따라서 본 논문에서는 모바일 환경에서 URL을 통제함으로써 악성링크에 접근하는 것을 실시간으로 차단하고 보다 안전한 모바일 환경을 제공하고자 한다[4][7].

그림 1에서와 같이 구글의 플레이 버튼을 통해 특정한 사이트를 유도하고 유도된 사이트는 의심스러운 행위를 유도한다. 하지만, 이 사이트는 추후에 재방문했을 경우 사이트가 사라진 것을 확인할 수 있으며 특정한 시점에 악성링크로 활용되었음을 알 수 있다. 이처럼 정상적인 행위를 가장하여 사용자의 모바일 환경에 악성코드 및 악성링크를 다운로드 하는 사례가 발견되고 있다.

본 논문에서는 모바일 환경에서 가장 많이 사용되는 안드로이드 환경에서 URL을 탐지하고 해당 URL이 악성링크인지를 판단하는 방안을 제안하고 이를 프로토타입으로 실험하였다. 특정 앱이나 웹을 통해 특정 URL로 유도되는 것을 실시간으로 탐지하고 이를 분석하여 악성링크일 경우 차단하는 방안을 제시하고자 한다. 다만 모바일 서비스를 제공하는 벤더들은 본 연구를 보다 확장하여 악성 앱이나 악성링크에 대한 근본적인 해결 방안을 제시하여야 할 것이다. 2장에서는 관련연구를 살펴보고 3장에서는 본 논문의 연구 방안을 제안하며 4장에서는 실험을 통해 제안을 검증하고 5장에서는 결론을 제시한다.

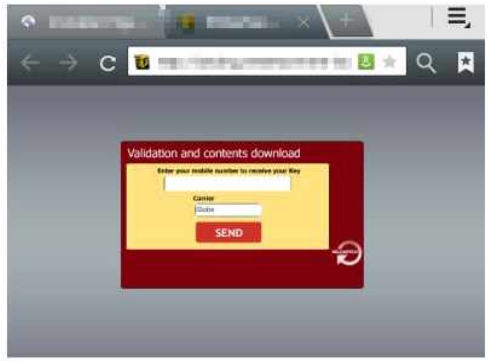

그림 1. 구글 플레이 버튼을 통한 악성 사이트 유도[16]
Fig. 1. The Google Play button leads to malicious site[16]

II. 관련연구

2.1 모바일 악성코드 특징

모바일 악성코드는 단말에 설치되어 개인정보 탈취, 스마트폰 원격 제어, 사용자 과금 유발 등의 행동을 수행한다. 이러한 모바일 악성코드의 행동은 해커에게 금전을 비롯한 다양한 이득을 제공한다. 일례로, 해커는 특정 번호로 문자를 보내면 보낸 사람에게 과금이 발생하고 받는 사람과 통신사에 수익이 생기는 프리미엄 SMS 서비스를 이용하게 함으로써 직접적인 금전적 이득을 획득할 수 있다. 또한, 휴대폰 인증번호를 가로채 소액 결제를 이용함으로써 직접적인 금전적 이득을 취할 수 있다[5][6]. 이 외에도 스마트폰을 좀비 폰으로 활용함으로써 DDoS(Distributed Denial of Service) 공격 및 악성 스팸 대량 유포 등과 같은 작업을 수행할 수 있다. 모바일 악성코드의 유포 방법은 악성코드가 생산하는 위와 같은 이득과 함께 빠른 진화를 보이고 있다[9].

2.2 앱 위변조(Repackaging)

앱 위변조는 모바일 악성코드 유포를 위하여 매우 일반적으로 사용되는 기법이다. 해커들은 이를 통해 기존 소스코드를 일부 수정하거나 다른 모듈을 삽입해 카피앱이나 위장앱으로 만든다. 그런 다음 기존 앱에서 입력받는 데이터를 공격자 서버로 전달하는 기능 등을 삽입해 재배포한다[8]. 악성코드 삽입, 앱 복제, 개인정보 불법수집 등 데이터 변조를 통해 해커 임의로 원하는 기능을 자유자재로 구현할 수 있게 되는 것

이다. 인앱결제 기능이 포함돼 있는 앱은 해커들의 공격이 특히 활발하다. 금전적 이득이 있는 곳에 당연히 해커가 모여들 수밖에 없기 때문이다. 해커가 임의로 디지털콘텐츠나 아이템 구매 등의 가격을 변조할 수도 있고, 결제서버를 가로채는 등의 형태로 개발사에 직접 금전적인 타격을 줄 수 있다. 요즘 공격의 주 타깃이 되는 산업이 게임, 금융, 전자상거래분야인 것도 이 때문이다[17].

2.3 모바일 악성코드 탐지 기법

모바일 환경에서 악성코드를 탐지하는 기법에는 여러 가지 기법이 있다. 우선 애플리케이션 위변조 탐지 기법을 둘 수 있다. 이는 애플리케이션의 유사성을 기반으로 한 탐지 방법과 무결성을 검증하는 방법 등으로 구분할 수 있으나 해킹 이후 리패키징을 이용할 경우 발견하기 어렵다는 단점이 있다. 또한 코드 난독화 기술을 통해 코드가 역공학을 통해 분석되는 것을 어렵게 하는 방법이 있다[10][11].

또한 애플리케이션 행동 분석을 통한 악성코드 탐지기법이 있으며 이는 정적 분석 방법과 동적 분석 방법으로 나누어 볼 수 있다. 정적 분석 방식의 경우 특정한 패턴이나 시그니처에 의해 분석하는 방법이지만 패턴이 너무 다양하고 위변조가 많아 효율성이 떨어진다[12]. 동적분석 방식은 실제 앱을 실행하여 그 결과를 토대로 분석하는 방식인데 실행에 매우 제한이 있고 실시간 성이 매우 떨어지는 단점을 가지고 있다. 이와 같이 다양한 방법으로 모바일 환경에서 악성코드에 대한 분석이 이루어지고 있지만 각각의 방법들의 특성상 부족한 부분이 생기기 마련이다[16].

본 논문에서는 이 중 악성코드나 앱을 통해 악성링크에 접근하는 것을 실시간으로 검사하고 만약 악성링크라고 판단이 될 경우 이를 차단하는 방안을 제안하고자 한다. 악성코드 자체에 대한 탐지도 중요하지만 악성코드가 있는 링크로 사용자를 유도하여 악성 앱을 다운받거나 의심스러운 행위를 사전에 차단하는 것도 매우 중요한 문제라고 판단한다.

III. 본론

이번 장에서는 모바일 환경의 앱이나 웹을 통해 악성링크로 접근하는 것을 실시간으로 탐지하고 차단하는 방안을 제안하고자 한다. 대상은 안드로이드 시스템을 활용하여 제안하도록 한다.

3.1 시스템 구성

본 논문에서는 대표적인 웹 엔진인 WebKit을 사용하여 제안하도록 한다. WebKit은 웹 서버에서 데이터를 받아오기부터 실제 화면으로 그리기까지 모든 일을 처리한다. WebKit을 사용한 대표적인 웹 브라우저로는 Google의 Chrome과 Apple의 Safari가 있는데 StarCounter의 통계에 따르면 이 두 브라우저는 전체 사용되는 브라우저에서 40% 이상의 점유율을 차지하고 있다[13]. 이 WebKit은 4개의 모듈 구조로 이루어져 있고 그림 2와 같은 구조를 갖는다[14].

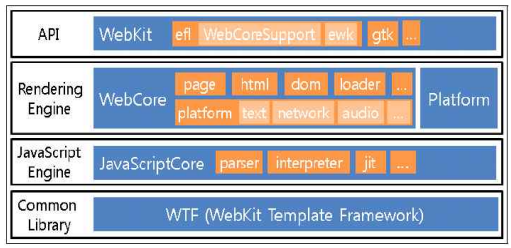

그림 2. WebKit의 모듈구조
Fig. 2. Module Structure of WebKit

이 중 WebKit API는 플랫폼과 통신을 담당하며 Source/WebKit 디렉터리 아래에 각 포트별로 나뉘어 있다. 이를 통해 인터페이스 및 웹 페이지 로드 및 렌더링 과정 중에 웹 브라우저 제작자가 결정해 주어야하는 부분들을 처리하는 코드들이 포함되어 있다. 여기에 특정 URL에 대한 접근 제어, 팝업 차단 여부, MIME 유형에 따른 행동을 결정할 수 있다[15]. 따라서 본 논문에서는 Rendering 엔진에서 악성링크를 판단하여 WebKit API를 통해 접근을 제어할 수 있는 모델을 제안하고자 한다.

WebKit을 사용하여 악성코드 URL을 판단한 후 해당 브라우저와 연결된 WebKit API를 사용하여 정상일 경우 원래 API를 통해 진행하지만 만약의 경우 WebKit에서 악성링크를 발견하였을 경우 그림 3과 같이 별도의 WebKit API를 통해 콘텐츠를 표시하도록 한다.

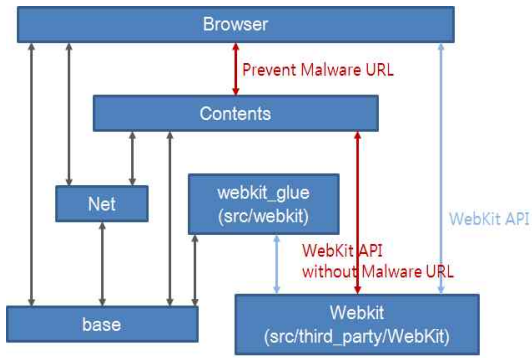

그림 3. 제안 시스템 구조
Fig. 3. System Architecture

WebKit을 통해 악성링크일 경우 붉은 색의 API를 사용하며 콘텐츠로 전달하는 API에는 악성링크에 대한 정보를 파라미터로 추가하여 전달한다.

3.2 엔진 설계

본 논문에서 제안한 모바일 악성코드 URL탐지 엔진은 WebKit의 WebCore 부분을 수정하여 설계하였다. 그림 4에서와 같이 기존 쓰레드에서 파싱을 하는 단계에서 스크립트를 수행하기 위한 모듈을 호출하게 되는데 이때 해당 스크립트에서 URL을 추출하여 설계한 악성링크 데이터베이스와 비교를 수행하고 데이터베이스에 없을 경우 별도의 쓰레드를 생성하여 크롤링을 통한 악성링크를 탐지하도록 설계하였다.

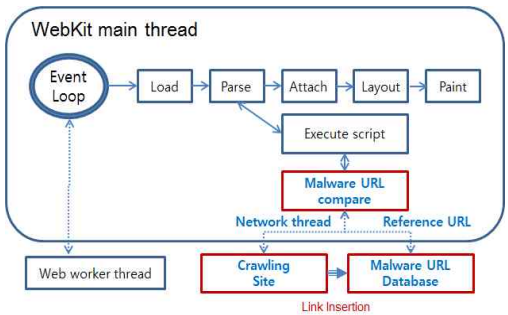

그림 4. 악성코드 URL 탐지 엔진 추가
Fig. 4. Adding the Malware URL Detection Engine

이 과정을 통해 사용자가 웹 브라우저를 통해 접근하고자 하는 URL을 통제할 수 있으며 악성링크를 차단할 수 있다. 악성링크를 판단하는 기능의 설계는 '다중 필터를 이용한 실시간 악성코드 탐지 기법'의 논문의 엔진을 적용하였다[3]. 만약 데이터베이스에 저장된 URL이 아닐 경우 별도의 쓰레드를 통해 독립적으로 URL을 방문하며 지정된 단계까지 이 과정을 반복한다. 다만, 이 결과를 통해 발견된 악성링크가 있을 경우 바로 사용자에게 보여주는 것이 아니라 악성코드 URL 데이터베이스에 추가만 한 후 향후 자료로 사용한다. 본 논문에서는 제한된 환경에서 실험을 진행하여 데이터베이스는 고정된 URL 리스트 100개를 미리 등록하여 처리하였으며 향후 온라인 업데이트를 통해 해당 URL 정보는 업데이트 가능하도록 설계하였다.

IV. 실험 및 고찰

본 논문에서 제안한 시스템을 검증하기 위해서 다음의 환경을 설정하여 실험하였다. 안정적인 실험을 위하여 모바일 통신은 WiFi만을 통하여 실험을 진행하였다. 다음 표 1은 본 논문의 실험환경을 나타내고 있다. 비고의 내용은 추가적인 검토 및 향후 확대 적용할 내용에 대해 언급하고 있다.

표 1. 실험 환경
Table 1. Test Environment

항목	내용	비고
모바일 폰	팬택 베가아이언2	Galaxy
WebKit	https://www.webkit.org/	Chrome
WebCore	WebCore 1.1	Chrome
Database	text file	MariaDB
Network	WiFi	LTE
Malware URL	10개 링크	악성링크

본 실험에서는 WebCore 부분을 변형하여 적재하였고 또한 크롬을 대체하기 위한 브라우저를 통해 악성링크가 발견될 경우 수정된 API를 통해 콘텐츠를 표현하는 시스템을 실험하기 위해 공개된 브라우저를 사용하여 구현 및 실험하였다. 향후에는 보다 다양한 스마트폰과 상용화된 브라우저에 적용할 수 있는 방안을 마련하여 진행할 예정이다. 또한 성능적인 이슈나 네트워크의 안정성 등의 인자를 확인하기 위해 네트워크 환경도 LTE나 기타 모바일 트래픽으로 확대하여 적용할 필요가 있다.

본 논문에서 실험한 URL의 대상은 다음의 표 2와 같으며 해당 URL과 정상적인 URL을 10회 실험하였으며 악성링크의 경우 수정된 API를 통해 그림 5와 같이 사전에 정의한 페이지가 출력되는 것을 확인하였다.

표 2. 실험 데이터 및 결과
Table 2. Test data and result

항목	내용	처리 결과
정상 링크	http://www.naver.com	통과
악성유포지	http://www.korarthro.com/mm/index222.html	차단
악성유포지	http://222.239.252.41/_img/index.html	차단
악성유포지	http://198.2.221.201/luku.html	차단
악성유포지	http://www.korarthro.com/mm/index222.html	차단
악성유포지	http://www.united.com/web/en-US/default.aspx?root=1	차단
악성유포지	http://www.eneeds.co.kr/data/upload/pop/1/a.html	차단
악성유포지	http://enolja.com/home/j/index.html	차단
악성유포지	http://www.creget.co.kr/_core/0/index.html	차단
악성유포지	http://www.4-ever.co.kr/pds/v/index.html	차단
악성유포지	http://ohfatech.com/pop/index.html	차단

위 실험에서 사용된 사이트에 접근하여 본 논문에서 제안한 실험이 정상적인 실험인지를 판단하기 위해 http://www.creget.co.kr/_core/0/index.html 사이트에 접근

한 후의 결과를 그림 5와 6을 통해 비교하였다. 그림 5에서는 PC상의 브라우저에서 직접적인 차단을 수행하는 swing 브라우저를 사용하여 해당 사이트가 차단됨을 알 수 있었고 그림 6은 본 논문에서 제안한 시스템을 통해 차단되는 것을 확인할 수 있었다.

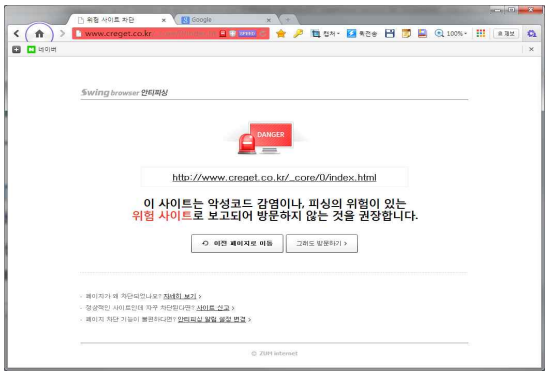

그림 5. PC상에서 악성링크 차단
Fig. 5. Malware URL prevention on the PC

그림 6. 모바일에서 악성링크 차단
Fig. 6. Malware URL prevention on the Mobile

다만, 본 실험의 대상인 악성코드는 PC에 설치되는 악성코드로 실제 악성코드 URL은 PC용과 모바일 용도가 구분되어야 할 것이다. 최근 스미싱[18]이나 메일을 통해 모바일용 악성링크가 많이 기승을 부리고 있으므로 모바일 전용 악성링크를 판단하는 엔진 연구가 추가로 진행되어야 한다. 다만, 기존에 모바일에서 스미싱이나 악성코드 URL을 처리할 수 있는 방안이 거의 없었고 최근 통신 사업자들이 자체적으로 서비스를 제공하고는 있으나 미흡한 실정이므로 본 논문에서 제안하는 연구를 토대로 근본적인 서비스를 제공할 수 있을 것으로 판단한다.

V. 결론

최근 들어 모바일의 환경은 PC 환경 못지않은 고사양, 고성능을 계속 출시하고 있다. 또한, 이러한 환경에서 PC 이상의 악성코드도 기승을 부리고 있으며 더 이상 앱 보안만을 통제하는 것은 안전하지 않다. 따라서 본 논문에서 제안한 형태의 악성코드 URL을 사전에 탐지하여 차단할 경우 보다 안전한 모바일 환경을 제공할 수 있을 것이다. 다만, 현재 모바일 환경에서 지원되는 브라우저가 매우 다양하고 또한 많은 수의 URL을 처리하기 위해서는 데이터베이스를 경량화하고 실시간으로 처리할 수 있는 개선이 필요할 것이다.

본 논문에서 제안한 모바일 환경에서의 악성코드 URL 탐지 연구를 통해 모바일용 악성코드가 스마트폰에 설치되는 것을 원천적으로 차단함으로 인해 PC보다 더 안전환 환경을 제공해야 할 것이다.

REFERENCES

[1] Jae-Kyung Park, Sang-Yong Choi, "Studing Security Weaknesses of Android System", International Journal of Security and Its Applications, Vol. 9, No.3, pp. 7-12, Mar. 2015.

[2] Jae-Kyung Park, Sang-Yong Choi, "An Integrity Checking Mechanism Using Physical Independent Storage for Mobile Device", International Journal Control and Automation, Vol.8, No.3, pp.109-114, Mar. 2015.

[3] Jae-Kyung Park, "A Realtime Malware Detection Technique Using Multiple Filter", Journal of The Korea Society of Computer and Information, Vol. 19, No.7, pp. 77-85, July 2014.

[4] Hyo-Nam Kim, "Realtime hybrid analysis based on multiple profile for prevention of malware", Hongik Univ. Feb. 2014.

[5] Jae-Kyung Park, Sung-Jin Kim, "The Design of the expanded BYOD solutions for business mobile users", Journal of The Korea Society of Computer and Information, Vol. 10, No.10, pp. 107-115, October 2014.

[6] Jin-Kyung Kim, "A design of anomaly detection

with automata dynamic profile", Hansei Univ., Feb. 2014.
〔7〕 S. Kim and D. H. Lee, "A study on the vulnerability of integrity verification functions of android-based smartphone banking applications". in Journal of The Korea Institute of Information Security & Cryptology (JKIISC), vol. 23, no. 4, pp. 743-755, Aug. 2013.
〔8〕 Hyo-Nam, Kim and Jae-Kyoung Park and Yoo-Hun Won, "A Study on the Malware Realtime Analysis Systems Using the Finite Automata", Journal of the Korea society of computer and information, Vol.18, No.5, pp.69-76, Apr. 2013.
〔9〕 H.S. Moon, B.H. Jung, Y.S. Jeon and J.N. Kim, "A Survey of Mobile Malware Detection Techniques", 2013 Electronics and Telecommunications Trends, Vol. 23. No. 3, pp. 39-46, May. 2013.
〔10〕 Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution", Proc 33rd IEEE Symp Security and Privacy, Aug. 2012.
〔11〕 Mobile security technology research society, "Demand and outlook for mobile security technology", Data collection for Mobile security technology research society seminar, Sept. Jun. 2011.
〔12〕 Androulidakis, Digital evidence in mobile phones. IT security professional magazine, Issue 13, pp 36 - 39, Feb. 2010.
〔13〕 http://www.cnet.com/how-to/protect-your-android-device-from-malware/
〔14〕 http://blog.trendmicro.com/trendlabs-security-intelligence/the-communication-function-of-malicious-urls/
〔15〕 http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/10-tips-to-prevent-mobile-malware.aspx
〔16〕 http://blog.trendmicro.com/trendlabs-security-intelligence/android-installer-hijacking-bug-used-as-lure-for-malware/
〔17〕 http://www.etnews.com/20150210000170
〔18〕 http://www.siminilbo.co.kr/news/articleView.html?idxno=391594

저 자 소 개

박 재 경
1994: 동국대학교
컴퓨터공학과 공학사.
1996: 홍익대학교
전자계산학과 이학석사.
2002: 홍익대학교
전자계산학과 이학박사
현 재: 학국과학기술원
사이버보안연구센타 책임연구원
관심분야: 네트워크 보안, 사이버 보안
Email : wildcur@kaist.ac.kr