http://dx.doi.org/10.14400/JDC.2014.12.4.327

멀웨이 공격을 예방하기 위한 스마트폰 콘텐츠 보호 기법

정윤수
목원대학교 정보통신공학과

Smartphone Content Security Scheme for Protect Malware Attacks

Yoon-Su Jeong
Dept. of Information Communication & Engineering, Mokwon University

요 약 최근 스마트폰은 3G 망은 물론 Wi-Fi, Wibro 등 다양한 인터페이스를 통해 시간과 장소의 제약 없이 인터넷 뿐만 아니라 애플리케이션을 설치 및 삭제가 쉬워 점점 인기가 증가하고 있다. 그러나, 스마트폰의 보급과 활성에 따른 기존 PC에서 발생하던 보안 위협이 스마트폰에서도 발생하여 사회적으로 큰 파장을 일으키고 있다. 본 논문에서는 콘텐츠 서비스를 실시간으로 서비스하기 위해서 콘텐츠의 처음과 마지막에 전자 서명을 삽입하여 둘 중 하나의 서명이 손실되더라도 콘텐츠에 대한 인증과 부인방지를 모두 제공하는 콘텐츠 보호 기법을 제안한다. 제안 기법은 스마트폰 사용자가 콘텐츠를 안전하게 다운로드하여 설치하거나 애플리케이션을 통해 콘텐츠를 다운로드 할 경우 콘텐츠에 대한 안전한 인증을 수행한다.

주제어 : 스마트폰, 멀웨어 공격, 콘텐츠 보호

Abstract Recently, smartphone are increasing in Internet-enabled applications to install and delete benefits as well as internet through various interfaces such as 3G network, Wi-Fi, Wibro without the constraints of time and place. However, the prevalence of smartphones and the activity was generated from an existing PC smartphone security threats are causing a ripple in a society. In this paper, we serve live content services on the first and last content by creating an electronic signature is the signature of either the loss of any Content provided by both authentication and non-repudiation content protection scheme is proposed. The proposed method of secure smartphone users to download and install the content or an application for downloading content over the content for secure authentication.

Key Words : Smartphone, Malware attack, Content Security

1. 서론

스마트폰은 휴대전화와 개인용 휴대정보단말기(PDA)의 장점을 결합시킨 복합형 무선통신기기로써, 휴대전화의 기능에 PDA기능을 추가한 것 이외에 음성통신, PC연동, 개인정보관리, 무선 인터넷, 팩스 송수신 등의 기능이 있다[1,2].

스마트폰은 보급과 활성화에 따라 기존 PC에서 발생하던 보안 위협이 스마트폰에서 발생하여 사회적으로 큰 파장이 일어나고 있다. 스마트폰은 휴대전화에 비해 대용량 메모리를 채택하고 운영체제를 탑재하여 다양한 프

Received 1 March 2014, Revised 31 March 2014
Accepted 20 April 2014
Corresponding Author: Yoon-Su Jeong(Mokwon University)
Email: bukmunro@mokwon.ac.kr

ISSN: 1738-1916

로그램 및 데이터 사용이 가능하며, 프로그램의 지속적인 추가·삭제가 가능한 특징이 있지만 악성코드를 통해 스마트폰이 감염되어 스마트폰 내에 저장되어 있는 주소록의 사람들에게 이를 다시 전파시켜 감염되는 문제점이 존재한다. 특히, 스마트폰의 중앙 데이터 관리는 해커의 표적에 쉽게 노출되기 쉬기 때문에 2004년에 나타난 휴대전화 바이러스 이후 스마트폰 사용자는 중요 멀웨어 공격에 쉽게 노출되고 있다[3,4,5,6].

스마트폰 보안 위협은 애플리케이션 스토어 상에 저장된 데이터를 기한 없이 사용하기 위한 크랙 시도, 제작툴을 이용한 커스텀 펌웨어 생성, 탈옥(Jailbreak)한 아이폰과 안드로이드의 루팅폰에 의해 불법 애플리케이션 다운로드 및 개인 정보 유출 등이 있다. 스마트폰의 경우 신상정보, 금융정보, 개인민감 정보 등 중요한 정보를 내부에 저장하고 있기 때문에 이를 관리하는 것이 특히 중요하다.

최근 스마트폰에서 발생하고 있는 멀웨어 공격에 대해서 다양한 연구가 진행하고 있다. Park. et. al[7]는 다양한 웹 브라우저들과 호환성을 갖는 플러그 인(plug-in) 방식을 지원하는 방법을 제안하고 있다. 이 방법은 원격서버와 지역서버 간 통신을 지원하는 장점은 있지만 사용자의 허락없이 원격서버의 요청 및 응답이 발생하는 단점이 존재한다. Joelsson. et. al[9]은 모바일 웹 브라우저들이 스마트폰 관련 구성요소를 사용할 수 있는 방법을 제안하고 있다. 그러나, 이 방법은 원격 웹서버에서 실행되는 모든 script들을 다운로드 후 실행하도록 하여 지역 웹서버가 프록시와 같은 동작을 수행하지 못하는 문제점을 있다. MIDlet. et. al[10]은 [9]의 문제점을 개선하기 위해서 지역 웹 서버가 프록시와 같은 기능을 수행하도록 하고 있다. 그러나 이 방법은 지역 웹 서버의 보안을 고려하지 않은 문제점이 있다.

본 논문에서는 스마트폰 사용자가 콘텐츠를 안전하게 다운로드하여 설치하거나 애플리케이션을 통해 콘텐츠를 다운로드 할 경우 콘텐츠의 처음과 마지막에 전자서명 정보를 삽입하여 콘텐츠에 대한 안전한 인증을 수행하는 기법을 제안한다. 제안 기법은 콘텐츠를 제공하는 서버의 신원을 확인하고 콘텐츠가 변조되지 않았음을 확인하기 위해서 서버에서 제공되는 콘텐츠에 인증정보를 임의로 함께 전송함으로써 스마트폰 사용자는 콘텐츠를 끊김없이 연속적으로 콘텐츠를 제공받는다. 제안 기법은 콘텐츠 서비스를 실시간으로 서비스하도록 처음과 마지막 콘텐츠에 전자 서명을 생성하여 둘 중 하나의 서명이 손실되더라도 콘텐츠에 대한 인증과 부인방지를 모두 제공하여 멀웨어 공격에 안전성을 제공한다.

이 논문의 구성은 다음과 같다. 2장에서는 스마트폰과 멀웨어 공격에 대해서 알아본다. 3장에서는 이중 서명 기반의 컨텐츠 보호 기법을 제안하고, 4장에서는 제안 기법의 효율성을 평가하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 스마트폰

스마트폰은 3G 망은 물론 Wi-Fi, WiBro 등 다양한 인터페이스를 통해 시간과 장소의 제약 없이 인터넷을 이용할 수 있는 기기를 말한다. 스마트폰은 사용자의 요구에 따라 애플리케이션을 손쉽게 설치 및 삭제가 가능한 장점이 있다. 특히, 스마트폰의 보급과 활성화에 따라 스마트폰에서 이용할 수 있는 콘텐츠・앱 서비스등이 급속히 증가하고 있다. 그러나, 스마트폰을 대상으로 확대되고 있는 악성코드의 보안 피해는 사회적으로 큰 파장을 일으키고 있다.

2.2 멀웨이 공격

멀웨이는 바이러스, 웜 및 트로이 목마를 포함한 악성코드를 의미한다. 멀웨이는 크게 통신 도구를 이용하는 방법과 시스템의 취약점을 찾아내는 방법 등의 2가지로 구분된다. 파괴적인 멀웨이는 널리 이용되는 통신 도구를 사용하여 확산되며, 여기에는 이메일과 인스턴트 메시지를 통해 웜을 보내고, 웹 사이트에서 트로이 목마를 유포하고, P2P(Peer-to-Peer)에 연결해서 바이러스에 감염된 파일을 다운로드하는 등의 방법이 포함된다. 멀웨이는 시스템의 기존 취약점을 찾아내서 사용자도 모르는 사이에 쉽게 침투한다.

멀웨이는 시스템에서 자신을 숨기거나 사용자에게 모습을 드러내지 않는 방식으로 은밀히 활동한다. 멀웨이를 조치하기 위한 방법은 다음과 같다.

- 신뢰할 수 있거나 신뢰가 예상되는 출처에서 보낸 이메일 또는 인스턴트 메시지의 첨부 파일만 다운

로드
- 이메일에 첨부된 파일은 열기 전에 Norton Internet Security를 사용해서 검사
- 원치 않는 모든 메시지는 열지 말고 삭제
- 모르는 사람이 보낸 웹 링크는 클릭하지 않음
- 친구 목록에 있는 사람이 이상한 메시지나 파일 또는 웹 사이트 링크를 보내는 경우 인스턴트 메시지 세션을 종료
- 모든 파일은 자신의 시스템으로 전송하기 전에 Internet Security 솔루션을 사용하여 검사
- 출처가 잘 알려진 파일만 전송
- Norton Internet Security를 사용해서 모든 불필요한 외부 통신을 차단
- 보안 패치를 항상 최신 상태로 유지

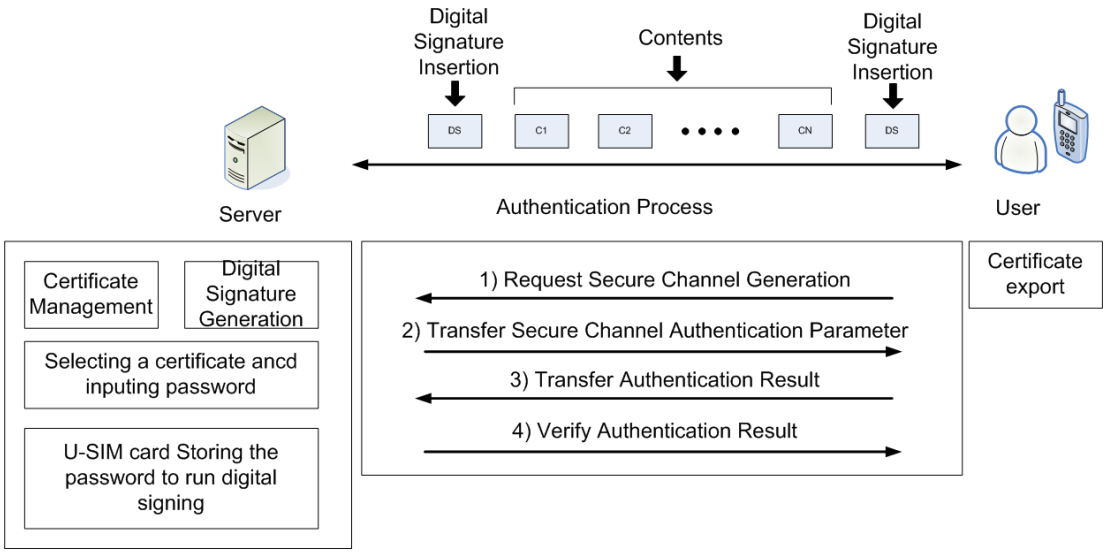
2.3 스마트폰 위협 및 보안기술

스마트폰은 기존 PC와 모바일 기기의 기능을 모두 지원하기 때문에 기존에 나타났던 많은 위협들이 그대로 상속되는 동시에 신규 서비스로 인하여 보안 위협이 늘어나고 있다. 스마트폰이 기존 PC와 모바일 기기보다 악성코드가 많이 발생하는 것은 음성 통신뿐만 아니라 인터넷 통신과 초고속 무선 데이터 통신이 생활주변에서 손쉽게 사용할 수 있어 악성 코드 전파가 더욱 쉬워졌기 때문이다. 악성 코드 전파의 주요 요인으로는 Wi-Fi 및 와이브로 등의 액세스 확대, 휴대폰 기기의 성능 향상, 휴대폰의 개인화 및 전자결재 지원, 공개 플랫폼화 등이 있다.

표 1은 현재까지 발생한 스마트폰의 보안 위협과 그에 따른 보안 기술들을 단말기 영역, 네트워크 영역, 서비스 영역, PC, 메모리 영역, 애플리케이션 스토어 영역, GPS 영역 등으로 분류하고 있다. 표 1처럼 스마트폰에서 손쉽게 발생되는 악성코드는 스마트폰을 원격으로 제어하거나, 애플리케이션의 동작 변경, 파일 실행 차단, 불필요한 통신 요금 발생, 사용자 데이터 도난, SMS 훔쳐보기, 위치정보의 유출, 다른 악성코드의 설치 및 타 스마트폰으로의 전파 등의 리스크를 초래한다. 또한, GPS는 스마트폰에서 편리한 위치기반 서비스를 제공할 수 있지만 사

〈Table 1〉 Smartphone security threats and security technology

Domain	Threats	Security Technology
Terminal domain	· Application exploiting the Analysis · Application using the exploits the features · Voice wiretapping · The loss or theft · Public the Exploit attack · The password cracking · Malicious code · The application installation and accept bypass	· The application of the code obfuscation technology application · Data Encryption · Theft and fraud prevention solutions · Regularly updates · Antivirus
Network Domain	· Data Sniffing and modulation · Mobile VoIP to VoIP vulnerability of existing applications and sniffing	· Data Encryption · Firewall, VPN · Device authentication
Service Domain	· The application exploits exploit · Web site phishing and malware via download · E-mail attachments and malicious code through · spam mails · Internal network, bypassing the external information disclosure	· Smartphone anti-virus technology · Attachment Filtering · Spam Mail Filtering · Illegal use of anti-AP and the Internet
PC, Memory Domain	· Smart phones and PC connectivity and access through the spread of malicious code · An external memory by using malicious code propagating · Personal Information Disclosure · AD-HOC unauthorized access through	· Smartphone anti-virus technology · Secure storage device · Personal information leakage prevention solution · AD-HOC through the access control
Application Store Domain	· Maliciously spreading malicious programs by developers · Security mechanisms to bypass the malicious program registration	· Digital signature technology by using code signing technology
GPS Domain	· Exposure location information via GPS	· Location Information Security



[Fig. 1] Processing Environment of Proposed Scheme

용자의 위치정보가 노출될 위협이 존재한다.

2.4 기존 연구분석

Park. et. al는 다양한 웹 브라우저들과 호환성을 갖는 플러그 인(plug-in) 방식의 지원방안을 제안하였다[7]. Park. et. al는 호환성 프레임워크(F4C)를 통해 지역 플러그 인을 호출하기 위한 지역 서버를 등록하여 원격 서버와 로컬 서버 간에 통신을 지원하고 있다. 그러나, 이 기법은 사용자의 허락없이 원격서버의 요청 및 응답이 발생할 수 있는 문제점을 존재한다.

Joelsson. et. al은 모바일 웹 브라우저들이 스마트폰 관련 구성요소를 사용할 수 있게 지역 웹 서버 방법을 제안하였다[9]. 이 방법은 원격 웹서버에서 실행되는 모든 script들을 다운로드 후 실행하도록 하여 지역 웹서버가 프록시와 같은 동작을 수행하지 못하는 문제점을 가진다. MIDlet. et. al은 [9]의 문제점을 개선하기 위해서 지역 웹 서버가 프록시와 같은 기능을 수행하도록 하고 있다[10]. 그러나 이 방법은 지역 웹 서버의 보안을 고려하지 않은 문제점이 있다.

3. 이중 서명 기반의 스마트 컨텐츠 보호 기법

이 절에서는 스마트폰 사용자가 콘텐츠를 안전하게 다운로드하여 설치하거나 애플리케이션을 통해 콘텐츠를 다운로드 할 경우 인증정보를 포함하여 연속적으로 콘텐츠를 사용자가 사용할 수 있는 기법을 제안한다. 제안 기법은 사용자가 다운로드하려고 하는 콘텐츠에 처음과 마지막에 전자 서명을 생성하여 전송함으로써 지연없이 실시간으로 사용자가 콘텐츠 서비스를 사용할 수 있다.

3.1 개요

제안 기법은 콘텐츠를 제공하는 서버의 신원을 확인하고 콘텐츠가 변조되지 않았음을 확인하기 위해서 서버에서 제공되는 콘텐츠에 인증정보를 임의로 함께 전송함으로써 스마트폰 사용자는 콘텐츠를 끊김없이 연속적으로 콘텐츠를 제공받는다. 제안 기법은 콘텐츠 서비스를 실시간으로 서비스하도록 처음과 마지막 콘텐츠에 전자서명을 생성하여 둘 중 하나의 서명이 손실되더라도 콘텐츠에 대한 인증과 부인방지를 모두 제공하여 멀웨어 공격에 안전성을 제공한다.

그림 1은 서버와 사용자간 제안 기법의 동작 과정 및 서버와 사용자의 동작 기능을 나타내고 있다. 그림 1에서 서버는 인증된 애플리케이션만이 접근할 수 있도록 인증서 및 고유키, 그리고 전자서명/복호화에 사용되는 비밀정보를 보유하고 있다. 사용자는 스마트폰에 내장 및 외장 메모리를 모두 지원하며, USIM 카드를 통한 비밀 정

보의 저장을 지원한다.

제안 기법은 URL 프로토콜을 지원하여 서로 다른 응용 또는 웹 브라우저와 통신할 수 있는 플랫폼을 모두 지원하고 표준형식을 지원한다고 가정한다. 이 같은 가정은 URL, 프로토콜 호출시 자동으로 서비스를 사전에 실행시킬 필요가 없기 때문이다.

3.2 서명기반 콘텐츠 인증

서명기반 콘텐츠 인증을 수행하기 위해서 우선 사용자는 서버에 요청할 콘텐츠를 N 행, K열로 나열한다. 이때, N 번째 줄의 K번째 콘텐츠를 A_{NK} 라고 할때 A_{N_1}은 첫 번째 전자서명에 대한 값으로써 항상 1이라는 값이 나오도록 한다. 또한 A_{MN}은 콘텐츠의 마지막 값으로써 전자서명에 대한 값으로 1이라는 값이 나오도록 한다. 이때, A_{MN} 는 식 (1)과 같은 식으로 나타낸다.

$$A_{(n-1)(k-1)}+A_{(n-1)k} \tag{1}$$

여기서, A_{n1}과 A_{nn}은 1을 의미하고, A_{nk}는 $A_{(n-1)(k-1)}+A_{(n-1)k}$을 의미한다.

n과 k가 $n \geq k$인 양의 정수라 하면, 식 (2)가 성립한다.

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \tag{2}$$

서명기반 콘텐츠 인증을 수행하기 위해서 제안 기법에서는 이항계수를 기하학적 형태로 배열한다. 제안 기법은 멀웨어 공격에 대응하기 위해서 아래와 같이 콘텐츠를 표현한다.

n 번째 줄의 k 번째 콘텐츠를 a_{nk}라고 하면, 콘텐츠는 식 (3) ~ 식 (5)처럼 정의한다.

$$a_{n1} = 1 \tag{3}$$

$$a_{nn} = 1 \tag{4}$$

$$a_{nk} = a_{(n-1)(k-1)}+a_{(n-1)k} \ (n,k > 1) \tag{5}$$

이때, 식 (6)과 같은 성질에 의해서 콘텐츠는 식 (7)과 같이 생성된다. 즉 n번째 열의 k번째 값은 $\binom{n-1}{k-1}$과 같은 값을 가진다.

$$\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k} \tag{6}$$

$$a_{nk}=\binom{n-1}{k-1} \tag{7}$$

식 (6) ~ 식 (7)처럼 생성된 서명기반 콘텐츠들은 이항전개에서 계수들의 값을 계산하는 데에 사용된다. 일반적으로, 이항전개에서 생성된 계수들의 값은 식 (8)과 같은 전개식에서, $a_i=\binom{n}{i}$가 성립한다. 즉, a_i는 콘텐츠의 $(n+1)$번째 줄의 $(i+1)$번째 값과 대응된다.

$$(x+y)^n=a_0x^n+a_1x^{n-1}y^1+a_2x^{n-2}y^2+\cdots+a_ny^n \tag{8}$$

제안 기법은 스마트폰을 사용하는 사용자가 멀웨이 공격에 안전하도록 콘텐츠를 사용할 수 있도록 전자 서명 관련 기능과 URL 스푸핑 공격 방어 기능을 제공한다.

제안 기법에서 전자 서명 관련 기능은 콘텐츠의 연속적인 제공을 위해서 콘텐츠 import 및 전자서명을 관리한다.

URL 스푸핑 공격 방어에서는 악의적인 멀웨어가 스마트폰에 설치되어 있을 경우, 해당 멀웨어는 다중 url 프로토콜 핸들러를 조작하여 합법적인 핸들러가 수행되기 전에 자신을 수행하도록 등록한 후, 합법적인 핸들러가 수행될 때, 해당 핸들러에 의해 조작되는 모든 정보를 가로챌 수 있다. 제안 기법에서는 사용자가 스마트폰에 콘텐츠를 다운로드 할 경우 인증정보를 사전에 컨텐츠에 포함하여 연속적으로 콘텐츠를 사용할 수 있도록 하여 URL 스푸핑 공격에 대응하고 있다.

4. 평가

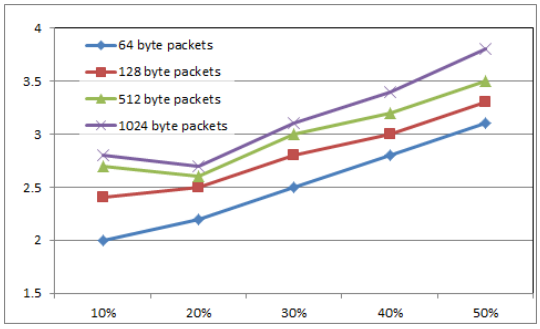
4.1 실험환경

제안 기법의 객관성을 유지하기 위해서 [10]의 모델을

참조하여 실험 환경을 구축하였다. 총 패킷 수는 10,000으로 설정하고, 패킷 크기는 64, 128, 256, 512 바이트로 UDP를 이용하여 전송하도록 실험한다. 송/수신자의 큐 사이즈는 100으로 하고 초당 패킷을 처리하는 처리율은 10으로 설정한다. 패킷 드롭율은 10%, 20%, 30%, 40%, 50%, 60%으로 나누어 실험하고 버스트 드롭의 평균 길이는 10으로 설정한다.

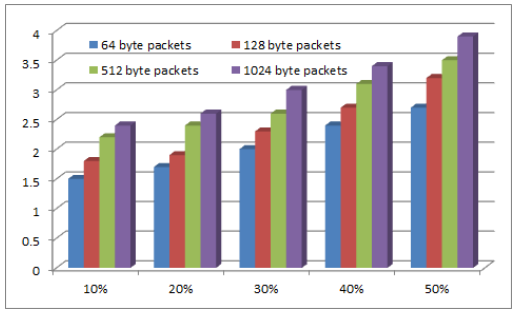
4.2 결과 및 분석

그림 2는 스마트 사용자가 서버에게 콘텐츠 서비스를 요구하였을 경우에 콘텐츠의 패킷 손실율에 따른 지연시간을 평가하고 있다. 제안 기법은 수신자가 첫 번째 패킷을 받자마자 인증할 수 있어 실시간 어플리케이션에 적용할 수 있는 장점이 있으며 첫 번째 패킷이 전송 중에 손실되지 않는 한 마지막 패킷에 포함된 서명을 검증하지 않더라도 부인 방지가 이루어지므로 수신자의 처리 시간을 단축할 수 있는 장점이 있다.



[Fig. 2] dealy time(ms) per packet loss rate

그림 3은 패킷 당 처리되는 컨텐츠 처리량을 비교 평가하고 있다. 그림 3의 결과처럼 패킷 손실률이 증가할수록 컨텐츠 처리량이 비례적으로 증가하였다. 패킷 손실이 적을수록 바로 이웃하지 않은 컨텐츠에 대한 인증정보가 함께 전송하기 때문에 패킷 손실률의 차이에 따른 인증성공률이 3.8% 차이가 나고 있다.



[Fig. 3] Throughput per packet loss rate

5. 결론

본 논문에서는 스마트폰 사용자가 콘텐츠를 안전하게 다운로드하여 설치하거나 애플리케이션을 통해 콘텐츠를 다운로드 할 경우 인증정보를 포함하여 연속적으로 콘텐츠를 사용자가 사용할 수 있는 기법을 제안하였다. 제안 기법은 컨텐츠 처음과 마지막에 전자 서명을 삽입하여 컨텐츠의 끊김없이 사용자가 서버로부터 콘텐츠를 안전하게 다운로드 받을수 있도록 하였으며, 멀웨어 공격에 안전하도록 실시간으로 컨텐츠 서비스가 가능하다. 향후 연구로 본 연구의 결과를 기반으로 스마트폰에 실제 적용할 계획이다.

REFERENCES

[1] M. Becher, C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf(2011), “Mobile security catching up? revealing the nuts and bolts of the security of mobnile devices”, in Proceedings of IEEE Symposium on Security and Privacy, pp. 96-111.

[2] Panda-Security-Labs, “Quarterly report pandalabs”, Panda Security Labs, Tech. Rep.

[3] W. Zhou, Y. Zhou, X. Jiang, and P. Ning(2012), “Detecting repackaged smartphone applications in third-party android marketplaces”, in proceedings of the second ACM conference on Data and Application Security and Privacy, ACM 2012, pp.

317-326.

[4] J. Sahs and L. Khan(2012), “A machine learning approach to android malware detection”, in Intelligence and Security Informatics Conference(EISIC) 2012 European, IEEE 2012, pp. 141-147.

[5] A. Bose, X. Hu, K. Shin, and T. Park(2008), “Behavioral detection of malware on mobile handsets”, in Proceedings of the 6th international conference on Mobile systems applications and services, ACM 2008, pp. 225-238.

[6] C. Amrukar, P. Traynor, and P. Oorschot(2012), “Measuring ssl indicators on mobile browsers: Extended life, or end of the road?”, Information Security, pp. 86-103.

[7] Sang Ok Park(2009), "The Framework for Providing Compatibility to various Web Browser Plug-ins," Master's Thesis, KAIST.

[8] R. Petke and I. King(1999), "Registration Procedures for URL Scheme Names," RFC 2717.

[9] T. Joelsson(2008), "Mobile Web Browser Extensions," Master of Science Thesis, KTH Information and Communication Technology.

[10] S. Li and J. Knudsen(2005), "Beginning J2ME Platform, From Novice to Professional," Apress, third edition, 2005.

정 윤 수(Jeong Yoon-Su)

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@gmail.com