JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 5 : 1117~1124 May. 2015

BYOD 환경을 고려한 모바일 웹을 위한 세션 관리 개선 방안 연구

김영훈 · 박용석*

A Study of Improved Session Management for Mobile Web under BYOD environment

Young-hun Kim · Yongsuk Park*

Graduate School of Information Security, Sejong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul 143-839, Korea

요 약

본 논문은 BYOD(Bring Your Own Device)를 포함한 모바일 웹 환경을 위한 웹 세션 관리 시스템에 대해서 기술한다. 이 시스템은 보안이 강화된 세션 토큰으로 운영되며, 고유 식별자, time stamp, 암호 알고리즘으로 구성된다. 시스템에서 고유 식발자는 BYOD를 포함한 모바일 환경에서 보안을 위하여 각 단말기를 구분한다. 시스템에서 time stamp는 BYOD를 포함한 모바일 환경에서 보안을 위하여 세션 유효성을 판단한다. 시스템에서 암호 알고리즘은 세션 토큰의 내부 정보를 보호한다. 본 논문은 시뮬레이션 기법을 사용해서 모바일 웹 상에서 세션 관리 시스템의 보안성을 분석한다. 제시된 방법은 기존 방법에 비하여 BYOD 환경의 모바일 웹 보안에 있어서 더 적합하다.

ABSTRACT

This paper explains a web session management system for mobile web environment with BYOD(Bring Your Own Device). This system operates by enhanced secure session token. This system consists of an unique identifier, time stamp, and encryption algorithm. The Unique identifier in this system classifies each mobile device for web security based on mobile environment with BYOD. And the Time stamp in this system that determine session effectiveness for web security. Also the Cipher algorithm in this system that protects session token information for web security. This paper analysis a security of session management system running on mobile web environment using the simulation techniques. The proposed method is more suitable than the other methods under enviroment mobile web environment with BYOD.

키워드 : BYOD, 모바일 웹, 세션, OWASP, IMEI

Key word : BYOD, Mobile Web, Session, OWASP, IMEI

Received 16 March 2015, **Revised** 06 April 2015, **Accepted** 21 April 2015

* **Corresponding Author** Yongsuk Park(E-mail:yongspark@sjcu.ac.kr, Tel: +82-2-2204-3894)
Graduate School of Information Security, Sejong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul 143-839, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.5.1117 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 업무 환경은 개인이 보유한 스마트기기를 회사 업무에 활용하는 BYOD(Bring Your Own Device)으로 발전하고 있다. BYOD의 기반이 되는 모바일 환경은 사이버 침해 공격, 웜·바이러스 감염, 개인정보 유출 등 기존 PC 환경에서 발생했던 보안위협에 노출되어 있다[1-4].

기존 PC 환경에서는 보안을 강화하기 위한 세션 관리 방안으로 암호 알고리즘 적용이나 주기적인 재인증, 세션 토큰 활용 등이 있다[9-14]. 세션 관리에는 세션의 생성, 종료 및 지각자 처리 등의 기능이 있다[5]. 기존 세션 관리에서는 모바일 환경을 고려한 기능이 거의 없는 실정이다. 세션의 유효성을 제대로 보장할 수 없게 되면 모바일 서비스 제공은 치명적인 취약점을 가지게 된다. 이런 취약점들이 악용될 경우, 사용자 및 시스템 관리자 권한이 침해되며 대부분의 주요 서버 침해로까지 이어질 수 있다는 점에서 보안 위험성이 매우 크다. 따라서 본 논문에서는 모바일 환경에 적합한 웹 세션 관리 방안을 제안한다.

본 논문에서 제안하는 시스템은 고유 식별자와 time stamp, 암호 알고리즘을 활용하여 모바일 환경에 적합하게 웹 세션을 관리하는 ISeBM(Improved Session Based Management) 시스템으로 악의적인 세션 도용에 대응할 수 있다. ISeBM 시스템은 사용자의 단말기 정보를 조합한 Session Token을 활용하며, 고유 식별자로 활용한 IMEI(International Mobile Equipment Identities)는 국제 표준 기관인 3GPP에서 표준으로 제정한 스마트폰마다 할당되는 유일한 국제 이동 장비 식별자이다. 시뮬레이션을 통해 모바일 웹 환경에서 ISeBM 시스템의 보안성을 실험하였다.

ISeBM 시스템을 활용하면 개인은 안심하고 모바일 단말기로 편리한 기밀 업무 처리를 할 수 있다. 기업은 업무 환경 개선으로 생산성이 향상되고 보안 비용이 줄어들어 이익이 증가될 것으로 기대된다.

본 논문의 구성은 다음과 같다. 2장에서는 모바일 웹 보안과 관련된 연구에 대해 살펴본다. 3장에서는 제안하는 세션 관리에 대해 제시하며 4장에서는 이에 대해 프로토타입을 구현한다. 마지막으로 5장에서는 본 논문의 결론을 내린다.

Ⅱ. 관련 연구

웹 애플리케이션 서비스는 개별 사용자들의 접속을 유지하기 위해 세션을 활용한다. 이는 사용자가 인터넷을 이용할 때, 세션 탈취 및 도용과 같은 악성 행위를 방지할 수 있는 세션 관리가 필요함을 의미한다. 본 장에서는 모바일 웹의 세션 보안과 관련된 사항에 대해 확인해보도록 한다.

2.1. 웹 어플리케이션 보안

국제 웹 보안 표준 기구인 OWASP(The Open Web Application Security Project)는 Top Ten Project와 Mobile Security Project에서 세션 관리 취약점을 경고한다. 표 1과 표 2에서 보는바와 같이 A2: Broken Authentication and Session Management'와 'M9: Improper Session Handling'에서 세션 관리를 강조한다[6,7].

표 1. OWASP Top 10 프로젝트(2013)[6]
Table. 1 OWASP Top Ten Project(2013)[6]

No	vulnerability
A1	Injection
A2	Broken Authentication and Session Management
A3	Cross-Site Scripting(XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery(CSRF)
A9	Using Components with Known Vulnerabilities
A10	Unvalidated Redirects and Forwards

표 2. OWASP 모바일 보안 프로젝트(2014)[7]
Table. 2 OWASP Mobile Security Project(2014)[7]

No	vulnerability
M1	Weak Server Side Controls
M2	Insecure Data Storage
M3	Insufficient Transport Layer Protection
M4	Unintended Data Leakage
M5	Poor Authorization and Authentication
M6	Broken Cryptography
M7	Client Side Injection
M8	Security Decisions Via Untrusted Inputs
M9	Improper Session Handling
M10	Lack of Binary Protections

인증 및 세션 관리와 관련된 애플리케이션 기능이 정확하게 구현되어 있지 않으면 공격자가 패스워드, 키 또는 Session Token을 해킹하거나 다른 구현 취약점을 공격하여 다른 사용자로 위장할 수 있으므로 강력한 인증 및 세션 관리가 필요하다[6].

2.2. 세션 관리 방안

인터넷에서 사용되고 있는 HTTP 프로토콜은 사용자 인증 및 통신의 연속성을 제공해 주기 위해 세션을 사용한다. 즉, 웹 애플리케이션은 정상적인 인증 이후 재접속을 하는 경우 세션 정보로부터 사용자 인증 정보를 획득하여 추가적인 입력 없이 인증을 유유지하기 위해 공유되므로 근본적으로 보안이 보장되어야 한다[8].

표 3. 세션 관리 비교·분석
Table. 3 Session Management Comparison

Alternative	feature
encrypted session[9]	session ID encryption
security protocol[10]	reliable transport
re-certification session [11]	Re-certification in web page
Disposable sesion [12]	re-issuing session
Session Token [13,14, 33,34]	use of unique information

표 3 같이 세션을 암호화하거나 보안 프로토콜인 TLS(Transport Layer Security)로 전달하거나 반복적인 재인증으로 갱신하거나 일회용으로 생성해서 활용하거나 클라이언트 IP(Internet Protocol)주소나 HMAC (Hash-based Message Authentication Code)와 같은 정보로 구성된 Session Token을 조합해서 세션을 관리하는 방안이 연구되었다[9-14].

OWASP와 같은 표준 기관이나 많은 연구에서 세션 관리의 중요성을 강조함에도 불구하고 모바일 웹의 안전성 보장은 미흡한 실정이다[2]. BYOD나 모바일 웹 등과 같이 무선네트워크에서 휴대용 단말기를 활용하는 환경을 고려한 세션 관리 방안에 대한 연구가 필요하다[7].

2.3. 스마트폰 고유식별자

4G 망에서는 모바일 단말기가 통신망에 접속할 때마다 사설 IP 주소를 동적으로 할당하기 때문에 각각의 단말기를 구별할 수 있는 별도의 식별자가 필요하다[15]. IMEI(International Mobile Equipment Identity)는 스마트폰마다 할당되는 유일한 국제 이동 장비 식별자이다[16].

몇몇 단체에서는 IMEI의 섣부른 남용을 경계하고 있다. 구글의 안드로이드 개발자 커뮤니티는 애플리케이션이 IMEI에 지나치게 종속적으로 개발되면 서비스가 오작동하거나 단말기가 다른 사람에게 악용되는 문제 발생할 수 있다고 경고한다[17,18]. OWASP Mobile Security Project는 IMEI로 인해 단말기 정보가 노출되는 위험성에 염려를 표하고 있다[19]. 국내에서도 2011년 9월 시행된 개인정보보호법에서 IMEI와 전화번호, USIM 등이 조합된 정보는 특정 사용자를 구분할 수 있기 때문에 IMEI를 활용하려면 사용자 동의가 필요한 실정이다[20].

그렇지만 IMEI는 도용이 어려운 특징이 있고, 모바일 서비스에서는 단말기를 검증하는 고유 식별자로 활용하기에 효과적이다[21,22]. IMEI가 모바일 단말기를 업무에 활용하는 비즈니스 환경에서 효과적이라는 연구는 계속 발표되고 있다. BYOD나 생체 서명, 모바일 공인인증서 관리와 DRM(Digital Right Management) 콘텐츠 유통 모델, 일회용 모바일 인증 QR코드, 기업 클라우드 ERP 시스템 등 다양한 모바일 서비스에서 IMEI는 핵심 수단으로 제안되고 있다[23-29]. 구글과 삼성은 이용 약관에서 모바일 서비스를 제공받으려면 IMEI를 포함한 기기 정보 수집에 동의해야 한다고 명시하고 있다[30,31].

Ⅲ. ISeBM 시스템 제안

본 논문은 개선된 세션 관리로 암호화된 일회성 Session Token을 활용하는 ISeBM(Improved Session Based Management) 시스템을 제안한다.

3.1. 시스템 구조

본 논문에서 제안하는 ISeBM 시스템은 그림 1과 같이 구성된다. 블록암호의 key를 생성, 발급, 관리하며

Session token을 검증하는 서버와 블록암호의 key를 수령하고 Session token을 조합하고 암호화해서 서버로 전달하는 모바일 단말기로 구성한다.

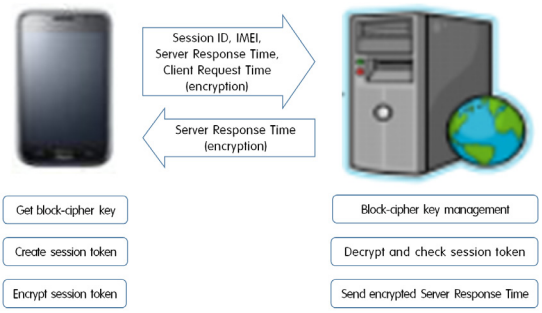

그림 1. ISeBM 시스템 구조
Fig. 1 System Architecture of ISeBM

3.2. 시스템 플로우

본 시스템의 세션 관리 절차는 그림 2와 같다. Session token을 소유하지 않았으면 인증 절차를 거쳐 서버에서 Session token을 생성해서 저장하고 main page로 이동한다. 그리고 매 요청마다 Session token을 검증하여 적합할 경우 main page로 이동하고, 다르거나 유효시간이 경과하면 해당 세션을 무효화하고 로그인 페이지로 이동한다.

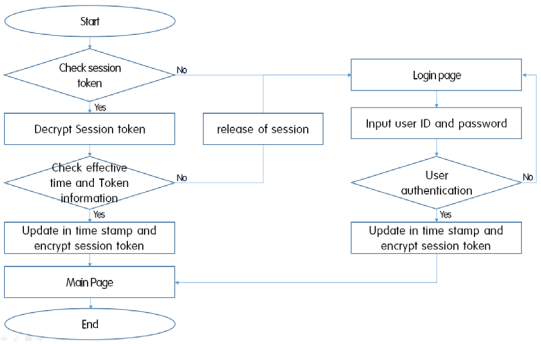

그림 2. 세션 관리 절차
Fig. 2 Session Management Procedures

3.3. 시스템 동작 과정

본 시스템의 동작 과정은 그림 3과 같다. 시스템 동작 중 서버와 클라이언트의 블록암호 Key는 안정적으로 분배된다고 전제한다. 사용자의 브라우저는 수령한 블록암호 Key로 사용자 인증 정보(ID, password)와 IMEI를 암호화해서 서버로 전송한다. 서버는 클라이언트가 보내온 Session Token을 복호화해서 이전 세션 정보와 비교하여 검증한다. Sessino ID가 동일한지, IMEI 동일한지, 서버의 직전 응답시간이 동일한지, 클라이언트의 요청시간이 최신화가 되었는지 그리고 해당 세션의 유효 시간을 검증해서 클라이언트로 결과를 전송한다.

또한 제안하는 ISeBM 시스템에서 IMEI는 접속한 단말기를 검증하는 하나의 Key 값으로써 활용된다. 하지만 보다 좋은 별도의 고유 식별자가 존재할 경우 IMEI를 대체하여 활용할 수 있다.

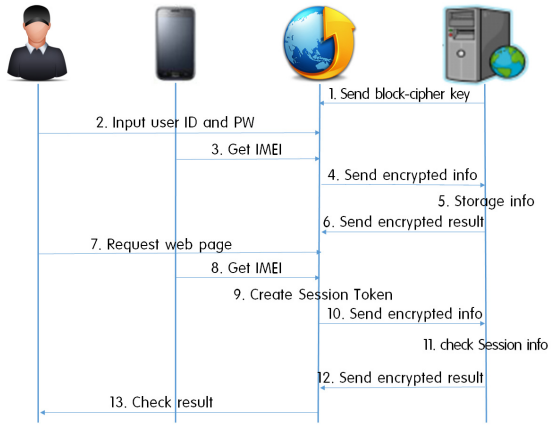

그림 3. ISeBM 동작 과정
Fig. 3 Operation Process of ISeBM

3.4. 시스템 보안성

표 4 같이 기존 연구는 단일 값을 기반으로 Session token을 운영하여 상대적으로 보안에 취약하다는 단점이 내제되어 있다. 제안하는 ISeBM 시스템은 IMEI와 time stamp 등 검증에 필요한 여러 정보를 조합하여 보다 안전한 세션 관리를 보장한다.

ISeBM은 Session token을 블록 암호로 암호화하므로 XSS Attack이나 Packet Sniffing으로 탈취 당해도 내부 구성 정보를 알 수 없으므로 악용되기 어렵다. 또한 매 요청(Request)마다 시스템 시간으로 갱신되므로, 탈취된 이전 Session token으로는 인증을 우회할 수 없다. 서버는 HTTP요청마다 모바일과 세션 토큰의 IMEI를 비교하므로, 공격자가 세션을 도용해도 검증을 통과할 수 없다.

표 4. ISeBM과 기존 연구 비교
Table. 4 Comparison between ISeBM and other studies

Classification	based on factor	feature
IP blocking [13]	IP address	single
Web browser Extension[33]	Random value	
Secure Scheme [34]	Time stamp	
ISeBM system	complex information	multi

Ⅳ. 프로토타입 구현

본 논문에서는 ISeBM의 프로토타입을 웹 애플리케이션으로 구현하고 보안성을 확인하였다. Android 모바일 플랫폼에서 제공되는 API를 통해 애플리케이션은 IMEI를 획득할 수 있다[32]. 그러나 브라우저가 모바일 단말기로부터 IMEI를 가져오는 부분과 서버가 클라이언트에게 블록암호 Key를 분배하는 부분은 목적에서 벗어나므로 구현하지 않는다.

4.1. ISeBM 구현

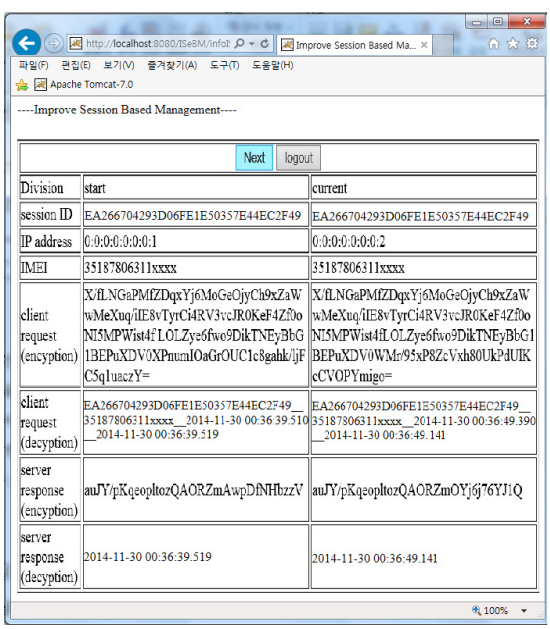

그림 4. 메인 페이지
Fig. 4 Main Page

Java Servlet과 JSP(Java Server Page)을 이용하여 구현한 프로토타입의 로그인 화면에서 사용자 인증에 성공하면 그림 4의 Main Page에서 자신의 세션 정보를 확인할 수 있다.

4.2. 안정성 점검

XSS 공격, CSRF 공격, Sniffing 공격 등 여러 해킹 기법을 대상으로 안정성을 점검했는데, 그 결과는 아래와 같이 거의 유사했다.

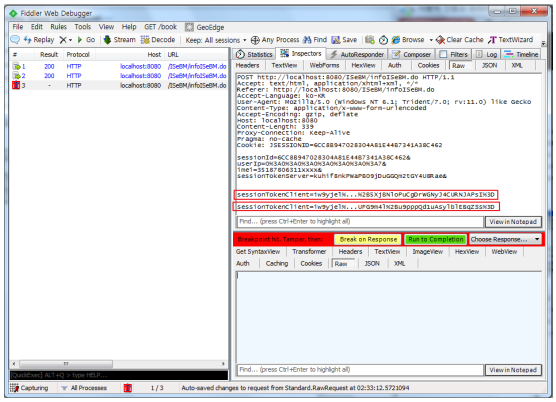

그림 5. 세션 하이재킹
Fig. 5 Session Hijacking

정상적인 사용자가 HTTP Request를 시도할 때마다 주고받는 암호화된 Session token을 그림 5에서처럼 공격자가 Proxy 툴인 Fiddler4로 탈취해서 도용해 서버로 전송했다.

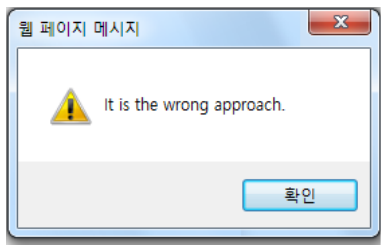

그림 6. 실패 메시지
Fig. 6 Fail Message

이 경우 정상적인 Session token은 클라이언트 요청 시간(2014-11-30 00:36:49.390)과 서버 응답 시간(2014-11-30 00:36:49.141)으로 갱신된다. 그러나 공격

자가 도용한 Session token은 클라이언트의 요청시간(2014-11-30 00:36:49.390)은 동일하지만, 새로 갱신되지 않은 서버의 응답 시간(2014-11-30 00:36:39.519)으로 구성되어 있으므로, 서버 응답 시간이 맞지 않아 공격은 실패하고 그림 6과 같은 메시지가 뜨며 세션은 해제된다.

Ⅴ. 결 론

모바일 웹에서 세션은 인증 상태를 유지하는 중요한 정보이다. 앞서 살펴본바와 같이 모바일 환경에서 웹 세션 보안은 취약하다. 따라서 본 논문에서는 모바일 환경에 적합한 세션 관리 방식을 제안하였다.

기존 Session Token 방식과 비해 ISeBM은 보안이 강화됐고 BYOD 운영에도 도움을 준다. Session Token을 적절한 암호 알고리즘으로 암호화하여 단말기의 고유 정보를 보호할 수 있다. 매 요청마다 timpstamp로 갱신되는 일회성 Session Token을 주고받고, 세션 유효 시간을 확인하여 기간이 만료된 세션은 무효화해서 세션 도용도 방지할 수 있다. NAT 기반의 이동통신망에 적합한 고유 식별자인 IMEI를 Session Token에 활용함으로써 모바일 웹 기반의 BYOD에서 단말기 인증에 도움을 준다. 지난 Session Token을 이력으로 관리해서 보안과 관련된 빅데이터 분석을 가능하게 한다.

본 논문의 향후 발전 과제로 수집된 세션 접속 이력을 통해 악성 행위 유형과 패턴을 분석하고, 이에 선 대응이 가능하도록 개선하면 보다 안전한 모바일 웹 애플리케이션 서비스를 보장할 수 있다.

REFERENCES

[1] K. Y Kim, and D. H. Kang, “Smartphone Security in Open Mobile Environment,” *Korea Institute of Information Security and Cryptology,* vol. 19, no. 5, pp. 21-28, 2009.

[2] S. G. Lee, “Mobile security theater and measure,” in *White Paper of Country Information Security*, 6th ed. Korea, Korea Internet & Security Agency., ch. special, pp. 262-274, 2013.

[3] K. J. Lee, “Vulnerability Analysis of the domestic mobile environment,” in *A research on discovering new vulnerabilities and analyzing methods in domestic mobile environment,* 1st ed. Korea, Korea Internet & Security Agency., ch. 3, pp. 25-58, 2012.

[4] H. H. Kim, et al. “Testing and Countermeasures of HTTP Session Hijacking Attacks in 802.11ac networks,” in *Proceeding of the Annual Korean Institute of Communications and Information Sciences, Korea,* pp. 684-686, 2013.

[5] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1,* IETF(Internet Engineering Task Force), 1999.

[6] OWASP(The Open Web Application Security Project). OWASP Top 10 Project(2013) [Internet]. Available: https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents/.

[7] OWASP(The Open Web Application Security Project). OWASP Mobile Security Project(2014) [Internet]. Available: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks/.

[8] Ahnlab. HTTP Session Hijacking [Internet]. Available: http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=5780/.

[9] J. S. Park, Ravi Sandhu, and SreeLatha Ghanta, “RBAC on the Web by Secure Cookies,” in *IFIP TC11 WG11.3 13th Working Conference on Database Security,* pp. 49-62, 1999.

[10] M. Dietz, A. Czeskis, D. Balfanz, and D. S. Wallach, “Origin-Bound Certificates : A Fresh Approach to Strong Client Authentication for the Web,” in *Proceeding of 21st USENIX Security Symposium*, pp. 317-331, 2012.

[11] J. S. Kim, “A study on the improvement for Authentication and Session Management in Web Application,” M.S. dissertation, Korea University, 2005.

[12] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, “One-time cookies: Preventing session hijacking attacks with stateless authentication tokens,” *ACM Transactions on Internet Technology (TOIT)*, vol. 12, no. 1, 2012.

[13] S. M. Hong, “Web Attack Blocking Algorithm Using User Authentication and Parameter Encryption,” M.S. dissertation, Chungbuk University, 2007.

[14] De Ryck, Philippe, et al. “Eradicating bearer tokens for session management,” in *W3C/IAB workshop on strengthening the internet against pervasive monitoring (STRINT)*. pp. 1-6, 2014.

[15] B. M. Goo, et al. “User Identification of 4G Network attack/anomaly traffic through the session management,” in

Proceeding of Korean Society for Internet Information, pp. 81-82, 2013.

[16] 3GPP TS 23.003 V7.9.0, *3GPP Standard for Numbering Addressing and Identification*, 3GPP, 2009.

[17] Android Developers Blog. Identifying App Installations [internet]. Available: http://android-developers.blogspot.kr/2011/03/identifying-app-installations.html.

[18] Android. Security Tips [internet]. Available: http://developer.android.com/training/articles/security-tips.html.

[19] Praveen Nallasamy. (2011, July). Security and Privacy issues in iOS and Android Apps. OWASP New York chapter meeting [Online]. pp. 1-50. Available: https://www.owasp.org/images/5/5e/Mobile_Security_-_Android_and_iOS_-_OWASP_NY_-_Final.pdf.

[20] M. G. Kim, "A Study of Smart-Phone Location Data Network Packet Analysis," M.S. dissertation, Hoseo University, 2007.

[21] A. J. F. Loureiro, D. Gallegos, and G. Caldwell, "Substandard cell phones: Impact on network quality and a new method to identify an unlicensed IMEI in the network," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 90-96, 2014.

[22] S. Yu, K. Sood, and Y. Xiang, "An Effective and Feasible Traceback Scheme in Mobile Internet Environment," *IEEE Communications Letters*, Vol. 18, no. 11, pp. 1911-1914, 2014.

[23] R. Copeland, and N. Crespi, "Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules," in *16th IEEE International Conference on Intelligence in Next Generation Networks (ICIN)*, pp. 194-201, 2012.

[24] T. Ramya, et al. "Personalized authentication procedure for restricted web service access in mobile phones," in *2014 5th IEEE International Conference on the Applications of Digital Information and Web Technologies(ICADIWT)*, pp. 69-74, 2014.

[25] J. P. Lee, Y. H. Kim, and J. K. Lee, "SSL Application for Managed Security between the Mobile and HIS Biometric Information Collection Client," in *28th IEEE International Conference on Advanced Information Networking and Applications Workshops(WAINA)*, pp. 55-60, 2014.

[26] K. A. Rahad, "A new initiative for ERP system architecture with mobile cloud aspects of Bangladesh," in *International Conference on Electrical Engineering and Information & Communication Technology(ICEEICT)*, pp. 1-4, 2014.

[27] S. J. Lee, "A one time QR-code authentication system using international mobile equipment identity," M.S. dissertation, Korea Aerospace University, 2014.

[28] S. S. Shin, and Y. Y. Kim, "A Study on Multi-Media Contents Security Using Android Phone for Safety Distribution," *The Korea Society of Digital Policy & Management*, vol. 10, no. 6, pp. 213-239, 2012.

[29] T. Ramya, "PERSONALIZED AUTHENTICATION PROCEDURE FOR RESTRICTED WEB SERVICE ACCESS IN MOBILE PHONES," in *The 5th IEEE International Conference on the Application of Digital Information and Web Technology(ICADIWT)*, pp. 69-74, 2014.

[30] Google. Privacy Policy [Internet]. Available: http://www.google.com/policies/privacy/#infocollect.

[31] Samsung. Privacy Policy [Internet]. Available: https://account.samsung.com/membership/pp.

[32] Android. Android API Guides [Internet]. Available: http://developer.android.com/reference/android/telephony/TelephonyManager.html.

[33] Lukanta, Raymond, and Yudistira Asnar, "A vulnerability scanning tool for session management vulnerabilities," in *2014 1st International Conference of Data and Software Engineering(ICODSE) on IEEE*, pp. 1-6, 2014.

[34] Alohali, Bashar, Madjid Merabti, and Khasif Kifayat, "A secure scheme for a smart house based on Cloud of Things (CoT)," in *2014 6th Computer Science and Electronic Engineering Conference(CEEC) on IEEE*, pp. 115-120, 2014.

김영훈(Younghun Kim)

단국대학교 컴퓨터과학과(학사)
(주) 신도리코 솔루션 개발
현재 세종사이버대 정보보호 대학원 석사 과정
※관심분야 : 웹/컴퓨터 보안

박용석(Yongsuk Park)

서강대학교 컴퓨터공학 (학사)
뉴욕(POLY)대 (석사, 박사)
AT&T Bell Labs
삼성전자
현재 세종사이버대학교 정보보호 대학원 주임교수
현재 정보보호컴퓨터정보통신 학부 교수
※관심분야 : IT 서비스 및 보안, 산업보안, 클라우드, 웨어러블 컴퓨팅 등