ISSN 2234-4438
중소기업융합학회 논문지 제6권 제2호 pp. 31-36, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.2.031

효율적인 Sniffing 공격 대응방안 연구

홍성혁[1*], 서유정[2]
[1]백석대학교 정보통신학부, [2]중부대학교 정보보호학과

Countermeasure of Sniffing Attack: Survey

Sunghyuck Hong[1*], Yujeong Seo[2]
[1]Baekseok University, Div. Information and Communication
[2]Joongbu University, Information Security

요 약 Sniffing은 공격자가 암호화 되지 않은 패킷들을 수집하여 순서대로 재조합 하고난 후 공격 대상의 개인정보, 계좌정보 등 중요 정보를 유출하기 위한 수동적 형태의 공격이다. Sniffing 공격으로 인해 패킷들이 유출되는 것을 방지하기 위해 기존의 방법들을 살펴보고, 효율적인 방어대책을 제시하였다. Sniffing공격은 공격 대상의 근거리 네트워크를 Promiscuous Mode을 이용해 조작한 후 필터링을 해제하고 패킷을 훔치는 방식으로 작동한다. 공격의 형태로 Switch Jamming, Port mirroring, ARP Redirect, ICMP Redirect 공격 등이 있다. 제안하는 공격 대응 방법으로는 SSL을 통한 패킷의 암호화, 스위칭 환경의 네트워크 구성 관리, DNS를 이용하는 방법과 decoy방법을 이용하면 안전한 통신이 가능할 것으로 기대하며, 더 효율적이며 안전한 ICT 연구에 기여한다. 향후 프로토타입 프로토콜을 통하여 효율성을 증명하는 것은 향후 연구로 진행할 예정이다.

키워드 : Sniffing 공격, 웹 해킹, 수동적 공격, 네트워크 보안

Abstract Sniffing attack is a passive attack which is reassembling packets to collect personal information, bank accounting number, and other important information. Sniffing attack happens in LAN and uses promiscuous mode which is opening filtering by pass all packets in LAN, attackers could catch any packets in LAN, so they can manipulate packets. They are Switch Jamming, Port mirroring, ARP Redirect, and ICMP Redirect attack. To defend these attacks, I proposed to use SSL packet encryption, reconfiguration of switching environment, DNS, and decoy method for defending all kinds of Sniffing attacks.

Key Words : Attacks sniffing switch, Data protection, mobile security, Web security, Switch

1. 서론

IoT 관련 신제품과 서비스가 증가하는 등 IoT시장이 본격적으로 성장하고 있다. 이에 따른 IoT 보안 문제의 심각성을 보여주는 많은 사례가 보고되고 있다. 서비스가 늘어감에 따라 공격의 경로가 다양해지고 있기 때문이다.

Capemini Consulting에서 IoT제품 개발과 관련된 대기업의 CEO, 사이버보안 전문가를 대상으로 IoT 보안 위협 공격 유형에 따른 설문 조사를 실시한 결과에 따르면 패스워드공격, ID 스푸핑 공격, 데이터변경 공격, 도청/스니핑 공격, 서비스거부 공격 중 스니핑 공격이 39%로 높은 비율을 차지했다[1].

스니핑은 정보보안의 3요소 중 기밀성을 해치는 공격이다. 하지만 IoT제품 개발에서 보안에 신경을 쓰는 기업은 전체의 48% 밖에 없는 것으로 나타난다[1]. 시장이

Received 2016-06-07 Revised 2016-06-15 Accepted 2016-06-16 Published 2016-06-30
*Corresponding author : Sunghyuck Hong (shong@bu.ac.kr)

성장해가는 것처럼 보안에 대한 수준도 더욱 높아져야 한다.

본 연구의 구성은 다음과 같다. 2장에서는 스니핑의 원리, 형태 등을 기술하였으며, 3장에서는 스니핑의 대응 방법을 기술하였다. 그리고 4장에서 연구를 마무리하는 결론을 맺는다.

2. 스니핑 (Sniffing)

2.1 스니핑 (Sniffing)

스니핑은 암호화가 되지 않은 패킷들을 수집하여 순서대로 재조합 하고난 후, ID, PASSWORD나 계좌의 비밀번호 같은 중요 정보를 유출하기 위한 수동적 형태의 공격으로. 공격대상의 네트워크 패킷을 수집하여 분석 또는 도청한다. 도청할 때 사용하는 도구를 스니퍼(sniffer)라고 한다. 이것이 위협적인 이유는 네트워크 내의 여러 패킷들은 상당수가 암호화되어 있지 않아 공격 대상이 되기 쉬우며, 그로인해 우리의 사생활이 노출되며 자산이 위협을 받을 수 있기 때문이다.

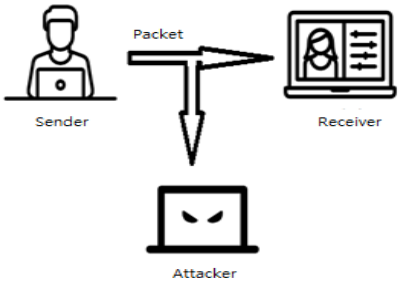

Fig. 1. Sniffing Concept

2.2 스니핑의 원리

스니핑의 원리를 이해하기 전에 먼저 이더넷 로컬네트워크의 동작원리를 이해해야 한다[2-5]. 이더넷 로컬 네트워크의 모든 호스트는 동일한 선을 공유하도록 설계되어 있다. 즉 같은 네트워크 내에 있는 컴퓨터는 다른 컴퓨터가 통신하는 트래픽을 모두 볼 수 있는 것이다. 그래서 LAN상에서 각각의 호스트를 구별하기 위한 방법으로써 이더넷 인터페이스는 하나의 MAC주소를 갖는다. 모든 이더넷 인터페이스는 서로 다른 MAC주소의 값을 가진다. 따라서 네트워크상의 모든 호스트들은 MAC 주소로 구별할 수 있다.

전송자는 자신의 MAC주소와 수신자의 MAC주소, 그리고 데이터를 포함하여 전송하게 되는데 이때 로컬 네트워크 내의 모든 호스트는 수신자의 MAC주소를 확인하여 본인이 아닐 경우 필터링을 거쳐 해당 패킷을 폐기하는 방식으로 동작한다. 그러나 공격자가 공격 대상의 랜카드를 Promiscuous Mode를 이용해 조작하면 필터링이 해제되고 패킷을 폐기하지 않기 때문에 다른 호스트의 통신 내용을 수신할 수 있게 된다.

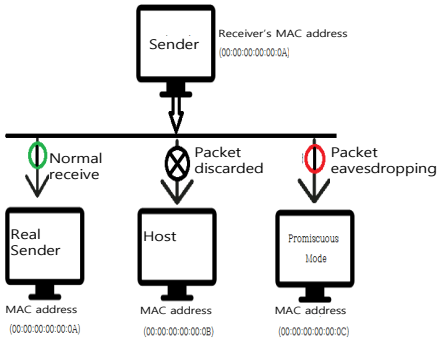

Fig. 2. Sniffing Actually Works

2.3 스니핑의 공격 기법

과거의 Dummy Hub 환경과는 달리 현재의 스위칭 허브 환경에서는 이런 스니핑 툴을 사용한다고 해서 패킷 스니핑이 되지 않기 때문에 정상적인 스위치 환경이라면 스니핑 공격은 불가능하다. 그러나 이 불가능을 가능으로 바꾸는 공격 기법이 존재한다.

첫 번째 공격 기법으로는 Switch Jamming 기법이 있다. 스위치는 문제가 생기면 모두 허용해주는 정책인 Fail Open을 따르는 장비이다. 스위치의 이러한 장비적 특성은 맥 주소 테이블을 가득 채우면 모든 포트로 트래픽을 전송 하는 특징을 가지고 있다[3, 6-8]. Switch Jamming 공격 기법은 이 특징을 이용하여 고의적으로 변조한 맥 정보를 담고 있는 ARP Reply 패킷을 전송하여 맥 주소 테이블을 가득 채운다. 그리고 스위치가 Dummy Hub처럼 모든 프레임을 스위치의 모든 포트로 전송하도록 만들어서 스니핑이 가능한 환경을 만든다. 그리고 공격자는 이러한 환경을 이용하여 자신의 주소 테이블을 오버플로우 시킨다. 그리고 다른 네트워크로 거짓된 맥 주소를 지속적으로 네트워크에 흘린다. 그럼으로써 공격자는 공격 대상의 네트워크 세그먼트의 데이

터를 스니핑 할 수 있게 된다[9,10].

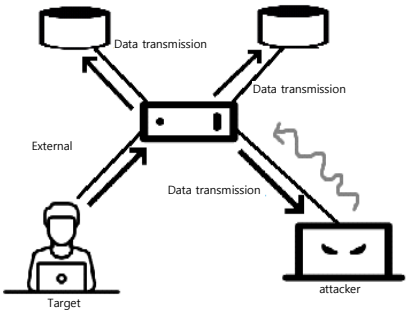

Fig. 3. Switch Jamming

이것은 장치의 문제점이 아닌 아주 일반적인 스위치의 특징을 이용한 공격방법이다. 그러나 이 방법을 사용하면 스위치가 Dummy Hub처럼 동작하므로 공격자 입장에서는 통신 속도가 저하되는 단점이 있으며, 최근에는 맥 주소 테이블을 가득 채우지 않아도 프레임을 드랍시키는 스위치 기술이 개발되어 무용지물인 공격법이 되었다.

두 번째 공격 기법으로는 Port mirroring기법이 있다. Port mirroring은 다른 말로 SPAN라고도 부른다. SPAN이란 어떠한 특정 포트에서 특정 분석 장비에 접속하고, 또 다른 포트의 트래픽을 해당 분석 장비로 자동 복사해 주는 기술을 말한다. 사실 Port mirroring의 원래의 목적은 만약 네트워크에 이상이 발생 시 이 문제점을 파악하기 위해 사용하였다. 그러나 스위치에 존재하는 모든 포트에서 이동하는 데이터들의 정보를 복제하여 보내주는 포트이기 때문에 이를 역으로 이용해 공격자가 트래픽을 스니핑 할 수 있는 용이한 환경을 제공해 준다.

세 번째 공격 기법은 ARP Redirect 공격 기법이다. 이 공격 기법을 설명하기 전에 장상적인 ARP 프로토콜에 대하여 알아야 한다. IP주소는 32bit이고 MAC주소는 48bit이다. 그리고 전송 호스트가 수신 호스트에게 패킷을 보내기 위해서는 수신 호스트의 맥 주소를 알아야 한다. 결국 사용자는 IP주소를 MAC주소로 바꾸어야 하는데 이 과정을 Address Resolution Protocol, 즉 ARP이라고 한다. ARP의 과정은 다음과 같다. 우선 네트워크 내의 호스트들에게 ARP Request를 보낸다. 응답을 받을 수신자 호스트의 IP를 포함하고 있는 ARP Request는 모든 호스트들 중 MAC주소가 일치하는 호스트를 찾는다. 수신자 호스트는 송신자 호스트에게 자신의 MAC주소를 보내주는데 이것을 ARP Reply이라고 한다. 그리고 ARP Redirect 공격은 이 ARP Reply를 위조하여 보내는 방법을 쓰는 공격 기법이다. 즉, 공격자 호스트가 위조된 ARP Reply를 네트워크에 지속적으로 브로드캐스트하고, 다른 호스트들이 공격자 호스트를 수신자 호스트인 것처럼 속게 만든다. 결국 그림4와 같이 네트워크의 모든 트래픽은 필터를 통과하여 공격자 호스트에게 도달하고 공격자는 스니퍼를 하여 필요한 정보를 빼낼 수 있게 된다.

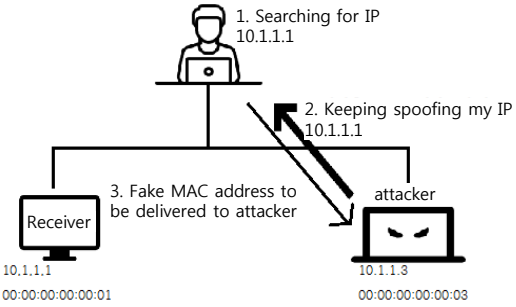

Fig. 4. ARP Redirect

네 번째 공격기법으로 ICMP Redirect공격이 있다. ICMP이란 Internet Control Message Protocol의 약자로 네트워크내의 에러가 적힌 메시지를 전송하거나 네트워크의 흐름을 통제하기 위한 프로토콜을 말한다[5]. 인터넷에는 라우터의 수 보다 더 많은 수의 호스트가 존재한다. 효율성을 위해 호스트는 라우팅 갱신에는 참여하지 않는데, 그 이유는 호스트의 라우팅 테이블을 동적으로 갱신하면 트래픽이 과하게 많아지기 때문이다.

그렇기 때문에 호스트는 보통 정적 라우팅을 사용하며, 라우터나 특정 게이트웨이를 default 게이트웨이로 설정하여 사용한다. 호스트가 동작할 때 호스트 라우팅 테이블은 한정된 수의 엔트리를 가지고 있다. 바로 디폴트 라우터의 IP주소를 한 개만 가지고 있는 경우다. 그렇기 때문에 다른 네트워크로 데이터를 보낼 때 호스트는 잘못된 라우터에게 보낼 수 있다. 이럴 경우 데이터를 받은 라우터는 데이터를 올바른 라우터에게 전송해야 하는데, 이 때 라우터는 자신보다 더 좋은 최적의 경로가 있다는 뜻의 메시지를 호스트에게 보내는데 이것이 ICMP Redirect 메시지이다.

이 방법을 악용하는 공격인 ICMP Redirect공격은 3계층에서 동작하는 스니핑 기법으로 공격자는 라우터가 호스트에게 ICMP Redirect 메시지를 보낼 때 공격 대상에

게 자신이 라우터이고, 최적의 경로라고 변조된 ICMP Redirect 메시지를 호스트에게 보낸다. 그렇게 공격 대상은 변조된 메시지를 받고 가짜 게이트웨이를 거치게 되므로 취약점이 발생하고, 공격자는 그점을 악용하여 스니핑이 가능해진다.

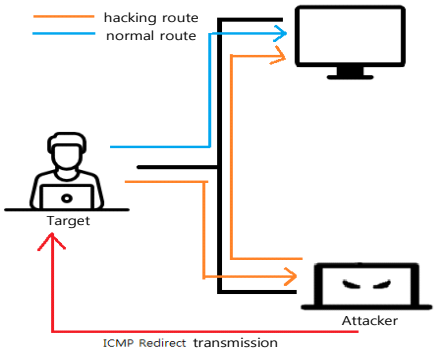

Fig. 5. ICMP Redirect

2.4 스니핑의 공격 사례

영화 '타짜'에서 나올 법한 사기도박수법이 pc온라인 게임에 등장해 화제가 되었다. 상대의 패를 미리 확인하기 위해 스니핑 공격을 시도, 패를 확인하거나 바꾸는 방식에 의해 해킹피해를 당했다는 사례가 늘어나고 있다. 현재 알려진 것으로는 해커들이 스니핑 공격을 통해 일반 유저들의 패를 가로챈 뒤 임의적으로 승부를 조작하고 있는 것으로 알려져 있다. 스니핑 공격에 피해를 당했다고 주장하는 게이머들은 "카드 게임 중 정해진 패턴이 반복되는 경우가 많다"등의 사기도박을 의심하고 있다[6-8].

2.5 하나은행 해킹시도

서울지방경찰청에 구속된 이모(50)씨 등이 하나은행 해킹시도에 스니핑을 사용하였다. 이씨 일당은 하나은행 외부 고객용 PC관리자 번호를 확보했고, 본격적인 은행 전산망 침투를 12차례 시도하던 중 다행이 검거 됐다. 경찰은 다른 은행돌도 대부분 인터넷 뱅킹에 AP를 사용하고 있기 때문에 이런 공격에 주의해야한다고 밝혔다[11-14].

2.6 우크라이나 정전사태.. 도구는 스니퍼

지난 12월 우크라이나 대규모 정전사태에 사용된 도구에 네트워크 스니퍼가 사용되었다는 사실이 발표되었다. 보안 전문 업체인 센티넬원의 CSO인 메후드 샤미르는 당시 발견된 블랙에너지3이 리버스 엔지니어링을 했으며, 매크로가 악용된 엑셀 스프레드시트가 네트워크 스니핑 툴이 포함된 페이로드를 피해 입은 시스템에 다운로드 시킨 것을 밝혀냈다. 네트워크를 스니핑 함으로써 공격자들은 많은 정보를 얻어낼 수 있었다. 로그인 정보는 물론, 그렇게 하기 위해 패치 되지 않은 오피스가 설치된 시스템을 찾은 것으로 보인다[13,15].

3. Sniffing 공격 대응 방안

스니핑 공격을 방어하는 방법중 가장 좋은 방법은 데이터를 암호화하여 스니핑을 당하더라도 내용을 볼 수 없게 만드는 방법이다.

암호화의 방법 중 하나는 SSL이다. SSL은 Secure Sockets Layer의 약자로, 웹 서버와 웹 브라우저 사이의 보안을 위해 중요한 데이터를 전송할 때 사용되는 인터넷 통신 규약 프로토콜이다. 인터넷 프로토콜이 보안면에서 기밀성 유지에 부족하다는 문제를 극복하기 위해 개발되었으며, 현재 전 세계에서 보안 유지에 가장 많이 사용되는 프로토콜이다. 기밀성, 무결성, 인증, 암호화, 웹 서버의 인증 등 많은 보안을 담당하고 있다.

첫 번째로는 스위칭 환경의 네트워크 구성을 관리하는 것 이다. 스위치를 설정할 때, 스위치의 주소 테이블을 정적 설정하여 스위칭 환경의 스니핑을 막을 수 있다. 아래의 Table 1 같이 스위치의 각 포트에 대해 맥주소를 정적으로 대응시킨다면 ARP Redirect공격을 막을 수 있다. 이 방법은 보안 관리에 시간을 많이 소모하게 되지만 매우 효과적이고 강력한 대응방법이다.

Table 1. Switch Table

Port	MAC	Permanence
1	0:60:2f:a3:9a:16	Yes
2	0:60:97:c4:f:3e	Yes
3	8:0:20:79:c9:ea	Yes
4	0:60:97:c4:f:3e	Yes

두 번째로는 스니퍼 탐지 방법이다[9]. 모든 스니퍼는 'promiscuous mode'를 설정하여 공격을 실행한다. 따라서 관리자는 호스트가 'promiscuous mode'로 설정되어

있는지 주기적으로 검사하여 스니퍼가 실행되고 있는 시스템을 탐지해야한다. 스니핑 기술이 고도화되는 것과 마찬가지로 스니퍼를 탐지하는 방법도 점점 다양해지고 있다. 스니퍼 탐지에는 4가지 방법이 있다. 우선 ping을 사용하는 방법으로는, 스니퍼는 TCP/IP스택에서 동작하기에 응답을 받으면 그에 해당하는 응답을 전달해야 한다. ping을 이용한 스니퍼 탐지방법은 의심가는 시스템에게 ping을 보내되 맥주소를 위장하여 보내는 방법이다.

세 번째로는 ARP를 이용하는 방법이다[10]. ping을 이용하는 방법과 유사한 방법이지만 non-broadcast로 위조된 ARP응답을 보냈을 때 ARP response라고 온다면 상대방 호스트가 'promiscuous mode'로 설정되어 있다는 것이다.

네 번째로는 DNS를 이용하는 방법이다. 스니핑 프로그램은 스니핑한 호스트의 IP주소를 보여주지 않고 도메인 명을 보여 주기 위해 Inverse-DNS lookup을 수행하게 된다. 이러한 특성을 이용해 DNS트래픽을 감시하면 스니퍼를 탐지할 수 있다. 이 방법은 원격, 로컬네트워크 모두에서 사용할 수 있는 방법이기도 하다.

네 번째는 decoy방법이다. 스니퍼 공격자는 사용자 ID와 패스워드를 도청하고 도청한 계정을 이용하여 다른 시스템을 공격 한다[16,17]. 따라서 네트워크상에 미리 설정된 계정을 지속적으로 흘려서 공격자가 이 계정을 사용하게 만든다. 관리자는 네트워크 감시프로그램이나 IDS를 이용하여 미리 설정된 계정을 사용하는 시스템을 탐지하여 스니퍼를 탐지할 수 있게 된다.

4. 결론

Sniffing 공격은 공격자가 암호화 되지 않은 패킷을 가로채어 사용자의 금융정보, 개인정보 등을 알아내어 손해를 입히는 공격을 할 수 있다.

이러한 Sniffing의 대표적인 공격 방법으로는 Switch Jamming, Port mirroring, ARP Redirect, ICMP Redirect 등 이 존재한다. 이러한 공격들의 대응 법으로는 SSL을 통한 패킷의 암호화, 스위칭 환경의 네트워크 구성 관리, DNS를 이용하는 방법, decoy방법 등이 있으며, 관리자는 점검을 자주해야하고 새로운 대응 법을 항상 공부하해야 하고, 사용자들은 출처나 정보가 불확실한 프로그램의 사용을 멀리하고 보안 업데이트를 통해 취약점을 보안함으로써 보안을 높일 수 있다.

제안된 프로토콜의 효율성을 보장하기 위한 시뮬레이션을 통한 기존 프토로콜의 비교 연구는 향후 연구에서 진행할 예정이다.

ACKNOWLEDGMENTS

이 논문은 2016학년도 백석대학교 대학연구비에 의하여 수행된 것임.

REFERENCES

[1] J. Born, T. Lange, W. Kern, G. P. McGregor, U. Bickel and H. L. Fehm, "Sniffing neuropeptides: a transnasal approach to the human brain," *Nature neuroscience*, Vol. 5, No. 6, pp. 514-516, May. 2002.

[2] N. Sobel, V. Prabhakaran, J. E. Desmond, G. H. Glover, R. L. Goode, E. V. Sullivan, J. D. Gabrieli, "Sniffing and smelling: separate subsystems in the human olfactory cortex." *Nature*, Vol. 392, No. 6673, pp. 282-286, May. 1998.

[3] D. Song, D. Brumley, H. Yin, J. Caballero, I. Jager, M. G. Kang, Z. Liang, J. Newsome, P. Poosankam, and P. Saxena, "BitBlaze: A new approach to computer security via binary analysis," *Information systems Security, LNCS 5352*, pp. 1-25, Dec. 2008.

[4] J. Caballero, S. McCamant, A. Barth, and D. Song, "Extracting models of security-sensitive operations using stringenhanced white-box exploration on binaries," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-36*, Mar 2009.

[5] B. S. Thakur and S. Chaudhary, "Content Sinffing Attack Detetion in Client and Server Side: A Survey," *International Journal of Advanced Computer Research*, Vol. 3, No. 2, pp. 7-10, Jun. 2013.

[6] P. Godefroid, M. Y. Levin and D. Molnar, "Automated whitebox fuzz testing," *Proceedings of the Annual Network and Distributed System Security Symposium*, San Diego, California, pp. 1-16, 2008.

[7] P. Noiumkar, "Top 10 Free Web-Mail Security Test Using Session Hijacking," *Proceeding of 2008 International Conference on Convergence and hybrid Information Technology*, Vol. 2, pp. 486-490, 2008.

[8] L. B. Noe, "The Software Architecture of A Secure and

Efficient Group Key Agreement Protocol," *Journal of Convergence Society for Small and Medium Business*, Vol. 4, No. 3, pp. 21-58, Sep. 2014.

[9] N. Bjorner, N. Tillmann and A. Voronkov, "Path feasibility analysis for string-manipulating programs," *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems 2009(TACAS 2009)*, LNCS 5505, pp. 307-321, 2009.

[10] S. H. Lee and D. W. Lee, "A Study on Internet of Things in IT Convergence Period," *Journal of Digital Convergence*, Vol. 12, No. 7, pp. 267-272, Jul. 2014.

[11] K. J. Lee and K. H. Lee, "A Study of Security Threats in Bluetooth v4.1 Beacon based Coupon Convergence Service," *Journal of the Korea Convergence Society*, Vol. 6, No. 2, pp. 65-70, Apr. 2015.

[12] T. Hoppe and J. Dittman, "Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy," *Proceedings of the 2nd workshop on embedded systems security (WESS)*, pp. 1-6, 2007.

[13] A. Kiezun, V. Ganesh, P. J. Guo, P. Hooimeijer and M. D. Ernst, *HAMPI: A solver for string constraints*, MIT CSAIL, Tech. Rep. MIT-CSAIL-TR-2009-004, 2009.

[14] C. Cadar, V. Ganesh, P. M. Pawlowski, D. L. Dill and D. R. Engler, "EXE: Automatically generating inputs of death," *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 322-335, 2006.

[15] J. H. Soo and G. S. Chae, "Detection of Forgery of Mobile App and Study on Countermeasure," *Journal of Convergence for Small and Medium Business*, Vol. 5, No. 3, pp. 27-31, Sep. 2015 .

[16] K. Moore, *RFC 2047: Multipurpose Internet Mail Extensions (MIME) part three: Message header extensions for non- ASCII text*, 1996.

[17] B. C. Kim, "A study on Utilization of Big Data Based on the Personal Information Protection Act," *Journal of Digital Convergence*, Vol. 12 No. 12, pp.87-92, Dec. 2014.

저 자 소 개

홍 성 혁(Sunghyuck Hong) [종신회원]

- 1995년 2월 : 명지대학교 컴퓨터공학과 (학사)
- 2007년 8월 : Texas Tech University, Computer Science (Ph.D.)
- 2007년 9월 ~ 2012년 2월 : Senior Programmer, Texas Tech University, Office of International Affairs
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야> : 네트워크 보안, 해킹, 센서네트워크

서 유 정(Yujeong Seo) [학생회원]

- 2013년 2월 : 대전성모여자고등학교 졸업
- 2013년 3월 ~ 현재 : 중부대학교 정보보호학과 재학

<관심분야> : 네트워크 보안, 정보보호