Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Reliable Service Provided Model for Session Hijacking Attacks in Big Data Service Environments

Jae-Yeong Choi[1], Jae-Heung Park[1], Yeong Geon Seo[1], Suk-Won Hong[2], Sang-Bok Kim[*1]

[1]*Department of Computer Science, Gyeongsang National University*
[2]*Division of Academic Affairs, Gyeongnam Provincial Geochang College*

ABSTRACT

Today, big data environments in which a large quantity of data are produced and collected are managed based on cloud computing. In addition, the new data environment using big data is leading the development in a variety of information and service technologies in today's society. However, this network environment can be vulnerable to session hijacking attacks, which exploit a valid computer session and use it to attack a server or computer system. This study classified different levels of stable services and sensitive information during session hijacking in a cloud computing environment in which various network services are provided, and encrypted the relevant services. To do so, the levels of values of session interruption data and access data were classified and combined in order to create an encryption bit pattern for each level. And then, the service levels related to data request at the time of an attack were analyzed so that the data are sent after encryption by using the bit pattern, instead of providing instant service. As a result, this study proposed a security model that improved both stability and availability of service against illegal access that can be found in the conventional network environment.

KEYWORDS: TCP 3-way, Session hijacking, Data encryption standard, Big data, Sniffing

ARTICLE INFO: Received 5 October 2016, Revised 12 December 2016, Accepted 12 December 2016.

[*]Corresponding author is with the Department of Computer Science, Gyeongsang National University, 501, Jinju-daero, Jinju-si, Gyeongsangnam-do, 52828, KOREA.
E-mail address: sbkim@gnu.ac.kr

1. 서 론

오늘날 인터넷을 통한 정보 서비스 환경은 클라우드 기술을 기반으로 하는 빅데이터 서비스로 전환되고 있다. 그렇지만 빅데이터의 생성 과정에는 다양한 정보 수집이 발생하기 때문에 민감한 자료에 대한 강화된 보안 정책은 필수 요구 사항이 되고 있다. 특히 개인정보와 프라이버시 침해문제는 인터넷 정보 환경의 발전을 저해하는 주요 원인이 되고 있다. 이에 따라 빅데이터 생성 과정에서 노출되는 중요한 개인정보 또는 자료들의 조합에 의해 특정 개인이나 조직에 위해를 끼칠 수 있는 자료들은 별도의 보안 정책 적용이 더욱 필요하다.

현재 기업들은 고객들의 소비패턴을 분석한 후 이를 고객 맞춤형 서비스에 반영하기 위하여 빅데이터 기술을 활용하고 있다. 그렇지만 이로 인해 민감한 개인정보들 또한 외부로 유출될 가능성이 더욱 높아질 수 있다. 또한 클라우드 컴퓨팅 기술을 기반으로 하는 빅데이터 환경은 불법적인 접근을 시도하는 해커들의 집중적인 공격 대상이 될 수 있다.

본 논문은 발생 가능한 공격 기법 중 세션하이재킹 공격을 통한 불법적인 자료 유출에 대한 방어 모델을 제안하고 있다.

본 논문에서 제안하는 서비스 제공 모델은 송신자와 수신자의 통신 과정에서 RST 신호가 발생하면 서버에서 사용자 정보와 서비스 정보에 대한 암호화 과정을 수행한다. 그 다음 클라이언트로 암호문을 전송하고 해당 클라이언트는 이를 복호화 시켜 서비스 내용을 열람할 수 있도록 하였다. 이 과정에서 서비스 자료가 공격자에게 서비스 될 경우, 공격자는 암호문에 대한 키가 없기 때문에 서비스 내용을 열람할 수 없다.

본 논문에서 클라이언트에 대한 인증 과정은 TCP 3-Way 핸드셰이킹 과정에서 발생하는 임의의 시퀀스 넘버와 사용자 정보를 이용하였다. 해당 인증 과정은 별도의 암/복호화를 위한 Key교환 없이 클라이언트에서 암호문을 생성한 후 이를 서버로 전송하고 서버에서 정상적인 복호화 과정이 이루어지면 그 결과에 따라 서비스 여부를 결정하도록 하였다.

또한 클라우드 컴퓨팅 환경의 특성상 네트워크를 통한 상호협력 서비스를 수행하는 시스템들은 각 시스템에서 운용하는 단일 보안정책 보다 상호협력이 가능한 보안모델로 구성하였다[1].

2. 관련연구

2.1 빅데이터의 개념

일반적인 빅 데이터의 정의는 단순히 데이터가 많은 것으로 정의하고 있다. 하지만 최근의 빅 데이터 정의는 기존의 데이터 환경과 비교하여 기존의 방법이나 도구로는 데이터 수집, 저장, 분석 등이 어려운 정형화된 데이터뿐만 아니라 비정형화된 데이터까지 포함하는 테라바이트 이상의 데이터라고 정의하기도 한다.

빅 데이터에 대한 또 다른 시각은 빅 데이터를 다양한 종류의 대규모 데이터를 이용하여 저렴한 비용으로 가치 추출과, 필요 데이터에 대한 빠른 수집, 발굴 및 분석을 할 수 있는 차세대 기술 또는 아키텍처를 의미한다.

빅 데이터의 특징으로는 기존의 크기(Volu me), 속도(Velocity), 다양성(Variety)의 3V에, 최근 중요하게 인식되고 있는 가치(Value)를 포함하는 4V로 그 특징을 나타내고 있다[2].

크기(Volume)는 물리적인 크기뿐만 아니라 개념적인 범위까지 포함하는 데이터의 규모적 의미를 나타낸다고 할 수 있다. 속도(Velocity)는 데이터가 생성되는 시간 및 이를 처리하는 과정에 소요되

는 시간적 측면의 의미를 나타낸다. 다양성(Variety)은 정형화된 데이터에 비정형화된 데이터까지 포함하는 취급하는 데이터 형식의 다양성 측면을 의미한다. 그리고 이러한 특징을 바탕으로 도출된 결과를 가치(Value)라고 할 수 있다.

그렇지만 이러한 4V의 특징을 가지고 있는 빅데이터 환경에는 다양한 장애 요인이 존재하고 있다. 그 중 보안 문제는 빅데이터를 수집하는 과정에 존재하는 클라우드 컴퓨팅 환경에 대하여 그 공격 기법이 날로 발전하고 있으므로, 이에 대한 대비책이 강구되어야 할 것이다[3][4][5].

2.2 세션 하이재킹 공격

클라우드 컴퓨팅 환경을 통하여 실시간 서비스를 하고 있는 서버들은 항상 공격자들에게 노출되어 있다고 보아야 할 것이다. 이러한 공격자들의 공격 기법들 중 정상적인 사용자로 가장하여 내부 보안망을 무력화 시킬 수 있는 공격 기법에 세션 하이재킹 공격이 있다[6]. 세션 하이재킹(Session Hijacking)이란 정상적인 사용자들의 접속 과정에 필요한 TCP-3Way 핸드셰이킹 과정에서 발생하는 세션에 대하여 '세션 가로채기'를 하는 것을 의미한다. 여기서 세션이란 사용자와 컴퓨터, 또는 두 대의 컴퓨터간의 연결 활성화 상태를 말한다.

TCP 세션 하이재킹 공격은 정상적인 사용자로 위장을 한 후 공격을 시도하는 부분에서 IP 스푸핑과 비슷하다고 할 수 있다. 하지만 IP 스푸핑의 경우는 상호 트러스트 정보를 이용한 공격을 시도하는 것이고, TCP 세션 하이재킹 공격은 활성화 되어 있는 세션을 RST 신호를 이용하여 강제로 빼앗아 가는 부분에 그 차이가 있다[7][8][9].

TCP 3-Way 핸드셰이킹 과정에서 발생하는 신호들은 시퀀스 번호를 통하여 상호 인증을 하고 있다. 즉, TCP 세션 하이재킹 공격은 서버와 클라이언트가 상호 세션 연결 과정에 발생하는 시퀀스 번호를 가로챈 다음 이를 이용하여 공격자 자신이 정상적인 클라이언트로 위장한 후 연결을 시도하는 것이다.

이렇게 TCP 3-Way 핸드셰이킹 과정을 통한 세션의 재설정은 인증의 성립을 의미하고, 재설정 과정을 거친 공격자는 모든 인증 과정을 우회할 수 있는 것이다.

일반적인 세션 하이재킹 공격을 탐지하는 방법에는 일반적으로 다음과 같은 방법들이 있다.

첫째, 서버와 시퀀스 넘버를 주기적으로 체크하여 비동기화 상태에 빠지면 이를 탐지 한다. 둘째, 전송중인 윈도우 크기와 시퀀스 번호가 맞지 않는 상태가 되면 상호 교정 패킷이 정상적으로 동작할 수 없기 때문에 루프 상태로 빠지면서 ACK 패킷 비율이 급격하게 증가한다. 셋째, 공격자가 중간에 개입하여 동작하는 것이므로 패킷의 손실 및 재전송 상황이 발생하기 때문에 응답 시간이 증가할 수 있다. 이상과 같이 세션 하이재킹 공격 발생 시 여러 가지 탐지방법들이 존재하지만 오늘날 빠르게 발전하고 있는 공격 기법에 능동적으로 대응하기에는 많은 어려움이 있다. 따라서 세션 하이재킹에 대한 최우선 대책은 이를 탐지하고 요구 데이터에 대한 적절한 수준의 암호화 과정을 수행한 후 서비스를 할 수 있어야 한다.

2.3 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅은 인터넷 기술을 활용하여 서버, 스토리지, 어플리케이션, 서비스 등 IT 자원을 필요한 만큼 빌려서 사용하고, 사용한 만큼의 요금을 지불하는 컴퓨팅 환경을 의미한다[10][11].

클라우드 컴퓨팅은 비공유 구조로 연결된 수많은 노드들을 이용한 병렬 처리를 하고, 서비스 부

하에 따라서 자원이 확장, 축소할 수 있도록 클라우드를 구성하는 노드 PC들의 추가와 제거가 유연하게 이루어진다. 이러한 환경은 기존의 일반적인 네트워크 환경보다 더욱 강화된 보안 정책을 요구하고 있다. 또한, 클라우드 컴퓨팅 환경에서는 다양하고 불법적인 공격으로부터 중요한 정보를 보호할 수 있는 보안 모델 개발이 절실하다[12][13].

3. 제안 모델 동작과정

본 논문에서 제안하는 모델은 <그림 1>과 같은 서비스 환경을 가진다. 서비스에 참여하는 각 서버는 자신들이 관리하는 정보들을 1등급, 2등급, 일반 자료로 구분하여 관리한다. 본 논문에서 1등급 자료는 그 자체로 민감한 정보가 될 수 있는 자료를 의미한다. 그 다음 2등급 자료는 각 서버에서 사용자 요청 자료 서비스를 수행할 경우 이들 자료간의 조합을 통해 민감한 정보로 변환 가능한 자료들로 분류하였다. 마지막으로 일반적인 서비스가 가능한 자료는 일반 자료로 분류하였다. 본 논문에서는 이들 자료 중 2등급 자료에 대하여 그 요청 기록을 데이터베이스에 등록하여 동일한 사용자가 다른 2등급 자료를 요청할 경우에는 서비스 정보를 암호화하여 전송하는 과정을 시뮬레이션을 수행하였다.

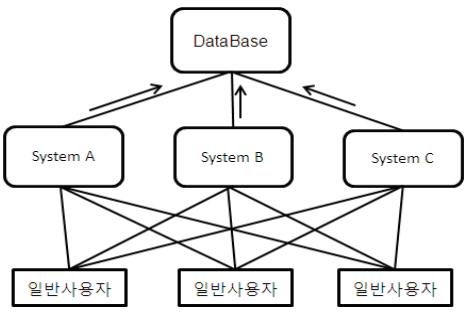

그림 1. 접근자료 정보 구축
Figure 1. Building Access Data Information

이와 함께 서버와 사용자 상호간 송/수신 과정에서 RST 신호 발생 유무, 등급에 따라 서비스 정보에 대한 암호화 과정을 수행한 후 서비스를 할 수 있도록 하였다.

<그림 2>는 일반적인 초기 연결 설정 과정에서 발생한 시퀀스 번호(Client_My_Seq)와 사용자 정보를 클라이언트의 암호화 버퍼에 저장하고 이를 이용하여 사용자 정보를 암호화 한 후, 자신의 인증 정보로 사용하게 된다.

아울러 서버에서는 사용자에 대한 인증 여부를 해당 클라이언트로부터 전송되어온 시퀀스 번호(Server_Client_Seq)를 이용하여 정상적인 복호화 여부로 결정하게 된다.

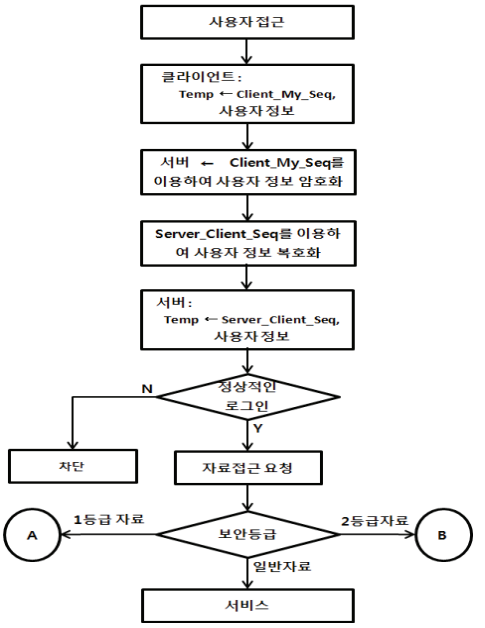

그림 2. 일반적인 세션 정보 암호화 및 자료 처리 과정
Figure 2. General Session Data Encryption and Data Processing

복호화된 사용자 정보는 시퀀스 번호와 함께 서버의 암호화 버퍼에 저장한다. 그 다음 재 설정요구가 발생하면 서버는 자신의 버퍼에 저장된 시퀀

스 번호를 이용하여 사용자 정보와 서비스 정보를 클라이언트에 전송하고, 클라이언트는 자신의 버퍼에 저장된 시퀀스 번호를 이용하여 복호화 한 후 초기 사용자 인증 정보에 대한 일치 여부를 판단한다[14][15].

본 논문에서는 일반 자료 접근 요청인 경우에는 RST 신호의 발생과 상관없이 서비스를 수행한다.

<그림 3>은 2등급 자료 요청이 발생한 경우에 2등급 자료의 조합 유무에 따라서 조합이 발생하지 않은 경우에는 별도의 암호화 과정없이 서비스 작업을 수행한다. 만일 조합이 발생한 경우 본 논문에서는 RST 신호 발생 유무에 따라 암호화 강도를 다르게 수행하였다. 먼저 RST 신호가 발생하지 않은 경우에는 해당 서비스 자료에 대한 암호화 과정을 수행하였다. 그 다음 RST 신호가 발생한 경우의 서비스에는 해당 사용자 정보와 서비스 자료를 모두 암호화 하여 클라이언트로 서비스 하도록 하였다.

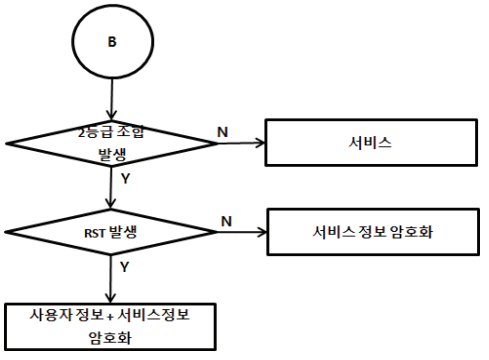

그림 3. 2등급 자료 처리 및 서비스 과정
Figure 3. Processing and Service of Level 2 Data

<그림 4>는 1등급 자료 요청이 발생한 경우 2등급 자료 처리와 동일한 과정을 수행하도록 하였다. 먼저 RST 신호가 발생하지 않은 경우에는 서비스 정보에 대한 암호화 과정을 수행하고, RST 신호가 발생한 경우에는 사용자 정보와 서비스 정보를 모두 암호화하여 클라이언트로 전송하도록 하였다.

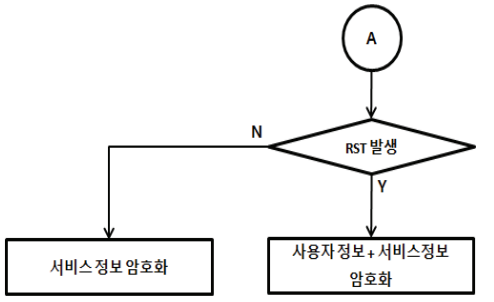

그림 4. 1등급 자료 전달 과정
Figure 4. Transfer of Level 1 Data

<그림 5>는 클라이언트가 서버로부터 수신한 암호문으로부터 사용자 정보를 추출한 후 <그림 1>의 Temp에서 보관하고 있던 정보를 이용하여 수신한 정보를 복호화 시키는 과정을 보이고 있다.

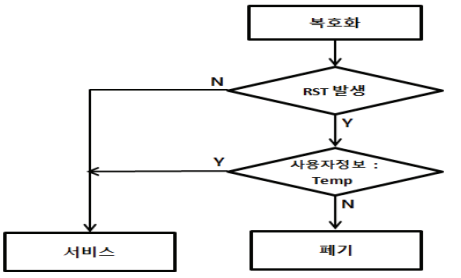

그림 5. 클라이언트에서 복호화 과정
Figure 5. Decryption Process in Client

4. 시뮬레이션 및 결과

본 논문은 다음과 같은 실험 과정을 거쳤다. 먼저 네트워크 환경에서 NIC(Network Interface Card) 정보 확인과 선택에 필요한 패킷 수집을 위하여 와이어샤크 프로그램을 사용하였다. 시뮬레이션을 위한 운영체제는 Windows 7이고, 시스템 사양은 8G 메모리를 채택한 Xeon E5506 2.13 Ghz Dual System으로 구성된 3대의 컴퓨터를 사용하였다.

본 논문의 시뮬레이션 수행을 위하여 <그림 6>에서 정상적인 서버(192.168.0.3)와 클라이언트

(192.168.0.2)의 연결 상태와 'LEN' 항목의 패킷 크기를 와이어 샤크를 통하여 보여주고 있다.

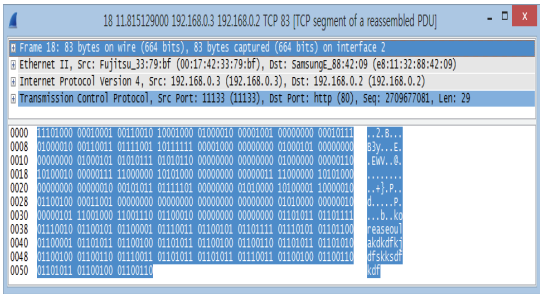

그림 6. 정상적인 연결
Figure 6. Normal Connection

<그림 7>은 서버(192.168.0.3)와 클라이언트(192.168.0.2)의 정상적인 접속 과정에서 공격자(192.168.0.4)가 RST 신호를 서버로 발생시키는 과정을 보이고 있다.

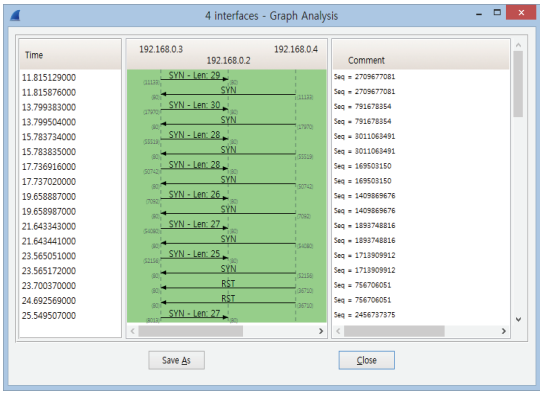

그림 7. RST 신호 발생
Figure 7. RST Signal Generation

<그림 8>은 RST 상태가 발생한 경우 정상적인 연결 상태의 'Len' 항목의 패킷에 대하여 그 크기가 '0'으로 되어 있는 것을 알 수 있다. 본 논문에서는 이를 이용하여 RST 발생 여부를 탐지하도록 하였다.

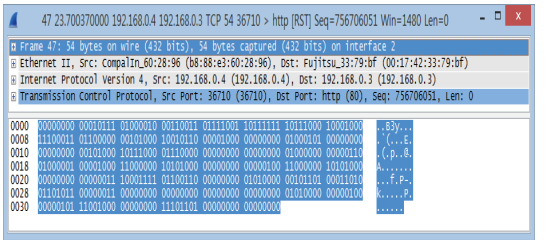

그림 8. RST 신호 발생
Figure 8. RST Signal Generation

<그림 9>는 클라이언트에서 사용자 정보를 암호화 한 후 서버로 전송하여 정상적인 사용자 여부에 대한 인증과정을 보이는 것이다.

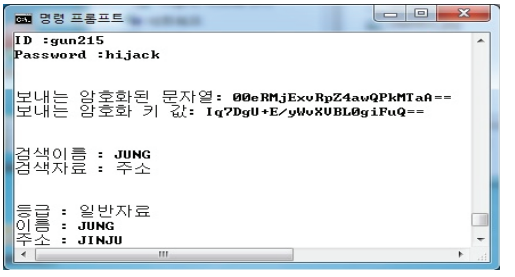

그림 9. 클라이언트에서 사용자 정보 암호화 및 일반자료 처리 과정
Figure 9. Process of User Data Encryption and General Data Processing

<그림 10>에서는 암호화된 사용자 정보를 클라이언트에서 서버로 전송하는 과정을 와이어샤크를 이용하여 나타내고 있다.

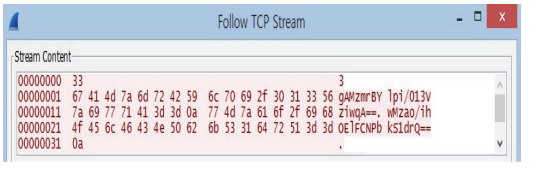

그림 10. 전송중인 암호화된 사용자 정보
Figure 10. Encrypted User Data being Transferred

<그림 11>은 2등급 자료 요청에 대하여 자료의 조합은 발생하였지만 RST 신호가 발생하지 않

은 경우 서버에서 해당 자료의 암호화 과정을 수행하는 과정을 보이고 있다.

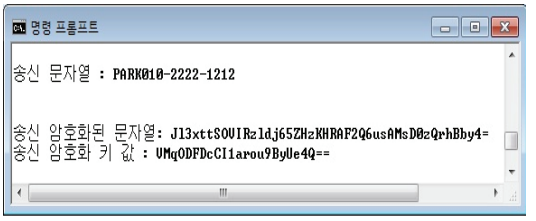

그림 11. RST 신호 발생이 없는 2등급 자료 암호화 과정
Figure 11. Encryption Process of Level 2 Data Without RST Signal Generation

<그림 12>는 <그림 11>의 암호문을 클라이언트에서 복호화 과정을 수행한 후 그 결과를 보여주고 있다.

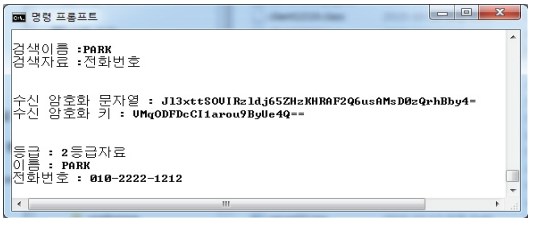

그림 12. RST 신호 발생이 없는 2등급 자료 복호화 과정
Figure 12. Decryption Process of Level 2 data without RST Signal Generation

<그림 13>은 2등급 자료이고, 자료 조합과 RST 신호가 함께 발생한 경우 그 처리 과정을 보이는 것이다. 본 논문에서는 1등급 자료 요청시 RST 신호가 발생하면 동일한 수행 과정을 거치도록 하였다.

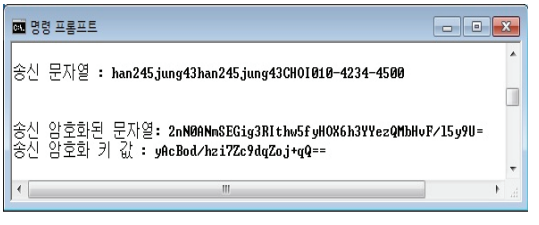

그림 13. RST 신호 발생이 있는 2등급 자료 암호화 과정
Figure 13. Encryption Process of Level 2 Data with RST Signal Generation

<그림 14>은 <그림 13>에서 전송된 자료를 복호화 결과 사용자 정보인 ID와 패스워드, 서비스 자료가 모두 정상적으로 전달된 결과를 보이는 것이다.

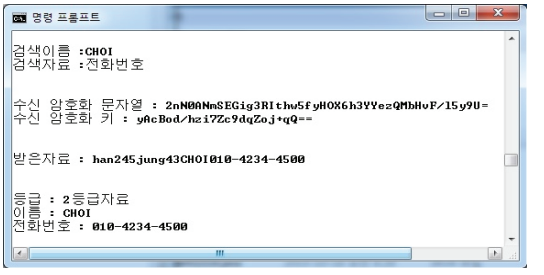

그림 14. 서버에서 사용자정보에 서비스정보를 합하여 암호화
Figure 14. Encryption by Adding Service Data to User Data on the Server

5. 결 론

오늘날 발전하고 네트워크 기술은 클라우드 컴퓨팅 및 사물인터넷 환경으로 빠르게 진화하고 있다. 그렇지만 이렇게 다양한 네트워크 환경은 그 연결 설정에 TCP-3Way 핸드셰이킹 과정을 기반으로 하고 있다. 이러한 연결 설정 과정은 연결에 필요한 세션 정보를 하이재킹 하여 불법적으로 정보를 탈취해가는 공격자들로 인해 날로 그 위협이 증대되고 있는 상황이다. 본 논문에서 제안하고 있는 보안 모델은 이러한 세션하이재킹 공격을 통한 불법적인 자료 접근에 대하여 서비스 자료의 등급별 암호화를 통하여 각 서비스에 대하여 안정적이고 가용성을 향상시킨 보안 모델이라고 할 수 있다. 아울러 기존의 단일 서비스시스템이 아닌 클라우드 컴퓨팅 환경에서 능동적이고 상호 협력적인 보안 모델 구축에 많은 참고가 될 수 있는 모델이라고 할 수 있다. 향후 연구과제로는 해당 모델을 적용함으로써 발생 가능한 통신상의 지연문제를 해결하여 전체 서비스 기능과 보안성을 모두 만족할 수 있는 시스템 개발이 우선과제라고 할 수 있다.

References

[1] J. H. Ra, and J. S. Lee, *A study on the security requirement for transforming cloud data center : Focusing on N - data center, Journal of Digital Convergence*, Vol. 12, No. 11, pp. 299-307, 2014.

[2] J. K. Park, *A study on measures to active cultural contents service in big data age*, Journal of the Korean Society of Design Culture Vol. 20, No. 1, pp. 324～334, 2014.

[3] J. K. Park, *A study on measures to active cultural contents service in big data age,* Vol. 20, No. 1, pp. 324-334, Mar. 2014.

[4] Y. Y. Mu, H. C. Baek, J. Y. Choi, W. C. Jeong, and S. B. Kim, *A proposal of a defense model for the abnormal data collection using trace back information in big data environments*, Journal of The Korea Knowledge Information Technology Systems. Vol. 10, No. 2. pp. 753-162, 2015.

[5] D. H. Lee. J. C. Park, C. G. Yu, and H. S. Yun, *On the design of a big data based real-time network traffic analysis platform*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 4, pp. 721-728, August. 2013.

[6] N. Nishanth, J. Zareena, and S. S. Babu, *Pseudo random alteration of sequence numbers (PRAS): A novel method for defending sessiion hijacking attack in mobile adhoc network,* Communication Technology, 2013 15th IEEE International Conference on. IEEE, pp. 20-25, 2013.

[7] J. Y. Choi, H. C. Baek, S. B. Kim, J. C. Sim, and J. H. Park, *Encryption of TCP sequence numbers for session hijacking attacks*, Journal of The Korea Knowledge Information Technology Systems. Vol. 9, No. 6. pp. 707-714, 2014.

[8] P. H. Jo, J. I. Lim, and H. K. Kim, *A study on the improvement of security vulnerabilities in intelligent transport systems*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 3, pp. 531-543, 2013.

[9] J. W. Seo, and S. J. Lee, *A study on the detection of DDoS attack using the IP Spoofing*, Journal of the Korea Institute of Information Security & Cryptology. Vol. 25, No. 1. pp. 147-153, 2015.

[10] S. H. Park, and H. S. Yang, *A study on the method of existing system migration for cloud computing*, Journal of Digital Convergence, Vol. 12, No. 10, pp. 271-282, 2014.

[11] C. H. An, H. C. Baek, J. H. Park, and S. B. Kim, *A cloud-based security model designed to prepare deployment nationwide the regional public hospitals telemedicine clusters*, Journal of Knowledge Information Technology and Systems. Vol. 11, No. 5. pp. 489-497, 2016.

[12] J.-H. Jeon, *A study on the vulnerability of the Cloud computing security*, Journal of The Kore a Institute of Information Security & Cryptolog y, Vol. 23, No. 6, pp. 1239-1246, Dec. 2013.

[13] S.-J. Jung, K.-Sung, and Y.-M. Bae, *Comparison and analysis of resource usage for open source server virtualization techniques,* Journal of The Korea Knowledge Information Technology Society, Vol. 27, No. 2, pp. 43-44, April 2011.

[14] D.-S. Choi, D.-H. Oh, J.-S. Park, and J.-C. Ha, *An improved round reduction attack on triple DES using fault injection in loop*

statement, Journal of The Korea Institute of Information Security & Crypto logy, Vol. 22, No. 4. pp 709-717, 2012.

[15] K. H. Song, H. C. Kang, and J. C. Sung, *An efficient new format-preserving encryption algorithm to encrypt the personal information*, Journal of The Korea Institute of Information Security & Crypto logy, Vol. 24, No. 4. pp. 753-763, 2014.

빅데이터 서비스 환경에서 세션하이재킹 공격에 대한 안정적 서비스 제공 모델

최재영[1], 박재홍[1], 서영건[1], 홍석원[2], 김상복[1]

[1]*경상대학교 컴퓨터과학과*

[2]*경남도립거창대학 교무부 정보지원팀*

요 약

오늘날 정보의 대량 생산과 수집이 이루어지는 빅데이터 환경은 클라우드 컴퓨팅 환경을 기반 기술로 운영하고 있다. 아울러 빅 데이터를 이용한 새로운 정보 환경은 우리 사회에 다양한 정보 서비스 기술 분야의 발전을 이끌고 있다. 그렇지만 이러한 네트워크 환경은 정상적인 사용자의 연결 세션을 탈취한 후 이를 이용하여 공격을 시도하는 세션하이재킹 공격에 취약점을 드러낼 수 있다. 본 연구는 다양한 네트워크 서비스를 실시하는 클라우드 컴퓨팅 환경에서 세션하이재킹 공격 발생시 안정적인 서비스와 민감한 정보를 등급별로 분류하고 암호화를 통한 서비스 제공을 할 수 있도록 하였다. 이를 위하여 세션 단절 정보와 접근 자료에 대한 가치 정도를 분류하고 조합하여 등급별로 암호화 비트 패턴을 생성 하였다. 그 다음 공격 발생 시점의 자료 요청에 대한 서비스 등급을 분석하여 즉각적인 서비스 대신 생성한 암호화 비트 패턴을 이용하여 암호화 과정을 거친 후 전송하도록 하였다. 그러므로 본 논문은 기존의 네트워크 상황에서 발생할 수 있는 불법적인 접근에 대하여 서비스의 안정성과 가용성을 향상시킬 수 있는 보안 모델이라고 할 수 있다.

Jae Yeong Choi received the Master´s degree in the Department of Computer Science from Gyeongsang National University in 2014. His current research interests include network architecture, network security.

E-mail address: jyoungc67@naver.com

Jae Heung Park received the Ph.D. degree in the Department of Computer Engineering from Chung-ang University in 1989. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1983. He has been a researcher in the Software Engineering Research Institute at The Gyeongsang National University since 1984. His current research interests include computer network and security, S/W Reliability. He is a member of the KKITS.

E-mail address: pjh@gnu.ac.kr

Yeong Geon Seo received the B.S. degree from computational statistics of Gyeongsang national univ.(GNU) and, M.S. and Ph.D. degrees from computer science of Soongsil univ. in 1987, 1989 and 1997, respectively. During 1989 - 1992, he worked in Trigem computer inc. developing 4GL(XL/4). And now he has been working for GNU, dept. of computer science and graduate school of CCBM since 1997. His research interests include medical imaging, cultural convergence and computer network.

E-mail address: young@gnu.ac.kr

Suk Won Hong received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2011. His current research interests include network, multimedia.

E-mail address: swhong@gc.ac.kr

Sang Bok Kim received the Ph.D. degree in the Department of Electronics Engineering from Chung-ang University in 1989. He was a director in the Department of Education Information Computer Center at The Gyeongsang National University from 2007 to 2010. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. He has been a researcher in the Computer Data Communication Research Institute at The Gyeongsang National University since 1984. His current research interests include computer network and security, computer system architecture. He is a member of the KKITS.

E-mail address: sbkim@gnu.kr