Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

The Responding Model for Sniffing and Session Hijacking Using Traffic Variation Information and RST Signal Analysis

Jae-Yeong Choi[1], Hyun-Chul Baek[2], Jae-Heung Park[1], Sang-Bok Kim[*1]

[1]*Department of Computer Science, Gyeongsang National University*
[2]*Department of Smart Information Convergence, Gyeongnam Provincial Namhae College*

ABSTRACT

At present, our society requires fast and accurate information in various fields, and shares information collected and processed through various devices existing around us. However, in the process of collecting, establishing and providing this information, the number of cases of illegal access to important information about person, country or company sharply increases. These cases of illegal access cause enormous damage to person, country or company. Illegal access to information may occur diversely, and in case an attack occurs, the situation is that a sniffing attack, which regular users cannot perceive, aggravates material/psychological damage to the corresponding company or person who gets damaged. Besides, with regard to a session hijacking attack making an illegal access attempt to actively steal information after attackers themselves pretending to be true sender/receiver in the process of sniffing, the situation is that damage gets worse. Nowadays, in the environment where each individual person has various devices that enables networking, the number of these attack techniques continue to increase. This paper analyzes whether RST signal is generated, which is needed for session reconnection and traffic information between users so as to make it possible to take countermeasures against sniffing and session hijacking attack. In the process of session hijacking, a regular user session is temporarily interrupted by generating RST signal inevitably. And this paper analyses whether this RST signal is generated. Besides, traffic information is analyzed because, in case a sniffing attack using ARP redirect or ICMP redirect occurs, the previous path changes, which may show deviation from traffic information in the ordinary path. This paper designed a model for countermeasures enabling proper and stable service against sniffing and session hijacking and it was made possible to be applied to the detection of attack that may occur diversely in the future on the basis of these data for analysis.

KEYWORDS: TCP 3-Way, Session Hijacking, Sniffing, ARP Spoofing, ICMP Redirect

ARTICLE INFO: Received 30 April 2017, Revised 29 May 2017, Accepted 9 June 2017.

[*]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

스니핑 공격이란 공격자가 정상적인 송/수신자 사이에서 중계 역할을 하면서 송/수신 정보를 불법적으로 엿볼 수 있는 공격 기법이다. 스니핑 공격은 주로 ARP 스푸핑과 ICMP 리다이렉트 기술을 악용하여 불법적인 정보 접근을 시도한다. 이러한 스니핑 공격은 공격자 자신이 중계역할을 통하여 송/수신 과정상의 정보를 엿보기 때문에 소극적인 공격 기법이라고 할 수 있다. 하지만 스니핑 대상이 되는 시스템은 자신의 시스템이 공격당하고 있다는 것을 인지하지 못하는 경우가 대부분이므로 스푸핑 공격보다 그 심각성을 더할 수 있다. 반면에 스푸핑 공격이나 세션 하이재킹 공격은 공격 대상 시스템의 특정 정보를 자신이 위장하여 직접 불법적인 접근을 시도하기 때문에 적극적인 공격 기법이라고 할 수 있다[1][2].

이와 함께 리다이렉트를 기반으로 하는 스니핑 공격은 해당 공격의 특성상 정상적인 TCP 연결 세션을 강제로 리셋 시킨 후 불법접근을 시도하는 세션 하이재킹 공격으로 전환할 가능성이 매우 크다. 즉, 기존의 공격 대응 시스템들은 일반적으로 각 공격 유형에 대하여 단일화 되어있는 대응 과정을 독립적으로 수행하고 있다. 그러므로 본 논문에서는 이러한 리다이렉트 공격과 세션하이재킹 공격에 대하여 이상 트래픽 발생을 탐지한 후 각각의 공격 유형에 동시에 대응할 수 있는 모델을 제안하였다[3-5].

2. 관련연구

2.1 ARP 스푸핑 공격

ARP 스푸핑 공격은 공격자가 동일한 네트워크 상에 존재하는 공격 대상 시스템의 MAC 주소를 변조한 후 공격대상 시스템의 송/수신 패킷이 정상적인 송/수신 경로대신 공격자 자신의 시스템을 경유하도록 하는 스니핑 공격을 위한 사전 작업이라고 할 수 있다[6].

2.2 ICMP 리다이렉트 공격

네트워크 통신에 있어 송신자로부터 수신자까지 송/수신 경로 설정은 최소비용의 원칙에 따라 다수의 라우터를 경유하는 최적의 경로 설정이 이루어진다. 이러한 특성으로 인하여 ICMP 리다이렉트는 송신자로부터 최종 수신자까지 정상적인 라우팅 경로에 문제가 발생할 경우 최적의 경로를 다시 설정해 주는 과정이라고 할 수 있다.

ARP 스푸핑은 동일한 네트워크 상에 존재하는 시스템에 대하여 MAC 정보를 이용하여 스니핑을 시도하는 공격 기법이다. 이에 반해 ICMP 리다이렉트 공격은 공격자가 특정 송신자와 수신자의 송/수신 과정에 필요한 라우터들의 정보를 이용하여 리다이렉트를 시도한 후 공격자 자신이 송/수신자의 라우팅 과정에 개입을 하는 것이다. 즉, 공격자 자신의 시스템이 특정 송/수신자의 네트워크 경로상에 존재하는 정상적인 라우터로 위장을 한 다음 송/수신 정보를 스니핑 할 수 있는 공격 기법이다. 이렇게 ICMP 리다이렉트를 통하여 경로의 재설정이 이루어지면 기존 정상적인 경로상의 트래픽 정보와는 상이한 트래픽 상태를 나타내게 된다. 그러므로 본 논문에서는 이러한 트래픽 변이 정보를 비교 분석하여 정상적인 접속자 여부를 탐지할 수 있도록 하였다[7][8].

2.3 세션 하이재킹 공격

네트워크 연결을 위하여 정상적인 송/수신자들은 3회의 ACK 신호 교환을 하는 TC P-3Way 핸드셰

이킹 과정을 수행한 후 정보를 송/수신 한다. 이렇게 연결 설정이 완료되면 정보의 송/수신 작업이 수행 가능하지만, 통신 과정에서 예기치 못한 이유로 인하여 연결에 대한 세션의 재설정 과정이 필요할 경우가 있다. 이때 사용하는 것이 RST 신호인데, 세션 하이재킹(Session Hijacking) 공격은 정상적인 접속자들의 세션 재연결 과정에 필요한 RST 신호를 공격자가 강제로 발생시키는 것이다. 공격자는 강제로 RS T 신호를 발생시켜 정상적인 세션 연결을 단절시키고, 이 과정에서 획득한 정상적인 세션 연결 정보를 이용하여 공격자 자신이 위장을 한다[9-11].

이러한 공격 기법은 오늘날 클라우드 컴퓨팅 환경에서 실시간 서비스를 기반으로 하는 서버들을 집중 공격 대상으로 다발적으로 발생할 가능성이 있다[12-14].

본 논문은 이러한 연결 재설정 과정에 공격자가 발생시키는 트래픽과 RST 신호의 발생 유,무를 분석하여 적절한 대응 과정을 수행하도록 하고 있다.

3. 제안 모델 동작과정

본 논문은 스니핑 공격 과정에서 발생할 수 있는 트래픽 변이를 탐지하여 스니핑 공격을 분석한다. 이와 함께 공격자가 스니핑 과정에서 탐지해낸 송/수신자간 TCP-3Way 연결 정보를 이용하여 세션 하이재킹 공격을 할 경우 이를 실시간 탐지를 한 후 즉각적인 대응을 할 수 있도록 하였다.

동일 LAN 상에서는 주로 ARP 스푸핑을 이용하여 스니핑 공격을 시도한다. 반면에 ICMP 리다이렉트 공격은 일반적으로 외부망의 라우터를 이용하여 스니핑 공격을 시도하는 경우라고 할 수 있다.

고도의 공격 기술을 보유한 공격자는 외부망에 존재하는 라우터를 이용한 리다이렉트를 시도하여 보다 많은 정보에 대한 불법적인 접근을 시도 할 수 있다.

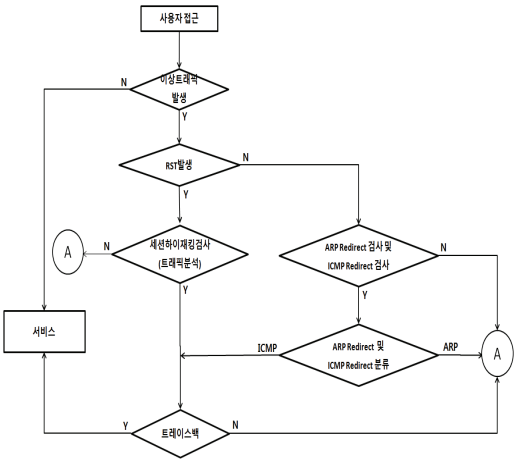

그림 1. 제안 모델의 접근처리 과정-1
Figure 1. Accessing Process in the Proposed Model-1

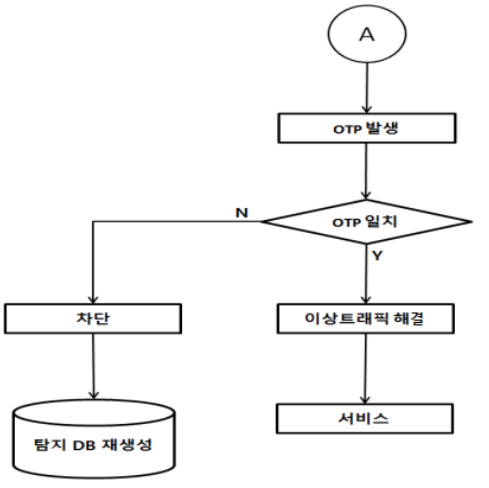

그림 2. 제안 모델의 접근처리 과정-2
Figure 2. Accessing Process in the Proposed Model-2

본 논문에서는 ARP 스푸핑에 대한 실험 과정은 동일 LAN 상에서 수행하였다. 아울러 I CMP 리다이렉트 관련 실험은 외부망의 라우터를 경유하는 실험 과정을 수행하여 정상적인 경로 상태의 트래픽과 비교 분석하였다. 본 논문에서는 이러한 실험 과정을 거친 후 모든 수행 과정을 <그림 1>, <그림 2>로 도식화 하였다. 아울러 이러한 수행

과정을 위하여 정상적인 연결 상태의 인증 정보와 트래픽 정보를 탐지 데이터베이스에 등록 해 두었다. 그러므로 본 논문에서는 스니핑을 통하여 인증 과정을 통과하더라도 트래픽 상태의 변이를 비교 분석하여 실시간 대응 과정을 수행할 수 있도록 하였다.

다음은 <그림 1>, <그림 2>에 대한 수행 과정을 나타낸 것이다.

1. 사용자 접근이 발생하면 해당 접속자 사이에 발생하는 트래픽 분석 작업을 수행한다.
2. 이상트래픽을 보이는 접속자에 대한 탐지과정을 수행한다.
   2-1. 트래픽 분석 결과가 정상적이면 10번의 서비스 과정을 수행한다.
   2-2. 트래픽 분석 결과가 비정상적이면 세션하이재킹 공격 탐지를 위하여 3번 과정을 수행한다.
3. RST 발생에 대한 탐지 과정을 수행한다.
   3-1. RST 신호 발생이 없으면 4번 과정을 수행한다.
   3-2. RST 신호를 탐지할 경우 6번 과정을 수행한다.
4. ARP Redirect, ICMP Redirect 공격 여부에 대한 탐지 과정을 수행한다.
   4-1. ARP Redirect, ICMP Redirect 공격으로 판단되면 5번 과정을 수행한다.
   4-2. ARP Redirect, ICMP Redirect 공격으로 인한 이상트래픽이 아니므로 7번 과정을 수행한다.
5. ARP Redirect, ICMP Redirect 공격에 대한 분류 과정을 수행한다.
   5-1. ICMP Redirect 공격으로 판단되면 6번 과정을 수행한다.
   5-2. ARP Redirect 공격으로 판단되면 7번 과정을 수행한다.
6. 세션하이재킹 공격과 ICMP Redirect 공격에 대한 최종 확인을 위하여 트레이스백 정보 분석 과정을 수행한다[15].
   6-1. 트레이스백 정보가 일치하지 않으면 8번 과정을 수행한다.
   6-2. 트레이스백 정보가 일치하면 10번 과정을 수행한다.
7. 정상 사용자 유, 무를 검증하기 위하여 OT P를 해당 접속자에게 전송한다.
8. OTP 인증 과정을 수행한다.
   8-1. OTP 인증이 정상적이지 못하면 9번 과정을 수행한다.
   8-2. OTP 인증을 정상적으로 완료하면 이상 트래픽을 해결한 후 10번 과정을 수행한다.
9. 불법적인 접속자로 판단하여 즉각 차단 작업을 수행하고 해당 접근 정보를 향후 불법적인 재접속 정보로 활용하기 위하여 탐지 DB에 등록해 둔다.
10. 모든 분석 과정을 통하여 정상적인 접속자로 인증되면 서비스를 실시한다.

4. 시뮬레이션 및 결과

본 논문의 실험을 위한 운영체제로는 Windows 7을 사용하였으며, 시스템 사양은 8G 메모리를 채택한 Xeon E5506 2.13 Ghz Dual System으로 구성된 3대의 컴퓨터를 LAN으로 연결하였다. 그 다음 내부 공격자를 Attacker 1, 외부 공격자를 Attacker 2로 설정하여 다음과 같은 실험 과정을 거쳤다. 먼저 스니핑을 위한 ARP Redirect, ICMP Redirect 공격이 발생할 경우 이들에 대한 트래픽 변이를 분석할 수 있도록 <그림 3>과 같이 네트워크를 구성하여 트래픽을 측정 분석하였다.

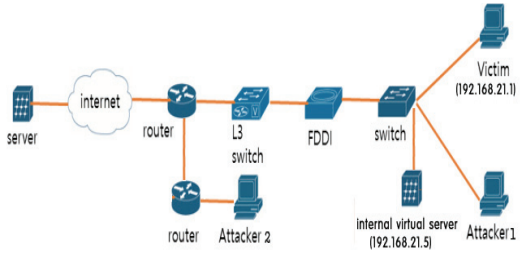

그림 3. 트래픽 실험을 위한 네트워크 구성도
Figure 3. Network Diagram for Traffic Test

<그림 3>의 네트워크 과정에서 발생하는 NIC(Network Interface Card)정보 확인과 패킷 분석을 위하여 와이어샤크 프로그램을 사용하여 'RST' 신호를 분석하였다.

<그림 5>, <그림 6>, <그림 7>은 <그림 3>의 네트워크 구성을 이용하여 트래픽 변이를 분석한 결과이다.

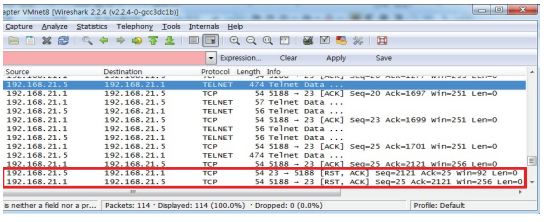

그림 4. RST 신호 탐지 결과
Figure 4. RST Signal Detection Result

<그림 4>는 가상서버(192.168.21.5)와 클라이언트(Victim ; 192.168.21.1)의 정상적인 접속과정에서 발생하는 트래픽을 와이어 샤크를 이용하여 나타낸 결과이다. 이는 세션하이재킹 공격에서 필연적으로 발생하는 'RST' 신호를 탐지한 후 이에 대한 적절한 대응을 하기 위하여 필요한 과정이라고 할 수 있다. <그림 4>를 보면 'RST' 신호가 발생할 경우 'LEN' 항목의 패킷 크기가 ' 0 '으로 나타나는 것을 볼 수 있다.

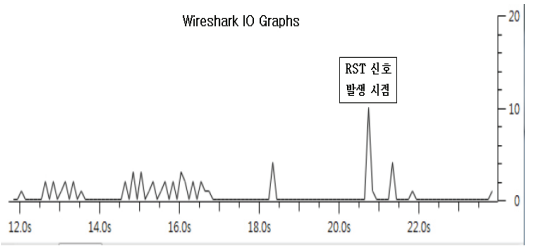

그림 5. RST 발생 후 트래픽 변이 상태
Figure 5. Traffic Variation Status After RST Occurs

<그림 5>에서는 약 20초 지점에서 세션 하이재킹 공격을 위한 'RST' 신호가 발생하여 이후 트래픽의 변이 상태를 나타내는 것이다. 본 논문에서는 이를 이용하여 'RST' 신호가 탐지되면 세션하이재킹 공격에 대한 대응을 하기 위하여 트래픽 분석 작업을 수행한다.

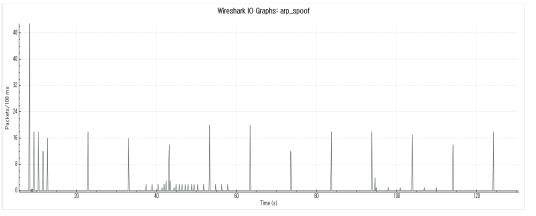

그림 6. ARP Spoofing 공격 후 트래픽 변이 상태
Figure 6. Traffic Variation Status after ARP Spoofing Attack

<그림 6>은 공격자가 ARP Spoofing 공격을 시도한 후 스니핑 과정에서 발생하는 트래픽 변이 상태를 나타내는 것이다. 공격자의 ARP 스푸핑 공격이 성공할 경우 정상적인 송/수신자의 정보는 공격자 시스템을 경유하기 때문에 <그림 6>과 같은 트래픽의 변이를 일으키게 된다.

<그림 7>은 공격자가 ICMP Redirect 공격을 시도하여 스니핑 과정에서 발생하는 트래픽 변이 상태를 나타내는 것이다. ICMP Redirect 공격은 일반적으로 라우터를 공격하기 때문에 ARP 스푸핑에 의한 트래픽 변이와는 또 다른 트래픽 변이 상태를 나타내게 된다. 이상의 시뮬레이션 과정은 다음

두 가지 경우를 고려하였다. 먼저 이미 스니핑을 성공한 공격자가 인증 정보를 이용하여 적극적인 세션 하이재킹 공격을 시도할 경우에 대비하여 이를 우선 분석하고 대응 과정을 수행하도록 하였다. 그리고 나머지 경우는 공격자가 적극적인 세션 하이재킹 공격을 하기 위해 스니핑을 시도할 경우 트래픽 변이 정보를 이용하여 분석할 수 있도록 하였다. 즉 공격자는 적극적인 세션 하이재킹 공격을 하기위해 사전 스니핑을 시도할 수 있기 때문이다.

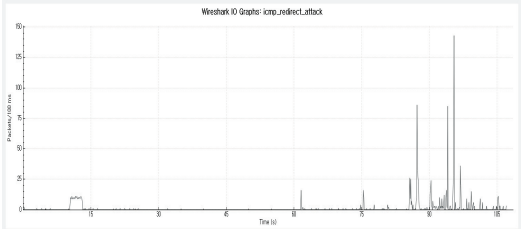

그림 7. ICMP Redirect 공격 후 트래픽 변이 상태
Figure 7. Traffic Variation Status after ICMP Redirect Attack

5. 결 론

오늘날 네트워크 기술은 클라우드 컴퓨팅 및 사물인터넷 환경으로 빠르게 진화하고 있다. 하지만 이렇게 다양한 디바이스들을 통한 네트워킹 환경은 다양한 공격자들의 집중 표적이 되고 있다. 그리고 기존의 대응 모델들은 다양한 공격 기법에 대하여 일반적으로 독립적인 대응 과정을 수행한다. 하지만 공격자들이 복합적인 공격을 시도할 경우 실시간 대응의 어려움을 초래하게 된다. 본 논문은 이러한 복합적인 공격발생시 그 대응 방안을 제시한 것이다. 특히 스니핑을 통한 불법적인 공격은 표적이 되고 있는 피해자 자신이 오랜 기간 동안 자신의 소중한 정보 자산이 빠져나가는 것을 알 수 없기 때문에 그 심각성을 더한다고 할 수 있다. 아울러 이러한 스니핑 기법은 공격 과정에서 탈취한 정보를 이용하여 세션하이재킹 공격으로 전환할 가능성이 아주 높다. 본 논문에서 제안하고 있는 보안 모델은 스니핑 공격과 세션하이재킹 공격을 통한 불법적인 자료 접근에 대하여 트래픽 변이 정보와 'RST' 신호의 발생 여부를 이용하여 해당 공격들을 실시간으로 동시에 탐지할 수 있도록 한 것이다. 또한 클라우드 컴퓨팅, 사물인터넷 환경에서 경유하게 되는 미들웨어의 보안에도 적용가능하다고 본다. 향후 연구과제로는 해당 모델을 적용함으로써 발생할 수 있는 연결 서비스에 대한 가용성을 향상시켜야 한다고 본다. 이를 위하여 암호화 과정을 통하여 연결의 단절 보다 정보 서비스에 대한 가치를 높일 수 있는 방안이 함께 연구되어야 할 것이다.

References

[1] C. W. Yang, and A. R. Khil, *A secure routing protocol against sniffing attacks in grid sensor networks,* Journal of Computing Science and Engineering, Vol. 38, No. 2, pp. 108-116, 2011.

[2] Y. J. Ma, H. C. Baek, C. G. Kim, and S. B. Kim, *Prevention of DDoS attacks for enterprise network based on traceback and network traffic analysis,* International Journal of Maritime Information and Communication Sciences, Vol. 7, No. 2, pp. 157-163, 2009.

[3] J. Y. Choi, J. H. Park, Y. G. Seo, S. W. Hong, and S. B. Kim, *A reliable service provided model for session hijacking attacks in big data service environments*, Journal of The Korea Knowledge Information Technology Systems. Vol. 11, No. 6, pp. 597-606, 2016.

[4] S. H. Yoon, H. M. An, and M. S. Kim, *Study on classification scheme for multilateral*

and hierarchical traffic identification, Journal of information processing systems, Vol. 3, No. 2, pp. 47-56, 2014.

[5] K. H. Son, T. J. Lee, and D. H. Woo, *Design for zombie PCs and APT attack detection based on traffic analysis*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 24, No. 3, pp. 491-498, 2014.

[6] C. R. Seo, and K. H. Lee, *ARP spoofing attack scenarios and countermeasures using CoAP in IoT environment,* Journal of the Korea Convergence Society, Vol. 7, No. 4, pp. 39-44, 2016

[7] B. H. Kim, *Analysis of IP marking for tracing to origin of attack* , Journal of Industrial science researches, Vol. 28, No. 2, pp. 207-212, 2011.

[8] S. W. Seo, *A study on stabilizing a network security zone based on the application of logical area to communication bandwidth*, Journal of the Korea Academia-Industrial, Vol. 16, No. 5, pp. 3462-3468, 2015.

[9] 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.

[10] 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.

[11] 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.

[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, Apr. 2011.

[14] 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.

[15] H. C. Baek, S. B. Kim, and C. G. Kim, *A design of remote access false-positive rate improvement modelusing trace route information and access statistics information*, Journal of The Korea Knowledge Information Technology Systems, Vol. 6, No. 4, pp. 1-7, 2011.

트래픽 변이정보와 RST 신호분석을 이용한 스니핑 및 세션하이재킹 대응 모델

최재영[1], 백현철[2], 박재홍[1], 김상복[1]

[1]*경상대학교 컴퓨터과학과*

[2]*경남도립남해대학 스마트융합정보과*

요 약

현재 우리 사회는 여러 분야에 있어 빠르고 정확한 정보 요구를 하고 있으며, 주위에 존재하는 여러 디바이스들을 통하여 수집, 가공된 정보를 공유하고 있다. 아울러 정보를 수집하고 구축, 제공하는 과정에 개인

이나 국가 또는 기업의 중요 정보에 대한 불법적인 접근 사례 또한 빠르게 증가하고 있다. 이러한 불법적인 접근 사례는 개인이나 국가, 기업에 막대한 손실과 정신적 피해를 배가시키고 있는 실정이다. 정보에 대한 불법적인 접근은 다양하게 발생할 수 있는데, 그 중 공격이 발생할 경우 송/수신자가 인지할 수 없는 스니핑 공격과 공격자 자신이 정상적인 송/수신자로 위장을 하는 세션하이재킹 공격이 있다. 오늘날 각 개인이 네트워킹이 가능한 다양한 디바이스를 보유하고 있는 환경에서는 이러한 공격 기법은 꾸준히 증가하고 있다. 본 논문은 이러한 공격에 대응할 수 있도록 사용자 간의 트래픽 정보와 세션 재연결에 필요한 RST 신호 발생 여부를 분석한다. 즉, 세션하이재킹 과정에는 반드시 RST 신호를 발생시켜 정상적인 사용자 세션을 일시적으로 단절시키게 되는데 해당 정보의 발생여부를 분석한다. 또한 트래픽 정보 분석은 ARP 리다이렉트나 ICMP 리다이렉트를 이용한 스니핑 공격이 발생할 경우 기존 연결 경로가 바뀌게 되고, 이는 정상적인 경로상의 트래픽 정보와 편차를 나타낼 수 있기 때문이다. 본 논문은 이러한 분석 자료를 기반으로 스니핑 공격에 적절하고 안정적인 서비스가 가능한 대응모델을 설계하여, 향후 다양하게 발생할 수 있는 스니핑 공격 탐지에 응용할 수 있도록 하였다.

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

Hyun Chul Baek received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2003. He was a chairman in the Committee of Computer System technology at The Korea Association of Regional Public Hospital in 2007. He has been a professor in the Department of Smart Information Convergence, Gyeongnam Provincial Namhae College since 2013. His current research interests include network, network security, encryption, bigdata security, cloud computing. He is a member of the KKITS.

E-mail address: dosi_gas@lycos.co.kr

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

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