Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

User Authentication Service Model Using Euclidean Distance Baesd on Encryption

Yang Liu[1], Hyun Chul Baek[2], Suk-Won Hong[3], 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*

[3]*Division of Academic Affairs, Gyeongnam Provincial Geochang College*

ABSTRACT

Nowadays, network technology is changing rapidly in the environment of cloud computing and Internet of Things, but there are still many difficulties in providing dynamic correspondence and efficient services when illegal attacks occur. In particular, attackers with high-end attack techniques will try to use the IP spoofing attack. For IP spoofing attacks, it is based on the connection path of the client to detect and correspond. This is based on traceback, after the normal path information is generated, the client connection information is compared and analyzed. But the benchmark detection method in the process of connection intelligence analysis will make OTP (One Time Password) occur frequently, resulting in low service availability. In order to improve this problem, this paper takes traceback information , and uses the Euclidean law calculation method (Euclidean Distance) and the security model put forward by phases of encryption method. Based on this, abnormal path intelligence in the simple comparison process, the different path information of block first policy can complement. After analyzing the changing path information, also implement phases of encryption. Then, the process of decryption is used to certify whether service is needed.

KEYWORDS: Big data, Cloud computing, Euclidean distance, Encryption, Traceback

ARTICLE INFO: Received 5 October 2018, Revised 13 November 2018, Accepted 7 December 2018.

[*]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 네트워크 서비스는 빅데이터 서비스를 위한 클라우드 환경 구축을 요구하고 있으며, 이는 공격자들의 집중적인 공격 대상이 되고 있다. 특히 IP(Internet Protocol) 스푸핑 공격(IP Spoofing Attacks)은 송신자와 수신자의 상호 인증 정보인 IP 주소를 속여 불법적인 접근을 시도하는 공격 기법이다.[1] 즉, 보안 시스템이 집중되어 있는 환경으로 직접적인 공격이 어려울 경우 해당 시스템에서 신뢰하고 있는 호스트의 IP 정보를 이용하여 목표 시스템을 공격하는 것이다. 이러한 IP 스푸핑 공격은 상호 신뢰 관계를 유지하는 호스트 정보를 이용하여 인증 과정을 수행하기 때문에 클라우드 기반의 빅데이터 서비스 환경에서는 그 공격 빈도수가 더욱 증가할 수 있다.

IP 스푸핑 공격에 대한 기존 탐지 방식에는 트레이스 백 정보를 비교하여 정상적인 접근 여부를 판정하는 방식이 있다[2][3]. 그렇지만 트레이스 백 정보를 단순 비교하는 방식은 정상적인 사용자를 공격자로 판정하는 오류를 발생시킬 수 있다. 그리고 공격 분석에 필요한 경유 라우터들의 IP 정보를 모두 비교하기 때문에 이에 대한 오버헤드를 초래할 수 있다. 아울러 경로 정보가 상이할 때 마다 OTP(One Time Password)를 통한 빈번한 재인증 과정의 수행은 서비스 가용성을 저해할 수 있다. 본 논문은 클라우드 기반의 빅데이터 서비스 환경에서 IP 스푸핑 공격 탐지와 대응, 서비스 가용성을 보장하기 위한 보안 모델을 설계한 것이다. 즉, 상호 신뢰 호스트에 대한 접근성을 향상시키기 위하여 기존의 인증 과정에 필수적인 OTP 대신 단계별 암호화 과정을 수행하도록 하였다. 그리고 수학적 유클리드 거리 계산식을 이용하여 정상적인 경로 상에 존재하는 라우터들의 IP 정보를 각 두 개씩 짝을 지어 거리 좌표로 도출하였다. 그 다음 이들 좌표 값을 기반으로 탐지 및 분석 과정을 개선하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구를 살펴보고, 3장에서 트레이스 백 정보를 이용한 유클리드 거리 좌표 값을 생성한 후 IP변이를 추적하기 위한 제안 모델을 설계하였다. 그 다음 4장에서는 도출한 유클리드 좌표 값을 기반으로 정상적인 사용자 여부에 대한 분석과 암호화 과정을 수행하였다. 마지막 결론에서는 본 논문의 향후 이용 가능성에 대한 언급을 하였다.

2. 관련연구

2.1 클라우드 환경의 개념

클라우드 환경이란 네트워크 기술을 기반으로 서버, 스토리지, 어플리케이션 등 서비스 가능 IT 자원을 필요한 만큼 임대 사용 한 후 해당하는 요금을 지불하는 네트워크 환경을 의미한다[4][5].

그러므로 이러한 클라우드 환경은 기존의 일반적인 네트워크 기반의 서비스 환경보다 더욱 강화된 보안 정책이 필요하며, 불법적인 공격으로부터 중요 정보 자원을 보호할 수 있는 새로운 보안 모델이 요구된다.

2.2 IP 스푸핑

네트워크 기반의 공격 기법에는 다양한 공격이 존재하는데, 특히 IP 스푸핑은 적극적이면서 고도의 해킹 기술을 보유한 전문 해커들이 주로 사용하는 공격 기법이다[6].

네트워크상에 존재하는 호스트들은 접근 과정의 편의성과 스니핑에 의한 접근 정보의 유출을 회피하기 위하여 상호 신뢰하고 있는 시스템의 인증에 IP 주소를 사용한다. IP 스푸핑은 이러한 인증

과정에서 요구되는 특정 시스템의 IP를 보유한 후 이를 이용하여 불법적인 접근을 시도하는 것을 의미한다[7]. <그림 1>은 이러한 공격 과정을 도식화 해 놓은 것이며, 네트워크상에는 동일한 IP가 두 개 이상 존재할 수 없기 때문에 IP를 도용한 시스템을 다운시키기 위하여 필연적으로 서비스 거부 공격 등 자원 고갈 공격 등을 시도한다.

그러므로 클라우드 환경에서는 이러한 IP 스푸핑 공격이 집중적으로 발생할 가능성이 아주 높을 것으로 예측된다.

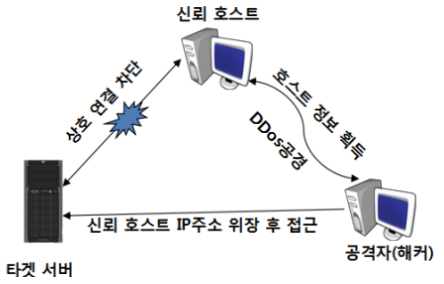

그림 1. IP 스푸핑 과정
Figure 1. A process of IP Spoofing

2.3 트레이스 백 정보의 개념

네트워크상에 존재하는 송신자와 수신자 사이에는 경로 관리를 위한 라우터들이 존재한다. 트레이스 백이란 IP를 추적한 후 송신자와 수신자 사이의 경로 정보를 제공해 주는 프로그램이다[8].

본 논문에서는 상호 신뢰하고 있는 시스템들에 대하여 트레이스 백을 수행한 후, 이 과정에서 생성되는 라우터들의 IP를 기반으로 유클리드 거리 값을 생성하였다. 그리고 이를 통하여 유클리드 거리 값 분포도와 공격 탐지를 위한 임계치를 설정한 후 그 결과에 따라 적절한 대응을 할 수 있도록 하였다.

2.4 유클리드 거리

유클리드 거리 식이란 두 점 사이의 거리를 계산할 때 사용하는 일반적인 방법이다. 즉, 임의의 두 점 p, q에 대응하는 p = (p1, p2,..., pn)와 q = (q1, q2,..., qn)의 유클리드 노름(Norm)을 직교 좌표계로 나타낸 것으로 식 1에 의하여 해당 좌표 값을 도출할 수 있다. 본 논문에서는 트레이스 백을 통하여 획득 가능한 신뢰 시스템들의 경유 라우터들에 대한 IP 주소 값을 두 개의 쌍으로 설정하고, 이를 유클리드 거리 값으로 계산하여 분석 자료로 사용하였다[9][10].

유클리드 거리 좌표 유도식

임의의 두 점 $p=(x_1, y_1), q=(x_2, y_2)$에 대해

$$d_E(p,q) = \sqrt{(x_1-y_1)^2+(x_2-y_2)^2} \quad (1)$$

2.5 암호화

AES(Advanced Encryption Standard)는 대칭키 기법의 미국 연방 표준 알고리즘으로서 20년이 넘게 사용되어 온 DE S를 대신할 차세대 암호화 알고리즘이다. AES는 암호화 복호화 과정에 사용되는 키의 길이에 따라 AES-128, AES-192, AES-256으로 구분하며, 대칭키의 길이와 블록의 크기에 따라 10, 12, 14 Round를 수행한다[11][12][1 3].

3. 제안 모델 동작과정

본 논문에서 제안하는 사용자 인증 과정의 암호화 기반 서비스 모델 수행 과정은 <그림 2>와 같다.

먼저 클라우드를 구성하는 신뢰 호스트에 대한 사용자 접근이 발생하면 클라우드에 속한 호스트들이 상호 공격탐지를 위하여 구축해 놓은 탐지 DB(DataBase)를 참조한다. 그 다음 신뢰호스트에 대한 자원고갈 공격여부를 검사한다. 이 과정에서

자원고갈 공격이 발생하지 않았으면 암호화에 대한 단계별 수행 여부를 검사하고, 자원고갈 공격이 발생했다면 즉시 해당 IP를 차단한다. IP 스푸핑 공격에 있어 공격자는 신뢰 호스트의 IP를 도용하기 때문에 신뢰 호스트를 무력화시키기 위한 자원 고갈 공격을 시도한다. 본 논문에서는 클라우드를 구축하고 있는 각 시스템에 이러한 공격이 발생할 경우, 해당 정보를 클라우드상의 모든 호스트가 상호 공유할 수 있도록 하였다.

암호화 수행 여부 단계는 본 논문에서 OTP 발생 없이 1, 2단계별로 인증 과정을 수행하기 위한 전 단계이다. 암호화 1단계는 접근자의 IP가 기존 정상적인 사용자의 IP와 상이하지만 물리적으로 다른 위치로부터 접근한 경우 그 인증 과정을 수행하기 위함이다. 즉, 사용자 계정을 이용하여 암호화 1단계에 해당하는 키를 생성한 후 정상적인 복호화 여부로 인증 과정을 수행한다. 그 다음 트레이스 백 분석과정에서 해당 경로 정보가 상이하면 유클리드 거리 값 비교 단계로 진행한다.

본 논문에서 유클리드 거리 값 비교 분석을 위한 비정상적인 임계치 범위는 두 가지 상태로 구분하였다. 한 가지 상태는 유클리드 거리 값이 일정 범위를 유지하는 경우이면 2단계 암호화 과정을 수행한다. 아울러 해당 과정에 대한 암호화/복호화 과정을 정상적으로 수행하면 서비스 작업이 가능하도록 하였다. 그 다음 유클리드 거리 값이 일정 범위 이상의 수치를 나타내면 예외 값으로 판단하고 바로 차단하도록 하였다.

1, 2단계 암호화 과정에서 새롭게 인증 과정을 수행한 경로는 탐지 데이터베이스에 정상적인 사용자 경로로 등록한다. 아울러 인증 과정을 정상적으로 수행하지 못한 경로는 공격자 정보로 등록한다.

<그림 3>은 본 논문의 암호화 과정을 나타내고 있으며 그 과정은 다음과 같다.

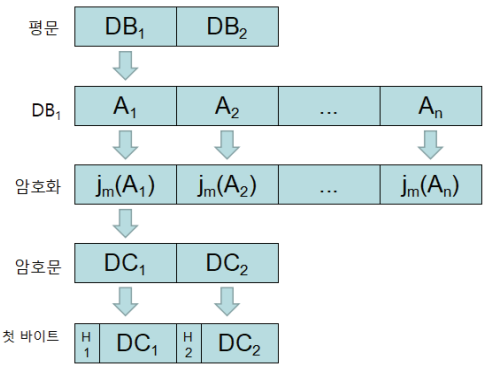

그림 3. 암호화 과정
Figure 3. Encryption process

1. j는 알고리즘의 암호화 등급m={1, 2}과정을 나타낸다.

2. j_m(An)는 m번째 암호화하기 위한 키를 나타낸다.

3. m단계 암호화 과정의 평문을 DB_m으로 나타낸다.

4. 암호화된 m개의 암호문 DC_m생성한 후 암호문을 완성한다.

5. 암호문 첫 바이트의 헤더(H)에 단계를 추한 후 암호화 과정을 완료한다.

<그림 4>는 본 논문의 복호화 과정을 나타내고 있으며 그 과정은 다음과 같다.

1. 암호문의 헤더(H)를 읽어서 암호화 단계 정보를 추출한다.

2. 사용자가 소유한 동일한 단계 키를 이용하여 K_m(An)를 계산한다.

3. k는 알고리즘의 복호화 과정을 수행한 후 평문 DB_m를 도출한다.

4. 평문을 얻어 복호화 과정을 마친다.

본 논문에서는 접근자 IP에 대한 트레이스 백 정보가 완전히 일치하면 서비스 작업을 수행한다.

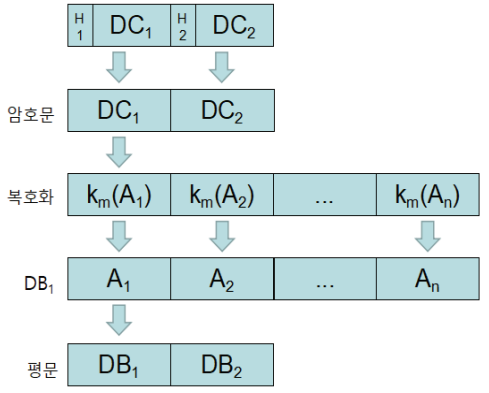

그림 4. 복호화 과정
Figure 4. Decryption process

아울러 유클리드 거리 값 분석을 통하여 획득한 임계치 범위 내의 결과 값도 정상적인 범위로 판정하고 서비스를 수행한다. 즉, 접근 경로에 대한 IP 변경이 일부 존재하더라도 유클리드 거리 값에 기반한 임계치와 암호화를 이용하기 때문에 OTP 발생 없이 서비스 가용성을 향상 시킬 수 있다. 또한 모든 경로 정보를 비교하는 기존의 방식보다 유클리드 거리 값에 기반한 좌표 값을 비교하기 때문에 그 분석 횟수를 감소시킬 수 있다.

4. 실험 및 평가

4.1 유클리드 거리 이용과정

본 논문에서 요구되는 트레이스 백 정보는 본 연구자의 컴퓨터를 출발지로 하고 국내 임의의 지역에 존재하는 서버를 목적지로 하여 해당 정보를 획득하였고, 이를 <그림 5>으로 나타내었다. <그림 5>에서 획득한 트레이스 백 정보를 분석 해 보면 정상적인 사용자가 동일한 IP를 이용한 접근이 발생했지만 8번째에 존재하는 라우터 IP 정보가 일치하지 않는 것을 알 수 있다.이 경우 본 논문에서는 유클리안 거리 값 분석을 통하여 해당 정보를 임계치 범위와 비교하고 그 결과에 의해 서비스, 암호화, 차단 작업을 각각 수행한다[14].

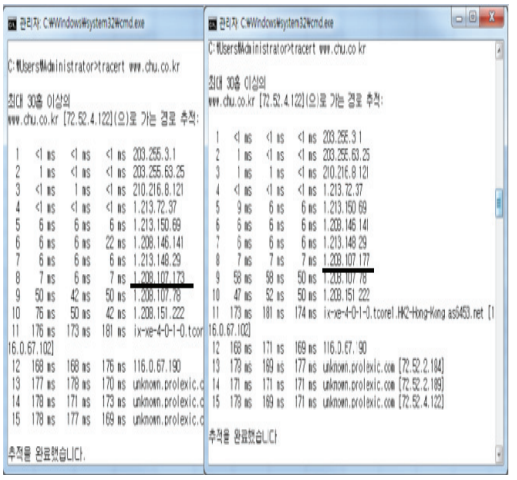

그림 5. 트레이스 백 정보 결과
Figure 5. Results of traceback information

HOP개수	X1	X2	Y1	Y2	Euclidean distance.1
1	203	3	255	1	323.289
2	203	63	255	25	269.258
3	210	8	216	121	223.224
4	1	72	213	37	189.781
5	1	150	213	69	207.212
6	1	146	208	141	159.731
7	1	148	213	29	235.510
8	1	107	208	177	110.440
9	1	107	208	78	167.738
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

HOP개수	X1	X2	Y1	Y2	Euclidean distance.2
1	203	3	255	1	323.289
2	203	63	255	25	269.258
3	210	8	216	121	223.224
4	1	72	213	37	189.781
5	1	150	213	69	207.212
6	1	146	208	141	159.731
7	1	148	213	29	235.510
8	1	107	208	173	111.629
9	1	107	208	78	167.738
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

그림 6. 유클리드 거리 계산 과정
Figure 6. Euclidean distance calculation process

<그림 6>은 트레이스 백 정보를 이용하여 유클리드 거리를 계산한 값에 대한 표이다.

유클리드 기반의 임계치 분석 그래프의 예는 <그림 7>에 나타내었다.

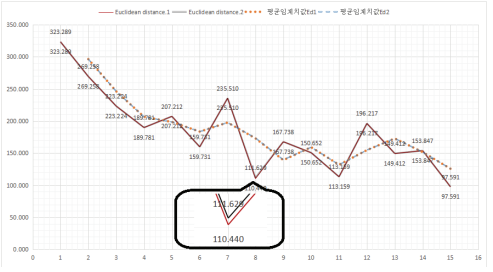

그림 7. 임계치 분석 그래프
Figure 7. Threshold analysis graph

<그림 7>은 유클리드 거리 값 계산을 통하여 도출된 결과와 <그림 5>의 분석 결과를 함께 비교 분석한 그래프이다. <그림 5>에서 유클리안 거리 값은 8번째 라우터에서 상이함을 보이고 있다. 그렇지만 <그림 7>의 임계치를 나타내는 분석 그래프에는 정상적인 임계치 범위 안에 위치하고 있다. 그러므로 이 경우에는 암호화 과정 등을 통한 서비스를 수행하기 때문에 서비스 가용성을 향상시킬 수 있다[15].

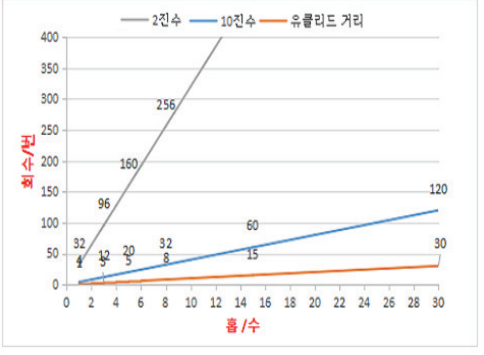

그림 8. 홉당 비교 회수
Figure 8. Times of comparison

<그림 8>은 유클리드 거리 좌표 값을 이용하여 그 비교 과정을 그래프로 나타낸 것이다. 그 결과 일반적접근을 시도한 시스템으로 트레이스 백을 수행하여 획득한 각 홉의 정보를 2진수, 10진수 형태로 수집한 것과, 본 논문에서 주장하는인 트레이스 백 정보를 수집하여 비교 분석을 수행하는 경우보다 유클리드 거리 값을 계산한 후 해당 좌표 값을 비교하는 과정이 분석에 필요한 횟수를 감소시킬 수 있다는 것을 알 수 있었다.

4.2 암호화 복호화 과정

그림 9. 1단계 암호화 결과
Figure 9.The first stage of Encryption results

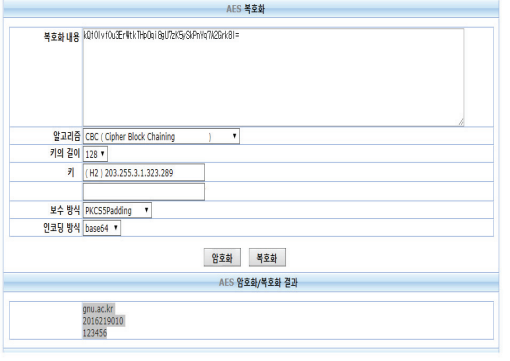

그림 10. 키를 이용한 복호화
Figure 10. Use key to decrypt

<그림 9>는 <그림 3>에 기반한 암호화 과정으로 <그림 2>의 암호화 2단계 과정을 보인 것이다. <그

림 2>의 1단계 암호화 과정에서는 상호 인증에 필요한 특정 IP를 설정하여 암호화 키로 사용한다. 그렇지만 2단계 과정에서는 특정 IP에 유클리드 좌표 값을 더하여 암호화 과정을 수행한다.

<그림 10>은 <그림 9>의 암호화 과정을 통하여 생성된 암호문을 복호화 시킨 결과를 나타낸 것이다.

5. 결 론

본 논문은 클라우드 환경에서 서비스 접근성 및 가용성을 향상시키기 위한 암호화 기반의 능동적이고 안정적인 서비스 모델을 제시한 것이다.

신뢰 네트워크 환경에서 클라이언트의 서비스 요청에 대한 일반적인 기존 탐지 방식은 트레이스 백 정보를 단순 비교 하는 방식을 기반으로 한다. 그렇지만 이러한 트레이드 백 정보의 단순 비교 방식은 정상적인 사용자를 공격으로 판정하는 오류가 발생할 수 있다. 아울러 이를 분석하는 과정에서 경유하는 모든 라우터들의 IP 정보를 순차적으로 비교하기 때문에 오버헤드를 초래할 수 있다.

본 논문은 각 서비스에 대한 안정적이면서 탐지 오류를 개선하기 위하여 유클리안 거리 계산법을 이용하였다. 그리고 이를 통하여 트레이스 백 과정에서 획득한 경유 라우터들의 IP 정보를 유클리안 거리 값으로 계산 한 후 그래프로 나타내었다. 또한 암호화 과정을 통해 정상적인 사용자의 접근성을 최대한 보장할 수 있도록 하였고, 이를 통하여 안정적인 서비스 수행이 가능하도록 하였다. 향후 연구 과제로는 서비스 데이터에 대한 등급을 구분하고, 이를 단계별 등급 키로 암호화 한 후 실시간 서비스가 가능한 연구가 병행되어야 할 것이다.

References

[1] S.T. Zargar, J. Joshi, and D. Tipper, *A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks*, Communications Survers & Tutorials, IEEE, Vol. 15, No. 4, pp. 2046-2069, 2013.

[2] H-D. Lee, H-T. Ha, H-C Baek, C-G. Kim, and S-B. Kim, *Efficient detction and defence model against IP spoofing attack through cooperation of trusted hosts,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 24, No. 12, pp. 2649-2656, 2012.

[3] R-W. Huang, X-L. Gui, S. Yu, and W. Zhuang, *Privacy-preserving computable encryption scheme of cloud computing,* Chinese Journal of Computers, Vol. 34, No. 12, pp. 2391-2402, 2011.

[4] O. Chen, and O-n.Deng, *Cloud computing and its key techniques,* Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, Vol. 29, No. 9, pp. 2562-2567, 2009.

[5] Y-T. Mu, H-C. Baek, J-Y. Choi, W-C. Jeong, and S-B. Kim, *A proposal of a defence model for the abnormal data collection using trace back information in big data environments,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 10, No. 2, pp. 153-162, 2015.

[6] D. Pansa, and T. Chomsiri, *Architecture and protocols for secure LAN by using a software-level certificate and cancellation of ARP protocol*, Third 2008 International Conference on Convergence and Hybrid Information Technology, pp. 21-26, 2008.

[7] J. H. Sun, and K. J. Kim, *Cloud computing in the vulerability analysis for personal*

information security, Journal of Information and Security, Vol. 10, No. 4, pp. 77-82, 2010.

[8] S. Bellovin, M. Leech, and T. Taylor, *ICMP traceback message*, IETF, draft-ietfitrace-04, Feb, 2003.

[9] S. Li, and S. G. Kang, *Design of 3-dimensional cross-lattice signal constellations with increased compactness,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 20, No. 4, pp. 715-720, Apr. 2016.

[10] M-S. Kim, J-H. Kim, J-H. Wo, L-S. Lee, and B-H. Kim, *A function of a variety of distance in accordance with the definition of a regular polygon.* The Korean Soc. Math. Ed. Proceedings of the 47th National Meeting of Math. Ed., pp. 259-268, Nov. 4-5, 2011.

[11] Y. H. Shin, G. H. Lim, and E. G. Im, *A research on the possibility of ARP spoofing attack in SCADA system based on TCP/IP environment,* Convergence security journal, Vol. 9, No. 3, pp. 9-17, 2009.

[12] 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.

[13] M-H. Kim, H-C. Beak, S-W. Hong, and J-H. Park, *An encrypted service data model for using illegal applications of the government civil affairs service under big data environments*, Convergence security journal, Vol. 15, No. 7, pp. 31-38, 2015.

[14] Y. Liu, H-C. Baek, J-Y. Park, and S-B. Kim, *An improved model design for traceback analysis time based on Euclidean distance to IP spoofing attack*, Korea Convergence Security Association, Vol. 17, No. 5, Dec, 2017.

[15] Y. Liu, H-C. Baek, J-Y. Park, and S-B. Kim, *Model design for reduce OTP reauthorization based on Euclidean distance,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 12, No. 5, pp. 737-745, 2017.

유클리드 거리식을 이용한 암호화 기반의 사용자 인증 서비스 모델

유양[1], 백현철[2], 홍석원[3], 박재홍[4], 김상복[4]

[1]경상대학교 컴퓨터과학과 대학원생
[2]경남도립남해대학 컴퓨터SW공학과 교수
[3]경남도립거창대학 정보지원센터 팀장
[4]경상대학교 컴퓨터과학과 교수

요 약

현재 네트워크 기술은 클라우드 및 사물인터넷 기반 환경으로 빠르게 변화하고 있다. 그렇지만 불법적인 공격 발생시 이에 대한 능동적인 방어와 효율적인 서비스 제공에는 그 한계성을 보이고 있다. 특히 전문적인 해킹 기술을 보유하고 있는 공격자들은 IP 스푸핑 공격을 주로 시도하고 있기 때문에 이를 탐지하고 대응하기에는 많은 어려움이 있다. IP 스푸핑 공격을 탐지를 위한 기존 방식에는 접속을 요청한 클라이언트의 트레이스 백 경로 정보를 서버에서 미리 보유하고 있는 정상적인 경로 정보와 비교하는 방식을 사용하고 있다. 이러한 탐지 방식은 정상적인 접근과 불법적인 접근에 대한 분석과정에서 빈번한 OTP 발생을 가져오면서 서비스 가용성을 저하시킬 수 있다. 본 논문은 이러한 문제점을 개선하기 위하여 기존의 접근 정보의 단순 비교 방식에 유클리드 거리 계산식과 단계별 암호화기법을 사용하는 보안모델을 제안하였다. 그리고 이를 기반으로 경로 정보의 단순 비교 과정에서 발생하는 상이한 경로 정보에 대한 차단 우선 정

책을 보완할 수 있었다. 또한 접근 경로의 변이 정보를 분석한 후 단계별 암호화 과정을 수행하고, 이에 대한 복호화 과정을 통하여 정상적인 인증과 지속적인 서비스 수행이 가능하도록 하였다.

Yang Liu received the Master´s degree in the Department of Computer Science from Gyeongsang National University in 2015. His current research interests include network architecture, bigdata security, network security.

E-mail address: a2633558a@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 Depart -ment of Computer SW, 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

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

Jae Heung Park received the Ph.D. degree in the Department of Computer Engineering from Chungang 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 Chungang 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