https://doi.org/10.33778/kcsa.2023.23.1.019

서비스 사용자의 능동적 피싱 사이트 탐지를 위한 트레이스 백 기반 인증 모델

백 용 진*, 김 현 주**

요 약

현재 네트워크 환경은 초기의 단방향 정보제공 서비스에서 실시간 양방향 서비스를 제공하고 있다. 이에 따라 웹 기반의 정보 공유 형태는 사용자 상호간 다양한 지식 제공과 서비스가 가능하다. 그렇지만 이러한 웹 기반의 실시간 정보 공유 환경은 네트워크 취약점을 악용한 불법적인 공격자들에 의해 그 피해 사례를 빠르게 증가시키고 있다. 특히 피싱 공격을 시도하는 공격자들의 경우 특정 웹 페이지 서비스가 필요한 사용자들에게 위/변조된 웹 페이지를 생성시킨 다음 해당 웹 페이지에 대한 링크를 유도한다. 본 논문은 사이트 위/변조 여부를 기존의 수동적인 서버 기반 탐지 방식이 아닌 사용자가 직접 능동적으로 특정 사이트에 대한 위/변조 여부를 분석할 수 있도록 하였다. 이를 위해 트레이스 백 정보를 이용하여 불법적인 웹 페이지 접속을 유도하는 공격자의 위장된 웹 페이지를 탐지하여 정상 사용자들의 중요한 개인 정보 유출을 방지할 수 있도록 하였다.

A Traceback-Based Authentication Model for Active Phishing Site Detection for Service Users

Baek Yong Jin*, Kim Hyun Ju**

ABSTRACT

The current network environment provides a real-time interactive service from an initial one-way information provision service. Depending on the form of web-based information sharing, it is possible to provide various knowledge and services between users. However, in this web-based real-time information sharing environment, cases of damage by illegal attackers who exploit network vulnerabilities are increasing rapidly. In particular, for attackers who attempt a phishing attack, a link to the corresponding web page is induced after actively generating a forged web page to a user who needs a specific web page service. In this paper, we analyze whether users directly and actively forge a specific site rather than a passive server-based detection method. For this purpose, it is possible to prevent leakage of important personal information of general users by detecting a disguised webpage of an attacker who induces illegal webpage access using traceback information

Key words : Traceback, Phishing, Encryption, Authentication, Similarity

접수일(2022년 08월 31일), 수정일(2022년 09월 14일), 게재확정일(2023년 02월 10일)

* 경상국립대학교 컴퓨터과학과(주저자)
** 경상국립대학교 컴퓨터과학부(교신저자)

1. 서 론

현재 일반적인 네트워크 환경은 네트워크 서비스 제공에 있어 단편적인 서비스 형태를 벗어나 품질과 형태 등에 있어 다양성을 가지고 발전하고 있다. 그렇지만 네트워크 환경의 다양성은 불법적인 공격자들의 신규 공격 대상 증가와 함께 기존 공격기법을 응용한 새로운 공격 기법 형태로 나타나고 있다[1][2].

단방향 정보제공을 수행하는 초기의 네트워크 서비스는 현재 실시간 양방향 서비스를 통해 다양한 기능 제공과 사용자 상호 정보 공유를 가능하게 한다. 그렇지만 웹 기반의 실시간 정보 공유는 이를 악용한 불법적인 공격자들에 의해 그 피해 사례가 급증하고 있는 실정이다. 특히 피싱 공격을 시도하는 불법적인 사용자들의 경우 웹 페이지 서비스를 요청하는 사용자들에게 팝업창을 통해 위/변조된 웹 페이지에 대한 링크를 유도하고 있다[3][4].

아울러 일반적인 웹 사이트 접속자에 대한 검증은 서비스 제공자가 수행하는 방식을 채택하고 있기 때문에 실시간 다발적인 피싱 공격에 효율적으로 대응하기 어렵다. 본 논문은 빠르게 증가하는 피싱 공격에 사용자 측면의 능동적 대응을 위해 트레이스 백 정보를 기반으로 위조된 웹 페이지를 사용자 측면에서 실시간으로 분석하고 탐지할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구 부분을 살펴보고 3장에서는 본 논문에서 제안하고 있는 모델과 동작 과정을 설명하였다. 4장에서는 본 논문의 전반적인 과정에 대한 시뮬레이션을 보였으며 마지막에 결론과 본 논문의 향후 응용 가능성에 대한 설명을 하였다.

2. 관련 연구

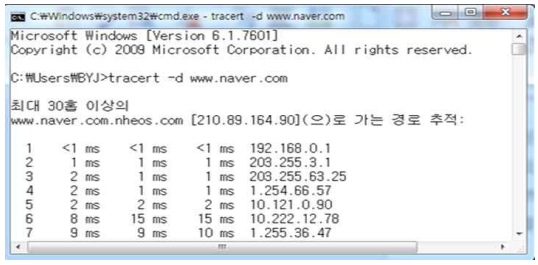
2.1 기존 탐지 방법

현재 피싱 사이트에 대한 탐지기법 중 대표적인 탐지 방법은 URL 정보를 미리 수집한 뒤, 사용자가 방문하는 사이트의 URL과 미리 저장된 정보를 비교하여 피싱 사이트를 탐지 하는 기술이 있으며[5], 서버로 들어오는 Http Requset Header를 분석하여 탐지의 지표로 사용하는 기술과 정상적인 사이트 서버 측에서 탐지하는 Request 헤더의 Referrer 필드를 분석한 후 Request URI와 Referrer의 URL을 비교하여 탐지하는 기술이 있다[6].

2.2 트레이스 백

트레이스 백이란 (그림 1)과 같이 특정 송신자와 수신자 사이에 존재하는 경유 라우터들의 정보를 분석하며, 라우터들의 IP를 추적하여 해당 연결 경로 정보를 제공해 주는 프로그램이다.

본 논문에서는 트레이스 백 정보를 기반으로 사용자의 단말 장치에서 특정 웹 사이트에 대한 위장 사이트 여부를 판정할 수 있도록 하였다[7][8].



(그림 1) 트레이스 백

2.3 피싱(Phishing)

2.3.1 피싱의 의미

피싱이란 개인 정보를 의미하는 Private Data오 낚시를 의미하는 Fishing의 합성어라고 할 수 있으며, 그 공격 과정에 이메일이나 메신저를 이용하고 있다[9].

피싱 공격자들은 정상적인 금융 사이트와 유사한 피싱(Phishing)사이트를 이용하여 금융거래가 가능한 특정 개인의 정보를 탈취한다.

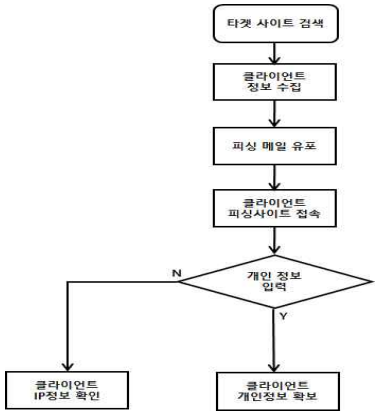
일반적인 사용자들은 위장된 피싱 사이트가 정상적인 실제 사이트와 상당히 유사하기 때문에 직접 위·변조 여부를 판단하기가 어렵다.

아울러 피싱 사이트의 위협에 대응하기 위한 국정

원의 국가사이버안전센터, 한국인터넷진흥원의 인터넷침해대응센터 등이 있으나 지속적으로 다수의 피싱 사이트가 발생함에 따라 탐지 및 대응에는 한계가 있다[10].

2.3.2 피싱 공격 과정

피싱 공격 과정 (그림 2)와 같이 나타낼 수 있다. 피싱 공격자의 경우 먼저 위장 사이트생성을 위한 타겟 사이트를 탐색을 한다. 그리고 이를 통해 피싱 메일을 유포한 후 사용자 접속을 유도한 다음 불법적인 개인 정보를 수집하게 된다.



(그림 2) 피싱 공격 과정

(그림 2)의 동작 과정은 다음과 같다.

STEP 1. 공격자는 위장 사이트 생성을 위해 타겟 사이트 탐색을 한 다음 위장 사이트를 생성한다.

STEP 2. 불특정 다수를 상대로 사용자 정보를 수집한다.

STEP 3. 수집된 사용자들에 대해 피싱 메일을 유포한다.

STEP 4. 클라이언트의 피싱 사이트 접속을 유도한다.

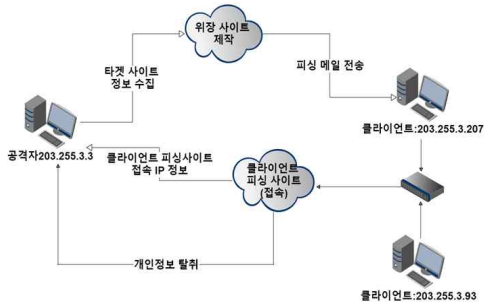
STEP 5. 클라이언트의 접속과 개인정보 입력 여부에 따라 다음의 결과가 나타난다.

5-1. 클라이언트의 개인정보 입력이 발생하면 공격자는 클라이언트의 개인정보를 획득할 수 있다.

5-2. 클라이언트의 개인정보 입력이 없다면 공격자는 클라이언트의 IP 정보를 획득할 수 있다.

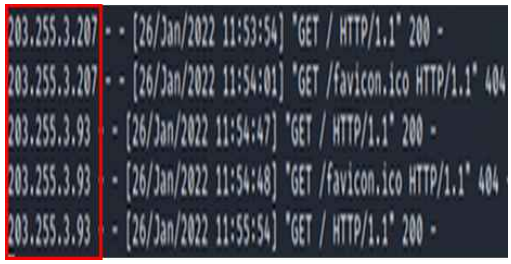
3. 제안 모델 동작 과정

본 논문에서 피싱 공격자의 피싱사이트 생성과 유포 과정에 대한 네트워크 환경은 (그림 3)과 같이 구성하였다. (그림 3)에서 공격자는 위장사이트를 생성한 다음 임의의 클라이언트의 접속을 유도한 다음 해당 클라이언트의 정보를 확보하게 된다.



(그림 3) 피싱 공격 네트워크 구성도

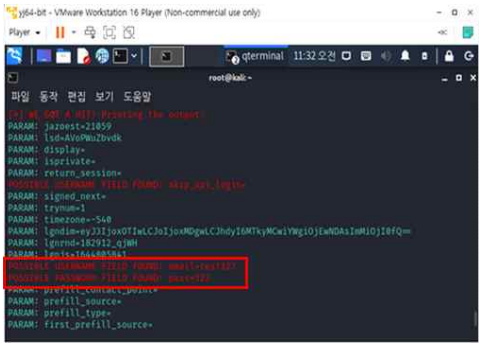
(그림 4)는 (그림 3)의 클라이언트를 대상으로 피싱 사이트를 유포한 결과를 Kali Linux를 통해 공격자가 클라이언트의 초기 접속 정보를 확인한 결과이다.



(그림 4) 피싱 메일 유포

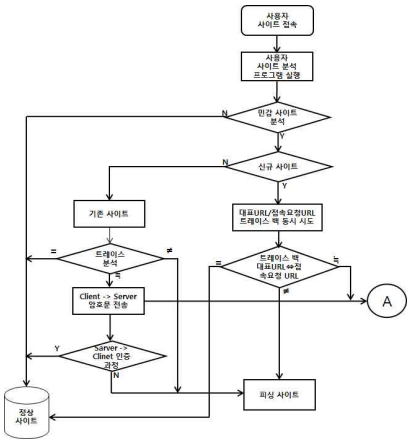
(그림 5)는 클라이언트가 피싱사이트 접속을 한

다음 개인정보를 입력하게 되면 해당 개인정보를 획득하는 과정이다.



(그림 5) 클라이언트 개인정보 획득

(그림 6)은 본 논문에서 제안하는 모델의 동작 과정이다.



(그림 6) 제안 모델 동작 과정

STEP 1. 사용자가 사이트 접속 요청이 발생하면 사용자 접속 요청 사이트 분석을 한다.

STEP 2. 사용자 판단이 가능한 민감 사이트 분석 작업을 수행한 후 다음 과정을 수행한다.

2-1. 사용자 민감 사이트일 경우 STEP 3.의 과정을 수행한다.

2-2. 사용자 민감 사이트가 아닐 경우 정상적인 접속 과정을 수행한다.

STEP 3. 민감 사이트에 대한 신규 사이트 여부를 분석한 후 다음 과정을 수행한다.

3-1. 신규 사이트일 경우 대표 URL과 접속 요청 URL에 대한 동시 트레이스 백을 수행한 후 STEP 4. 과정을 수행한다.

3-2. 신규 사이트가 아닐 경우 기존 사이트에 대한 STEP 5. 과정의 트레이스 백 분석 작업을 수행한다.

STEP 4. 트레이스 백 정보 분석 결과에 따라 다음 과정을 각각 수행한다.

4-1. 대표 URL 정보와 트레이스 백 정보가 동일할 경우 정상적인 접속 과정을 수행한다.

4-2. 대표 URL 정보와 트레이스 백 정보가 일치하지 않을 경우 피싱 사이트로 판정한다.

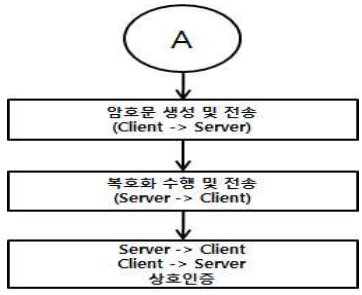
4-3. 대표 URL 정보와 트레이스 백 정보의 일치도가 임계치 범위에 존재하면 (그림 4)의 암호화 과정을 수행한다.

STEP 5. 트레이스 백 정보 분석 결과에 따라 다음 과정을 각각 수행한다.

5-1. 트레이스 백 정보가 동일할 경우 정상적인 접속 과정을 수행한다.

5-2. 트레이스 백 정보가 일치하지 않을 경우 피싱 사이트로 판정한다.

5-3. 트레이스 백 정보의 일치도가 임계치 범위에 존재하면 (그림 7)의 암호화 과정을 수행한다.



(그림 7) 제안 모델 암호화 과정

4. 실험 및 평가

본 논문은 정상사용자에 대한 검증을 위하여 트

레이스 백 정보를 수집하여 활용하고 있다. <표 1>은 정상적인 트레이스 백 정보 수집을 위해 임의의 사이트를 설정한 것이다.

<표 1> 임의 사이트에 대한 트레이스 백 결과

1	172	172	172
2	218.154.215.1	218.154.215.1	218.154.215.1
3	112.174.211.125	112.174.211.125	112.174.211.125
4	* *	* *	* *
5	* *	* *	* *
6	112.174.10.142	112.174.10.142	112.174.10.142
7	210.107.53.193	* *	210.107.53.193
8	1.208.174.97	1.208.174.97	1.208.174.97
9	1.208.147.6	1.208.147.6	* *
10	1.213.8.234	1.213.8.234	1.213.8.234
11	58.75.221.106	58.75.221.106	58.75.221.106
12	122.199.255.160	122.199.254.160	122.199.254.160
13	* *	* *	* *
14	221.132.73.150	221.132.73.150	221.132.73.150

본 논문에서 해당 사이트에 대해 50회의 트레이스 백을 실시하였으며 <표 2>와 같은 결과를 얻었다.

<표 2> 트레이스 실험 결과

100%일치	90% ≤ 1 *Hop* 불일치 ≤ 99%
42／50 = 84%	8／50 = 16%

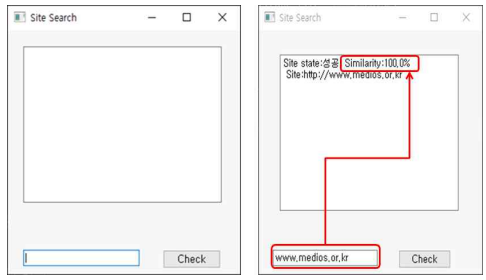
실험 결과를 기반으로 해당 사이트의 임계치 설정은 (식 1) 같이 설정하였고 트레이스 백에 대한 임계치가 90% 이상이거나 99%이하일 경우 유사도 검사를 진행하도록 하였다.

$$90\% \leq \text{트레이스 백 임계치} \leq 99\% \quad (1)$$

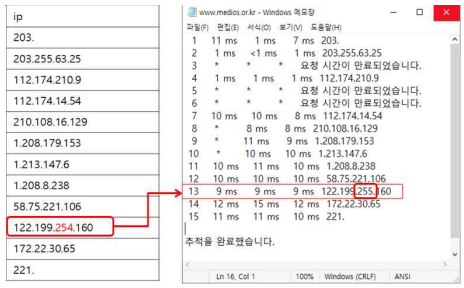
그러므로 특정 사이트의 임계치 설정은 해당 사이트의 트레이스 백 정보를 일정 횟수만큼 수집한 다음 이를 기반으로 설정할 수 있다.

(그림 8)과 (그림 9)는 본 논문에서 사이트 분석프로그램을 수행하여 해당 사이트에 대한 분석을 진행한 결과이다.

본 논문의 제안 모델 DB에 등록 되어 있는 정상 사이트 유무에 대해 유사도 검사를 통해 분석하는 과정을 보이고 있다.

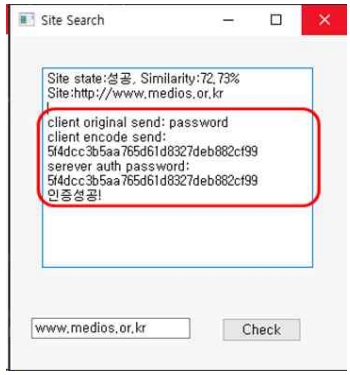


(그림 8) 민감 사이트 분석 과정



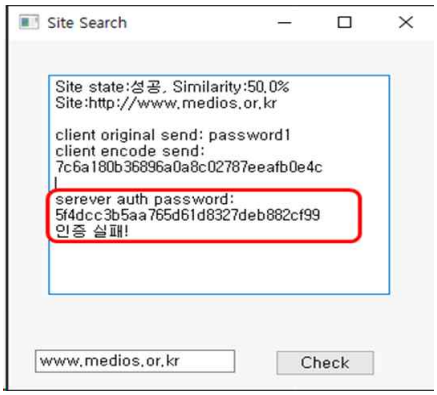
(그림 9) 사이트 실시간 트레이스 백 수집 정보

(그림 10)은 실시간 사이트 분석프로그램을 수행하여 해당 사이트에 대한 트레이스 백 검사와 유사도 분석 후 유사도가 임계치에 존재할 경우 암호문 전송과 그 접속 과정을 보이는 것이다.



(그림 10) 서버 -> 클라이언트 인증 과정 성공

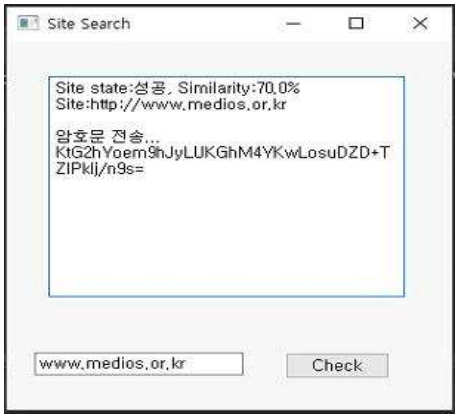
(그림 11)은 유사도가 임계치 이하일 경우 그 대응 과정을 보이는 것이다. 암호문 전송 후 인증이 성공 하면 정상 적인 사이트로 판정하지만, 인증 과정이 실패 하면 피싱 사이트로 판정하게 된다.



(그림 11) 서버 ->클라이언트 인증 과정 실패

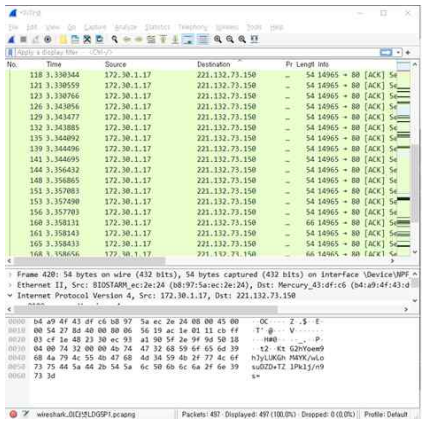
(그림 12)는 신규 사이트의 경우 대표 URL과 접속 요청 URL에 대한 동시 트레이스 백 과정을 수행한 후 트레이스 백 정보가 모두 일치할 경우 정상적인 사이트로 판정하는 과정을 보이는 것이다.

본 논문에서는 해당 인증과정을 성공적으로 수행할 경우 정상적인 사이트로 판정하고, 암호화 인증 과정을 정상적으로 수행하지 못할 경우 피싱사이트로 판정한다.



(그림 12) 신규 사이트에 대한 인증 과정

(그림 13)은 신규 사이트 접속 과정에서 대표 URL과 접속 요청 URL에 대한 동시 트레이스 백을 수행하는 과정에서 발생하는 암호문에 대해 와이어 샤크를 통해 분석한 결과이다.



(그림 13) 신규 사이트에 대한 암호문 전송 후 와이어 샤크 분석 결과

5. 결 론

다수의 사용자들이 실시간으로 접속하는 웹 서비스는 불법적인 공격자들의 표적이 될 수 있다. 특히 피싱 공격의 경우 이러한 공격자들은 위/변조된 웹 페이지를 통해 정상적인 웹 서비스 가입자의 계정과 패스워드 등 공격에 필요한 정보의 입력을 유도한 다음 탈취한 정보를 이용하여 공격을 시도한다.

일반적인 피싱 공격은 하이퍼링크를 통해 변조된 사이트로 연결을 유도하는데, 이 과정에서 정상적인 사이트의 주소나 도메인 이름이 아닌 피싱 공격을 위한 변조된 사이트의 IP 주소가 URL 주소창에 나타나게 된다. 그러므로 고도의 해킹 기법을 보유하고 있는 공격자들은 특정 스크립트를 이용하여 위장된 시스템의 IP 주소와 도메인 이름을 은닉하기 때문에 웹 서비스 이용자는 이를 인지하지 못하고 위장된 사이트로 자신들의 중요 정보를 유출하게 되는 것이다.

본 논문의 경우 클라이언트를 대상으로 한 피싱 사이트 공격에 대해 트레이스 백 기반의 피싱 사이트 탐지를 위한 암호화 모델을 제안하였다.

본 논문은 특정 사이트에 대한 피싱 공격이 발생할 경우 사용자가 능동적으로 피싱 사이트 검사를 진행할 수 있도록 제안하였다. 아울러 사이트에 대한 실시간 트레이스 백 정보 수집을 통해 유사도 검사를

할 수 있도록 하였다. 아울러 유사도 검사의 경우 클 사용자 측에서 보유하고 있는 트레이스 백 정보와 실시간 트레이스 백 정보를 상호 비교할 수 있도록 하였다.

오늘날 네트워크 환경은 급속도로 빠르게 발전하고 있으며, 불법적인 공격의 빈도수도 증가하고 있다. 그러므로 이에 따른 보안 서비스도 한층 필요한 시점이다. 아울러 현재 모바일 네트워크 환경의 경우 트레이스 백에 대한 실시간 정보 수집이 미흡한 단계이기 때문에 향후 모바일 네트워크 환경에서 트레이스 백에 대한 실시간 정보 분석을 통해 이를 기반으로 한 모바일 피싱 사이트 탐지연구가 활발하게 진행되어야 할 것이다.

참고문헌

[1] The Design of Authentication Model based on Symmetric Key Encryption for Improving Network Availability in Cloud Environment 2019, pp.47 - 53.

[2] Asymmetric Key Cryptographic Authentication Model for IP Spoofing in Cloud Environments 2019, vol.14, no.6, pp. 683-691.

[3] A Reliable Service Provided Model for Session Hijacking Attacks in Big Data Service Environments 2016, vol.11, no.6, pp. 597-606 (10 pages).

[4] D.-H. Seo, H.-J. Kang, Suggest of TCP sequence number Encryption, Journal of Korea Multimedia Society, Autumn Annual Conference, pp. 498~501, 2000.

[5] A Study on the responses of Spear Phishing mail attacks, 2021.

[6] A Phishing Site Detection Method with Utilizing Password, 2017.

[7] An Efficient Detection and Service Model in case of IP Spoofing in Cloud Environment, 2019.

[8] An Efficient Detection and Service Model in case of IP Spoofing in Cloud Environment, 2019.

[9] Messenger Phishing Modus Operandi in South Korea 2021, vol.18, no.3, 통권 58호 pp. 241-258 (18 pages).

[10] A Study on Website Forgery/Falsification Detection Technique using ImagesVolume 16 Issue 1Pages.81-87 2016.

〔저자소개〕

백 용 진(Yong-Jin Baek)
2015년 2월 경남과학기술대학교 컴퓨터공학과 학사
2019년 경상국립대학교 컴퓨터과학과 석사
2019년 3월 경상국립대학교 컴퓨터과학과 박사 과정

email : qhanffkwk@nate.com

김 현 주(Kim-Hyun Ju)
1988년 2월 경상대학교 전산통계학과 이학사
1990년 8월 숭실대학교 전자계산학과 공학석사
2000년 8월 경상대학교 컴퓨터과학과 이학박사
2023년 3월~현재 경상국립대학교 컴퓨터과학부 교수

email : hjkim328@gnu.ac.kr