# 트레이스 백 정보에 기반한 매크로 공격 탐지 모델

백 용 진*, 홍 석 원**, 박 재 흥***, 강 경 원****, 김 상 복*****

## 요 약

오늘날 정보 통신 기술의 발전은 네트워크 기반의 서비스 사용자 수를 빠르게 증가시키고 있으며, 인터넷 상에서 사용자 상호간 실시간 정보 공유를 가능하도록 한다. 정보의 공유 과정에는 다양한 방법들이 존재하지만 일반적으로 포털 서비스 기반의 정보 공유가 대중화 되어있다. 그렇지만 이러한 정보 공유 과정은 특정 이해 당사자 상호간 해당 정보의 사회적 관심도 증폭을 위한 불법 행위를 유발시키는 원인이 되고 있다. 그 중 매크로 기능을 이용한 여론 조작 공격은 정상적인 여론의 방향을 왜곡시키기 때문에 이에 대한 보안 대책이 시급한 실정이다. 일반적으로 매크로 공격이란 불법적인 사용자들이 다수의 IP나 아이디를 확보한 후 특정 웹 페이지의 내용에 대하여 여론을 조작하는 공격으로 정의한다. 본 논문은 특정 사용자의 매크로 공격에 대하여 트레이스 백 기반의 네트워크 경로 정보를 분석한 후 해당 사용자의 다중 접속을 탐지할 수 있도록 하였다. 즉, 특정 웹 페이지에 대한 전체적인 접근 경로 정보와 사용자 정보가 일치하는 접근이 2회 이상 발생하면 이를 매크로 공격으로 판정하였다. 또한 동일한 지역에서 특정 웹 페이지에 대하여 다수의 아이디를 이용한 접근이 발생하는 경우, 이에 대한 임계 카운트 값 분석을 통하여 특정 웹 페이지에 대한 전체적인 여론 결과를 왜곡 할 수 없도록 하였다.

# A Macro Attacks Detection Model Based on Trace Back Information

Baek Yong Jin*, Hong Suk Won**, Park Jae Heung***, Kang Gyeong Won****, Kim Sang Bok*****

## ABSTRACT

Today, the development of information and communication technology is rapidly increasing the number of users of network-based service, and enables real-time information sharing among users on the Internet. There are various methods in the information sharing process, and information sharing based on portal service is generally used. However, the process of information sharing serves as a cause of illegal activities in order to amplify the social interest of the relevant stakeholders. Public opinion attack using macro function can distort normal public opinion, so security measures are urgent. Therefore, security measures are urgently needed. Macro attacks are generally defined as attacks in which illegal users acquire multiple IP or ID to manipulate public opinion on the content of a particular web page. In this paper, we analyze network path information based on traceback for macro attack of a specific user, and then detect multiple access of the user. This is a macro attack when the access path information for a specific web page and the user information are matched more than once. In addition, when multiple ID is accessed for a specific web page in the same region, it is not possible to distort the overall public opinion on a specific web page by analyzing the threshold count value.

**Key words : Macro, Traceback, CAPTCHA, Analyis DataBase, TargetText**

접수일(2018년 11월 19일), 게재확정일(2018년 12월 17일)

* 경상대학교 컴퓨터과학과(주저자)
** 경남도립거창대학 교무부
*** 경상대학교 컴퓨터과학과
**** 진주보건대학 의약복지정보계열
***** 경상대학교 컴퓨터과학과(교신저자)

# 1. 서 론

오늘날 정보 통신 기술은 지속적인 발전 과정을 거쳐 인터넷 사용자들에게 다양한 서비스를 온라인으로 공유할 수 있도록 한다. 그러므로 상호 공유가 가능한 웹페이지의 서비스 자료들은 공유자들의 의견을 정확하게 반영할 수 있어야 한다.

인터넷을 통한 서비스 정보의 공유 과정에는 해당 정보에 대한 이해 당사자가 존재하며, 이러한 이해 당사자들은 해당 공유 정보가 자신에게 유리하게 작용하도록 불법적인 행위를 시도한다.

특정 웹페이지에 대한 매크로 공격이란 일반적으로 불법적인 사용자들이 다수의 IP나 로그인 정보를 확보한 후 특정 웹 페이지의 내용에 대하여 여론 조작을 시도하는 공격을 의미한다.

네트워크를 통한 정보의 공유는 그 전파 속도가 아주 빠르기 때문에 정상적인 정보의 왜곡된 전파는 많은 역기능을 초래하게 되고 그 피해가 아주 심각한 수준이라고 할 수 있다. 그러므로 이러한 매크로 공격에 대비하여 빠르게 변하고 있는 네트워크 환경에 대한 이해와 이에 따른  적절한 보안 시스템 구축이 필요하다고 할 것이다.[1-3]

불법적인 정보 접근에 대응할 수 있는 기술에는 일반적으로 인증 기법, 탐지 기법, 암호화 기법이 있으며, 이들은 각 네트워크 환경의 특성에 따라 단일 또는 둘 이상의 기능이 복합적으로 운용되고 있다[4]. 그렇지만 이러한 대응 기법들은 현재 빠르게 발전하고 있는 다양한 공격 기법들에 대하여 효율적이고 신속한 대응을 제공해주지 못하고 있다.[5] 본 논문에서는 이러한 문제를 해결하기 위해 송/수신자 상호간에 존재하는 트레이스 백 정보를 기반으로 매크로 공격을 분석 탐지한 후 신속한 대응이 가능한 모델을 제안하였다. 즉, 상호 공유하고 있는 웹페이지의 특정 정보에 대하여 동일한 IP로 다수의 로그인 정보를 이용하여 접근을 시도하는 경우와 특정 네트워크에서 다수의 상이한 IP를 이용하여 접근을 시도하는 경우를 매크로 공격으로 판정할 수 있도록 하였다. 아울러 이러한 매크로 공격을 효율적으로 분석하고 관리할 수 있도록 이에 대한 로그 기록을 저장하여 이를 기반으로 유사 공격에 실시간으로 신속한 대응이 가능하도록 하였다.

# 2. 관련연구

## 2.1 매크로(Macro) 기능

매크로란 특정 작업의 전반적인 수행을 위하여 조작자가 매번 해당 명령을 입력하지 않고 특정 기능을 가진 키를 입력함으로써 자동적으로 해당 모든 작업이 수행되도록 하는 프로그램을 의미한다.[4],[6]

## 2.2 캡차(CAPTCHA)

캡차란 광고, 스팸메일, 게임 자동사냥 매크로, DDoS 등의 공격에 사용되는 자동 프로그램을 막기 위한 인증도구라고 할 수 있다. 포털 서비스를 수행하는 시스템들은 매크로 공격을 통한 불법적인 자동 조작을 방지하기 위하여 일반적으로 CAPTCHA 기능을 제공 한다. 즉, 텍스트가 출력된 이미지를 왜곡시킴으로써 컴퓨터가 판독하기 힘들게 하는 방법이라고 할 수 있다. 그렇지만 인공 지능 기법이나 이미지 처리 기법을 통하여 이를 무력화 시킬 수 있고 서비스 가용성 면에서 효율적인 대안이라고 할 수 없다.[7],[12-14]

## 2.3 트레이스 백의 의미

트레이스 백이란 네트워킹 과정에서 특정 송신자와 수신자 사이에 존재하는 경유 라우터들의 정보를 분석하기 위한 프로그램이다. 그러므로 상호 네트워킹을 구성하고 있는 특정 송/수신자의 패킷은 최종 목적지까지 도달하기 위해 다수의 라우터를 경유하게 되며, 이렇게 경유하는 각 구간의 정보를 획득하여 패킷의 이동 경로를 분석하는 것을 트레이스 백이라고 한다.[8] 그러므로 이러한 네트워크 과정에 있어 안정성과 신뢰성 확보를 위하여 해당 경로들에 대한 정확한 분석이 필요하다. 본 논문에서는 기존의 인증 정보 대신 트레이스 백 정보를 이용하여 인증과정에 필요한 정보로 사용하고 있다.[9-11]

# 3. 제안 모델 동작 과정

## 3.1 제안 모델

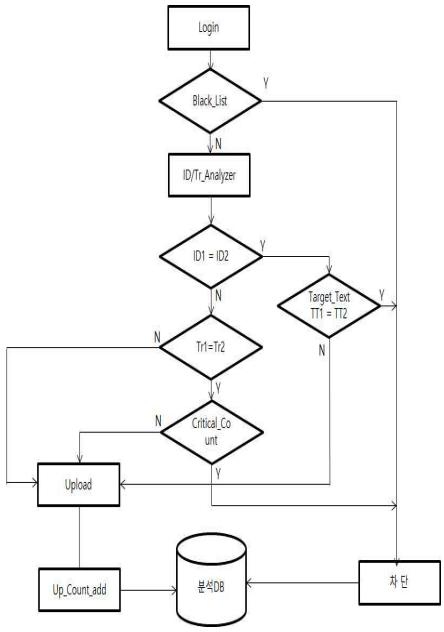
본 논문에서는 불법적인 매크로 공격을 탐지하기 위해 접근 정보에 대한 로그 기록을 분석 데이터베이스로 사용하였으며, 이를 위한 정보 구조는 다음과 같다.

<표 1> 분석데이터베이스 자료구조

| 항목명 | 용도 |
|---|---|
| ID_Info | 사용자 접속정보 |
| Tr_Info | 사용자 접근 경로 정보 |
| Up_Count | 동일정보 참조횟수 |
| Black_List | 매크로 공격자 정보 |
| Critical_Count | 임계 카운트 |
| Target_Text | 매크로 표적 페이지 |

<표 1>의 ID_Info는 사용자 접속 정보로 특정 사용자의 정보가 중복 사용될 경우 이를 탐지하기 위함이다. Tr_Info는 동일 네트워크 환경에서 다수의 상이한 IP를 이용하여 불법적인 접근을 시도하는 것을 탐지하기 위한 정보로 사용한다. Up_Count는 동일 사용자에 의한 동일 웹페이지의 참조 횟수를 탐지하기 위함이다. Black_List는 매크로를 시도한 공격자의 정보를 이용하여 실시간 탐지에 이용한다 Critical_Co unt는 임계 카운트로 공격이 분명하지 않은 접속자에 대하여 일정 범위 안에서 정상적인 사용을 허용하기 위함이다. Target_Text는 동일 사용자에 의한 동일 페이지에 대한 참조횟수를 분석하기 위한 값으로 사용하고 있다.

다음은 (그림 1)은 본 논문에서 제안하는 모델의 동작 과정을 도식화 한 것을 나타낸 것이다.




(그림 1) 제안모델 동작 과정

본 논문에서는 사용자의 접속이 발생하면 다음 과정을 수행한다.

STEP 1. 분석데이터베이스에서 보유하고 있는 Black_List 정보를 비교한다.
- 1-1 Black_List 정보와 일치하는 접속자이면 차단 작업을 수행한다.
- 1-2 Black_List에 존재하지 않는 접속자이면 STEP 2 과정을 수행한다.

STEP 2. ID_Info와 Tr_Info를 비교 분석한다.

STEP 3. 동일 사용자의 재접속 유무에 대한 분석 과정을 수행한다.
- 3-1. 동일 사용자 접속일 경우 STEP 4 과정을 수행한다.
- 3-2 동일 사용자 접속이 아닐 경우 STEP 5 과정을 수행한다.

STEP 4. 동일 사용자의 매크로 표적 페이지 접속 여부를 분석한다.
- 4-1 매크로 표적 페이지 접속이면 차단 작업을 수행한다.
- 4-2 매크로 표적 페이지에 대한 접속이 아니면 STEP 8의 과정을 수행한다.

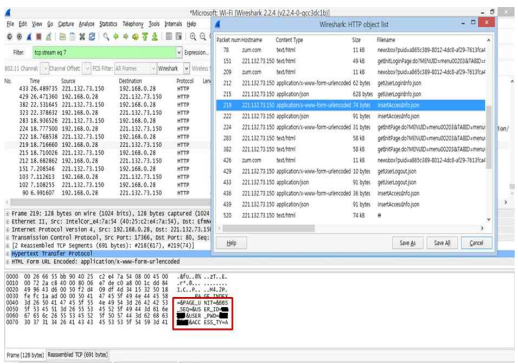
STEP 5. 접속자의 접근 경로 정보를 분석한다.
- 5-1 접속자의 출발지 주소가 동일한 경우이거나, 출발지 주소는 상이하지만 나머지 경유 정보가 일치하면 STEP 6

의 과정을 수행한다.
5-2 접속자의 접근 경로 정보가 상이하면 STEP 8의 과정을 수행한다.
STEP 6. Critical_Count의 범위를 비교 분석한다.
6-1 Critical_Count의 범위 미만이면 STEP 7을 수행한다.
6-2 Critical_Count의 범위 이상이면 차단 작업을 수행한다.
STEP 7. 접속자의 동일 페이지 참조 횟수를 증가시킨다.
STEP 8. 접속자가 참조를 요구하는 페이지에 대한 접근을 허용하고, 그 결과를 분석데이터베이스에 저장한다.

## 4. 실험 및 평가

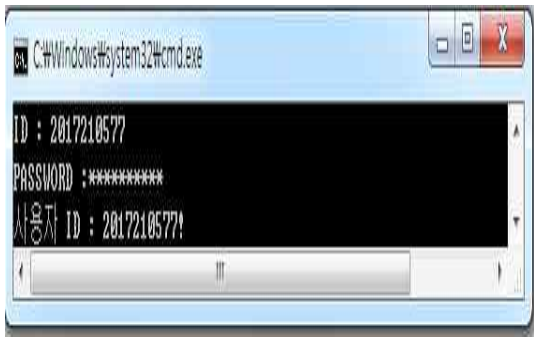
본 논문에서 제안하는 트레이스 백 정보에 기반한 매크로 공격 탐지를 위한 시뮬레이션 환경은 다음과 같다. 사용된 응용소프트 웨어는 Visual S-tudio 017, 구현 언어는 C++를 사용하 였다. 시뮬레이션을 위한 운영체제는 Windows7 Ultimate K 32비트이고, 시스템 사양은 4GB 메모리를 채택한 2Core(TM)i5 2.60Ghz System으로 구성하였다. 아울러 본 논문의 실험을 위하여 특정 웹사이트의 접속과 차단 과정에 대한 결과 확인을 위하여 와이어샤크 2.0을 사용하였다.

다음 (그림 2)는 본 논문의 실험을 위하여 인터넷 상의 특정 홈페이지에 대한 정상 사용자 정보를 이용하여 로그인 한 결과를 와이어샤크를 실행하여 획득한 결과이다. (그림 2)에서 정상적인 접속이 완료되면 접속자의 로그인 정보와 패스워드를 획득할 수 있다.



(그림 2) 사용자 로그인 상태

다음 (그림 3)은 사용자 아이디 '2017210577'인 사용자가 인터넷 상에 존재하는 특정 웹 페이지에 대한 접속을 시도할 경우 로그인 과정에서 수집 가능한 초기 정보를 나타낸 것이다. 본 논문에서는 해당 정보를 이용하여 '2017210577'인 사용자의 블랙리스트 여부에 대한 1차 분석을 수행한다.




(그림 3) 사용자 로그인 정보

(그림 4)는 사용자 아이디 '2017210577'인 사용자가 분석데이터베이스에 블랙리스트로 등록되어 있을 경우 이를 차단한 결과를 보여주는 것이다.

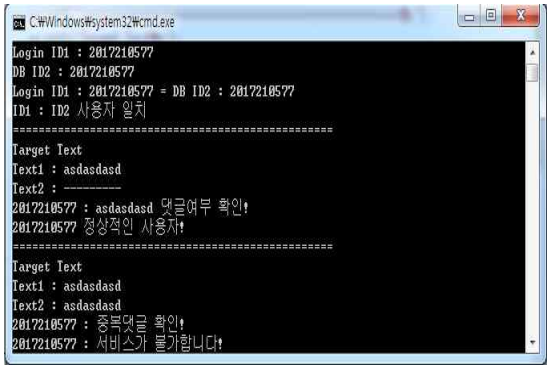

(그림 4) Black_List 분석 결과

(그림 5)는 '2017210577'인 사용자가 블랙리스트가 아닐 경우 첫 번째 트레이스 백 정보를 수집하는 과정을 나타낸 것이다. 이는 동일 사용자가 특정 웹 페이지에 대하여 재접속을 시도할 경우 동일 아이디 여부와 접근 경로 분석을 위한 정보이다.


(그림 5) ID/Tr분석 과정

(그림 6)은 '2017210577'인 사용자의 ID와 트레이스 백 정보를 분석한 후 동일 아이디 사용자의 표적 페이지 접속 여부를 분석하고 차단하는 과정을 나타 낸 것이다.

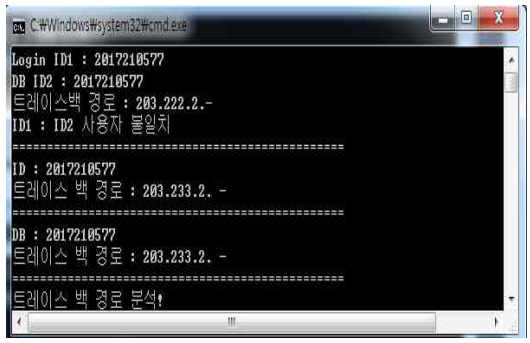
.




(그림 6) 동일 ID에 대한 표적 페이지 접근분석 과정

(그림 6)은 동일 사용자가 표적 페이지가 아닌 다른 웹 페이지를 참조할 경우 이에 대한 서비스 수행 과정을 보이는 것이다.

(그림 7)은 사용자 아이디 '2017210578'인 새로운 사용자가 신규 접속을 시도한 경우, 이를 새로운 사용자 아이디로 판정하고 분석한다. 그 다음 신규 접속 아이디이면서 접근 경로 정보가 분석데이터베이스에 존재하지 않는 새로운 경로이면 표적 페이지에 대한 정상적인 서비스를 허용하는 과정을 보이고 있다.

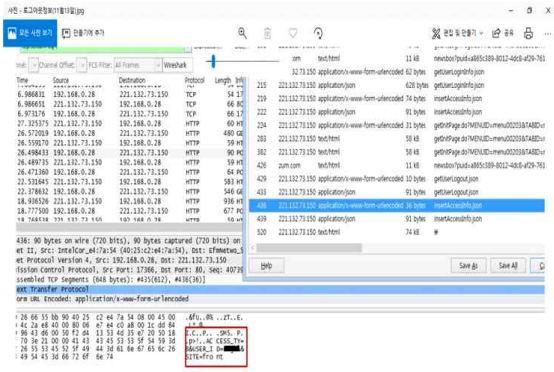



(그림 7) 상이한 ID에 대한 표적 페이지 접근분석 과정

(그림 8)은 표적 페이지에 대하여 동일 경로 정보를 이용하면서 상이한 아이디의 접근이 발생할 경우 이에 대한 대응 과정을 나타낸 것이다. 이는 동일인이 다수의 아이디를 생성한 후 이를 이용하여 매크로 공격을 시도하는 경우로 가정할 수 있다. 그렇지만 이러한 경우는 동일 지역에서 정상적인 접근일 경우도 존재하기 때문에 이에 대한 대응 과정도 필요하다. 본 논문에서는 임의의 임계 카운트 값을 설정한 후 해당 임계 카운트 이상의 표적 페이지에 대한 참조가 발생할 경우 동일 지역에서 일정 횟수 이상의 참조를 할 수 없도록 하였다.


(그림 8) 임계 카운트 분석 후 차단 과정

(그림 9)는 와이어샤크를 실행하여 블랙리스트 또는 동일인의 표적 페이지에 대한 2회 이상 접속이거나, 임계 카운트를 초과하여 해당 접속자를 차단했을 경우 접속자 정보의 변화를 보이는 것을 나타내고 있다.



(그림 9) 접속자 차단 후 상태

## 5. 결 론

본 논문은 빠르게 발전하고 있는 네트워크 환경에서 다양한 정보 공유 과정 중 언제든지 발생 가능한 정보의 왜곡된 전달을 방지하는데 그 목적이 있다. 정보통신 기술은 4차 산업혁명의 핵심 기술로 4차 산업혁명의 성공여부는 정보의 정확한 전달에 있다고 할 것이다. 그러므로 모든 분야에 있어 정보의 정확한 전달은 필수적이라고 할 수 있다. 특히 다수의 사용자들이 실시간으로 접속하고 있는 포털 서비스에서 생산되는 정보들은 특정 이해당사자의 불법적 조작에 의한 왜곡 없이 해당 정보의 요구자들에게 정확한 전달이 이루어져야한다. 본 논문은 특정 정보에 대한 이해당사자 상호 불법적인 조작에 일반적으로 사용되는 매크로 공격에 대한 탐지 모델을 제시한 것이다.

아울러 본 논문의 탐지 모델은 네트워킹 과정에 필수적으로 존재하는 라우터들의 경유 정보를 기반으로 동일 사용자 다중 접속 및 다중 IP를 이용한 특정 웹페이지에 대한 매크로 공격을 탐지한 후 차단할 수 있도록 설계한 것이다. 향후 연구 과제로는 다지점에서 매크로 공격을 시도할 경우 이를 탐지하고 차단할 수 있는 연구가 진행되어야 할 것이다.

## 참고문헌


[1] Telecommunication Technology Association 2008. *Botnat trend and respond technology present*, TTA Journal, 118(Special Report) : 58-65.

[2] W. I. Kim, S. H. Yoo, Y. C. Jang and C. H. Lee, "A Design and Implementation of Abnormal Permission-Flow Detecting Security Module", J. of Korean Institute of Next Generation Computing, Vol.10, No. 2, pp 66-74, 2014.

[3] J.z. Li, and X.M. Liu *An important aspect of big data : Data usability,* School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150 00 1, pp. 1147~1162, 2013.

[4] Y, H. Jung, "A Study of the Android OS -based touch macro detection method", Korea Univ., 2016.

[5] Y. L, S. B. Kim, J. H Park, and J. M. Bae, "An Encrypted Response Model using Application Access Failure information for the Attack of IP Spoofing in a Cloud Computing Environment", KKITS, Vol. 10, No. 6, pp. 643~651, 2015.

[6] K. J. Kim, S. J. Lee, "A study on macro detection using information of touch events in Android mobile game environment", Journal of the Korea Institute of Information Security and Cryptology, Vol. 25, No. 5, pp. 1123-1129, 2015.

[7] Blum,M.;Ahn,L,V.;Langford,J,The CAPTCHA Project,"Completely Automatic Public Turing Testto TellComputers and Humans Apart," www.captcha.net,Dept.ofComputerScience,Carnegie-MellonUniv.2000.

[8] C. H, An, H. C. Baek, Y. G. Seo, W. C. Je ong, and S. B. Kim. "Designing Mutual C ooperation Security Model for IP Spoofing Attacks about Medical Cluster Basis Big Data Environment", Convergence security journal, Vol. 16, No. 7, pp. 21-29, 2016.

[9] M. H. Kim, H. C. Baek, S. Y. Hong and. H. Park "An Encrypted Service Data Mo del for Using Illegal Applications of the Government Civil Affairs Service under Big Data Environments", Convergence se curity journal, Vol. 15, No. 7, pp. 31-38, 2015.

[10] 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, 2015.

[11] C. H. An, "Medical treatment cluster co mposition and security model design of r egional public hospitals in Korea for tele medicine", Gyengsang Univ., 2016.

[12] H. B. Lim, W. H Kim, S. J. Kim, "Using Image Visualization Based Malware Dete ction Techniques for Customer Churn Pr ediction in Online Games", KSCI., Vol. 2 77, No. 6, pp. 1431-1439, 2017.

[13] Y. J. Choi, "Saliency map object extracti on method for breaking image-based CA PTCHA", Korea Univ., 2016.

[14] W. S. Yang, "Emerging Imge Cue CAPT CHA Resisting Automated and Human-S olver-Based Attacks", Yonsei Univ., 2017.

## 〔저자소개〕


백 용 진(Yong-Jin Baek)
2015년 2월 경남과학기술대학교
컴퓨터공학과 학사
2017년 11월 경상대학교
컴퓨터과학과 석사 과정

email : qhanffkwk@nate.com

홍 석 원 (Suk-Won Hong)
2003년 2월 경남과학기술대학교
컴퓨터공학과 학사
2006년 2월 경상대학교
컴퓨터과학과 석사
2011년 2월 경상대학교
컴퓨터과학과 박사
1999년 4월 ~ 현재 : 경남도립
거창대학

email : swhong@gc.ac.kr

박 재 흥 (Jae-Heung Park)
1978년 2월 충북대학교
수학교육과 학사
1980년 9월 중앙대학교
전자계산학과 석사
1989년 8월 중앙대학교
전자계산학과 박사
1984년 4월 ~ 현재 : 경상대학교
교수

email : pjh@gnu.ac.kr

강 경 원 (Gyeong-Won Kang)
1984년 2월 중앙대학교
전자계산학과 학사
2003년 8월 동아대학교
산업공학과 박사

1997년 ~ 현재 : 진주보건대학
보건행정과 교수

email : aragon4u@hanmail.net

김 상 복 (Sang-Bok Kim)
1979년 2월 중앙대학교
전자공학과 학사
1981년 2월 중앙대학교
전자공학과 석사
1989년 2월 중앙대학교
전자공학과 박사
1984년 3월 ~ 현재 : 경상대학교
교수

email : sbkim@gnu.ac.kr