보안관제 위협 이벤트 탐지규칙 표준 명명법 연구

박원형* · 김양훈* · 임영환** · 안성진***

요 약

최근 해킹과 악성코드 등 사이버 공격기법은 매우 빠르게 변화 발전하고 있으며 그에 따른 사이버공격 기법이 다양해지고 지능화된 악성코드의 수가 증가하고 있다. 악성 코드의 경우 악성 코드의 수가 급격하게 증가함으로서 분류나 이름의 모호함으로 인해 악성코드에 대처함에 있어 어려움이 있다. 본 논문은 이러한 문제점을 해결하기 위해서 국내에 있는 백신업체들의 명명규칙을 조사·분석하고 이를 기반으로 현재까지 나온 탐지규칙의 패턴을 비교 분석해 보안관제 이벤트 탐지규칙에 적합한 명명규칙을 제안 한다.

Naming Scheme for Standardization of Detection Rule on Security Monitoring Threat Event

Wonhyung Park* · Yanghoon Kim* · YoungWhan Lim** · Sungjin Ahn***

ABSTRACT

Recent, Cyber attacks such as hacking and malicious code techniques are evolving very rapidly changing cyber attacks are increasing, the number of malicious code techniques vary accordingly become intelligent. In the case of malware because of the ambiguity in the number of malware have increased rapidly by name or classified as malicious code may have difficulty coping with. This paper investigated the naming convention of the vaccine manufacturers in Korea to solve this problem, the analysis and offers a naming convention for security control event detection rule analysis to compare the pattern of the detection rule out based on this current.

Key words : SNORT, IDS, IPS, Security Monitoring, Threat Event, Naming Scheme, Standardization

접수일(2015년 6월 2일), 수정일(1차: 2015년 6월 30일),
게재확정일(2015년 6월 30일)

* 극동대학교 사이버안보학과, 1저자
** 현대오토에버 인프라수행팀
*** 성균관대학교 컴퓨터교육학과, 교신저자

1. 서 론

최근 해킹, 악성코드 제작 유포 등 사이버 공격기법은 매우 빠르게 변화 발전하고 있으며 그에 따라 사이버공격 기법이 다양해지고 지능화된 악성코드의 수가 증가하고 있다. 악성 코드의 경우 악성 코드의 수가 급격하게 증가함으로서 분류나 이름의 모호함으로 인해 악성코드에 대처함에 있어 어려움을 겪었다. 그리고 각기 다른 방식으로 진단명을 부여함으로서 일관성이 없고 혼란스러워지는 문제를 초래하였고 한 회사에서 여러 백신을 프로그램을 사용할 경우 같은 악성 코드를 다르게 불러 혼란이 발생 할 수 있었다. 그래서 각 백신업체는 분류체계는 상이하지만 자신들의 고유의 악성 코드 명명법을 정해 악성코드의 이름을 지어내고 있다.

악성코드의 경우 각 백신업체들이 자신들의 고유 악성코드 명명법을 가지고 있어 현재 각 업체별로 악성코드에 대한 명명법이 나와 있지만 탐지패턴에 대한 구체적인 탐지규칙 명명법이 없는 실정이다. 본 연구에서는 이러한 문제점을 해결하기 위해서 국내에 있는 백신업체들의 명명규칙을 조사·분석하여 탐지규칙의 패턴을 비교 분석해 탐지규칙에 적합하고 명확한 표준화된 규칙을 제안 한다.

2. 관련연구

2.1 국내 안티바이러스백신 업체 명명법

2.1.1 Ahnlab 악성 코드 명명법

초기 Ahnlab의 설립자인 안철수 박사는 V3에서 Caro 악성 코드 명명법에 맞춰 진단명을 변경하였다. 하지만, 1990년대 중 후반 매크로 악성코드, 윈도우 악성 코드, 스크립트 악성코드 등 새롭게 등장하는 유형의 악성코드를 표현할 수 없는 문제가 발생했다. 현재 Ahnlab은 사용중인 악성코드 명명법이 약 10년 전쯤에 만들어져 스파이웨어 등의 새로운 유형 및 악성코드 길이가 증가하면서 악성 코드 길이를 나타내는 숫자가 더 이상 불필요한 문제가 발생한다.

이로 인해 Ahnlab은 기존 명명법을 보강한 새로운 명명법을 내놓았는데 이는 다음과 같다.

<표 1> 최초 Ahnlab 악성 코드 명명법

접 두 어(플랫폼)	이 름(종류)	접 미 어(변형)
Win 32	Goner	Worm

플랫폼은 이전과 동일하게 사용한다. 악성코드의 가장 큰 특징을 나타내 는 종류는 Adware, AppCare, Packer, Spyware, Trojan, Virus, Worm을 사용하며 이는 윈도우 실행 파일(Win32, Win64)와 리눅스에만 구분된다. 즉, 스크립트, 매크로 등 다른 플랫폼은 종류를 구분하지 않는다. 추천 이름은 유사 특징을 가진 유형을 정리한 것으로 분석가에 따라 다 른 이름을 정할 수 있다. 상세 이름은 악성코드 추천 이름에서 별도 구분이 필요하다고 판단 될 때 사용한다.

<표 2> 정보 변형

정보변형	설 명
Generic	포괄적진단(Generic detection)으로 여러 변형에 대해 한번에 진단함.
Suspicious	의심스러운(Suspicous) 진단으로 확인을 위해 샘플을 접수 받아야 함.
Variant	여러변형(Variant)에 대한 하나의 진단명 (매우 많은 변형이 존재할 때 사용하며 사용이 제한적)

단, 여러 Generic 이름이 올 수 있으므로 이때는 이름에 숫자를 붙인다.

ex) Win32-Worm/IRCBot.Generic
Win32-Worm/IRCBot1.Generic

새로운 명명법을 기존 명명법과 비교하면 다음 표와 같다. 악성코드의 경우 사이즈가 붙는데 예에서는 편의상 12345로 통일했으며 새로운 명명법의 변형도 A로 통일 했다[1].

2.1.2 잉카인터넷 악성 코드 명명법

잉카인터넷에서는 악성코드 종류를 접두어로 표시

하는데 악성코드의 종류는 다른 업계와 유사하였으나 Trojan 유형의 악성코드를 조금 세분화 하여 분류한다. <표 3>는 잉카인터넷 악성코드 명명법의 기본 형태를 보여 준다.

<표 3> 잉카인터넷 악성코드 명명법[2][8]

[접두어]/플랫폼.[악성코드 명].[악성코드의 크기].[변형정도]	
접두어	악성코드의 분류
플랫폼	플랫폼이 정확하지 않은 경우 생략 가능
악성코드명	유사한 기능을 가진 악성코드를 분류하기 위한 이름
악성코드 크기	악성코드의 파일 사이즈
변형정도	경우에 따라 생략 가능
예시	Trojan/Win32.Badvirus.12345.A

2.1.3 하우리 악성 코드 명명법

하우리에서는 기존에 사용하여 오던 명명법에 대하여 보완・수정하여 새로운 바이러스 명명규칙을 마련하여 사용하고 있다. 새로운 바이러스 명명 규칙은 “형태(Type), 이름(Name), 변형정도(A, B, ...), 크기(Size)”의 형태로 기존의 명명 규칙에서 플랫폼(OS)과 형태(TYPE)를 같이 사용하여 형태(TYPE)로 바꾸어 표현하였다. <표 4>는 하우리의 악성 코드 명명법의 표현을 보여준다.

<표 4> 하우리 악성 코드 명명법[3]

접 두 어	이 름	접 미 어
I-Worm	Win32	Goner

2.2 해외 안티바이러스백신 업체 명명법

2.2.1 CARO 악성코드 명명법

CARO(Computer Anti-virus Research Organization)는 유럽을 중심으로 한 안티-바이러스단체로써, 악성코드에 대한 명명 규칙을 1991년에 제정하였다. 이 단체에서 제시하는 전체적인 악성 코드의 구성은 Family_Name, Group_Name, Major_Varient, Minor_Varient의 4부분으로 이루어져있으며, 각 부분은‘.’으로 구분한다. 각 부분은 대문자와 소문자, 숫자0~9, 그리고 특수문자들을 사용하여 명명하고, 글자 수가 20글자 이상일 경우에는 가급적 짧은 이름을 정한다. 초기에 모든 백신업체에서 이 기준에 기반을 두고 분류 및 명명을 해왔다[4][8].

그런데, 그 기준은 예전의 도스에 기반을 두고 있어 현 실정에는 부적절한 부분이 많다. 그래서 일부업체는 이 기준을 따랐지만 새롭게 등장하는 다양한 악성 코드를 표현할 수 없는 문제가 발생하였고 현재는 각 회사별로 나름대로의 분류지침 및 명명법을 만들어 사용하고 있다. 그리고 이러한 문제를 해결하기 위해서 닉 피츠제랄드(Nick Fitzgerald)는 2002년 AVAR 컨퍼런스에서 새로운 명명법을 마련하였다.

2.2.2 시만텍 악성 코드 명명법

시만텍의 악성 코드 명명법의 기본적인 구성은 “접두사・이름・접미사”의 형태로 이루어져 있으며, 도스형 악성 코드에서는 보통 접두사를 포함하지 않는다. 접두사는 악성코드가 복제되거나 또는 특성의 표시이며, 이름은 널리 사용되는 패밀리네임을 의미한다. 접미사는 같은 패밀리네임을 구별지어주고 악성코드의 크기를 표시하여준다. <표 5>는 시만텍의 악성 코드 명명법의 한 예를 보여준다[6][7].

<표 5> 시만텍 악성 코드 명명법

접 두 어	이 름	변형	접 미 어
W32	Goner	A	@MM

2.2.3 맥아피 악성코드 명명법

맥아피의 악성코드 명명법은 다음 <표 6>와 같이 접두어, 이름, 접미사가 표현된다. 접두어는 악성코드의 특성을 표시하며, 이름은 신종 바이러스로서 구분짓는 일련의 특징을 가진 패밀리 네임을 의미하고 접미사는 변종을 지정하거나 추가정보를 표시한다[2].

<표 6> 맥아피 악성코드 명명법

접 두 어	이 름	접 미 사
W32.	BadVirus	a

3. 보안관제 탐지규칙 표준화 명명법

3.1 국내 IPS 탐지 규칙

3.1.1 윈스(주) 스나이퍼

윈스(주)社의 스나이퍼 IPS는 국내 IPS 시장 1위 제품으로 시스템 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 실시간 탐지, 분석 후 비정상으로 판단된 패킷을 차단해 보다 안정적인 네트워크 보안 기술을 제공하는 침입방지시스템(IPS) 이다. 아래 <표 8>는 스나이퍼 IPS 탐지 규칙에 대한 분류 현황이다.

<표 8> 스나이퍼 IPS 탐지 규칙 현황

항목	분류키워드	개수
Backdoor	Poison Ivy, WebShell, Web Shell	178
Trojan	Banker, Bredolab, Downloader, Dropper, Exploit, FakeAlert, Harebot, Oficla, Pushdo, Spambot, Waledac	307
DDoS	DDoS	68
DoS	Denial, Remote Code, Remote Command, BoF, overflow, Exhaustion, Corrupt, Arbitrary, Arbitary, Format String, Code, Overlfow, Overrun, remote exec, Remote cmd exec	741
Worm	Dumaru, Enigma, IRCBot, Mytob, Nimda, Prolaco, Sality, Spybot	477
Malware	Arp Spoofing Tool	14
Protocol_Vulnerability	FTP, HNAP, HTTP, NetBIOS, Remote Desktop, RPC, search-ms, SMB, SMTP, SSH, SSL, TCP-445, TELNET, WebDAV, WINS	74
Web_access	Apache, ASP, Certificate, CSRF, Cross, Disclosure(Web), JSP, PHP, RFI, Remote File Inclusion, Source Code, Struts, Web server vulnerability, WordPress, XML, XSS	448
Access_attempt	Access, Injection, IIS Unicode vulnerability, rlogin, tftp -i	173
Scan		15
Information	/etc/, login, msg, passwd, password	268
기타		189
계		2952

3.1.2 코닉글로리(주) TESS TMS

코닉글로리(주)社의 TESS TMS는 주로 국가·공공기관에 납품되는 IPS 장비로 인터넷 웜, 바이러스, 해킹 등 사이버 위협에 대한 조기 탐지, 예경보, 관제 및 분석을 통한 피해 확산 방지 및 완화를 위한 사이버 위협에 대한 종합 관제 및 대응하는 침입방지시스템(IPS) 이다. 아래 <표 9>는 TESS TMS 탐지 규칙에 대한 분류 현황이다.

<표 9> TESS TMS 탐지 규칙 현황

항목	대표 탐지 이벤트 명
Access_attempt	rservice rlogin root
	mssqlsp_delete_alert
Backdoor	backdoor Boat v1.0 - Flood attack
	backdoor access title response
Keylogger	smtp Ardamax Keylogger 2.71 SMTP Log
	http Computer Keylogger
Malware	trojan dropper/Malware.34304.AR file download
	malware MS06-040 W32.Randex.GEL forum.ednet.es dns lookup
Trojan	trojan andriod FakeKakaoTalk
	backdoor RAT trojan_nunks_login
DDoS	http ddos script get request 3
	DDoS perfecttool simulated open attack
DoS	MS Windows SMTP Service DOS exploit - MS10-024
	http Novell iManager Tomcat HTTP POST Request Handling DOS
Information	P2P BitTorrent - DHT ping
	P2P SkyPe - client login
Scan	icmp ping Httprint scan
	icmp ping X-scan scan

Protocol_Vulnerability	MSSMB2Negotiateprotocolrequestremotecrash
	MicrosoftWSDAPIremotecodeexecutionattempt
Worm	worm W32.Flamer propagation activity
	worm W32.Disttrack malicious communication
Web_access	Adobe Reader and Acrobat CVE-2014-8452 XML External Entity Information Disclosure Vulnerability
	Microsoft Internet Explorer XSS Filter CVE-2014-6365 Security Bypass Vulnerability

3.2 해외 IPS 탐지 규칙

3.2.1 IBM(주) Security SiteProtectorTM

IBM(주)社의 Security SiteProtectorTM 는 전 세계 시장점유율 1위 제품으로 네트워크, 서버 및 Desktop Endpoint Security 에이전트와 소형 네트워크나 어플라이언스를 위한 관리 및 분석을 통합하는 중앙 집중된 관리 시스템이다. 또한, SiteProtector를 쉽게 확장하여 대형 엔터프라이즈 전반의 환경을 위한 보안을 제공할 수 있다.

<표 10> Security SiteProtectorTM 탐지 규칙 현황

항목	분류키워드	개수
Backdoor	SNMP, Request, HTTP	30
DDoS	UDP, DNS, IRC, FLOOD, HTTP	14
DoS	HTTP, FLOOD, SMTP, KERBEROS, ORACLE, EMAIL, SSL, PING, ICMP	333
COMMAND AND CONTROL	HTTP, CnC, POST	22
Content Analyzer	EMAIL, User Defined	24
Cross-Site Scripting	HTTP, PHP, Script, Apache	49
SQL Injection	HTTP, GET, POST, SQL, SELECT	28
Instant Messenger	HTTP, IRC, JOIN, LOGIN	54
Peer to Peer	BitTorrent, Edonkey, Download, HTTP	39
Rootkits	Linux, Solaris, Login	8
Scada	DNP, Overflow, Modbus	33
Voice Over Internet Protocol	SIP, CISCO, Transmission, Name, Overflow, DOS	68
계		702

4. 국내외 IPS 보안장비 탐지 규칙 명명법 비교분석

위 내용들을 살펴보면 각 IPS에서 사용하는 탐지규칙에 대한 항목이 상당부분 유사한 것을 확인할 수 있다. 즉,

아래 <표 11>에서 서로 비교하여 살펴보면, 국내 두 업체는 큰 항목에 대해서는 공통된 것을 확인 할 수 있다. 하지만, IBM社의 탐지규칙에 다소 차이가 있었다.

<표 11> 국내외 IPS 탐지 규칙 공통 항목 비교

스나이퍼	TESS TMS	Security SiteProtectorTM
Access_attempt	Access_attempt	SQL Injection
Backdoor	Backdoor	Backdoor
Keylogger	-	-
Malware	Malware	-
Trojan	Trojan	-
DDoS	DDoS	DDoS
DoS	DoS	DoS
Information	Information	Peer to Peer
Scan	Scan	-
Protocol_Vulnerability	Protocol_Vulnerability	-
Worm	Worm	-
Web_access	Web_access	Cross-Site Scripting

IBM社의 탐지규칙은 Access_attempt 부분이 SQL Injection 공격 기법으로 분류되어 있으며, Web_access 부분은 Cross-Site Scripting 해킹 기법으로 분류되어 있다. Information 부분도 P2P로 분류되어 있어 IBM社의 탐지규칙은 좀 더 구체적으로 표현되어 있는 반면, 국내 탐지규칙 명명 분류는 좀 더 큰 개념으로 포괄해서 설명하고 있다.

또한, Scada, Voice Over Internet Protocol 항목은 전 세계적으로 이슈가 되고 있는 항목을 구체적으로 큰 항목으로 분류한 반면, 국내에서는 이러한 분류가 기타부분으로 설정되어 있다.

<표 12>은 국내외 IPS 탐지 규칙의 이름을 비교한 것이다. 아래와 같이 탐지 규칙에 대한 이름이 비슷한 구조로 되어 있지만, 전체적인 부분은 대분류 항목과 소분류 항목이 다른 경우가 많았다. 또한, 각 업체별로 기준이 되는 명명법이 없는 것으로 조사 되었다.

<표 12> 국내외 IPS 탐지 규칙 이름 비교

스나이퍼	TESS TMS	Security SiteProtectorTM
TFN2K DDoS Attack (ICMP Flooding)	icmp ping X-scan scan	ICMP_Flood
rlogin Remote Authentication Bypass	rservice rlogin root	Rlogin_Login
-	P2P BitTorrent - DHT ping	BitTorrent_DHT_Ping

현재까지 분석한 결과 국내외 IPS/IDS 탐지규칙을 통해 발견된 악성코드나 해킹 프로그램의 종류를 나타내는데 표시할 때 11가지 대표적인 분류키워드로 분석되었다. 그리고 세부적인 IPS/IDS 장비의 이름을 입력하고 싶을 시에는 세부적인 해킹 도구의 이름을 나타내도 된다. 이름(Family name)은 탐지를 통해 발견된 악성코드의 널리 알려진 이름(Family name)을 사용해야한다. 여기서 Family name은 유사한 기능을 가진 악성코드를 분류를 통해 생성되어진 이름이다. 이름과 상세이름은 '.'로 구분하고 이름은 첫 글자만 대문자이고 나머지는 소문자로 한다. 여기서 상세 이름은 악성코드 추천 이름에서 별도 구분이 필요하다고 판단 될 때 사용한다. 하지만 문제점은 악성코드의 이름이 회사 제품군에 따라 다르기 때문에 혼돈을 피하기 위해서는 공통 코드에 대한 기준명이 필요하다. 그래서 여기서는 바이러스토탈[5]에서 제시하는 악성코드로 공통된 이름으로 작성하고 알려지지 않은 악성코드가 탐지시에는 악성코드를 위 사이트에 등록을 하여 악성코드 명에 대한 체계도를 확립해야 한다. 그리고 악성코드의 명을 입력한 후 악성코드의 특징이나 정보를 간략하게 써주거나 악성코드가 작동하는 기능에 대해서 표시해줄 수 있는데 생략해도 상관없다. 마지막으로 변형이나 버전 정보는 탐지규칙을 통해 발견되는 악성코드가 변형되어 있는 경우가 많은데 대부분의 악성코드 명의 경우 악성코드의 이름 뒤에 변형 혹은 버전정보를 표시 해 준다. 그래서 탐지규칙 명에서는 악성코드 명 뒤에 통일 된 분류 표시를 해 준다. 여기서는 앞에 버전을 의미하는 Ver을 이용해 '.'을 찍어준 다음 변형이 탐지되는 순에 따라 숫자순으로 표시 한다. 하지만 변형된 악성코드가 기존의 악성코드와 특별히 다른 기능을 하지 않은 것을 제외 할 수 있다.

<표 13> 탐지규칙 명명법 표준 제안

	①대분류	②공격형태	③악성코드/해킹명	④변종/버전
1	Backdoor	prorat	BA	-
Backdoor-prorat-BA				
2	Malware	rat(drat)	Gen	Ver.1
Mareware-rat(drat)-Gen(shell)-Ver.1				
3	Malware	rat(darkcomet)	Comet	Ver.3
Mareware-rat(darkcomet)-comet(health)-Ver.3				

5. 결 론

앞서 연구한 악성코드 명명법과 기존 IPS의 탐지 규칙 현황에 대한 조사를 통해 악성코드는 각 업체별로 명명법이 상이한 것으로 확인이 되나, 국내 업체은 분류항목이나 명명법이 유사한 것으로 확인 되었다. 하지만, 세부 탐지 규칙에 따른 공격 이벤트 명은 공통된 것이 없는 상황이다. 결국 이러한 명명법은 표준화하기 상당히 어려운 실정이며 이러한 상황에서 표준화를 하기 위해 몇가지 전제조건이 필요로 한다.

이러한 이유로 악성코드나 해킹공격의 탐지 규칙 이름을 정할 때 해당 악성코드 이름이 업체별로 다르기 때문에 전반적인 탐지조건을 추후에 확인하면 공동으로 수집되는 경우가 있지만 세부 내역은 조금 다를 수도 있다. 따라서, 알려진 코드에 대해서는 공통 코드명에 대한 기준이 필요하며 알려지지 않은 악성코드에 대해서는 분류나 패턴 생성 명명 시 코드에 대한 체계도를 확립하여 제시할 필요가 있다. 그리고 악성코드를 수집해서 패턴을 생성 시 생성 후에 바이러스토탈(www.virustotal.com:해외악성코드수집분석) 같이 유사한 사이트를 구축하여 소스와 패턴명을 지정해줄 필요가 있다. 그래서 국가기관을 중심으로 보안관제협의체를 운영하여 탐지 규칙에 대한 공통의 명명법을 회의를 통해 결정하여 공동으로 운영되는 악성코드 및 취약점 DB가 있어야 된다. 이를 위해서는 외부기관이 아닌 국가기관에서 패턴 등록 절차와 탐지규칙에 대한 규정을 만들어야 한다.

참고문헌

[1] Ahnlab 악성코드 명명법, "Asec Report" 안철수 연구소에서 발행하는 월간보안보고서 Volume 11, 2009년

[2] 이학용, "침해사고 초기대응 시간 단축을 위한 악성코드 명명 규칙 연구 : 제한된 다수의 네트워크 환경에서 발생한 악성코드 침해사고에 대하여", 숭실대학교 정보과학대학원 석사논문, 2014년 8월

[3] 최준호, 곽효승, 공현장, 김판구, 이병권, 오은숙, "악성 코드 분류 및 명명법에 관한 연구", 정보과학회지 20권 11호, p 24-29, 2002년

[4] MS Malware Protection Center, CARO 악성 코드 명명법, http://www.microsoft.com/security/portal/mmpc/shared/malwarenaming.aspx, 2014년

[5] 바이러스토탈, http://www.virustotal.com, 2014년

[6] 임을규, 악성코드 유형에 따른 자동화 분석 방법론 연구, 한국인터넷진흥원 연구보고서, p35-38, 2009년6월

[7] 시만텍, 모바일 애드웨어 및 악성코드 분석 보고서, http://www.symantec.com/ko/kr/about/news/release/article.jsp?prid=20131114_01, 2013년

[8] 잉카인터넷 안티바이러스 명명법,http://www.nprotect.com/popup/virus_info/name.html, 2007년 12월

[9] 컴퓨터 바이러스 이름 명명법, http://tip.daum.net/openknow/38968640, 2006년

[저 자 소 개]

박 원 형 (Wonhyung Park)

2002년 서울과학기술대학교 산업정보시스템공학과 공학사
2005년 서울과학기술대학교 정보산업공학과 공학석사
2009년 경기대학교 정보보호학과 이학박사
2015년 성균관대학교 컴퓨터교육학 박사수료
현재 극동대학교 사이버안보학과 교수/학과장

E-mail:whpark@kdu.ac.kr

김 양 훈(Yanghoon Kim)

2005년 대진대학교 컴퓨터공학과 공학사
2007년 대진대학교 컴퓨터공학과 공학석사
2011년 대진대학교 소프트웨어공학 공학박사
2012년 ~ 2013년 : 상명대학교 소프트웨어&미디어 연구소 박사 후 연구원
현재 극동대학교 사이버안보학과 조교수

E-mail:yhkim@kdu.ac.kr

임 영 환 (YoungWhan Lim)

2014년 서울과학기술대학교
IT정책대학원 산업정보시스템전공
박사수료
현재 현대오토에버 인프라수행팀 과장

E-mail:yhlim@seoultech.ac.kr

안 성 진 (Seongjin Ahn)

1988년 2월 성균관대학교
정보공학과 공학사
1990년 2월 성균관대학교 대학원
정보공학과 공학석사
1998년 8월 성균관대학교 대학원
정보공학과 공학박사
현재 성균관대학교 컴퓨터교육학과
교수

E-mail:sjahn@skku.edu