http://dx.doi.org/10.14400/JDC.2015.13.4.235

실시간 해킹, 탐지 및 추적관리 ICT 융합 보안 솔루션 시험평가

김승범*, 양해술**
호서대학교 벤처대학원 정보경영학과 박사과정*, 호서대학교 벤처대학원 정보경영학과 교수**

Real-time hacking, detection and tracking ICT Convergence Security Solutions Test and Evaluation

Seung-Bum Kim*, Hae-Sool Yang**
Doctor Course, Dept. of Information Management, Graduate School of Venture, Hoseo University*
Professor, Dept. of Information Management, Graduate School of Venture, Hoseo University**

요 약 최근 다양한 불특정 다수의 해킹 및 반복되는 DDoS 사이버테러 공격을 이해하고, 그 해결책을 비로소 공격 기법에서 찾을 수 있었다. 공격자와 방어자, 공격 기법과 방어 기법의 접목이라는 자유로운 연구 방식은 항상 엉뚱함에서 가능성을 발견해가는 도전이라 할 수 있다. 본 논문에서는"KWON-GA"라는 세계적인 화이트 해커들 개발진이 오랜 경험의 침투 및 진단을 통해, 공격이 최상의 방어라는 미명하에 방어의 목적으로 구현된 지식 정보 보안 솔루션을 고객이 운용 중인 시스템 환경에 맞추어 필요한 기술을 적용하는 커스터마이징 정책으로 맞춤 솔루션을 제공할 수 있으며, 독창적인 원천기술로 처리되어 탐색이 불가능하고 내부적으로 유출되는 경우에도 분석이 되지 않아 해커에게 분석되어 취약점을 노출하거나 해킹의 수단으로 악용되지 않는 ITC융합 보안 솔루션을 시험평가 하였다.

주제어 : ICT융합, 지식정보보호, KWON-GA, 침투 및 진단, 독창적 기술

Abstract Understanding the various unspecified hacking and repeated cyber DDoS attacks, finally was able to find a solution in the methods of attacks. Freely researching approach that combines the attacker and defender, offensive and defensive techniques can be called a challenge to discover the potential in whimsy. In this paper we test and evaluate "KWON-GA", global white hackers team has made by many years of experiences in infiltration and diagnosis under guise of offence is the best defence. And it is knowledge information ICT Convergence security solution which is developed for the purpose of defence, it provide customization policy that can be fit to customer's system environment with needed techniques and it is processed with unique proprietary technology so that it's not possible to scan. And even if it has leaked internally it's impossible to analyze so hackers can't analyze vulnerability, also it can't be abused as hacking tools.

Key Words : ICT Convergence, Knowledge and Information Protection, KWON-GA, penetration and diagnostics, unique technology

* 이 논문은 2015년 ITC융합일환으로 본 제품을 생산한 CUVEPIA와 기업(금융) 및 공공기관의 적용가능성을 연구하였음
Received 18 February 2015, Revised 20 March 2015
Accepted 20 April 2015
Corresponding author: Hae - Sool Yang (Graduate Venture, Hoseo)
Email: hsyang@hoseo.edu

ISSN: 1738-1916

1. 서론

지금 지구촌은 폭발적인 인터넷사용으로 정보화물결 속에 넘쳐나는 정보를 어떻게 관리하고, 서비스 하면 고객의 정보유출을 예방할지 보안의 중요성을 고민하고 연구에 몰두 하고 있다. 어딘가에서 누군가가 유/무선을 통해 우리가 생산한 정보를 해킹, DDos 공격등 다양한 사이버테러를 하고 있을 것이란 의문 속에 보안에 대한 심각성을 교육하고 방어 및 보안사고 예방을 위한 최선안을 찾고자 노력해 왔다.

모든 기업의 업무처리가 컴퓨터를 기반으로 수행되고, 기업의 비즈니스와 관련된 중요정보, 고객정보, 그리고 기업의 핵심 기밀정보 등이 정보시스템으로 처리되고 있어 해킹 등 사이버 침해 위협이 날로 커지고 있다. 이러한 해킹 및 사이버테러 등 침해사고 대응에 대한 연구는 국제적 침해 사고 대응팀(CERT/CC)과 국가 또는 대응기관의 침해 사고 대응팀의 유형을 중심으로 연구되어 일반기업 환경에 적용하기에는 한계가 있었던 것이 사실이다.

본 논문에서는 해킹 및 사이버테러에 대한 이론적 배경을 토대로 해킹 및 사이버테러의 사례와 동향, “KWON-GA” 기술의 속성, 현존 보안 솔루션과의 특장점 비교, 솔루션의 기능 PoC 품질평가항목, 시험평가 사례 및 시험평가 결과를 토대로 실시간 일어나는 해킹 즉 사이버테러를 탐지 및 추적관리할 수 있는 제품을 정의하였고, “KWON-GA”솔루션을 국가기관 및 기업에 상용화할 수 있는 솔루션을 다음과 같이 정의하고자 한다.

2. 이론적 배경

2.1 해킹(Hacking)의 정의

2.1.1 해킹

시스템의 관리자가 구축해 놓은 보안 망을 어떤 목적에서건 무력화 시켰을 경우 이에 따른 모든 행동 보통 시스템 관리자의 권한을 불법적으로 획득한 것, 또 이를 악용해 다른 사용자에게 피해를 주는 것이라 할 수 있다.

2.1.2 크레킹(Cracking)

크래킹이란 허가받지 않은 시스템에 대해 정신적인 물리적인 피해를 입히는 행위이다. 특정 개인이나 특정 단체의 이익을 위해 허가받지 않은 시스템에 강제로 침입하는 것. 우리나라에서 해킹의 의미 뛰어난 컴퓨터 실력을 이용하여 정보 시스템에 침입, 그 속에 축적되어 있는 각종 귀중한 정보를 빼내거나 없애는 행위이다.

다음 <Table 1>은 많이 쓰이고 있는 해킹 관련 용어이다.

<Table 1> The definition of the term hacking

Division	Contents
White Hacker	Security Experts in the civil and government
Black hacker	Those who deliberately destroy the Internet system
cracker cracking	- person who damage to other through hacking - act which damage to other through hacking
backdoor	Secret passage system's security has been removed
firewall	Security system for the safe control of the interconnection and data transfer between the internal and external networks
log	Noted that the behavior of the system user in chronological order
Web Hacking	Malware infection, route (e-mail or Web site)
Jyokeu	The program for the purpose of making a joke
Bots	If the manager is away, automatically Role Irrevocably submit to the attacker's command of infection
Spyware	Advertising and marketing information collected without your consent
Grayware	False malware removal program
Trojans	Malware withdraw information in my computer, Worm or virus infection
Packet	Seperated message or piece of information, kind of data has been cut
Phishing Pharming Vishing	-Phishing: Fake website scam spam daily -Pharming: Seize the domain itself in the middle -Vishing: Internet Phone (VOIP) using automated recorded message sent to a bank account issues warning after PW extortion
IP Spoofing	Gastrointestinal system for an attacker to use the original host
Zero-day	Malicious code or hacking exploit them soon after the discovery of security vulnerabilities

2.2 네트워크의 계층

2.2.1 네트워크 OSI-7 Layer

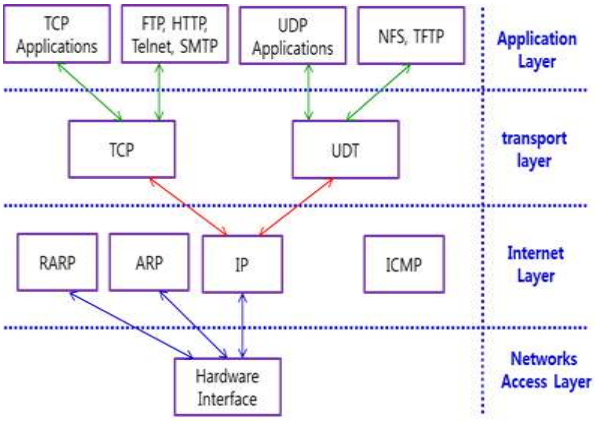
네크워크 상에서 정보를 교환할 때는 적절한 통신 절

차가 사용된다. 이절차중에서 비슷한 기능을 제공하는 것들을 하나로 묶어서 계층으로 나눈 후에 독립적인 역할을 담당하도록 한 것이 네트워크 계층 모델이다. 만약 모든 계층이 나누어져 있지 않고 하나로 통합되어 존재한다면, 모든 관계 업자들은 라우팅 규격, TCP/IP 규격 등 하드웨어/소프트웨어 전반의 모든 것을 알아야 할 것이며, 하나의 기능에 이상이 생긴다면 모듈 간 독립성이 떨어지기 때문에 전체적인 문제로 발전할 수 있다.

2.2.2 네크워크 TCP/IP

인터넷은 미국 국방성에서 개발한 TCP/IP를 사용하는 네트워크들의 네트워크로서, 전 세계적으로 수천 개의 네트워크와 수백만 대의 호스트로 연결되어 있는 네트워크이다. 초기에는 학교나 연구소들의 학술 및 연구망으로 활용되다가 최근에는 사용 망으로 확장되었다. 현재 인터넷 사용자는 폭발적으로 증가하고 있으며, 이러한 폭발적인 사용자 증가로 인해서 정상적인 사용이 아닌 다른 방법으로 시스템에 침입하여 시스템을 교란시키는 해커들 또한 매년 증가하고 있으며 침투방법 또한 매우 복잡하고 다양해지고 있다. 많은 경우가 패스워드의 문제점에 기인한다고 믿지만 최근보다 우수한 침입 수법을 이용하는 경우가 많이 발견되고 있다.

아래 그림 [Fig. 1]은 TCP/IP 내부의 계층별 프로토콜이다.



[Fig. 1] TCP/IP Inside each layer of the protocol

2.3 네트워크 취약점 분석

2.3.1 네트워크의 취약점 분석

네트워크취약점 분석은 스캐닝, Nmap, Super _Scan, WireShark, Cain & Able, 취약점 스캐닝 사용화 도구, DB보안의 취약성과 가용성 등을 통해 분석할 수 있다.

2.3.2 네트워크 취약점 스캐닝

네트워크의 스캔 도구는 주로 네트워크와 서버의 정보를 수집하기 위해 사용되는 점검도구이다. 동작 중인 시스템의 서비스 포트 및 OS에 대한 정보를 수집하여 네트워크 구조를 파악한다.

2.3.3 Nmap

Nmap(Network Mapper)은 네트워크 보안을 위한 유틸리티로, 대규모 네트워크를 고속으로 스캔하는 도구이다. Nmap은 raw IP 패킷을 사용하여 네트워크에 어느 호스트가 살아 있고, 그들이 어떠한 서비스(포트)를 제공하며, 운영체제(OS버전)가 무엇이며, filter/fire -wall의 패킷 타입이 무엇인지 등 네트워크의 수많은 특징들을 점검할 수 있다.

2.3.4 SuperScan

해킹 → Ping(네트워크가 살아 있는지) → IP 접속 → 포트(TCP/UDP) → PW/ID(ride)를 알아야 한다. 패킷 수집은 상대 정보를 획득하는 것으로 스캔은 모두 찾는다는 의미이다.

2.3.5 WireShark

WireShark는 세계에서 가장 널리 쓰이는 네트워크 분석 프로그램이다. 매우 강력한 이 프로그램은 네트워크 상에서 캡처한 데이터에 대한 네트워크/상위 레이어 프로토콜의 정보를 제공해 준다. 다른 네트워크 프로그램처럼, WireShark는 패킷을 캡처하기 위해 PCAP 네트워크 라이브러리를 사용한다.

2.3.6 포렌식 자료 생성

WireShark에서 수집한 패킷과 재생했던 도청 자료를 바탕으로 법적 효력이 있는 증거자료를 제시하게 된다. 도청된 VOIP 음성 패킷의 복사본의 시간과 패킷의 시간, 그리고 X-Lite 통화 기록의 시간이 일치함을 증명하여 무결성을 검증한다.

2.4 네트워크 공격(침입 패턴)

여러 대의 컴퓨터를 동시에 동작시켜 특정 사이트의 서버를 마비시키는 분산 서비스 거부 공격(DDoS : Distribute Denial of Service Attack, 이하 DDoS)은 더 이상 낯선 용어가 아니다. 쉽게 DDoS 공격을 할 수 있는 기술과 자동화 도구가 늘어나면서 누구나 마음만 먹으면 DDoS 공격을 시도할 수 있는 수준까지 도달했으며, 다음 <Table 2>는 DDoS 공격패턴이다

<Table 2> DDoS Attack pattern

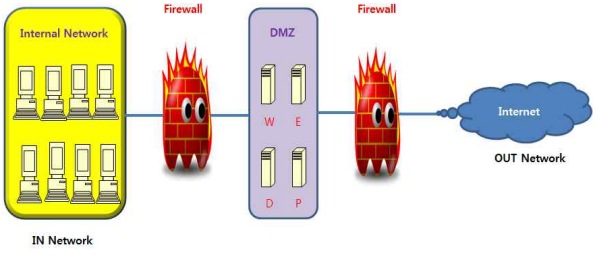
TCP attack	SYN flooding, Land attack, TFN
UDP attack	UDP Bomb, UDP Flooding, Trin00, TFN
ICMP attack	Ping flooding, Ping of Death, ICMP Redirect
SMTP attack	Mail Bomb, Mail Spam
IP attack	Tear Drop, Jolt/Sping
WINDOES attack	Wunnuke, NT-SPOOLSS, IIS-Longurl, IIS-get

※ TFN : Tribe Flood Network

2.5 침입 차단/탐지/방지 시스템

2.5.1 침입 차단(Firewall)시스템

침입탐지시스템은 대상 시스템(네트워크 세그먼트 탐지 영역)에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법 행위를 구별하여 실시간으로 침입을 차단하는 기능을 가진 보안 시스템으로 다음 [Fig. 2]와 같다.



[Fig. 2] Firewall (Firewall) system

2.5.2 침입탐지(IDS)시스템

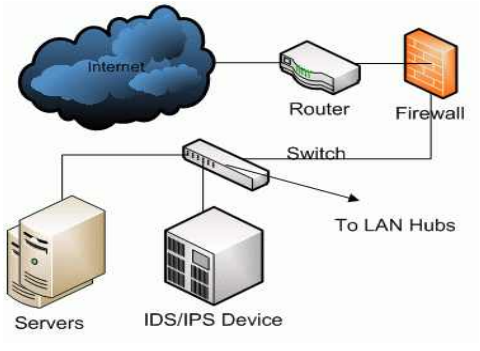
IDS(Intrusion Detection System)는 단순한 접근제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않는 사용자로부터 접속, 정보의 조작, 오용, 남용, 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 다음 <Table 3>는 미국의 COAST의 침입탐지시스템 분류이다.

<Table 3> Intrusion Detection System Classification of US COAST

DataSource-based	Single-host based IDS
	Multi-host based IDS
	Network based IDS
Model-Based Intrusion Detection	Anomoly Detection
	Misuse Detection

2.5.3 침입방지(IPS)시스템

네트워크에서 공격 서명을 찾아내 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션이다. 수동적인 방어 개념의 침입 차단(시스템)이나 침입탐지 시스템과 달리 침입 경고 이전에 공격을 중단 시키는데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다. 다음 [Fig. 3]는 침입탐지/방지(IDS/IPS)시스템 구성도이다.



[Fig. 3] Intrusion detection/prevention (IDS/IPS) system

3. 정보보안제품 Trend 및 문제점

3.1 정보보안제품 Trend

과거는 악성 프로그램과 외부로부터의 직접적인 침입 대응 위주(바이러스 백신, 방화벽, VPN, IDS)에서 현재

는 첫 번째 가용성 보장 강화 즉 가상화(Virtualization) 자원의 이원화 사고 발생 이후에도 가용 가능한 환경 구축이고, 두 번째 콘텐츠 보안 강화 DRM, DLP 등 정보유출 방지 제품군 스마트폰/TV 등 뉴미디어 출현 유통에 중심을 둔 보안이었다. 세 번째 관리적 수단 강화 수단으로 클라우드 컴퓨팅 즉 필요한 자원만 일시 사용 보안관제, NAC은 건전한 단말만 허용 관리하는 모니터링이다.

3.2 2013년 이후 Hacking Keyword

적용 가능한 모든 공격 방법을 최대한 이용하며 시간에 구애받지 않고, 오랜 시간(6개월~1년 이상) 동안 탐지되지 않으며, 일단 주도권이 장악되면 심각한 피해가 발생한다. 다음 [Fig. 4] 해킹의 키워드들이다.

[Fig. 4] Hacking Keyword

3.3 기존 보안 솔루션의 문제점

3.3.1 기존 보안제품 무용론

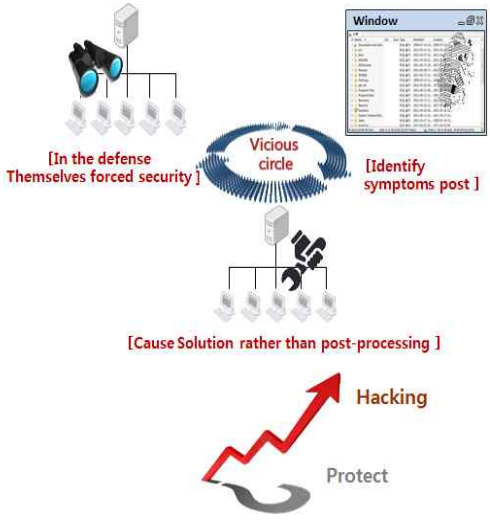
보안 제품을 만들어도 무한정으로 생겨나는 취약점은 열 명의 경찰이 있어도 도둑 하나 잡기 어려운 현실이며, 자기 방어 능력이 결여된 보안 제품들이다. 새로운 공격도구가 생기면 그것을 분석하여 보안 하고, 공격자는 다시 보안 솔루션을 분석하여 새로운 공격 도구를 만드는 먹이 사슬로 악순환이 반복되고 있다.

3.3.2 완벽하지 못한 기존의 해킹 방어 시스템

기존 시그니처 기반 엔진의 한계와 행위 기반이라 할지라도 언제든 Zero-Day 우회가 가능하고, 해킹 공격 의 특성상 공격 대상 예측이 불가능하다(미 탐지영역, 인지력 약화).

3.3.3 한계에 다다른 기존 정보보안 기술과 제품

OS 기능 역이용 등 기존 보안을 우회하는 공격이 이루어지고 있고, 사용자 행위에 의해 파생된 공격이 취약(사회공학기법 이용 공격, 문서파일 침입 및 탐지 력 약함) 하며, User 실수에 의한 대비책이 미비 (권한 관련, 암호 유출, 비정상적 운용, 조직 내 위반 & 위협) 하고, 사회공학기법에 의해 정당해 보이는 침입/ 유출이 무방비하다. 고가의 보안 솔루션, 24시간 모니터링 인력, 포렌식 전문가 필요로 과도한 비용이 소요되고, 해킹 사고 대비 너무 느린 실시간 대응체계로 기 존 가술과 제품은 한계가 있다. 다음 [Fig. 5]는 완벽하지 못하고 한계에 다다른 기술 및 제품의 악순환 흐름도이다.



[Fig. 5] cause solution rather than post processing-post processing rather than cause solving

결과적으로 기본 정보 보안의 기술적 대응 한계에 대한 대안이 필요하다. 더 이상 방어적인 보안기법으로는 해킹 차단이 불가능하고, 관제도 결국 사람, 행동과학 측면의 접근이 필요하다.

4. 해킹의 유형 및 사이버테러의 동향

4.1 해킹의 유형

트로이 목마, 쓰레기 주워 모으기, 논리폭탄 살라미 기법, 자료의 부정변개, 슈퍼 재프 등이며, 최근 해킹의 동향 IP 스푸핑 인증(Authentication) 기능을 가지고 있는

시스템을 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법 패킷 스니퍼링 네트워크에 연동돼 있는 호스트뿐만 아니라 외부에서 내부 네트워크로 접속하는 모든 호스트가 위험 대상 Send -mail, 버그 Sendmail 네트워크 간에 메일을 전송해 주기 위해 만들어진 메일 전송 프로그램이다.

4.2 사이버테러의 정의

컴퓨터 통신망상에 구축된 가상공간인 사이버 공간을 이용한 폭력 행위를 가리키는 용어로, 컴퓨터 통신망을 이용하여 정부 기관이나 민간 기관의 정보 시스템에 침입, 중대한 장애를 일으키거나 파괴하는 등의 범죄 행위이다.

4.3 사이버테러 집단별 현황 <Table 5>참조

<Table 5> Cyber terrorists Stars Status

Object	Time	Outline
Anonymous	2010 ~ 2015	Dictatorship, human rights abuses, censorship, Monopoly finance capital profits
Cyber Caliphate	2015	Retaliation against a group toward the IS/Three cases threatening cyber terrorism
Lizard Squad	2014	Three cases of cyber terrorism to the game server to the target
Guardians of Peace	2014	Movie: The Interview "for screening Conversely, inflicting terror

4.4 사이버테러 집단의 공격

4.4.1 사이버테러 집단 공격의 진화

최근 핵티비즘은 단순한 접속 방해 차원을 넘어서 내부 망을 침투해 비밀문서를 탈취하거나, 내부 망을 파괴하는 등의 사이버 하이재킹으로 양상이 바뀌었다.

4.4.2 사이버테러 집단 공격의 기법

DDoS, SQL인젝션을 사용한다. <Table 6>참조

<Table 6> Changes in attack mode and purpose

Division	Past	Today
Division	Web site attacks	Website + SNS + cyber-hacking hijacking
Purpose	Monetary purposes	Financial + political beliefs purposes

4.4.3 국내 주요 해킹사례 및 개인정보유출

2003년 KT 대상 DSN 서버 공격(1.25 인터넷 대란)은 SQL서버 취약점을 이용한 슬래머 웜에 감염된 PC들이 대량 KT 혜화 전화국에 있는 DNS 서버를 공격한 사례이며, 2008년 옥션의 1860명의 개인 정보 유출 사고로 중국 해커의 소행으로 CSRF(사이트 간 요청 위조)취약점을 이용한 공격이었다. 2009년 청와대, 국방부 등 30개 사이트에 7.7DDoS 공격으로 5월 초부터 치밀한 준비를 통해 진행된 대규모 공격이다. 공격을 감행한 해커는 미리 좀비들을 제어하기 위한 C&C 서버들을 수 천대 이상 확보하였으며, 다양한 채널을 이용해 정보를 유출하는 악성코드를 유포해 좀비 PC들로부터 각종 정보를 수집하였다. 이후 본격적인 DDoS 공격을 하기 위하여 7월 초 국내의 웹하드 홈페이지 두 곳을 해킹하여 업데이트 프로그램을 DDoS 악성코드로 바꿔치는 방법으로 국내의 많은 좀비 PC를 확보하여 DDoS 사이버테러를 감행하였다. 2011년에는 현대캐피탈의 175만 명의개인 정보가 유출되었는데 원인은 관리소홀과 퇴직 직원의 ID, 비밀번호를 이용하여 해킹 고객의 비밀번호 비 암호화하는 수법으로 진행하였다. 이외에도 수많은 사례가 있지만 아래 표<Table 7>의 주요 업계 개인 정보유출 현황에 제시된 바와 같다.

<Table 7> Disclosure of personal information into a major industry

시기	Company Name	Outflow Personnel
2008.01	Auction	1,860 ten thousand people
2008.04	Hanaro Telecom (Now SK Broadband)	6 million people
2008.09	GS Caltex	1,125 ten thousand people
2010.03	Shinsegae Mall	3.9 million people
2011.04	Hyundai capital firm	1.75 million people
2011.07	SK Communication (Nate / Cyworld)	33,500 ten thousand people
2011.08	Epson Korea	350,000 people
2011.11	Nexon	1,320 ten thousand people
2012.05	EBS	4 million people
2012.07	KT	8.7 million people
2013.06	Saenuri Party	2.5 million people (estimate)
2013.06	The Blue House	200,000 people (estimate)

지금까지 정보 보안의 이론적 배경을 기초로 해킹의 개념 및 용어, 네트워크 보안, 침투/차단/방지 시스템의 개념, 정보 보안제품 Trend 및 문제점, 해킹의 유형 및 동향에 대해 알아보았고, 다음은 이를 해결할 수 있는 "KWON- GA" 제품의 실시간 해킹, 탐지 및 추적관리 보안 솔루션에 대해 그 기술의 속성과 유사제품을 비교하여 특 장점을 분석하고, 솔루션 기능 PoC 품질평가 항목으로, 시험평가 사례 및 시험평가 결과를 토대로 제품의 우수성을 정의하고, 그 해결책을 "KWON-GA"에서 찾아볼까 한다.

5. "KWON-GA" 기술의 개념 및 속성

5.1 "KWON-GA" 기술

5.1.1 "KWON-GA" 개념

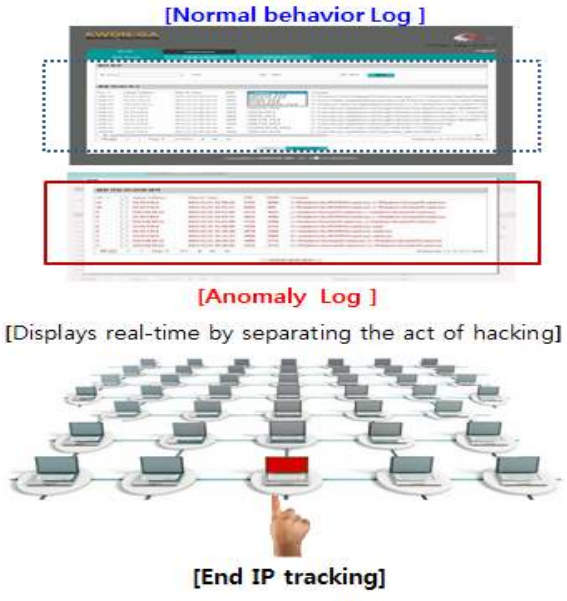
고객 시스템 환경에 맞춰 필요한 기능을 제공하고, 완벽한 커스터마이징 정책을 실현하는 New 패러다임 맞춤형 솔루션이며, 하드웨어 기술 기반의 필요 SW 솔루션을 탑재하는 어플라이언스의 형태이다.

5.1.2 KWON-GA의 속성

각 솔루션은 개별적 및 복합적으로 구성되어 있고, 고객 니즈에 최적화된 다양한 솔루션을 제공하며, 암호화, Hooking, 가상화 등 기존 알려진 보안 기술을 배제하였다. 패킷 수집이 없으며, 솔루션 적용 이후 속도에도 영향은 없다. 모든 OS에서 독립적 동작이 가능하다.

5.2 KWON-GA 해킹 추적관리 솔루션

해킹 발생 최초 발원지로부터 해커의 경로와 취약점을 실시간 추적이 가능하며, 기존 해킹사고가 오랜 분석 과정으로 적기 조치가 불가했던 문제점을 해결하였다. "KWON-GA 해킹 추적 솔루션은 보다 효율적인 보안관제 모니터링 환경을 제공한다. "KWON-GA는 첫 번째 실시간 해킹 행위 탐지를 구분 기술을 사용하여 해커 침입을 즉시 파악 및 대응할 수 있다. 또한 침입자 경로에 대한 완벽한 내/외부 접속 파악이 가능하며, 침입자가 발견할 수 없는 스텔스 모드를 개발 활용하였다. 두 번째 해킹 추적은 발화점부터 즉시 파악이 가능하다. 침입자가 거쳐 온 외부 망과 침투 중인 내부 망 접속점 즉시 침입경로를 파악하여 네트워크 취약점을 보완하였고, 침입자의 외부 침투 경로를 추적하여 최종 IP 주소를 파악하였다. 아울러 최종 IP가 외부인지 내부인지 실시간 파악이 가능하고, 침입자에 대한 즉각적인 대응이 가능하고, 솔루션 에이전트 스텔스 모드가 작동한다. [Fig. 6] 해킹 탐지 추적관리 참조.



[Fig. 6] Hacking detection tracking

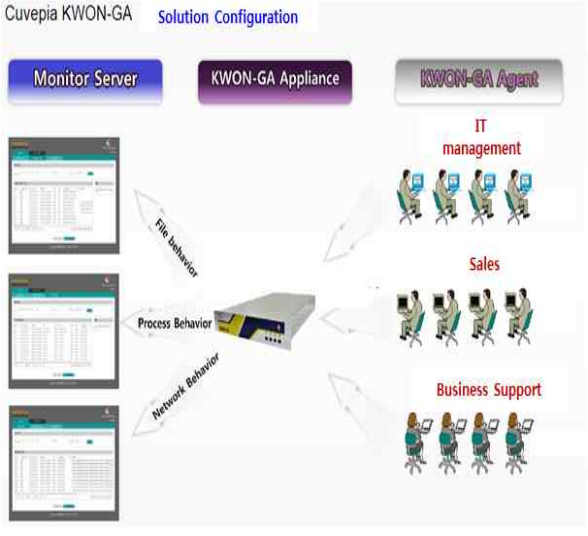
5.3 Behavior Monitoring[Concept]

첫 번째 실시간 해킹 대응은 모든 시스템에 대한 실시간 해킹 대응과 고도화된 지능을 가진 Agent로 모든 비정상 동작 감지한다. 두 번째 시스템 코어 검사/탐지는 시스템 Kernel Level Monit oring과 해킹 Behavior에 대한 즉각 탐지, Process, file, Network에 대한 생성/변경을 탐지한다. 세 번째 지능형 Agent Software 시스템 성능 영향 0%, 안정성을 보장하는 Stealth Agent와 OS의 패치와 상관없이 안정적 운영할 수 있다. 마지막 네 번째 해킹 발화점 추적으로 최초 해킹 공격 시작부터 종점까지 완전한 경로 추적 가능하며, 공격 원점에 대한 비정상 행동 탐지활동과 별도 포렌식 분석이 필요 없다. [Fig. 7] 행위 모니터링 개념 참조.

[Fig. 7] Behavior Monitoring Concept

5.4 Behavior Monitoring[Solution]

첫 번째 Profile로 해킹 발화점에 기초한 비정상 행동을 탐지하고, 정교한 사용자의 정의 Profile을 설정 다양한 조건에서의 정교한 예외 처리가 가능하다. 두 번째 Monitor Board인 File, Network, Process에 대한 직관적 모니터링 UI와 해킹 공격을 신속히 파악할 수 있는 필수적인 정보만 출력하고, 웹 기반 Monter Board, 복잡성 지양(예 : 화려한 그래픽 UI 지양) 세 번째 Analysis로 발생 Event에 대한 정교한 분석을 통한 File, Net work, Process를 동시에 모니터링한다. 공격에 상세 및 대응 정보를 제공한다. [Fig. 8] 솔루션 구성 참조.



[Fig. 8] Solution Configuration

6. 유사제품 비교(특 장점)

6.1 현존하는 이론공학은 해커를 볼 수 없다

해킹은 실시간 탐지 및 추적은 이론 공학적으로는 불가능하기 때문에 정보 방어도 불가능하다. 해커의 OS 영역 이용 및 기본 보안을 우회하는 등 창조적/선제적 공격에 무방비하다. 결과적으로 24시간 모니터링 인력, 디지털 포렌식 전문가가 필요하여 과도한 비용이 들어가며, 해킹 사고에 너무 느린 사후 실시간 대응체계의 단점과 보안 관계사가 담당할 Log는 너무 많고 지속적으로 발생하는 오탐 경고(Warning Signal)는 짜증을 유발한다. 해킹 방어책으로 기존 시그너처 기반 엔진으로는 한계가 있으며, 행위 기반이라 할지라도 언제든 Zero-Day 우회가 가능하다. 사용자 행위에 의해 파생된 결과물에 대한 공격이 취약하고 User 실수에 의한 대비책이 미비하고, 시회 공학기법에 의해 정당해 보이는 침입/유출에 무방비하다. 해커는 수많은 시스템 중 단 한 곳의 취약점만으로 공격한다. 보안 구성을 복잡화하더라도 해커는 네트워크 내부를 자유자재로 활보하고 다닌다. 관제사의 업무는 많은 중압감을 유발하며, 이를 일상 업무와 함께 수행해야 할 경우, 중요 경고에 대한 Alarm을 Off 상태로 관제하는 이유이다.

6.2 KWON-GA제품의 특 장점

KWON-GA는 내부/외부 해커를 실시간 보고, 잡는 기술이다. 내부/외부 해커를 전자동 탐지하고, 실시간 탐지 및 발원지 및 모든 이동경로의 추적이 가능하며, 기능만 일부 추가한다면 Fake 정보가 유출된다. 해커 침입 즉시 파악 및 대응이 가능함으로 포렌식 분석이 필요 없고, Process, File, Network에 대한 생성 및 변경 탐지가 가능하다. 또한 안정성을 보장하는 Stealth Agent와 OS의 패치와 상관없이 안정적으로 운영되며, 암호화, 후킹, 가상화 기술을 사용하지 않고, 패킷 수집도 없다. 솔루션 적용 이후 사용자 PC 속도와 시스템 및 에이전트의 속도에도 영향 없으며, 행위 로그에 대한 세부사항 표시 기능과 PID 및 부모 PID 표시 기능으로 사용자 관리를 통한 모니터링 권한을 제어하고, 슈퍼 관리자를 통한 모니터링 사용자를 관리한다. 단말 PC의 행위에 대한 탐지 및 전송이 가능하며 사용자 임의 삭제가 불가하다.

7. 해킹 실시간 탐지 및 추적관리 솔루션 기능 PoC 품질평가 항목

이장에서는 KWON-GA 보안 솔루션의 품질평가에 항목에 따라 어떻게 평가하는지 주요 평가 요소를 기초로 정의하였다.

7.1 시험평가 항목

7.1.1 평가 주요 항목

첫 번째 로그 수집 절차 및 기록의 근거를 정확히 기록 관리하는지(11개 요소) 여부와 두 번째 로그 모니터링의 정확한 자료제공인 및 행위인지 여부 확인(10개 요소), 세 번째 망 분리 및 어떠한 환경하에서도 운영 관리가 가능한지(5개 요소)를 평가한다.

7.1.2 항목별 주요 평가 요소

<Table 9> 로그수집, <Table 10> 로그 모니터링, <Table 11> 운영관리 평가요소 참조.

<Table 9> Log Collection

Turn	Evaluation factors
1	Agent installation file, Process, TCP log whether simultaneous acquisition
2	whether record the process create a successful exit logs only
3	whether the file log records successful logs in creating, deleting, renaming, moving, copying, etc.
4	TCP connection / disconnection, TCP Listen entry / exit only successful log
5	whether check all the logs source PID
6	Agent to be installed on the PC, the process should not be present, And, temporarily hiding the process behavior, gastrointestinal drive
7	whether agent is using encryption technology or not
8	whether agent is using hooking technology
9	whether it has any conflicts with other program
10	whether it includes remote/local separation, IP address, computer name, date and time occurs, PID, action occurring substance
11	exact log collection regardless of malware infections

<Table 10> Log Monitoring

Turn	Evaluation factors
12	whether provide a web interface to monitorr
13	File process, monitor all actions for the TCP log and provide separation administrator to find whether local/remote access act or not
14	Whether is it possible to find source PID from all action logs and decide
15	Whether is it possible to filter logs from all actions to monitor logs with time of occurrence
16	Offer search function using process log PID filterr
17	Whether is it possible to offer function to search TCP action that specific process tried using TCP log PID filter
18	Whether is it possible to offer function to search filing action that specific process tried using file log PID filter
19	provide detailed log monitoring function of actions acquiring control
20	If actions to acquire control authority occur, is detailed log provided in real time until the action shut down
21	Does it offer stored action log history by user profile

<Table 11> Operations Management

Turn	Evaluation factors
22	Whether is it possible to operate in concerned network isolated environment
23	Whether is it offer optional fuctions to prevent failure
24	Whether is it traceable in detected control acquisition action
25	Whether is it offer various(more than 2) search methods to each terminal action
26	Whether is it offer function to make standard export file (CSV) for report

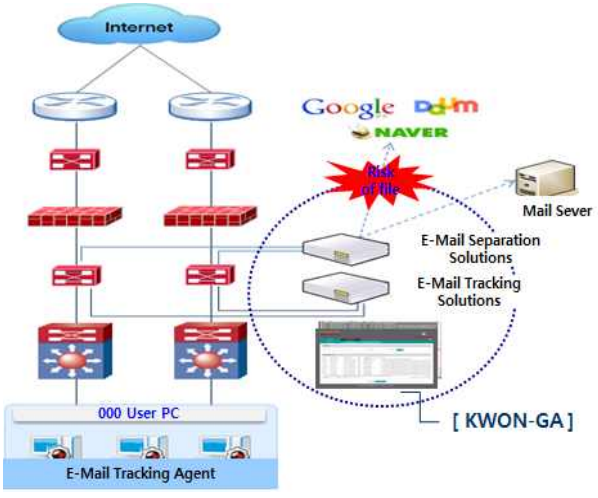
8. 시험평가 방법(환경구성), 사례 및 결과

이장에서는 공공기관 및 금융기업과 대기업 의 평가 사례는 7장의 평가항목을 기초로 KWON-GA 솔루션을 시험평가한 성공적 사례 및 결과이다.

8.1 “A” 공공기관 사례

2014년 2월 “A” 공공기관 내부 업무용으로 사용되는 공식 메일 등 이외에 외부 메일(네이버, 다음, 네이트, Gmail 등) 사 용 시 발생할 수 있는 내부 데이터 유출을

방지하기 위하여 KWON-GA 유출 방지 시스템으로 시험 평가하여 성공한 환경 구성도이다. [Fig. 9] 참조.



[Fig. 9] "A"Public agencies test and evaluation environment configuration

8.2 "A" 금융사 및 "A" 대기업 사례

8.2.1 "A" 금융사 사례

"A" 금융사는 2014년 4월에 1차 2015년 1월에 2차에 걸쳐 불특정 지역/시간에 해킹을 시도하는 시험평가를 하였다. 평가 프로세스는 첫 번째 사용자가 msf.pcap을 실행하고, 두 번째 사용자 PC 정보를 전송(좀비PC)하면, 세 번째 해커가 원격에서 CMD. exe을 실행한다. 이때 사용자 PC에서는 서버에 실시간 로그를 전송하게 된다. 네 번째 원격 CMD.exe 탐지 및 경고를 발생하여 관리자 화면에서 이를 식별하고 다시 발원지 및 모든 접속/이동 경로 등을 인지할 수 있는지 즉 실시간 해킹 탐지/추적하는가 가능한지를 [Fig. 11]의 시험평가 환경 구성도 처 럼 시험하여 성공하였다.

8.2.2 "A" 대기업의 사례

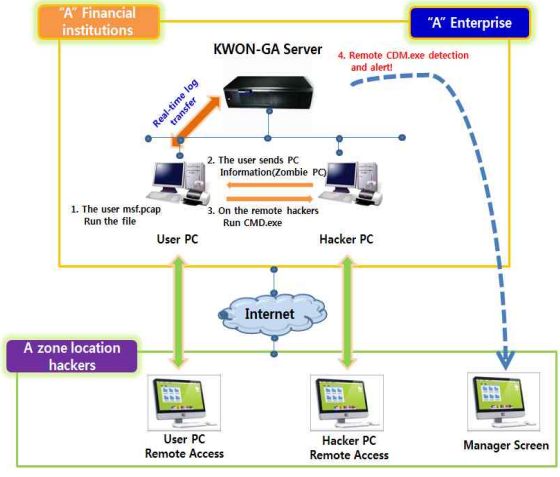
2014년 12월부터 2015년 1월까지 2차례에 걸쳐 "A" 금융사와 동일하게 진행하였다. "A" 기업은 특정지역에 시험용 PC를 설치하고 가상 IP 주소를 부여하여 그중에 한 대를 지정하여 VPN 터널을 지방에 있는 해커 쪽으로 열어주고 "A" 기업 특정지역 쪽 내부 PC에 3389포트 ID/Password를 열어주고, 지방에 있는 해커 쪽에서 해당 PC에 들어와서 여러 가지 작업들을 수행함. 당시 VPN 터널이 열려 있는 PC는 D:\드라이브 쪽에 "작업방" 폴더에 만들어서 외부에서 접근할 수 있도록 설정해 놓고 특정지역의 "A"사가 지정한 해커 쪽에 어떤 행동이든지 다 해보라고 하여 모든 행동을 실시간 해킹 탐지/추적 관리하는 형태로 진행하였다.

KWON-GA 실제로 모니터링 했던 해커들의 행동은 <Table 12>와 같고, 시험평가는 [Fig. 11]과 같다.

<Table 12> Detection / tracking information for hackers hacking behavior

Number	Contents
1	CMD.exe attempt to open the Network Scanning (netstat)
2	P Tech malware program installed
3	IceWord program implementation
4	Unlocker.exe program implementation
5	Process Explorer enforcement
6	Autorun.exe program implementation
7	Famous program which is one of two biggest hacking program(include PoisnIvy) used by Chinese hackers

※ Number 7 : Famous program which is one of two biggest hacking program(include PoisnIvy) used by Chinese hackers



[Fig. 11]"A"Conglomerates and "A" rated financial institutions test environment configuration

8.3 시험평가 결과

시험평가 결과는 7장에서 제시한 평가 항목의 3개 대분류 26개 세부평가 요소에 의해 공공기관, 금융기업, 대기업을 대상으로 실시한 결과로 평가요소별 상/중/하 기준으로 평가하였다. 이 기준에서 "상"(High)은 KWON-GA만이 가지고 있는 기술을 기준으로 하고,

“중”(Middle)은 다른 제품에도 있으되 KWON-GA제품이 좀도 우수한 경우로 분류하며, “하”(Low)는 다른 제품 보다 기능이 떨어지는 것을 의미한다. 하지만 하에 해당되는 기능은 없으며, 다음 <Table 13>, <Table 14>, <Table 15>와 같다.

<Table 13> Log Collection

Element order	"A" public authority	"A" financial institution	"A" large
1	"High"	"High"	"High"
2	"High"	"High"	"High"
3	"High"	"High"	"High"
4	"High"	"High"	"High"
5	"High"	"High"	"High"
6	"High"	"High"	"High"
7	"High"	"High"	"High"
8	"High"	"High"	"High"
9	"High"	"High"	"High"
10	"High"	"High"	"High"
11	"High"	"High"	"High"

<Table 14> Log Monitoring

Element order	"A" public authority	"A" financial institution	"A" large
12	"Middle"	"Middle"	"Middle"
13	"High"	"High"	"High"
14	"High"	"High"	"High"
15	"High"	"High"	"High"
16	"High"	"High"	"High"
17	"High"	"High"	"High"
18	"High"	"High"	"High"
19	"High"	"High"	"High"
20	"High"	"High"	"High"
21	"Middle"	"Middle"	"Middle"

<Table 15> Operations Management

Element order	"A" public authority	"A" financial institution	"A" large
22	"Middle"	"Middle"	"Middle"
23	"Middle"	"Middle"	"Middle"
24	"Middle"	"Middle"	"Middle"
25	"Middle"	"Middle"	"Middle"
26	"Middle"	"Middle"	"Middle"

전체 26개 항목 중 19개 항목이 “상”이고, 7개 항목이 “중”으로 평가되었다. 이것은 기본적인 요구 사항들도 우수하였고, KWON-GA만이 가지고 있는 독창적 기술이 있는 것을 확인할 수 있었다.

9. 결론

정보통신기술(ICT)의 발달로 쏟아지는 정보화 물결속에 우리는 많은 편리함을 누리고 있는 반면에 이에 따른 수많은 역기능과 악순환 속에 1.25인터넷 대란을 필두로 7.7, 3.4 DDoS 공격과 3.20, 6.25사이버 테러를 겪은 후 정보 보안의 중요성이 부각되면서 정보 보안관제 및 운영관리의 역할이 주목받게 되었고, 네트워크 시스템의 기반기술이 유비쿼터스 컴퓨팅이나 클라우딩 컴퓨팅 기술과 같은 차세대 컴퓨팅 기술로 다변화되어 사이버테러에 대한 피해가 더욱 커질 것으로 예상된다. 아울러 이러한 사태 속에 각종 보안 제품들이 정제되지 않고 시중에 유통되어 온 것도 사실이며, 국방/공공기관, 각 기업체에서 보유하고 있는 다른 보안 솔루션들과 어떤 기능들이 겹치며, 어떤 기능들은 겹치지 않는지에 대한 솔루션 분별 평가를 거친 후에 대체 가능한 솔루션들이 어떤 것인지를 판단하고 싶어 한다.

KWON-GA Behavior Monitoring 솔루션은 이러한 문제점들을 해결 할 수 있는 세계 최초 솔루션이다(기밀성, 무결성, 가용성). 또한 KWON-GA는 OS에 의존하지 않는 보안 기술이고, 침입자와사용자의 완벽한 구분과 시스템 구조 파악의 원천봉쇄와 역공학에 의해 분석되지 않는 솔루션이며, 기존 관제의 한계를 뛰어넘는 기술로써 사용자의 불편함이 없는 보안 솔루션이다.

지금까지 정보 보안에 대한 이론적 배경으로부터 해킹 사례 및 동향, KWON-GA 솔루션의 속성, 유사 제품과의 비교(특 장점) 분석, 품질시험 평가 항목, 각 분야별 시험평가 사례를 기초로 시험평가 결과에 대해 정의하고 검증하였다.

본 논문을 통해 KWON-GA 솔루션의 안정적인 보안관제와 모니터링이 가능하여 사이버테러에 대비할 수 있다는 것을 검증하였으니 도입이 시급하다. 이는 시스템 사용자로부터 책임자에 이르기까지 누구든지 사이버 공격의 대상이 될 수 있으며, 누구든지 사이버 공격자가 될 수 있다는 것이다. 개인 사용하는 PC에 중요하지 않는 데이터가 저장되어 있지 않다고 해서 보안에 허술해서는 안 된다. 왜냐하면 DDoS 공격이 공격 에이전트로 사용되는 좀비 PC로 사용될 가능성이 높기 때문이다.

끝으로 KWON-GA 솔루션의 다양한 비즈니스 모델이 많은데, 고객으로부터 기밀성, 무결성, 가용성에 대한

확고한 인식을 심어 주려면 특허 등록 및 국제표준 CC 인증을 조기에 받아서 고객의 니즈 와 특정 또는 불특정 대상 및 시간, 장소 등에서 사이버테러에 대응하여야 하겠다.

Acknowledgments

For this paper, I thank CubePia CEO and officials who worked Professor Yang, Hae - Sul gareucheo who you and well respected in the testing and evaluation

REFERENCES

[1] The 12th Conference of Defense Privacy and password Defense Security Command, pp. 34-61, pp. 113-124, 2014. 11. 07.
[2] Four nemon Against Cybercrime scale embodied in expense reports. 2014.
[3] Sung Jin Ahn, Kyung Ho Lee, Won Hyung Park. Study of Security Control pp183-245. 2013. 05.
[4] NSHC 3.20 cyberterrorism incident reports, 2013.
[5] NSHC 6.25 Cyber Terrorism Analysis Report, 2013.
[6] CERT Insider Threat Center(2011). Insider Threat Control : Using a SIEM signature to detect potential precursors to IT Sabotage. 2011.
[7] Jung Ho Eom, Sung Soo Choi, Tae Myung Jung, Introduction of Cyber Warfare, pp31-106, 2012.
[8] Sang Yong Choi, Reconstruction of hacking incidents, pp. 287-324, 2013, 07.
[9] Dae Woo Park, Theory of Network security, 2009.
[10] Dae Woo Park, Jung Man Seo. "Research of Security method for TCP/IP attack", Journal of the Korea Computer Information Association, Vol. 10, No. 5 pp. 217~226. 2005, 11. 30.
[11] Hoon Bae Gil, "A Study on Security Policy about PC communication", Master's thesis Graduate School of Polytechnic, Yonsei University, 1996.
[12] CERT/Coordination Center, "CSIRT Frequently Asked Questions," Pittsburgh, Pa.:CMU/SEI, 2007.
[13] Tae Myung Jung, CERT's functions and roles, education in course of operating CERT, 2002.
[14] Internet Security / Web Hacking domestic hacking case http://www.ahnlab.com 2014. 05. 09.
[15] Cuvepia Profile New Leader of Integrated Security Solution www.cuvepia.com(2013.04).

김 승 범(Kim, Seung Bum)

- 1997년 2월 : 성균관대학교 행정학과 졸업(학사)
- 2007년 8월 : 호서대학교벤처전문대학원 정보경영학과 졸업(석사)
- 2011년 8월 : 호서대학교 벤처전문대학원 정보경영학과(수료)
- 1985년 12월 ~ 2009년 8월 : 육군장교 24년 복무(정보화)
- 2004년 2월 ~ 2009년 8월 : 국방부 인사정보화 사업담당
- 2006년 5월 ~ 2007년 5월 : IT PMP 및 EA 전문가(취득)
- 2010년 3월 ~ 2012년 12월 : 두원공대(심화과정) 시간강사
- 2009년 9월 ~ 현재 : 한화S&C 입사 국방/공공사업 영업
- 관심분야 : 네트워크 보안관제(특히 모바일), 소프트웨어 품질보증과 평가, 프로젝트관리, 국방 CBD방법론
- E-Mail : sbkingjm@hanwha.com

양 해 술(Yang, Hae Sool)

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 SW공학 전공(공학박사)
- 2006년 2월 : Kazakhstan 유러시안 경제대학(명예경영학박사)
- 1975년 5월 ~ 1979년 6월 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대학교 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本 오사카대학 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국소프트웨어품질연구소 소장
- 2010년 3월 ~ 2012년 2월 : 호서대학교 창업대학원 원장
- 2012년 11월 : 대통령표창(SW산업발전유공) 수상
- 1999년 11월 ~ 현재 : 호서대학교 벤처전문대학원 교수
- 관심분야 : SW공학(특히, SW품질보증과 품질평가, 품질감리 및 컨설팅, SI), SW프로젝트관리, 품질경영.
- E-Mail : hsyang@hoseo.edu