제어망에서 화이트 리스트 기법을 이용한 이상 징후 탐지에 관한 연구★

이동휘* · 최경호**

요 약

폐쇄적으로 구축되었던 제어망이 최근 업무 상 편의 또는 대외 기관과의 협력 필요 등으로 외부와 연동되면서, 일반적인 네트워크 환경과 유사하게 변화하고 있다. 그리고 개방형 운영체제, 프로그램 및 프로토콜 등을 사용하는 제어망 환경은 기존에 알려진 보안 취약점을 그대로 갖고 있으며, 제어 시스템의 취약점과 관련한 공격 기법이 발달하는 등의 위험에 직면하고 있다. 이에 따라 본 연구에서는 화이트 리스트 기법을 적용한 이상 징후 탐지를 통해 보안성을 확보하고 위협을 최소화할 수 있는 방안을 제시하였다. 제시된 방법을 통해 업무망, 제어망 및 필드장치 내 트래픽을 모니터링하여 정상적인 데이터만을 수집 및 목록화 할 수 있고, 비정상행위로부터 격리된 상태를 확인하여 위협을 배제시킬 수 있다. 그러나 정상적·비정상적 트래픽 패턴에 대한 오경보가 발생할 수 있으며, 이를 최소화하는 노력도 함께 경주해야 한다.

A Study of an Anomalous Event Detection using White-List on Control Networks

DongHwi Lee* · KyongHo Choi**

ABSTRACT

The control network has been operated in a closed. But it changes to open to external for business convenience and cooperation with several organizations. As the way of connecting with user extends, the risk of control network gets high. Thus, in this paper, proposed the technique of an anomalous event detection using white-list for control network security and minimizing the cyber threats. The proposed method can be collected and cataloged of only normal data from traffic of internal network, control network and field devices. Through way to check the this situation, we can separate normal and abnormal behavior.

Key words : Control Networks, Misuse Detection, Traffic Signature, White-list, IDS, Snort

접수일(2012년 8월 27일), 수정일(1차: 2012년 9월 6일), 게재확정일(2012년 9월 7일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음

* 경기대학교 산업보안학과

** 경기대학교산업기술보호특화센터 (교신저자)

1. 서 론

제어망은 일반적인 네트워크와는 달리 폐쇄적인 구성으로 구축되어있기 때문에 최초 구축 시부터 보안에 대하여 고려되지 않고 구현되어왔다[1]. 그러나 최근에는 제어망을 구축하기 위해서 고려되어야 할 여러 가지 사항들 중 스턱스넷(Stuxnet)과 같은 사이버 위협의 증가로 보안에 대한 관심과 비중이 상당히 높아졌다[2]. 또한 위협으로부터 제어망을 보호하기 위한 다양한 장비와 기법들이 연구되고 있다[3].

이러한 흐름은 과거 폐쇄형으로 구축 및 운영되던 제어망이 업무 상 편의 또는 대외 기관과의 협력 필요로 인해 일정 부분 외부 네트워크와 연동하는 형태로 전환되고 있는 환경에 기인한다. 개방형 운영체제, 프로그램 및 프로토콜 등을 사용하는 제어망 환경은 기존에 알려진 보안 취약점을 그대로 갖고 있으며, 외부와 네트워크가 연동되어 제어 시스템의 취약점이 발견되고, 이와 관련한 공격 기법이 발달하는 등의 위험에 직면하게 되는 것이다[4].

그리고 제어망은 전력, 가스, 교통 등 국가적으로 중요한 기반시설들에 사용되고 있어 침해사고 시 심각한 위험이 발생하고 파급효과도 크다[5]. 따라서 제어망의 특성을 이해하고 위협을 최소화 할 수 있는 방안 마련이 절실히 요구된다.

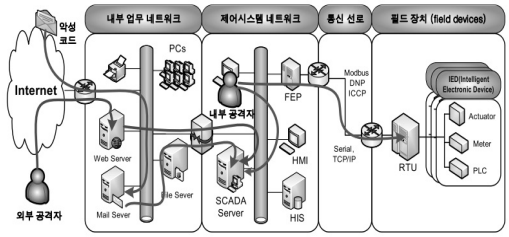
그러므로 본 연구에서는 제어망의 보안성 확보를 위해 외부와 연동하여 운영하는 환경 하에서 정상 이외의 네트워크 통신들을 탐지하여 불필요하거나 위협으로 간주되는 행위들을 차단할 수 있는 방안을 제시하고자 한다. 이를 위해 이어지는 2장에서는 제어망에서의 보안 위협과 이를 탐지하는 방법론들을 살펴보고, 3장에서 정상 이외의 행위들을 탐지하기 위한 방안을 화이트 리스트(White-List)에 기반하여 설계한다. 그리고 4장에서는 설계된 시스템을 분석하며, 마지막으로 결론을 맺는다.

2. 관련연구

2.1 제어망 보안위협요인

2.1.1 외부 연동에 의한 보안 위협

다양한 내부 업무용 정보통신기기들이 연결된 네트워크에 제어시스템을 연결하여 사용하는 경우와 업무용 네트워크와 제어망을 연동할 때 침입차단시스템(firewall)과 같은 정보보호시스템을 이용하여 적절한 접근통제를 하지 않을 경우, 제어망은 해킹 및 악성코드로 인한 내·외부의 모든 보안위협에 노출된다.



(그림 1) 제어시스템에 대한 보안위협[6]

그리고 웹 응용프로그램 취약점을 이용한 해킹사고는 외부로 공개된 포트를 사용한 침입으로 침입차단시스템을 무력화 시키고 있기 때문에[7], 추가적인 위협 대응책 마련이 필요하다.

2.1.2 시스템 취약성에 의한 보안 위협

제어시스템은 특정 제품과 고유 통신 프로토콜을 사용하고 있어 안전한 것으로 보이기는 하나, 증가하는 정보통신 기반시설에 대한 사이버 위협으로 인해 표적화된 공격을 받고 있다[8]. 이 위협들은 데이터에 대한 CIA(Confidentiality, Integrity, Availability)를 침해하게 된다. 또한 제어시스템에 악의적 명령이 허용된다면, 정상적인 운영에 문제가 발생할 수 있다.

대표적 사이버 위협인 악성코드는 제어 시스템의 성능저하, 가용성 손실, 데이터의 유출, 수정 및 삭제와 같은 결과를 발생시킬 수 있다. 그러나 이러한 위협에 대한 고려 없이 개발되고 운영되거나, 사용자의 보안의식이 결여된 환경에서 운영되는 제어시스템은 손쉬운 공격의 대상이 되고 있다[4][6].

2.2 침입탐지시스템

침입탐지시스템(IDS : Intrusion Detection System)을 이용한 제어망 보안은 관제를 용이하게 하고, 알려진 공격에 대해 높은 탐지율을 보이기 때문에 위협 대응을 위한 적절한 방법론이다[9]. 알고리즘은 비정상행위 탐지(anomaly detection), 오용 탐지(misuse detection) 및 하이브리드 방식이 사용된다[10].

2.2.1 비정상행위 탐지

비정상행위 탐지 방식은 네트워크 상의 트래픽이나 정보통신기기 자원의 사용이 정해진 모델과 상이한 점이 발견되는 경우를 찾는 방법이다. 이 방법은 제로데이 공격(zero-day attack)과 같은 비공개 취약점[11] 이용 공격과 다른 정보보호시스템에 탐지되지 않는 신규 및 지능적인 공격까지도 탐지할 수 있다는 장점이 있어 제어망 보안을 위한 많은 연구에서 활용하고 있다. 그러나 기존 비정상행위 탐지 방식의 단점인 대량의 보안 이벤트 상에서 오경보(False Alarm)를 분류해야 한다는 것[12]을 승계한다는 문제점과, 이상 징후 감지 후 해당 공격을 분석해야 한다는 점 및 정해진 모델 내에 행해진 공격을 탐지하지 못한다는 문제점은 여전히 남아 있다[13][14].

2.2.2 오용 탐지

오용 탐지는 패턴(pattern)을 이용하여 모든 알려진 공격을 정확히 탐지할 수 있는 장점이 있다[15]. 이 방법은 특정 현상에 대한 위협은 블랙 리스트(Black-List)로, 정상은 화이트 리스트(White-List)로 구분하여 판별한다[16]. 즉, 화이트 리스트 기반의 보안 기술 적용으로 '안전'이 증명된 것만을 허용하는 것과 '악의성'이 입증된 것을 차단하는 블랙 리스트 기반의 기술은 서로 상반되는 것이다. 이때 정상적인 데이터만을 수집하여 목록화 한다면, 이 그룹은 사실상 비정상행위로부터 격리된 상태가 된다[17].

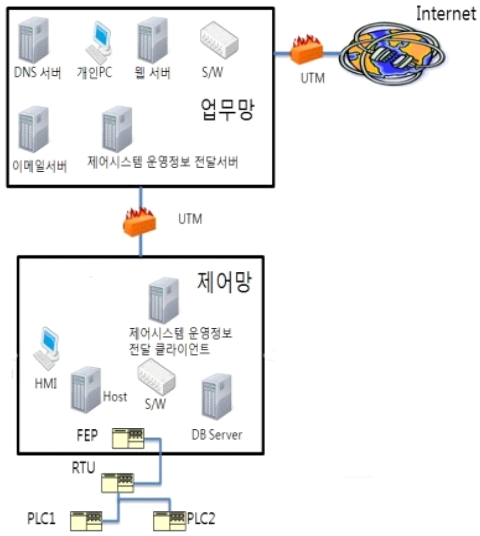
예를 들어 이메일에 IP 기반의 화이트 리스트 방식을 적용하면 사전에 입증된 정상 IP로부터의 이메일만 허용하고 이외의 IP로부터의 이메일은 차단하게 된다. 화이트 리스트는 일반적인 환경에서의 보안을 구성하기에는 많은 한계점을 지니는 것이 사실이지만, 특정 응용 프로그램만 동작하는 환경에서는 효용성을 지닐 수 있다. 응용 프로그램 수가 적고, 변동이 크지 않아 화이트 리스트로 보안성을 향상시키면서 동시에 효용성까지 확보할 수 있게 된다[18]. 따라서 화이트 리스트 방식은 제어망과 같이 민감도가 높은 환경에서 침입에 대한 탐지방식으로 적당하다.

3. 제안하는 방법

제어망에서 화이트 리스트 탐지 방식을 사용하기 위하여 우선 정상 트래픽 시나리오를 구상하고, 주요 프로토콜을 중심으로 정상 트래픽을 생성하였다. 이를 통해 알려지지 않은 트래픽에 대하여 비정상 트래픽으로 간주하고 공격으로 감지가 가능하게 하였다.

3.1 제어망 모델의 구성

(그림 2)는 본 연구에서 사용되는 제어망 모델이다.



(그림 2) 제어망 모델 구성도

3.1.1 업무망

업무망의 형태는 외부 인터넷과 UTM(United Threat Management)을 통해 연결이 되어 있고 일반적인 업무를 수행할 수 있는 사무실용 업무망으로 구성되어 있다. 여기서 UTM은 기본적인 라우터와 방화벽 기능 이외에도 AV(Anti-Virus), I

PS(Intrusion Prevention System, 침입방지시스템)등의 보안기능이 있다.

3.1.2 제어망

제어망은 인터넷과 연결되어 있지 않으며, 인터넷과 연결된 업무망과 데이터를 교환한다. 여기서 제어시스템을 구성하는 주요 디바이스를 살펴보면 <표 1>과 같다.

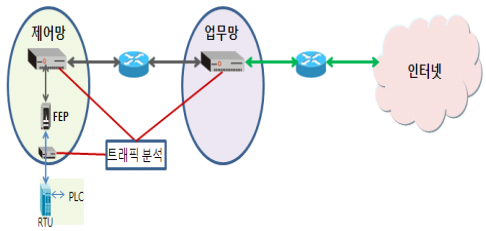
<표 1> 제어시스템 구성 디바이스

	기능
HMI (Human Machine Interface)	Host에서 처리된 정보로부터 각종 제어화면, 경보표시 및 보고서 출력 지원
HOST	제어망의 전체 노드 및 DB 관리, 각 노드로부터 취득한 실시간 데이터 처리 및 경보처리
DB Server	제어망 내의 모든 처리정보 기록
운영정보 클라이언트	서버로부터 제어망 시스템 수정/업그레이드 정보를 내려 받음
FEP (Front End Processor)	RTU가 연결된 통신회선과 주 제어장치인 Host 사이에서 메시지 전송과 수신, 패킷의 조립 및 해체를 수행하며 DNP3, TCP/IP 등 다양한 통신 방식을 지원
RTU (Remote Terminal Unit)	원격지에서 데이터를 수집해 FEP로 송신하는 원격 단말장치
PLC (Programmable Logic Controller)	각종 릴레이, 타이머, 카운터 등의 기능을 마이크로프로세서 프로그램을 통해 제어할 수 있도록 통합한 장치

3.2 제어망의 정상트래픽 생성

3.2.1 제어망 모델에서의 트래픽 분석

제어망과 연관되어 이동되는 패킷의 흐름은 보안 위협의 침입 경로가 된다. 그러므로 각 망을 연결하는 부분을 분류하여 트래픽 분석을 하는 것이 핵심이 되며 이와 같이 흐르게 되는 정상 트래픽은 화이트 리스트 탐지방식을 위한 배경 데이터(background data)가 된다. (그림 3)은 제어망 모델에서 트래픽 분석 지점을 나타낸 것이다.



(그림 3) 제어망 모델에서 트래픽 분석 지점

3.2.2 정상트래픽 배경 데이터 생성

제어망과 연관된 패킷의 흐름을 침입 경로에 따라 분류하면 업무망 내부, 제어망 내부, 업무망과 제어망 사이, 제어망의 FEP와 직렬로 연결된 원격 필드 사이트 사이로 나눌 수 있다. 따라서, 정상트래픽 배경 데이터 생성을 위한 경로 분류를 하게 되면 <표 2>와 같다.

<표 2> 배경 데이터 생성을 위한 경로 분류

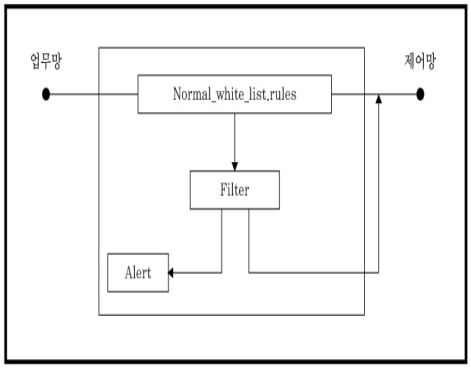
경로 분류	각 장치
업무망 내부 트래픽	DNS서버, 웹서버, 이메일서버, 개인 PC, 운영정보 전달 서버
제어망 내부 트래픽	HMI, HOST, FEP, DB서버, 운영정보 전달 클라이언트
업무망과 제어망 사이 트래픽	업무망 + 제어망
제어망과 필드 장치 사이 트래픽	제어망 + RTU, PLC

4. 화이트 리스트 기법 적용 결과

4.1 화이트 리스트 구성

업무망에서 제어망으로 들어오는 패킷들은 화이트

리스트 기법을 적용한 검사를 받게 되며, 이를 통해 비정상적 행위를 탐지할 수 있다. 이때, 정상 행위에 대하여 구성된 Normal_White_list.rules를 바탕으로 비정상행위에 대한 경고(Alert)를 하게 된다. (그림 4)는 이 과정이 수행되는 것을 구성도로 나타낸 것이다.



(그림 4) 화이트 리스트 적용 구성도

4.2 정상적 내부 트래픽 패턴 생성

4.2.1 업무망 내부 트래픽

업무망 내에서의 정상적인 내부 트래픽을 생성하기 위하여 구성된 세션 정보는 송신자 IP주소/Port, 수신자 IP주소/Port이며, 이를 통해 Normal1_White_list.rules 파일이 생성된다. <표 3>은 정상적 업무망 내부 트래픽 생성하여 세션정보를 추출하기 위한 표이다.

<표 3> 정상적 업무망 내부 트래픽

Form		To	
ADD_A(업무망)		ADD_B(업무망)	
Source IP	Source Port	Destination IP	Destination Port
192.168.1.10	4875	192.168.1.60	80
192.168.1.30	4875	192.168.1.50	80
…	…	…	…

4.2.2 제어망 내부 트래픽

제어망 내에서의 정상적인 내부 트랙픽을 생성하기 위한 세션정보를 구성하여 Normal2_White_list.rules 파일을 생성한다. <표 4>는 정상적 제어망 내부 트래픽 생성하여 세션정보를 추출하기 위한 표이다.

<표 4> 정상적 제어망 내부 트래픽

Form		To	
ADD_C(제어망)		ADD_D(제어망)	
Source IP	Source Port	Destination IP	Destination Port
192.168.100.13	80	192.168.100.18	28
192.168.100.6	5430	192.168.100.4	21
…	…	…	…

4.2.3 업무망과 제어망 사이 트래픽

업무망과 제어망 사이의 트래픽을 생성하기 위한 세션 정보를 구성하여 Normal3_White_list.rules 파일을 생성한다. <표 5>는 정상적 업무망과 제어망간 내부 트래픽 생성하여 세션정보를 추출하기 위한 표이다.

<표 5> 정상적 업무망과 제어망 사이 트래픽

Form		To	
ADD_A(업무망)		ADD_C(제어망)	
Source IP	Source Port	Destination IP	Destination Port
192.168.1.23	80	192.168.100.8	28976
192.168.100.30	28976	192.168.1.23	80
…	…	…	…

4.2.4 제어망과 필드장치 사이 트래픽

제어망과 필드장치 사이의 트래픽을 생성하기 위한 세션 정보를 구성하여 Normal4_White_list.rules 파일을 생성한다. <표 6>는 정상적 제어망과 필드장치간 내부 트래픽 생성하여 세션정보를 추출하기 위한 표이다.

<표 6> 정상적 제어망과 필드장치 사이 트래픽

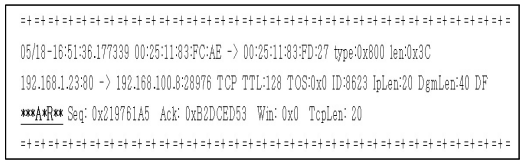
Form		To	
ADD_D(제어망)		ADD_E(필드장치)	
Source IP	Source Port	Destination IP	Destination Port
192.168.100.7	serial	192.168.109.3	serial
192.168.109.3	serial	192.168.100.7	serial
…	…	…	…

4.3 적용 시 문제점 및 개선방안

생성된 정상적 내부 트래픽 패턴에 대한 룰을 기준으로 설계된 제어망 모델에 적용하여 트래픽을 분석할 수 있다. 이 경우 트래픽은 정상과 비정상행위의 2그룹으로 분류되며, 정상적인 제어시스템 운영과 관련된 내용만을 확인할 수 있는 장점이 있다. 그러나 다음의 예와 같은 오경보가 발생할 수 있으며, 이에 대한 지속적인 대응이 필요하다.

4.3.1 정상적 내부 트래픽 패턴의 오경보

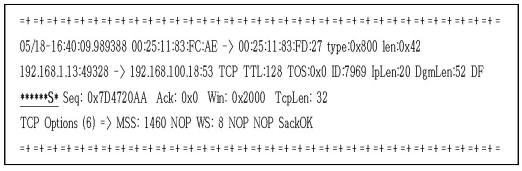
정상적인 내부 트래픽 패턴이 화이트 리스트에 등록되지 않았거나, 추가적으로 발생한 정상적 내부 트래픽 패턴에 대한 업데이트가 수행되지 않는다면 오경보가 발생하게 된다. (그림 5)는 업무망과 제어망 사이의 트래픽을 snort로 탐지한 결과이며, 정상적 내부 트래픽 패턴의 오경보 예를 보여준다.



(그림 5) 정상적 내부 패턴에 대한 오경보

4.3.2 비정상적 내부 트래픽 패턴의 오경보

(그림 6)은 업무망과 제어망 사이의 트래픽을 snort로 탐지한 결과이다. 비정상적 업무망과 제어망 사이의 트래픽을 일어났음에도 Normal3_White_list.rules에서 경보가 발생하지 않은 예를 보여준다.



(그림 6) 비정성적 내부 패턴에 대한 오탐

4.3.3 오경보 개선방안

이와 같이 정상적·비정상적 내부 트래픽 패턴의 오경보율을 줄이기 위해서는 첫째, Normal_Whit_list.rules를 정상적 시나리오에 맞게 설계를 하여야 한다. 둘째, 경보가 발생하였을 때는 해당 패킷에 대하여 정상적인지 오경보인지를 확인하여 룰에 적용하여야 한다. 셋째, 트래픽 패턴의 변경이 있는 경우 해당 룰을 업데이트 해야 한다. 그리고 마지막으로 비정상적 시나리오를 작성하여 주기적으로 Normal_Whit_list.rules를 점검하여야 한다.

5. 결 론

폐쇄적으로 구축되었던 제어망이 최근 업무 상 편의 또는 대외 기관과의 협력 필요 등으로 외부와 연동되면서, 일반적인 네트워크 환경과 유사하게 변화하고 있다[19]. 이에 따라 제어망에 대한 보안 위협이 증가하고 있기에 본 연구는 화이트 리스트 기법을 적용한 이상 징후 탐지를 통한 보안성 확보 방안을 제시하였다.

제시된 방법은 정상 행위 이외의 모든 데이터의 위험성을 경고하기에 위협으로 인한 피해와 파급효과가 큰 제어망을 감시하기에 적합하다. 그러나 네트워크 트래픽은 시간과 업무 형태 변화에 따른 변동성이 크고, 용량도 거대하여 분석에 필요한 시간 소요가 많다. 따라서 제시된 방법은 업무 절차를 기준으로 발생해야 할 트래픽 패턴을 예측하여 룰 업데이트에 활용하는 방안 등과 같은 추가적 연구를 통해 향후 더욱 발전되어야 한다.

참고문헌

[1] 김경아, 이대성, 김귀남, "공격 트리를 이용한 산업제어 시스템 보안 위험 분석", 정보·보안 논문지, 제11권, 제6호, 2011

[2] Béla Genge, Christos Siaterlis, Igor Nai Fovino and Marcelo Masera, "A cyber-physical experimentation environment for the security analysis of networked industrial control systems", Computers & Electrical Engineering, In Press, Corrected Proof, Available online 21 July 2012.

[3] A. Nicholson, S. Webber, S. Dyer, T. Patel and

H. Janicke, "SCADA security in the light of Cyber-Warfare", Computers & Security, Vol. 31, Issue 4, pages 418 - 436, June 2012.

[4] 최명균, 이동범, 곽 진, "제어 시스템에 대한 보안 정책 동향 및 보안 취약점 분석", 정보보호학회지, 제21권, 제5호, pages 55 - 64, 2011.

[5] 김인중, 정윤정, 고재영, 원동호, "중요핵심기반시설(SCADA)에 대한 보안 관리 연구", 한국통신학회논문지, Vol. 30, No. 8C, 2005.

[6] 김영진, 이정현, 임종인, "SCADA시스템의 안정성 확보방안에 관한 연구", 정보보호학회논문지, 제19권, 제6호, pages 145 - 152, 2009.

[7] "ScanSafe Global Threat Report", http://www.scansafe.com/__data/assets/pdf_file/9471/Q3_2008__GTR.pdf, 2008.

[8] 김민준, 김귀남, "데이터 마이닝 기반 보안관제 시스템", 정보・보안 논문지, 제11권, 제6호, pages 3 - 8, 2011.

[9] 고폴린, 최화재, 김세령, 권혁민, 김휘강, "트래픽 자기 유사성(Self-similarity)에 기반한 SCADA 시스템 환경에서의 침입탐지방법론", 정보보호학회논문지, 제22권, 제2호, pages 267 - 281, 2012.

[10] 김완집, 김휘강, 이경호, 염흥열, "도시 기반시설 SCADA 망의 위험분석 및 모니터링 모델 연구", 정보보호학회논문지, 제21권, 제6호, pages 67 - 81, 2011.

[11] Animesh Patcha and Jung-Min Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Computer Networks, Vol. 51, Issue 12, Pages 3448 - 3470, 22 August 2007.

[12] 신문선, 류근호, "침입탐지시스템의 성능향상을 위한 결정트리 기반 오경보 분류", 정보과학회논문지, 제34권, 제6호, pages 473 - 482, 2007.

[13] E. Carl, S. Eugene, and M. Jim, "Intrusion Detection and Prevention", McGraw-Hill, 2004.

[14] C. Frederic and M. Alexander, "Alert Correlation in a Cooperative Intrusion Detection Framework", IEEE Symposium on Security and Privacy, 2002.

[15] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel and Muttukrishnan Rajarajan, "A survey of intrusion detection techniques in Cloud", Journal of Network and Computer Applications, In Press, Corrected Proof, Available online, 2 June 2012.

[16] Tsong Song Hwang, Tsung-Ju Lee and Yuh-Jye Lee, A Three-tier IDS via Data Mining Approach, Proceedings of the 3rd Annual ACM Workshop on Mining Network Data, pages 1 - 6, MineNet 2007, 2007.

[17] Frédéric Giroire, Jaideep Chandrashekar, Nina Taft, Eve M. Schooler and Dina Papagiannaki, "Exploiting Temporal Persistence to Detect Covert Botnet Channels", Recent Advances in Intrusion Detection, 12th International Symposium, RAID 2009, Lecture Notes in Computer Science, 5758, Springer, pages 326 - 345, 2009.

[18] http://pdf.datanet.co.kr/207/207153.PDF

[19] J. Lee, H. Lee and S. Kim, "Development Plan of Korean - Energy Management System", Proc. of the 17th Conference of the Electric Power Supply Industry, pp.1-3, 2008.

[저 자 소 개]

이 동 휘 (DongHwi Lee)

2000년 경기대학교 컴퓨터과학과 (이학사)
2003년 경기대학교 정보보호기술공학과 (공학석사)
2006년 경기대학교 정보보호학과 (정보보호학박사)
2011년~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering, Researcher
2012년 ~ 현재 경기대학교 산업보안학과

email : dhclub@naver.com

최 경 호 (KyongHo Choi)

2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2012년 경기대학교 연구교수 (산업기술보호특화센터)

email : cyberckh@gmail.com