韓國 컴퓨터情報學會 論文誌
第8卷 第4號, 2003. 12.

2003 8-4 2-4

보안정책 기반 침입탐지 시스템 모델 설계

김 강*, 전종식**

Design of Security Policy-based Intrusion Detection System Model

Kim Kang*, Jong-Sik Jeon**

요 약

컴퓨터네트워크의 확대 및 인터넷 이용의 급격한 증가에 따른 부작용으로 컴퓨터 보안문제가 중요하게 대두되고 있다. 따라서, 침입자들로부터 위험을 줄이기 위해 침입탐지시스템에 관한 연구가 활발하다. 특히, 본 논문은 침입탐지시스템을 바탕으로 한 새로운 보안정책 기반 침입탐지 시스템 모델을 제안하고, 이를 설계 및 프로토타입을 구현하여 그 타당성을 보인다. 제안한 모델에서 보안정책 기반 침입탐지시스템들은 여러 컴퓨터에 분산되고, 분산된 보안정책 기반 침입탐지시스템들 중에서 어느 하나가 특정 프로세스에 의해 발생된 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지한 경우에 이를 다른 보안정책 기반 탐지시스템들과 서로 동적으로 공유하여 새로운 침입에 대하여 대응책을 향상시킨다.

Abstract

Computer security is considered important due to the side effect generated from the expansion of computer network and rapid increase of the use of internet. Therefore, Intrusion Detection System has been an active research area to reduce the risk from intruders. Especially, The paper proposes a new Security Policy-based Intrusion Detection System Model, which consists of several computer with Intrusion Detection System, based on Intrusion Detection System and describes design of the Security Policy-based Intrusion Detection System model and prototype implementation of it. The Security Policy-based Intrusion Detection Systems are distributed and if any of distributed Security Policy-based Intrusion Detection Systems detect anomaly system call among system call sequences generated by a privilege process, the anomaly system call can be dynamically shared with Security Policy-based Intrusion Detection Systems, This makes the Security Policy - based Intrusion Detection Systems improve the ability of countermeasures for new intruders.

▸ Keyword : 1. 보안정책, 2. 침입탐지, 3. 침입탐지 모델설계

* 강원관광대학 관광정보처리과 조교수 ** 강원관광대학 관광정보처리과 전임강사

Ⅰ. 서 론

최근에는 인터넷에 접속하는 사용자 수가 폭발적으로 증가하고 인터넷을 통하여 제공되는 다양하고 새로운 서비스는 개인뿐만 아니라 정부, 기업, 은행, 병원 등 사회 모든 분야에서 사용되고 있다. 이러한 서비스를 안전하게 이용할 수 있고 각종 보안 위협요소를 방어하기 위한 정보보호 서비스가 절실히 요구되고 있다[1].

특히 인터넷은 개방형 구조를 가지고 있어 서비스 품질(Quality of Service : QoS)의 보장과 네트워크의 관리가 어렵고, 기반 구조의 취약성으로 인하여 타인으로부터의 해킹 및 정보 유출 등의 위협으로부터 노출되어있다. 따라서 현재는 인터넷상에서 서비스 품질(Quality of Service : QoS), 네트워크 관리, 시스템 보안 등 에 대한 문제를 해결하기 위해 사용자나 침입자에 대한 불법적인 사용과 시스템의 남용에 대하여 여러 모델들이 개발되었다[2].

하지만 침입탐지 시스템에 대한 통제가 용이하지 않고 갈수록 다변화 된 침입에 대해 대처하기가 어렵고 시스템 환경에 적합한 시스템개발과 대규모 네트워크에 대한 효율적인 탐지 구조를 갖고 있지 않다. 이에, 본 연구에서는 탐지 대상을 특정 프로세스(Privilege Process)가 수행할 시 발생하는 비정상적인 시스템에 대한 탐지를 분산된 각각의 탐지 시스템들이 서로 능동적으로 공유하여 침입탐지시스템을 설계하고 구현하였다.

Ⅱ. 침입탐지 기법

1. 침입탐지 시스템

침입탐지 시스템은 데닝(Denning,1987년)이 최초로 제안한 후 많은 탐지 모델들이 개발되었다.

1.1 오용탐지 모델(Misuse Detection Model)

오용탐지 모델은 시스템의 로그정보와 네트워크에서 발생되는 패킷 정보와 미리 침입으로 알려진 침입 패턴들과 비교하여 침입을 검출하는 방법이다.

1.2 비정상 행위 탐지 모델(Anomaly Detection Model)

비정상 행위 침입은 컴퓨터시스템의 자원이 비정상적인 행위나 사용에 근거한 침입을 이야기하며, 사용자의 프로그램 사용과 시스템의 상태 등을 프로파일로 작성하고 이를 침입으로 규정된 프로파일과 비교하여 이들 행위간의 차이를 갖고 침입에 대한 판정을 내리게 하는 모델이다[3].

2. 침입탐지 모델

2.1 Dorothy Denning Model

침입탐지에 대한 연구는 1980년 John Andorson의 의해 처음 소개되어 1987년에 일반적인 침입탐지 모델이 제시되었다[4].

이 모델은 시스템의 비상적인 형태의 사용에 대해서 시스템의 로그 기록을 모니터링 함으로 침입을 탐지하는 모델로 미리 정의된 통계적인 방법들을 사용하여 시스템의 행위를 계산하는 변수들을 이용하고 있다.

2.2 Shiuh-Pyng Shieh Model

Shieh 모델은 직접관계에서 시스템 상태와 상태 전이, 주체(Subject)와 객체(Object)사이의 간접관계를 나타내는 규칙으로 정의된다. 시스템 상태는 감사추적에서 캡쳐되고, 보호그래프로 표현된다.

보호그래프는 주체와 객체 두 가지 타입의 노드를 가지고 있으며, 주체는 프로세스와 사용자들을 표현하는 능동적인 노드로서 주체와 객체 사이의 데이터와 권한의 흐름을 발생하는 것이다. 또한 객체는 수동적인 노드로서 파일이나 디렉토리와 같은 데이터 컨테이너(Container)를 나타내고, 데이터나 권한의 흐름과 같이 행위를 초기화한다.

시스템 상태는 방향에 있는 보호그래프 G(V, E, C, F)로 표현한다. 이 그래프는 노드들의 집합 V, 레이블에 있는 간선들의 집합 E, 보호집합들의 집합 C, 합법적인 흐름 행렬 F로 구성된 구조를 가진다.

즉 노드들의 집합 V는 주체와 객체들로 구성되고 주체 Si와 객체 Oi는 그래픽 보호로 표현되고 접속오퍼레이션은 노드 V_1과 V_2사이에서 발생하고 Present_relation (V_1, V_2)으로 표현된다.

여기서 Present_relation ∈ {r, w, d, cd}이다.

Present relation은 r, w, d, cd로 정의하는데 알려진 침입 패턴들은 데이터와 권한의 흐름의 네 가지 형태로 특성화시킨 모델이다.

2.3 Sandeep Kumar Model

Kumar 모델은 Jensen에 의해서 CPN에 근거하고 있으며, 침입행위는 칼라 페트리 네트로 표현하고 네트에서 하나 이상의 초기 상태들과 하나의 최종 상태는 모델에서 매칭을 정의하기 위해서 사용되는 모델이다[5].

특히 문맥은 토큰의 칼로로 저장되고, 조건(Condition)은 가드식(Guard expression)을 이용하고 행위(Action)는 상태의 행위를 이용하여 표현된다.

III. 제안 보안정책기반 침입탐지 시스템모델의 설계

1. 제안한 침입탐지 시스템 모델

제안한 보안정책기반 침입탐지시스템은 네트워크를 통하여 동질형의 여러 호스트에 분산된 탐지시스템을 포함하고, 각각의 호스트는 자신의 침입탐지시스템을 통해서 호스트에서 발생하는 이벤트들을 모니터링 하면서 이미 설정된 정상적인 이벤트 패턴 정보에 따라서 침입여부를 판단하도록 하였다[6]. 이때, 각 호스트에서 감시하는 대상은 모든 호스트에 존재하는 동일한 객체(Object)이며, 각 호스트는 각각의 객체에 대하여 비정상 이벤트를 공유하면서 새로운 침입으로부터 전체 시스템에 탐지를 향상시킨다.

제안한 보안정책기반 침입탐지시스템은 침입패턴을 공유하는 모델로서 서버에서는 모니터링하는 객체에 대하여 정상행위 정보를 갖고 있으며, 각 호스트의 침입탐지시스템은 각각의 객체에 대해 호스트에서 발생하는 정상적인 행위를 수집하여 침입을 탐지한다[7,8]. 특히 호스트에서 정상적인 행위를 수집한 후 호스트에 침입이 발생하면 침입시스템은 자신의 정상행위정보를 통하여 침입여부를 판단하고 침입이라 판단이 되면 서버에 침입 패턴을 전송한다. 또한 서버는 전송된 침입패턴이 서버의 정상적인 행위 정보에 존재하지 않는 경우에는 모든 침입탐지시스템에 이를 전달하여 모든 침입탐지시스템이 침입패턴을 이용하여 부정적인 탐지를 통해 침입을 탐지할 수 있게 하였다. 제안한 보안정책기반 탐지시스템은 침입을 탐지하였을 경우에는 침입행위를 계속할 수 없게 침입에 사용하는 프로세스를 강제로 종료시키도록 하였다.

2. 기존시스템과 제안한 시스템과의 관계

기존 침입탐지시스템과 제안한 보안정책기반 침입탐지시스템과의 관계를 〈표 1〉알아보면, 기존시스템은 외부로부터 침투를 방지하는 방화벽을 구성하는 반면에 제안한 보안정책기반 침입탐지시스템은 외부침입으로부터 보호하는 방화벽과 내부사용자의 오용을 방지하는 엑세스제어 및 암호시스템을 통해서 시스템을 보호하고, 침입이 탐지되면 사용하는 프로세스를 강제로 종료하도록 하였다. 또한 새로운 침입이 발생하면 정상적인 행위의 정보를 통해 침입 유무를 판단하고 침입으로 판단될 경우에는 침입패턴을 모든 침입탐지시스템에 추가하여 침입을 즉각적으로 탐지할 수 있도록 하였다.

표 1. 침입탐지시스템 비교
Table.1 Comparison of Intrusion Detection System

구 분	기존침입 탐지시스템	제안 침입탐지시스템
방어	방화벽	방화벽, 엑세스제어시스템, 암호시스템
대응방법	침입체소멸	- 프로세스 강제종료 - 정상적인 행위 패턴을 이용하여 모든 침입탐지시스템에 공유
탐지오류	자체문제발생	긍정적 결함

3. 보안정책기반 침입탐지시스템 설계

제안한 보안정책기반 침입탐지시스템은 분산된 각각의 호스트에 설치되어있는 침입탐지시스템이 서브감시시스템을 통해서 특정프로세스에 의해 생성된 시스템호출 정보를 추출하여 이미 설정되어 있는 비정상 시스템의 호출 패턴과 정상적인 시스템 호출 패턴을 비교하여 비정상적인 시스템 호출을 탐지하고 정책기반 네트워크를 이용하여 분산된 각각의 침입탐지 시스템들과 서로 정보를 공유하여 모든 호스트에 설치되어있는 침입탐지시스템들이 새로운 침입에 대한 정보를 증가시켜 침입으로부터 강력한 차별화된 대응책을 구축하는 보안정책기반 침입탐지시스템을 설계하였다.

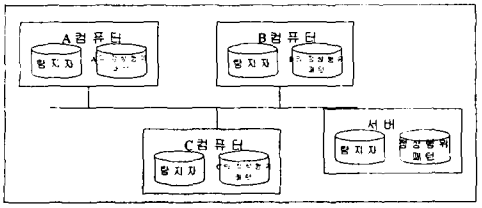

그림 1. 보안정책기반 침입탐지시스템 구성도
Fig. 1 System Configuration of security Policy-based Intrusion Detection

4. 보안정책기반 침입탐지시스템 기능설계

보안정책기반 침입탐지는 패킷의 헤더와 내용에서 얻은 정보와 침입으로 정의한 침입 패턴 정보와 비교하여 침입을 판정하는 구조로 동작하게 된다.

탐지 구성요소에서 침입이 탐지되는 경우에는 침입 경고 모듈로 전달되어 처리하게 된다.

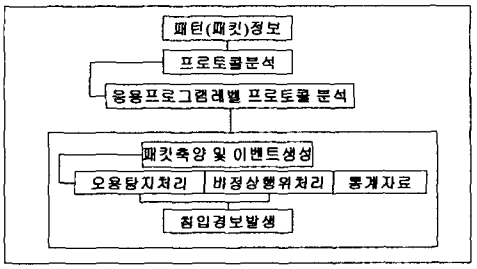

그림 2. 침입탐지 처리 흐름도
Fig 2. React of Process for Intrusion Detection

4.1 오용탐지

침입탐지는 크게 오용(misuse)탐지와 비정상적인 행위(anomaly)탐지의 두 가지 모듈로 이루어져 있으며, 먼저 패킷들을 프로토콜 별로 분류하여 침입탐지에 사용할 이벤트 정보를 축약하여 만든다. 이는 IP와 ICMP, TCP, UDP로 분류한 후 응용프로그램 레벨에서 패킷의 정보를 갖고 시스너쳐 파일에 이미 작성해 놓은 침입 패턴과 비교하여 판정을 내리게 했다. 패킷의 근원지인 주소, 목적지 주소, 목적지 포트번호(TCP, UDP), ICMP타입번호를 침입 패턴과 비교하여 탐지하도록 하였다.

IP, "src_ip = dest_ip" LAND공격
IP, "priv_OffsetData 〉 currOffsetData" TearDrop공격
ICMP, "CTYPE=20" ICMP 시간초과 공격
ICMP, "CTYPE=5, CCODE=1" ICMP PING 시도

4.2 비정상적인 행위 침입탐지

비정상적인 행위의 경우에는 패킷의 통계정보를 갖고 침입 판정을 하게된다. 서비스 거부 공격과 같은 비정상적인 행위의 탐지는 특정 호스트로 유입되는 패킷 카운터에 기반하여 탐지하게 된다. 침입탐지 시스템의 침입사건 목록에 서비스 거부공격과 관련된 목록을 포함하고 있으며 프로토콜별로 목록을 갖고 있다.

또한 패킷 카운터에 서비스 거부공격에 의한 침입탐지 방식은 주어진 시간 내에 침입사건 목록이 정의하고 있는 침입사건 항목에 해당하는 패킷이 임계치 이상 발생하였을 경우 이를 탐지하는 방식이다. 따라서 침입탐지시스템은 침입사건목록이 정의하고 있는 항목과 일치하는 패킷에 대한 지속적인 감시가 필요하며 연속적인 패킷 수신에 설정되어 있는 시간 내에 발생하였는가를 판단할 수 있는 구조가 필요하다. 따라서 먼저 침입사건목록으로부터 패킷의 프로토콜과 목적지 포트번호에 기초하여 해당 패킷의 조건에 일치하는 침입 사건의 존재 여부를 검색하도록 하였다. 만약 침입이 일치하면 해당침입사건이 탐지하도록 설정되어 있다면 침입사건 목록과 패킷의 목적지 주소에 기초하여 해당 호스트의 정보를 테이블에 추가하게 되는데 테이블에 호스트정보가 존재하지 않는다면 해당 패킷에 적당한 호스트정보를 생성하여 생성된 호스트의 카운터를 초기화하고 시작 시간을 설정한다. 일치하는 호스트 정보가 테이블에서 검색되면 해당 호스트 목록의 카운터를 검사한다. 검사결과 카운터가 0이라면 시작 시간을 기록하고 카운터를 증가시킨다.

카운터가 0이 아니면 해당 호스트 목록의 카운터를 증가시킨다. 증가된 카운터가 침입사건의 임계치와 동일한가를 검사하고 만약 호스트 목록의 카운터와 침입사건 목록의 임계치와 동일하다면 카운터를 초기화하고 침입사건 판정을 위해 카운터의 최초 시작 시간부터 현재까지의 시간 간격을 계산한다. 계산된 시간 간격이 침입 사건의 시간 간격보다 작다면 침입사건이 발생한 것으로 판단한다.

또한 정해진 시간동안 패킷 수를 갖고 침입을 판단할 때 시간 간격과 패킷의 수를 기초로 하여 임계치 자료로 침입탐지 관리 모듈에서 보안정책에 따라서 변화하게 되도록 하였다.

5. 통계적 분석

5.1 임계치를 구하는 알고리즘

(1) 임계치 알고리즘

$$T^2 = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n \quad \cdots\cdots \text{(식 1)}$$

T^2 : 비정상적인 행위를 추출하는 기준

$a_1, a_2, \cdots a_n$: 임계설정계수

$s_1, s_2, \cdots s_n$: 측정부분의 통계 값

(2) Q값 알고리즘

$$Q = \sum_{k=1} D_k \times 2^{-rt_k} \quad \cdots\cdots \text{(식 2)}$$

Q : 현재까지의 발생 총계

k : 발생사건의 인덱스

DK : k번째 감사자료와 (K+1)번째 발생사건의 데이터변화량

t_k : 가장최근에 발생된 데이터와 k번째 데이터 간의 시간차

r : Q 값의 감소율

6. 성능 평가

보안정책기반 침입탐지 모델의 특성을 고려하여 다중공격에 대하여 분석을 하고, 동적으로 동작되는 경우를 비정상적인 행위 침입탐지 시 사용하게 되는 임계치 변화에 따른 동작과 침입호스트들의 침입정보를 이용하여 성능을 비교분석하였다. 또한 기능은 서비스 거부공격 시 할당된 자원을 강제적으로 해제하는 기능 실험을 하여 성능을 분석하였다.

6.1 다중공격과 IP 스푸닝 탐지

침입탐지시스템으로부터 발생되는 침입을 탐지한 정보들을 보안정책기반 침입탐지시스템에서 분석하게 되면 한 호스트에 대하여 다중 공격들을 쉽게 탐지할 수 있다. 그리고 보안정책기반 침입탐지시스템의 침입탐지모델에서는 아래와 같은 단일 모델에서는 침입하기 어려운 침입을 효과적으로 탐지할 수 있도록 하였다. 시나리오는 다음과 같다. RST패킷을 보내 연결을 강제로 종료시키거나 호스트를 다운시키는 SYN 플러딩 공격 같은 침입 이벤트가 발생될 때는 보안정책기반 침입탐지시스템은 이를 전달해서 각 침입탐지시스템의 정책 캐쉬로 내려보내고 이를 참조하여 동일 수신 주소와 포트번호를 갖는 패킷의 경우 침입판정을 내리게 된다.

또한 스푸핑 공격을 위해 공격 탐지를 주고 있으며, 이는 RST패킷을 보내어 강제로 접속을 단절시키고 상대방 호스트와의 연결을 가로채어 정보를 보안정책기반 침입탐지시스템으로 전달되게 한다.

이 정보를 전달받은 보안정책기반 침입탐지시스템은 수신지 주소와 서비스 종류, 포트번호와 비교하여 공격을 탐지하게 된다. 기존의 단일 모델에서는 판단하기 어렵고 정보의 상호교환이 이루어지는 보안정책기반 침입탐지시스템에서는 탐지가 가능하다.

Host Attack	Attack for SYN Flooding
Alsrt ID : TCP-RST Time : 2003:08:16 11:36:09 Source Address : 129. 254. 10. 109 Destination Address : 129. 254. 10. 129 Source Port : 22250 Destination Port 18	Alsrt ID : SYN-Flood Time : 2003:08:19 14:18:05 Source Address : 129. 254. 10. 109 Destination Address : 129. 254. 10. 129 Source Port : 22256 Destination Port : 56

Alsrt ID : TCP-RST
Time : 2003:08:16 11:36:09
Source Address : 129. 254. 10. 109
Destination Address : 129. 254. 10. 129
Source Port : 22250

Alsrt ID : SYN-Flood
Time : 2003:08:19 14:18:05
Source Address : 129. 254. 10. 109
Destination Address : 129. 254. 10. 129
Source Port : 22256

그림 3. IP Spoofing 탐지 결과
Fig. 3 Detection of IP Spoofing

6.2 동적인 정책기반 집행

평가 모델에서는 정책에 따른 시스템 동작을 효율적으로 동작하는지를 알아보기 위해서, 먼저 서비스 공격 등과 같은 패킷 량에 따른 침입탐지 사건들이 발생할 경우 이를 정책 저장소에 등록하게 하였으며, 또한 침입을 시도한 호스트 주소와 호스트 서비스 프로토콜, 포트 등에 등록하여 탐지 시 사용하도록 하였다. 미리 목록에 등록되었을 경우에는 탐지 시간이 짧아짐은 시험을 통해 알 수 있었다.

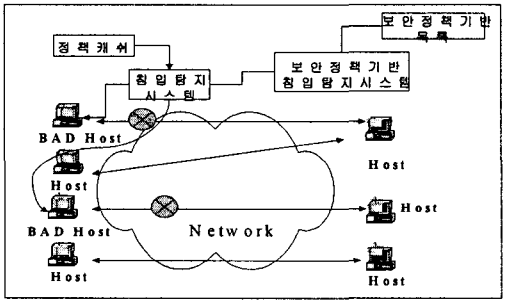

그림 4. 차단 목록에 따른 대응
Fig. 4 React with Prevent List

6.3 추적기능

추적경로를 판단하기 위하여 프로토타입에서는 수집된 정보들을 시간 값과 탐지된 영역의 침입탐지시스템으로 추정하게 되며, 특히 동작을 분석하기 위해 호스트로 Ping을 계속해서 발생시켜 보안정책기반 침입탐지시스템으로 전달하게 되고 이에 대한 정보를 각각의 침입탐지시스템으로 전달한다. 전달된 패킷의 수신주소와 프로토콜정보, 패턴 매칭을 하여 일치하는 패킷탐지 정보를 시간 값과 함께 보안정책기반 탐지시스템으로 전달하게 되며 보안정책탐지시스템에서는 호출 순으로 경로를 예측하게 된다.

Ⅳ. 결론

본 논문에서는 컴퓨터 침입탐지시스템을 바탕으로 새로운 보안정책 기반 침입탐지시스템 모델을 제안하고, 이를 설계하고 프로토타입으로 구현하여 그 타당성을 설명하였다. 제안 한 보안정책 기반 침입탐지시스템 모델은 보안정책전달을 위하여 서비스 품질보장을 위한 네트워크 관리에서 제안한 정책 기반 프레임워크를 도입하여 설계하였다. 따라서 제안한 보안정책 기반 침입탐지시스템은 어떤 공격이 특정 프로세스 행위를 정상적인 행위와 다르게 하는 경우 이를 침입으로 탐지할 수 있는 비정상적인 행위 탐지 방법을 기반으로 하는 침입탐지시스템이다. 특히, 제안한 모델에서 보안정책 기반 침입탐지시스템은 여러 컴퓨터에서 분산되고 분산된 보안정책 기반 침입탐지시스템들 중 어느 하나가 특정 프로세스에 의해 발생된 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지한 경우에는 이를 다른 보안정책 기반 침입탐지시스템들과 서로 동적으로 공유하도록 하였다.

본 논문에서는 제안한 모델의 타당성을 증명하기 위해서 모델에 대한 프로토타입에서 실험을 하였으며, 실험결과 단일시스템에서 탐지가 어려운 다중공격이나 IP스푸핑 등의 탐지에 효과적임을 알 수 있었다. 또한 상호협조를 통한 추적과 침입탐지 시 사용되는 탐지 임계 값들의 동적인 변화에 따른 기능과 효과를 확인하였다.

향후 연구과제는 침입탐지시스템의 보안정책관리를 위한 보안정책정보의 표준화 패턴들을 관리하는 통합관리 프레임워크의 확장에 대한 연구가 필요하다.

Ⅴ. 참고문헌

[1] 조은경, "이형 보안영역에서의 IP보안서비스를 위한 보안정책 시스템연구", 충남대 박사학위논문, 2000. 2.

[2] Mansour Esmaili, Rei Safavi-Naini, "Case-Based Reasoning for Intrusion Detection", Computer Security Applications Conference, pp. 214-222, 1996.

[3] Dorothy E. Denning, "A Intrusion-Detection Model.", IEEE Trans. on Software Engineering, No2. pp.222-232, 1997.

[4] D. E. Denning, "An Intrusion-Detection Model", IEEE Trans. on Software Engineering, No. 2, Feb., 1987.

[5] S. Kumar, E. Spafford, "A Pattern matching model for misuse intrusion detection", In Proceedings of the 17th National Computer Security Conference, pp. 11-26, Oct., 1994.

[6] CIAO, National Plan for Information Systems Protection, Version 1.0 : An Invitation to a Dialogue, Jan., 2000.

[7] NIST Security Requirement for Cryptographic Modules(FIPS 140-2), 2002.

[8] Guidelines on Firewalls and Firewall Policy, NIST SP800-41, 2002.

저 자 소 개

김 강

1992년 숭실대학교 정보산업학과 (석사)

2003년 대전대학교 컴퓨터공학과 (박사)

현 재 강원관광대학 관광정보처리과 조교수

전 종 식

1996년 청주대학교 전자공학과 (석사)

2001년 청주대학교 전자공학과 (박사수료)

현 재 강원관광대학 관광정보처리과 전임강사