정보시스템에 대한 보안위험분석을 위한 모델링 기법 연구

김 인 중[†] · 이 영 교[††] · 정 윤 정[†††] · 원 동 호[††††]

요 약

최근 대부분의 정보시스템은 대규모 및 광역화되고 있으며 이에 따른 사이버 침해사고와 해킹의 위험성이 증대되고 있다. 이를 해결하기 위하여 정보보호기술중에서 보안위험분석 분야의 연구가 활발하게 이루어지고 있다. 하지만 다양한 자산과 복잡한 네트워크의 구조로 인하여 위험도를 현실에 맞게 산정한다는 것이 사실상 불가능하다. 특히, 취약성과 위협의 증가는 시간에 따라 계속 증가하며 이에 대응하는 보호대책은 일정 시간이 흐른뒤 이루어지므로 제시된 결과가 효과적인 위험분석의 결과로 볼 수 없다. 따라서, 정보시스템에 대한 모델링 기법을 통하여 정보시스템의 구조를 단순화하고 사이버 침해의 방향성을 도식화함으로써 위험분석 및 피해 파급 영향 분석을 보호대책 수립의 허용 시간 내에서 이루어질 수 있도록 해야 한다.

이에 따라, 본 논문에서는 보안 위험을 분석할 수 있도록 SPICE와 Petri-Net을 이용한 정보시스템의 모델링 기법을 제안하고, 이 모델링을 기반으로 사례연구를 통하여 위험분석 시뮬레이션을 수행하고자 한다.

키워드 : 모델링, 위험분석, 페트리넷, 스파이스, 시뮬레이션

A Study on the Modeling Mechanism for Security Risk Analysis in Information Systems

Injung Kim[†] · Younggyo Lee[††] · Yoonjung Chung[†††] · Dongho Won[††††]

ABSTRACT

Information systems are today becoming larger and mostly broadband-networked. This exposes them at a higher risk of intrusions and hacking than ever before. Of the technologies developed to meet information system security needs, risk analysis is currently one of the most actively researched areas. Meanwhile, due to the extreme diversity of assets and complexity of network structure, there is a limit to the level of accuracy which can be achieved by an analysis tool in the assessment of risk run by an information system. Also, the results of a risk assessment are most oftennot up-to-date due to the changing nature of security threats. By the time an evaluation and associated set of solutions are ready, the nature and level of vulnerabilities and threats have evolved and increased, making them obsolete. Accordingly, what is needed is a risk analysis tool capable of assessing threats and propagation of damage, at the same time as security solutions are being identified. To do that, the information system must be simplified, and intrusion data must be diagrammed, using a modeling technique.

In this paper, we propose a modeling technique for information systems to enable security risk analysis, using SPICE and Petri-net, and conduct simulations of risk analysis on a number of case studies.

Key Words : Modeling, Risk Analysis, Petri-Net, SPICE, Simulation

1. 서 론

정보시스템에 대한 보안위험분석[1]은 요구되는 정보보호 서비스의 취약점을 해결하고 위협으로부터 시스템을 안전하게 관리할 수 있는 최선의 방법이다. 현재 정보시스템은 광역화되면서 자산의 규모도 대규모화되고 제어시스템과 같은 이기종 시스템과의 연동도 이루어지고 있다[2]. 따라서, 위험분석 프로세스도 새롭게 정의되어야 한다. 위험분석은 자산, 위협, 취약점을 분석하고 이에 대한 위험도를 계산하는 것으로 방법론 및 도구가 공개되고 있다. 최근에는 정보보호컨설팅 및 정보보안관리시스템에서 요구되는 보호대책 수립 및 잔여위험분석에 대한 객관성과 종합적이고 체계적인 타당성을 입증하기 위한 연구를 수행하고 있으며 이를 통하여 피해파급 및 영향분석분야에 연구가 많이 진행되고 있다 [26], [27], [31]. 한편, 정보시스템에 대한 위험분석 시뮬레이션은 매우 흥미로운 분야로 대두되면서 이 분야에 대한 연구와 토론이

† 정 회 원 : 국가보안기술연구소 선임연구원
†† 준 회 원 : 안양과학대학 컴퓨터정보학부 강사
††† 준 회 원 : 국가보안기술연구소 선임연구원
†††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2005년 2월 11일, 심사완료 : 2005년 10월 26일

많이 벌어지고 있다. 하지만, 정보시스템에 대한 모델링 기법이 제대로 이루어져 있지 않아서 위험분석 연구에 어려움을 갖게 되었다. 즉, 날로 복잡해지는 정보시스템 환경에서 보안요구사항에 즉각적이고 효율적이며 더욱 저렴한 비용으로 대응할 수 있는 위험분석을 수행하려면 시스템 모델링이 요구된다. 위험분석을 위한 정보시스템 모델링은 시스템 개발 조직, 관리 조직, 운영 조직 및 보안 조직간 통역 역할을 수행한다. 정보 관련 보안요구 사항을 정식화된 모델링을 통해 도식화하고 시각화하면 사용자나 운영자 모두 각자 사이버 침해에 대한 경로 및 피해 파급 영향을 이해 할 수 있고 자산의 중요성 측면뿐만 아니라 위협과 취약점에 대한 보안 요구사항들을 쉽게 파악할 수 있게 된다.

따라서, 정보시스템의 모델링을 통해 정보시스템의 활동, 자원, 정보흐름 등을 분석하고 이에 대한 사이버 침해에 따른 피해 영향 및 분포 등을 표현할 수 있어야 한다. 이러한 모델링은 시스템 관리자와 위험분석 컨설턴트간의 의사소통 수단이므로 정형성 및 표현성을 갖도록 한다. 어느 자산이 중요하고 어느 업무가 어떤 형태로 이루어지고 있는 지를 기존 네트워크 구성도만을 통해서 알 수 없기 때문이다. 이러한 배경에서 본 논문에서는 회로 설계에서 사용하고 있는 SPICE 모델링[3]과 Petri-Net[4]을 결합하여 정보시스템에 대한 정량평가가 가능하고 피해 파급 및 영향을 쉽게 분석 가능할 수 있도록 도형적인 모델링을 제안하고자 한다. 본 결과를 토대로 위험분석을 수행하는 데 사이버 침해에 대한 경로 분석과 정보보호대책에 대한 설계 단계에서 활용할 수 있게 되는 것이다.

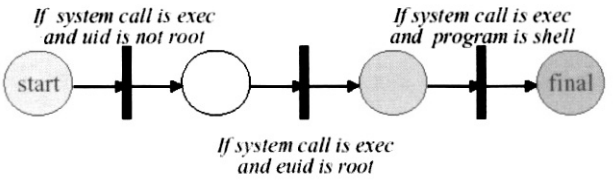
본 논문의 2장에서는 SPICE 및 Petri-Net와 기존의 위험분석 연구에 대하여 설명하고, 3장에서는 위험분석에 필요한 모형을 제시하며 이러한 모형을 통해 정보시스템을 표현하는 방법을 보인다. 4장에서는 보안위험분석을 위한 모델링 기법을 제시하고 5장에서 사례연구를 통해 유용성을 입증하고, 끝으로 결론을 맺는다.

2. 관련 연구

2.1 기존 정보시스템 모델링

기존의 정보시스템 모델링은 파워포인트나 VISIO 툴을 이용하여 네트워크를 구성하여 표현하는 것이 전부였다. 이는 자산의 현황 및 연결 형태만을 보여주는 것이 전부이며 업무의 흐름이나 피해 예상 및 파급에 대한 처리 등이 표시되지 않아서 위험분석을 수행하는 것이 적합하지 못했다.

정보의 흐름을 파악하기 위하여 플로우 차트(flow chart)나 상태전이방법(state transition approaches)을 이용할 수 있으나 정보시스템에 대한 전체적인 네트워크 구성을 표현하는 데 한계가 있다. 최근에는 상태전이 방법[5]을 좀 더 확장하여 DFSM(Deterministic Finite State Machine)[6]나 (그림 1)과 같은 Colored Petri Net(CPN)[7]을 통하여 이벤트의 순서와 요소를 직접 표현하고 사이버 침해의 행위와 결과를 시스템 상태에서 쉽게 표현 할 수 있도록 하는 방안이 제시되고 있다.

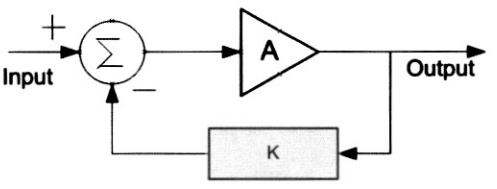


(그림 1) Colored Petri-Net 구조

상태 전이방법은 사이버침해에 대한 영향 및 피해 경로만을 구성함으로써 위험분석을 수행하기에는 여러가지 제한조건을 갖는다. 정보시스템을 모델링을 통해 표현하기에는 자산별로 독특한 특성을 포함할 수 없고, 방향에 따른 피해의 분포가 일정하지 않다. 그리고 패트리넷 기반의 모델링은 수행시간 및 비용에 대한 정량평가 방법이 제시되지 못하고 정보 시스템내의 업무 흐름만을 도식화하므로 사이버 침해의 흐름은 분석할 수 없다. 따라서 이러한 문제점을 해결하기 위해서는 침해 경로 및 피해 영향을 분석할 수 있는 방안이 필요하다.

2.2 SPICE 모델링

SPICE(Simulation Program with Integration Circuit Emphasis)[8]는 간단한 전자회로를 각 소자에 대한 등가회로를 중심으로 시뮬레이션을 할 수 있는 방법이다. 버클리 대학에서 개발한 SPICE(Simulation Program for Integrated Circuits Emphasis) 프로그램은 회로전압, 전류, 저항 및 컨덕턴스 등의 관계를 맺어주는 행렬 방정식의 해를 구하는 것이 기본이 된다. 이 시뮬레이터는 고도로 정확한 반면 회로가 복잡한 경우 긴 시뮬레이션 시간은 필요로 한다. 회로의 설계와 편집, 시뮬레이션 그리고 그래픽 출력을 볼 수 있으며 소자에 대한 특징과 회로에 대한 구성을 라이브러리로 구성하게 되면 회로에서 발생되는 특징들을 시간별로 쉽게 분석할 수 있다.




```
Square-root circuit
Vin 1 0 0
Rin 1 0 1Eb
Efwd 2 0 poly(2) (1,0) (3,0) 0 1Eb-1Eb ; error amplifier
Efwd 2 0 1Eb
Erev 3 0 poly(2) (2,0) (2,0) 0 0 0 0 1 ; feedback section
Rrev 3 0 1Eb
.DC Vin 0 10 .1
.PROBE
.END
```

(그림 2) SPICE도구를 이용한 모델링

다만, SPICE를 이용하여 사이버 침해를 모델링하는 경우 모든 정보시스템의 자산에 대하여 일일이 열거하기에는 불필요한 정보자산이 있으며 오히려 네트워크 구성도보다 더 복

잡한 형태로 디자인되어 사이버 침해에 대한 경로 및 피해 등을 분석이 더 어려울 수 있다. 따라서, 정보시스템의 위험분석을 위하여 사용가능한 모델링 기법이 요구된다.

2.3 위험분석 연구

IT 기술의 발달로 인하여 정보시스템은 대규모화되고 분산화됨에 따라 정보시스템 위험분석과 관련된 연구는 많은 분야에서 진행되고 있는 데 먼저 도메인을 크게 3단계로 나눌 수 있다.

- 위험분석 프로세스 및 위험도 계산
- 위험분석 도구 설계 및 개발
- 통제항목, 가이드라인 연구

위험분석 프로세스는 MICTS[9], CSE(Communications Security Establishment)[10], HAZOP(HaZard and Operability study)[11], FTA(Failure Model and Effect Croticality Analysis)[12], OCTAVE[13], CORAS[14] 등이 있다. 국내에서는 PRAHA[15]이라는 방법론이 개발되어 국가·공공기관 취약점분석·평가에서 적용되고 있다.

위험분석도구는 CRAMM(CCTA Risk Anaysis and Management Methodology)[16], BDSS[17], Buddy System[18] 등이 존재한다.

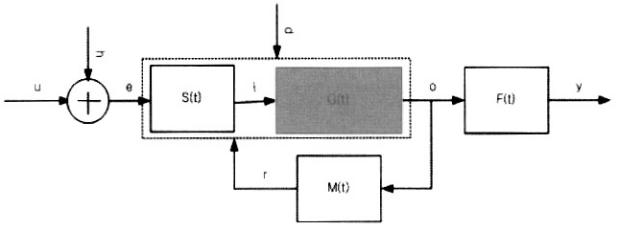
통제항목 및 기준 산정은 ISO/IEC 27001[19], BSI의 IT Baseline Protection Manual[20] 등이 연구되고 있다. 국내에서도 NCSC[21]에서 자체적으로 개발한 기준을 통해 주요정보통신기반시설에 대하여 정보보호수준을 산정할 때 기준으로 사용하고 있다.

지금까지의 대규모 정보시스템에 대한 위험분석 연구는 주기적으로 또는 변화된 정보 및 자산에 대하여 위험 변화 및 예측을 할 수 있는 기법이 제시되고 있지 않다. 즉, 정보시스템의 급격한 변화와 다양한 침해사고에 대하여 능동적으로 분석할 수 있는 기법이 아니다. 보통 위험분석은 정보시스템의 규모에 따라 최대 6개월 이상 소요될 수 있다. 따라서 보호대책을 제시한 후 적용하는 시점에서 보호대책이 불필요하거나 더 막강한 보호대책이 요구되는 경우가 발생하는 것이다. 따라서 위험분석이 실시된 후 변화된 환경에 즉시 적용가능하기 위해서는 위험분석 모델링 연구가 요구된다. 따라서 위험 변화 및 예측분야가 새롭게 연구되고 있다. 이에 대한 연구는 피해 파급과 관련된 연구분야에서 일부 수행[22]되고 있으나 아직 전체적인 구성은 미흡한 상태이다.

3. 모델링을 위한 준비 사항

3.1 정보시스템의 블록선도

일반적으로 모델링을 위해서는 대상 시스템과 자산을 정의하고 시스템의 목적, 구성 등 시스템의 기능적 한계에 대한 명확한 정의가 수행되어야 하나 본 논문에서는 시스템의 구성 자산 간의 상호 의존성과 자산 별로 비슷한 기능을 수행하는 것들을 블록으로 표현한다. 블록선도를 구성하기 전에 수행해야 할 사항으로 구성요소 및 구성요소간의 관계에 대한 관계가 명확해야 한다. 구성 요소는 자산을 식별하고 자산의 가치 및 중요성을 파악하는 것이 가장 먼저 수행되어야 한다. 이는 자산분석을 통해 이루어지는 데 정보 자산을 기밀성, 무결성, 가용성 측면에서 분류[25]하고 각 정보 자산에 대하여 매체(서버, 네트워크, 저장도구 등)와의 매핑[1]을 수행한 후 위협과 취약성을 등급별로 구분한다. 그리고 우선순위화를 통해 보호대책이 요구되는 자산을 기본으로 블록선도 내 중요자산으로 구성한다[23]. 블록선도내에는 능동적인 자산을 토대로 구성하며 수동자산 및 단말의 경우에는 중요도에서 상대적으로 낮게 나타나므로 가급적 생략하여 구성한다. 시스템을 모델링하기 위하여 (그림 3)과 같은 블록선도를 구성하고 다음과 같이 정의한다.



(그림 3) 정보시스템의 구조

[정보시스템의 구조]

IM = <G(t), S(t), M(t), F(t), e, r, y, t>

- G(t) : 정보시스템 = $\{g_1, g_2, \cdots, g_N\}$
- S(t) : 정보보호시스템 또는 암호장비
- M(t) : 모니터링 시스템 또는 관제시스템
- F(t) : 출력 자료의 통제시스템 또는 보안가드
- e : 정보보호시스템에 들어오는 입력
- r : 모니터링 또는 관제시스템으로부터 입력
- y : 정보시스템의 출력 또는 연동 시스템 입력
- h : 외부로부터의 해킹
- d : 내부자의 침해사고
- u : 사용자의 입력 또는 접근통제 수준
- t : 시간

여기서, g_i는 단위자산(elementary asset)으로 서버, 네트워크, PC를 총칭한다.

3.2 MORAIS의 구조

본 논문에서는 정보시스템 위험분석을 위한 모델링을 MORAIS(MOdeling for Risk Analysis of Information System)라고 정의하였다. MORAIS를 수행하기 위하여 먼저 모형을 정의한다. 모형은 가져야할 요구사항들을 고려하여 다음과 같이 정의한다.

3.2.1 MORAIS의 모형

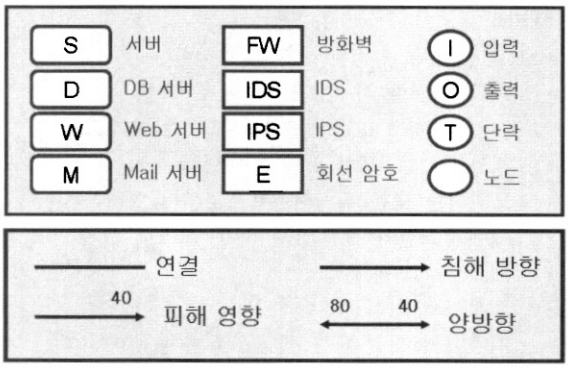
MORAIS 모형은 정보시스템 구조상의 복잡성을 단순화한

기호와 레이블된 방향성 그래프이며, 그 정의와 각 구성요소는 다음과 같이 정의한다.

- G는 정보시스템의 자산을 정의하는 집합이며, 끝이 둥근 사각형으로 표기한다. g_i에는 서버명, 보안 솔루션 여부, 각 위협 항목에 대한 시간별 장애 수준, 해당 취약성 리스트(ICAT DB)에 대한 피해 수준, 침해 입력 및 출력 방향, 시스템 활동시간, 활동비용 등이 저장된다. 사각형내에는 각 자산에 대한 이니셜을 기록한다. 피해가 발생하면 사각형의 색깔은 변하게 되며 5등급으로 구분된다.
  -흰색 : 1(안정), 노랑 : 2(주의), 파랑 : 3(경고)
  -분홍 : 4(심각), 빨강 : 5(정지)
- S, M, F는 정보시스템을 보호하기 위한 시스템이며, 끝이 각진 사각형으로 표기한다.
- node는 정보 흐름 및 사이버 침해활동에 대한 포크 및 조인관계를 정의하며 둥근 원으로 표기한다.
  -포크는 정보에 대한 분배를 의미한다.
  -조인은 정보에 대한 결합을 의미한다.
- 방향은 각 자산의 연동 및 연관관계를 위하여 선으로 구성하며 연관관계 및 피해 파급이 있는 경우에는 방향성을 갖는다. 방향성내에는 최대 피해율을 기록한다.

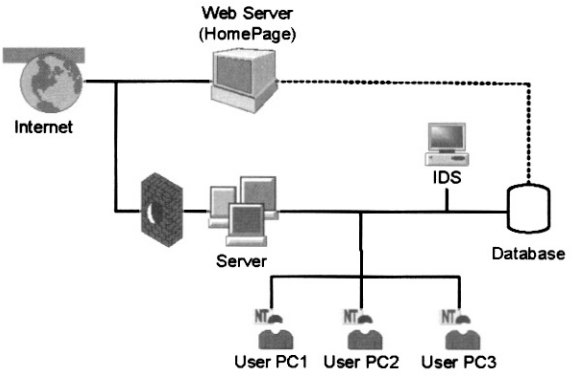
<표 1>은 이에 대한 모형들의 예이다.

〈표 1〉 각 모형의 구조

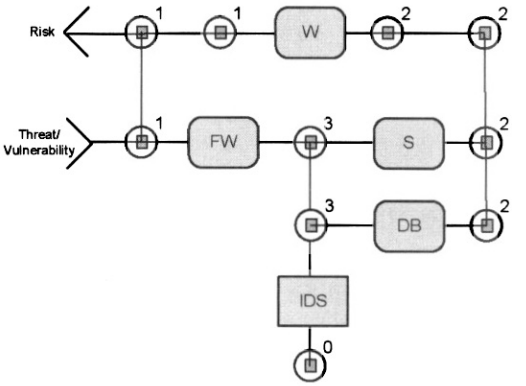


3.2.2 모형을 이용한 정보시스템의 표현

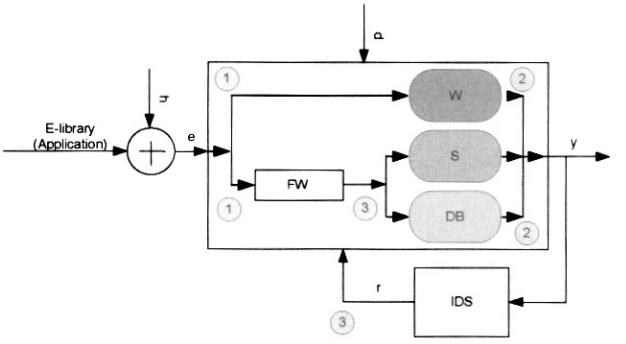
정보시스템의 표현은 블록선도를 기본으로 하여 구성 한다. (그림 4)에서와 같이 정보시스템 내부에는 웹서버, 응용서버, 데이터베이스 서버가 있다고 가정하자. 사용자는 전자 도서관 업무를 수행하면서 인터넷을 사용할 수 있다. 이러한 정보시스템의 구성도만으로는 쉽게 정보시스템의 사이버 침해에 대한 위협과 취약성을 통한 위험분석이 용이하지 않다. 따라서, (그림 5)와 같이 표현하게 되면 인터넷으로부터 해킹 위협이 발생할 수 있으며, 내부자에 의한 침해사고 등이 쉽게 인지하며 정보시스템이 보호하고 있는 대상 자산이 무엇인지를 명확하게 인지하게 된다. 5(a)는 SPICE 만을 이용하여 표현한 결과이다. SPICE 모델만으로는 모델링을 통한 분석이 용이하지 않으므로 5(b)와 같이 자산의 모형에 따라 배열을 재조정하여 분석이 용이하도록 한다. 그리고 자산간에 업무 흐름을 표시하고 흐름에 따른 상관관계를 나타낸다. 그리고 정해진 노드 사이에 자산들을 위치시킨 후 동 자산 파라메터와 네트리스트 파일을 만들어 데이터베이스화하면 시뮬레이션이 가능하게 된다. 그리고 CPN을 이용하여 각 침해로 인하여 자산에 미치는 피해 수준[32]을 색깔로 구분하게 되면 특정 자산에 대한 취약성과 위협의 크기를 파악하게 되므로 전체 위험과 피해 경로 및 범위를 알 수 있게 된다. 즉, 단순한 네트워크 구성도를 위험분석을 위한 모형과 표현을 통해 구성하면 시스템을 쉽게 이해 할 수 있으므로 사이버 침해에 따른 피해 경로 및 범위를 분석할 수 있는 기반을 마련할 수 있게 되는 것이다.



(그림 4) 일반적인 정보시스템 구성도



(a) SPICE를 이용한 표현



(b) SPICE와 CPN을 이용한 표현

(그림 5) 모형과 표현을 통한 정보시스템 구성

4. 보안위험분석을 위한 모델링

지금까지는 정보시스템에 대한 모델링을 위한 모형과 표현을 제안하였다. 이 모델링을 이용하여 보안위험분석을 수행하기 위해서는 각 자산과 네트워크 특징에 대하여 구조화해야 한다. 이를 위하여 자산에 대한 파라메터와 네트워크의 연결 구조를 다음과 같이 정의한다.

4.1 자산에 대한 파라메터

보안위험분석을 위한 자산 특징은 침해가 발생하였을 때 해당 위협 및 취약성에 대한 위험도 및 피해 영향을 포함시켜야 한다. 이를 위하여 다음과 같은 항목을 필수적으로 정의한다. 이중에서 위험도 계산을 위한 자산, 위협과 취약성과 관련된 매트릭스는 각각 5등급으로 분류[24]하였으며 사이버 침해별 위협은 각각 BSI의 위협분류[20], CC의 위협목록[34]을 이용하였으며 취약성은 ICAT DB[33]를 사용하였다. 위험 감소는 보호대책에 의하여 위협[29] 및 취약점이 해결[28]되는 경우 시스템이 안정적으로 운영될 수 있는 수준을 포함시킨다.

- 자산의 운영체제와 서비스 팩
- 보안 패치의 여부 및 버전
- 자산의 업무와 업무 소프트웨어
- 업무 소프트웨어와 관련된 개발 프로그램
- 상용 내장된 소프트웨어
- 시간별 피해액과 피해 영향
- 사이버 침해별 위협과 취약성[26], [27]
- 위험도 계산을 위한 자산, 위협과 취약성 매트릭스[24]
- 정보보호 대책에 따른 위험 감소[28]
- 연동 시스템과의 상관관계 등

선택적으로 정의해야 하는 항목은 다음과 같다.

- 운용 시간 및 운용 요일
- 업무 피크 시간 대역
- 사용자 권한 및 외부자의 접근 여부 등

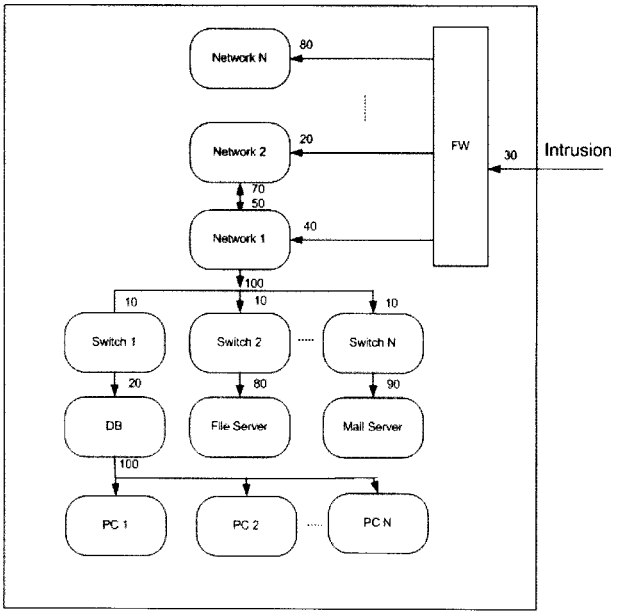
4.2 침해에 따른 피해 규모 분석

정보시스템에 대한 위협으로 인하여 단위 자산이 피해가 발생하였을 경우 피해 파급 및 피해 규모를 분석할 수 있는 형태로 구성한다. (그림 6)과 같이 서버군이 있고 각 서버에 연결된 네트워크가 구성되며 각각의 네트워크에는 단말들이 연결되어 있다고 하자. 위협에 의하여 DB가 피해를 발생하게 되면 DB 이하의 모든 자산들은 피해가 발생하게 되며, 네트워크 1에 피해가 발생하게 되면 네트워크 1이하의 모든 자산들이 피해를 입게 된다.

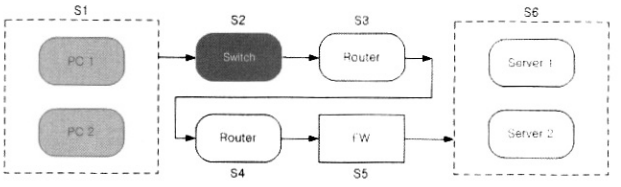
4.3 침해에 따른 피해 경로 분석

각 자산의 위험을 계산한 후 자산간 상관 관계를 이용하여 위험을 결합하게 시키면 전체 위험은 증가한다. 즉, (그림 7)과 같이 정보시스템내 침해에 따른 피해 경로를 분석하게 되면 위험 수준을 파악할 수 있다.

침해에 따른 피해 경로 분석은 업무 흐름도에 따라서 구분하게 되는데 업무흐름이 PC에서 스위치, 라우터를 거쳐 WAN 구간을 통해 서버에 이르게 되며 서버에 접근하는 구조를 가지게 된다. 정보시스템의 총 위험은 하나로 묶어서 수행하게 된다고 가정할 때 S1~S6까지 순차적으로 접근하는 직렬구조를 갖는다. 위의 모델링에서 S1-S2-S3-S4-S5-S6의 경로는 여러 개의 경로를 거쳐 순차적으로 접근하는 직렬구조를 갖게 되어 보안성 구조 중 가용성 측면에서 가장 나쁜 구조를 갖는다. 이는 하나의 자산이 기능 마비 또는 정지가 발생하는 경우 전체 시스템에 위험을 증가시킨다. 따라서 전체 위험도를 줄이기 위해서는 S1-S2-S3-S4-S5-S6 의 경로에 대한 기능을 병렬화 또는 독립화하는 것이 바람직하다.



(그림 6) 침해에 따른 피해 규모 분석



(그림 7) 침해에 따른 피해 경로 분석

보안위험분석의 전체 위험 수준 산정 및 계산은 개별 자산에 대한 위험도를 더한 후에 전체 자산으로 나눈후 백분율로 매핑을 한 후에 결정한다[24]. 각 자산에 대한 주요 계산식은 <표 2>와 같다.

그리고 정보시스템에 대한 피해액 및 피해수준은 시스템을 운영하는 시점에서 부하가 발생하여 시스템이 중지되고 이후 복구되어 정상으로 운영되는 시점까지를 운영비용으로 산정하여 시간대역에 따른 적분 값으로 계산하여 처리한다[22].

〈표 2〉 자산간의 주요 계산 알고리즘

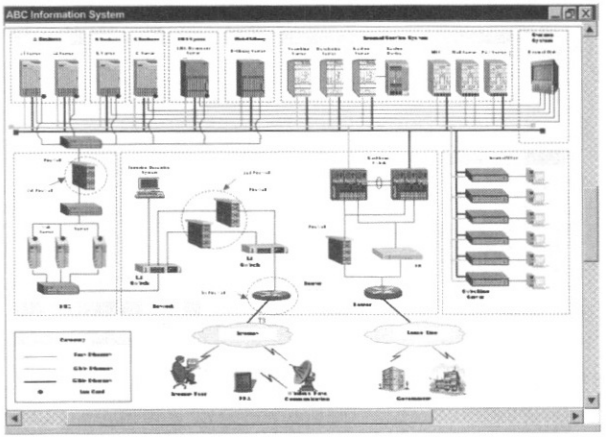
Index	Calculated rules	Resulted range
Level of asset a_i	Delpi	1,2,3,4,5
Cost of asset a_i (ac_i)		Real
Level of Threat a_i (t_{ij})	Delpi	1,2,3,4,5
Level of Vulnerability a_i (v_{ij})	Delpi	1,2,3,4,5
Level of Risk a_i (r_i)	Delpi	1,2,3,4,5
Total asset cost (AC)	$=\sum_{i=1}^{n} ac_i$	Real
Total asset cost level (A)	$=(\sum_{i=1}^{n} a_i)/n$	$1 \cdots 5$ (Real)
Threat of asset a_i (TV_i)	$=(\sum_{j=1}^{m} t_{ij})/m$	$1 \cdots 5$ (Real)
Threat level of asset a_i (TL_i)	$Int(TV_i)$	1,2,3,4,5 (Integer)
Vulnerability of asset a_i (VV_i)	$=(\sum_{j=1}^{m} v_{ij})/m$	$1 \cdots 5$ (Real)
Vulnerability level of asset a_i (VL_i)	$Int(VV_i)$	1,2,3,4,5 (Integer)
Risk value of asset a_i (RV_i)	$=a_i+TL_i+VL_i$	$3 \sim 15$ (Real)
Risk level of asset a_i (RL_i)	$=1,\ 3 \le RV_i < 5$ $=2,\ 5 \le RV_i < 8$ $=3,\ 8 \le RV_i < 11$ $=4,\ 11 \le RV_i < 14$ $=5,\ 14 \le RV_i < 15$	1,2,3,4,5 (Integer)
Total risk level of asset (RL)	$=(\sum_{j=1}^{n} RL_i)/n$	1,2,3,4,5 (Integer)
Safeguard rate of asset a_i (E_i)	$=(7.5 \times RV_i - 17.5)/100$	$0.05 \sim 0.95$ (Real)
Safeguard cost of asset a_i (AD_i)	$=ac_i \times E_i$	Real
Total Safeguard cost of asset (AD)	$=\sum_{i=1}^{n} AD_i$	Real

5. 사례 연구

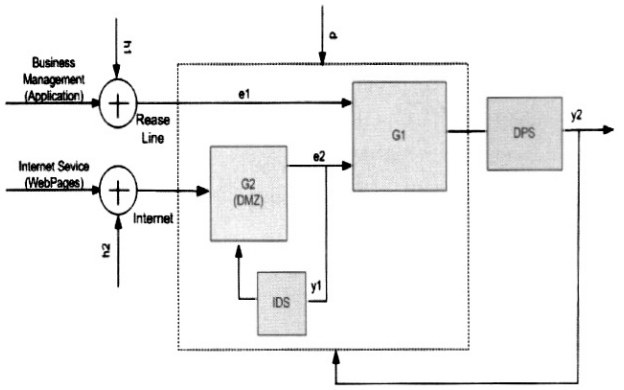
제안한 모델링을 통해 보안위험분석을 하기 위하여 위험분석 도구[30]를 통해 사례 연구를 수행하였다. 사례 연구를 위한 테스트 환경은 (그림 8)과 같이 구성되었으며 (그림 9)와 같이 모델링하였다.

모델링을 위하여 위험분석 도구를 구성하였으며 (그림 10)과 같이 설계하였다. 각 모듈의 구성은 상위위험분석과 하위위험분석으로 구분하고 하위위험분석에서는 자산, 위협, 취약점 보호대책 부분을 분석하여 데이터베이스화한다.

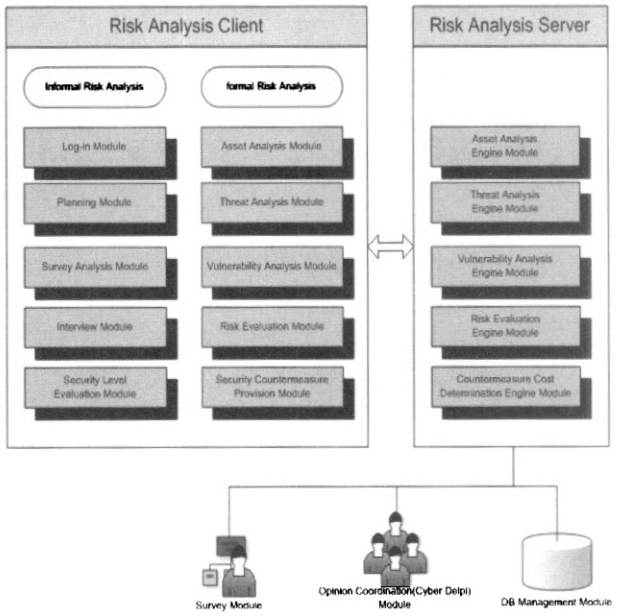
위험분석을 실시하기 위하여 각 평가자들은 네트워크를 통해서 원격으로 결과를 입력하고 결과를 최종 평가자가 분석 결과를 종합한다. 이에 대한 개발 환경은 Windows 2000 서버, MS-SQL 데이터베이스를 이용하였다.



(그림 8) 정보시스템 구성도



(그림 9) 정보시스템의 모델링



(그림 10) 위험분석 도구의 구성

테스트 환경의 업무 환경은 내부 망에서 사업관리를 수행하고 외부 망으로는 회사 홈페이지를 운영하고 있는 사례를 가정하였다. 클라이언트에는 데이터통제시스템(Data Protection System)을 설치 운영 중에 있다.

여기서, 정보보호시스템을 구축하기 위하여 양단에 설치하는 스위치와 허브의 경우에는 주요자산으로 볼 수 없으므로 주요 자산에서 생략한다. 이중화로 운영되는 시스템 및 듀얼로 운영되는 시스템들은 위협과 취약성이 같이 발생하므로 시스템을 겹쳐서 표시한다.

이상과 같이 정보시스템을 구성함으로써 자산, 위협, 취약성, 보호대책 이외에 위험도 및 피해파급 시뮬레이션 결과를 쉽게 분석할 수 있게 되었다.

5.1 자산 파라메터의 구조

자산 파라메터의 구조는 매우 쉽게 수정 및 제작이 가능하도록 한다. 내용은 단순한 text 파일의 형태로 되어 있으며, 대부분 해당 위협과 취약성에 위험도 및 피해도 등을 배열한

형태로 구성한다. <표 2>는 Windows2000 서버에 대한 자산 파라메터의 예제이다. <표 2>에서 보는 바와 같이 정보시스템을 운영하고 있는 윈도우즈2000 서버는 부적절한 암호관리(2.19), 로그 정책 부재(2.35), 작업인력의 교육인력 미비(3.09)의 위협을 가지고 있으며 각각의 시간마다 위험 및 피해규모가 증가하고 있는 것을 알 수 있다. 또한 취약점은 버퍼 오버플로워 공격과 포맷 스트링 공격에 취약하여 각각 피해가 서버 자산 비용의 70%와 40%를 갖는다.

포맷의 예에서 알 수 있듯이, 파일 내에 적혀있는 위협에 따른 피해 범위에서 주로 해석이 이루어져야 정확도를 보장할 수 있다. 앞에 있는 !는 주석문의 의미이다. 자산의 parameter 파일의 경우 침해에 대한 대응 조건을 따져서 파일 내용을 지정해야 한다.

5.2 네트리스트 파일의 구조

네트리스트 파일이란, 정보시스템에 대한 text 형식의 기본적인 네트워크 구조 입력 파일이다. (그림 8)과 같은 정보시스템을 네트리스트 파일로 만들면 그 내부는 <표 3>과 같이 나타난다. 대부분의 자산들은 스위치 또는 허브로 연결되어 있으므로 스위치 및 허브에 대한 위치를 노드로 선정하여 네트리스트 파일을 만들면 간단하게 구현할 수 있다.

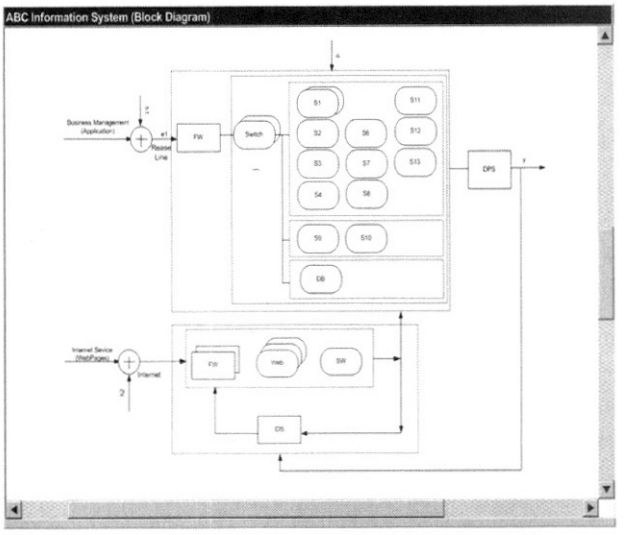
〈표 3〉 자산 파라메터의 파일 구조

```
! Windows2000 Server
! PARAMETER DATA
! Threat Table
! Table number : Threat_factor(1-5) :
  Damage_factor(%)
2.19 : 1, 2, 2, 3, 4, 5 : linear_function(a)
2.35 : 1, 2, 3, 4, 5, 5 : exp_function(a)
3.09 : 1, 3, 5 : log_function(a)
... ...
! Vulnerability Table
! CVE ID : Threat_factor(1-5) :
  Damage_factor(%)
CAN-2000-1186 : 4 : 70
CAN-2003-1022 : 3 : 40
... ...
! Risk Table
...
! Damage Table
...
! SageGuard Table
...
```

먼저 이 정보시스템서 사용하는 자산을 식별하고 분석한 후, 자산 종류와 그것이 위치하는 양쪽 노드 번호와 값을 표시한다. 네트리스트 파일형태의 핵심은 노드 번호를 기준으로 정보시스템을 표현하는 것이다.

〈표 4〉 각 자산에 대한 모델링 결과

```
! Information System Net-list
   DIM
   1 min                          ! Time Interval
   IN       0 1 Attack
   OUT      0 1 Risk, Damage
! Assets
   SERVER 1 2 S(WIN2000, SP2)  !S
   DB       2 3 D(ORACLE, V8.0)  !D
   PC       2 4 PC(WINXP, 3)     !PC set 3
   SERVER 1 3 S(HP, SP3, APACHE)  !S
.....
```

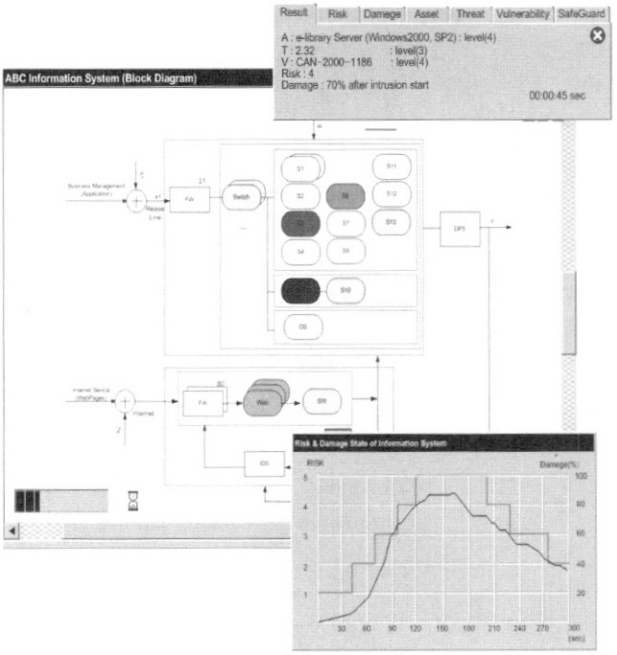


(그림 11) 위험분석 도구를 통한 정보시스템 구성

(그림 8)에서 보여주는 정보시스템에 대한 위험분석 모델링을 위하여 (그림 11)과 같이 나타낸 후 시뮬레이션을 하게 되면 위험도 분석과 피해 파급 결과가 (그림 12)와 같이 나타난다. 침해가 발생한지 120초 만에 정보시스템의 위험도가 1에서 5로 증가하였고, 전체 피해가 80%이상 발생함을 알 수 있다. 하지만 긴급 복구대책 및 정보보호시스템의 동작을 통하여 280초 후에 전체 위험도를 2로 줄이면서 피해를 40%내로 감소시킴을 알 수 있다.

이상과 같이 사례 연구를 통하여 정보시스템의 모델링으

로 위험분석을 실시하게 되면 좀 더 침해 분석 및 피해 영향을 일목요연하게 분석할 수 있다.



(그림 12) 위험분석 시뮬레이션 결과

6. 결 론

정보통신망의 위험분석은 필수적인 업무이나, 기존의 분석 기법은 정적인 분석 기법이므로 정보시스템 특성상 피해 파급 및 정보보호시스템의 역할이 제대로 이루어지고 있는 지를 도식적으로 알 수 없었다. 본 논문에서는 기존의 위험분석의 이러한 문제점들을 해결하기 위하여 정형적인 모델링을 새롭게 정의하였다.

또한 위험분석 모델링을 통해 정보시스템의 위험도 흐름과 피해 파급에 대한 영향을 시간별로 분석할 수 있음을 알 수 있었다. 즉, 사이버 침해의 유형과 수준을 위협과 취약성 테이블을 통해서 분석하고 각각의 자산들이 정보보호 대책에 따라 위험도 변화와 피해 파급에 대한 분석이 가능하게 된 것이다. 시뮬레이션을 통해 정보시스템에 대한 정보보호 대책을 단기간내에 구축할 수 있으므로 좀 더 안정적이고 효율적인 보안 운영관리가 가능하게 되었다.

향후에는 제시된 모델링을 토대로 시변 상태방정식을 구성하여 자산 상태에 따른 위험 예측이 가능한 설계 방안을 제시하고자 한다.

참 고 문 헌

[1] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, "Security Risk Analysis Model for Information Systems," LNCS 3398, Systems Modeling and Simulation : Theory and Applications : Third Asian Simulation Conference, AsianSim 2004.

[2] 김인중, 정윤정, 박중길, 원동호, "중요핵심기반시설(SCADA)에 대한 보안위험관리 연구", 한국통신학회논문지 Vol. 30, 2005년 9월.

[3] Kwang Min Park, Dong Kwang, PSpice Understanding and Application (revised), 1992, ISBN 89-85305-02-6.

[4] W. Reisig, Petri Nets, An Introduction, EATCS, Monographs on Theoretical Computer Science, W.Brauer, G. Rozenberg, A. Salomaa(Eds.), Springer Verlag, Berlin, 1985.

[5] Edward Yourdon, Modern Structured Analysis, Prentice-Hall, 1989.

[6] Paul E. Black, ed, "deterministic finite state machine", Dictionary of Algorithms and Data Structures, NIST. http://www.nist.gov/dads/HTML/determFinitStateMach.html

[7] L.M. Kristensen, S. Christensen, K. Jensen : The Practitioner's Guide to Coloured Petri Nets. International Journal on Software Tools for Technology Transfer, 2 (1998), Springer Verlag, 98-132.

[8] Paul Tuinenga, SPICE : A Guide to Circuit Simulation and Analysis Using PSpice (3rd Edition), Prentice-Hall, 1995, ISBN 0-13-158775-7

[9] MICTS(Previously GMITS), ISO/IEC 27005 ISMS Risk Management. 2005.

[10] CSE(Canadian Secutiy Establishment), "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment(CSE)", 1996.

[11] MacDonald, David/ Mackay, Steve (EDT), Practical Hazops, Trips and Alarms (Paperback), Butterworth-Heinemann, 2004.

[12] RAC, Fault Tree Analysis Application Guide, 1991.

[13] CMU, OCTAVE(Operationally Critical Threat, Assets and Vulnerability Evalustion), 2001. 12.

[14] Theo Dimitrakos, Juan Bicarregui, KetilStølen. CORAS - a framework for risk analysis of security critical systems. ERCIM News, number 49, pages 25-26, 2002.

[15] Young-Hwan Bang, YoonJung Jung, Injung Kim, Namhoon Lee, GangSoo Lee, "The Design and Development for Risk Analysis Automatic Tool," ICCSA2004, LNCS 3043, pp.491~499, 2004.

[16] http://www.cramm.com, CRAMM(CCTA Risk Analysis and Management Method).

[17] Palisade Corporation, @RISK, http://www.palisade.com

[18] Countermeasures, Inc., The Buddy System, http://www.buddysystem.net

[19] ISO/IEC17799 & ISO/IEC27001(revised BS7799 part 2), Code of Practice for Information Security Management. 2000.

[20] BSI, http://www.bsi.bund.de/english/gshb/manual/index.htm, 2003.

[21] NCSC, 사이버안전메뉴얼, 2004.

[22] InJung Kim, YoonJung Chung, YoungGyo Lee, Dongho Won, "A Time-Variant Risk Analysis and Damage Estimation for Large-Scale Network Systems," ICCSA2005, LNCS3043, May, 2005.

[23] Injung Kim, YoonJung Jung, JoongGil Park, Dongho Won, "A Study on Security Risk Modeling over Information and Communication Infrastructure," SAM04(Security and Management 2004), pp.249~253, 2004.

[24] Yoon Jung Jung, InJung Kim, JoongGil park, Dongho Won, "A Practical Security Risk Analysis Process of Information System," pp.576~581, 4th APIS, 2005.

[25] Yoon Jung Chung, InJung Kim, NamHoon Lee, Taek Lee, Hoh Peter In, "Security Risk Vector for Quantitative Asset Assessment", LNCS 3481/2005, Computational Science and Its Applications - ICCSA2005 May, 9~12, 2005.

[26] 정윤정, 김인중, 이철원, "실용적인 위험분석 방법론 설계와 모듈 구현," 한국통신학회 논문지 제27권 11C호, 한국통신학회 2002.

[27] 엄정호, 우병구, 김인중, 정태명, "정보시스템의 효율적인 위험관리를 위한 실용적인 위험감소 방법론에 관한 연구", 정보처리학회논문지C, 제10-C권 제2호, 2003.

[28] Namhoon Lee, YoonJung Jung, InJung Kim, JungGil Park, "The design and Implentation of Risk Analysis Tools and Suitable Countermeasure Choice Algorithm," pp.49~53, SCI2004, July, 2004. 3.

[29] 김인중, 정윤정, 이남훈, 이재욱, "국가 공공기관 정보통신기반 시설에 대한 위협 분석시 고려사항," WISC2003 논문집, 2003년 9월.

[30] YoonJung Jung, InJung Kim, SeungHyun Kim, "The Design and Implementation for the Practical Risk Analysis Tools", Second Summer School 2003 by IFIP WG9.2, 9.6/11.7, 9.8, August, 2003.

[31] D.S. Kim, Y..J. Jung, and T.M. Chung, "PRISM : A Preventive and Risk-Reducing Integrated Security Management Model Using Security Label," The Journal of Supercomputing, Volume 33, Number 1, Pages : 103~121, July, 2005.

[32] 김영갑, 이택, 인호, 정윤정, 김인중, 백두권, "정보통신기반에 대한 피해파급 모델," WISC2005. 2005년 9월.

[33] US-CERT, "US-CERT Vulnerability Notes Database," http://www.kb.cert.org/vuls.

[34] Common Criteria(CC), http://www.commoncriteria.org

김 인 중

e-mail : cipher@etri.re.kr

1992년 충남대학교 전자공학과(석사)

1992년~2000년 국방과학연구소 선임연구원

2001년~현재 성균관대학교 전기전자및컴퓨터공학부 박사수료

2000년~현재 국가보안기술연구소 선임연구원

관심분야 : 정보보안, 네트워크 보안, 위험분석, 보안관리

이 영 교

e-mail : yglee@dosan.skku.ac.kr

1986년 한양대학교 전자공학과(공학사)

1991년 한양대학교 대학원 전자공학과(공학석사)

2002년~현재 성균관대학교 대학원 전기전자 및 컴퓨터공학부 박사수료

1993년~1998년 대우통신 종합연구소 선임연구원

1999년~2001년 LG 전자/정보통신 중앙연구소 선임연구원

2002년~2005년 인하공업전문대학 정보통신과 강사

2004년~2005년 아주대학교 정보통신대학원 및 원격교육센터 강사

2005년~현재 안양과학대학 컴퓨터정보학부 강사

관심분야 : 암호이론, 정보통신 보안, 네트워크 이론

정 윤 정

e-mail : yjjung@etri.re.kr

1997년 성균관대학교 정보공학과

1999년 성균관대학교 정보공학과

1999년 하나로정보통신 연구원

2000년~현재 국가보안기술연구소 선임연구원

관심분야 : 정보보안, 네트워크 보안, 위험분석, 보안관리

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1988년~2003년 성균관대학교 교학처장, 전기전자및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장(정통부지정 ITRC) 정보보호인증기술연구센터 센터장

관심분야 : 암호이론, 정보이론, 정보보안관리