Journal of The Korea Society of Computer and Information
Vol. 19, No. 7, July 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.7.047

정보통신 기술을 이용한 물리보안 위협 계수기 구현 전략

강 구 홍*

An Implementation Strategy for the Physical Security Threat Meter Using Information Technology

Koo-Hong Kang*

요 약

정보보안 (인터넷 혹은 사이버) 위협 레벨을 공지하기 위해 많은 정보보안 회사들은 위협 계수기(Threat Meter)를 개발하였다. 본 논문에서는 물리보안 장치들이 지능화되고 네트워크를 통해 감시 및 제어가 가능함에 따라 물리보안의 현재 위협 수준을 결정하는 물리보안 위협 계수기(PSTM: Physical Security Threat Meter)를 제안한다. 따라서 PSTM은 정보보안에서 사용하는 위협 계수기와 유사하다. 이러한 목적을 위해 물리보안 이벤트를 분석하고 가중치를 결정하였으며 복수의 보안이벤트 발생에 따른 이벤트 간 시간 연관성 영향을 고려하였다. 또한 위협 레벨을 결정하기 위한 기준 값 설정 방법과 이들 기준 값을 이용한 실용적인 PSTM을 제안하였다. 특히 출입문 제어기와 CCTV(비디오 분석기 포함)로 구성된 실험환경에서 PSTM을 제작하기 위한 구체적인 블록도와 구현과정을 보임으로써 제안된 기법이 실현 가능함을 보였다. 마지막으로 몇몇 실험 시나리오를 대상으로 실시한 시뮬레이션 결과를 통해 제안된 PSTM이 물리보안 위협레벨을 적절히 공지함을 검증하였다.

▸ Keywords : 물리보안, 위협레벨, 정보보안

Abstract

In order to publicly notify the information security (Internet or Cyber) threat level, the security companies have developed the Threat Meters. As the physical security devices are getting more intelligent and can be monitored and managed through networks, we propose a physical security threat meter (PSTM) to determine the current threat level of physical security; that is a very similar compared with the one of information security. For this purpose, we investigate and prioritize the physical security events, and consider the impact of temporal correlation among multiple security events. We also present how to determine the threshold values of threat levels,

•제1저자 : 강구홍 •교신저자 : 강구홍
•투고일 : 2014. 4. 22, 심사일 : 2014. 5. 11, 게재확정일 : 2014. 7. 4.
* 서원대학교 정보통신공학과(Dept. of Information and Communication Engineering, Seowon University)

and then propose a practical PSTM using the threshold based decision. In particular, we show that the proposed scheme is fully implementable through showing the block diagram in detail and the whole implementation processes with the access controller and CCTV+video analyzer system. Finally the simulation results show that the proposed PSTM works perfectly under some test scenarios.

▸ Keywords : Physical security, Threat level, Information security

I. 서 론

국외 McAfee[1], Symantec[2], 그리고 국내 AhnLab[3]과 같은 주요 정보보안(Information Security) 기업들은 알려진 사이버 위협(cyber threat)들의 위험도와 이들 위협들이 인터넷과 비즈니스 운영 시스템, 그리고 가정에서 사용하는 개인 컴퓨터에 어떠한 영향을 미치는지 분석하여 자신들의 웹 사이트를 통해 실시간으로 위협레벨(threat level)을 공지하고 있다. 이러한 정보를 이용해 일반 사용자들은 자신의 컴퓨팅 시스템과 네트워크가 웜과 악성 코드의 행위, 그리고 새로운 취약점으로부터 얼마나 위험에 노출되는지를 쉽게 인식할 수 있게 된다. 뿐만 아니라, 최근에는 국가 차원에서 운영되는 인터넷침해대응센터[4]를 통해 사이버 위협레벨을 일반 사용자들에게 공지하고 있다. 이와 같은 정보보안 위협레벨은 위협 정도에 따라 일반적으로 4단계 (정상-주의-경계-심각) 혹은 5 단계 (정상-관심-주의-경계-심각)로 분류하고 있다. 본 논문에서는 정보보안에서 사용하는 이와 같은 실시간 정보보안 위협레벨과 동일한 개념과 목적으로, 물리보안(Physical Security)의 위협레벨을 결정하기 위한 체계적인 전략과 구현 방법을 제안한다. 정보보안 위협레벨과 동일하게 물리보안 장치에 의해 보호되는 보안영역이 외부로부터 받는 위협정도에 따라 4-5 단계로 나누어 위협레벨을 알림으로써 보안 영역 내 근무자들은 사전에 단계별 적절한 대응 체계를 수립할 수 있다. 본 논문에서는 이와 같이 현재의 물리보안 위험 정도에 따라 단계별 위협레벨을 결정하여 공지하는 물리보안 위협 계수기 (이하, PSTM - Physical Security Threat Meter - 로 약칭)를 구현한다. 또한 제안된 PSTM이 실제 구현 가능하도록 블록도 및 관련 주요 기능을 가상코드(pseudocode)를 이용해 자세히 설명하고 몇 몇 실험 시나리오 환경을 구성해 제안된 PSTM이 어떻게 동작하는지 확인한다.

초기 물리보안 장치는 시설물, 인적·물적 자원, 그리고 물리적 자산(assets)으로부터 침입자들이 불법 접근하는 것을 검출하고 방어하는 수단을 제공했다. 이러한 물리보안은 출입문을 잠그고 혹은 여러 단계의 경보장치를 설치함으로써 가능했다. 그러나 9/11 테러 사건이후, 더 이상의 테러와 범죄 발생을 방지하기 위해 물리보안 장치는 단순한 형태의 CCTV(Closed Circuit Tele-Vision)에서 IP(Internet Protocol) 기반의 네트워킹 기술과 영상분석 기술을 접목한 지능형 영상보안시스템으로 발전하고 있다[5,10]. 이러한 지능형 영상보안시스템은 네트워크가 연결되어 있는 곳이면 어디든지 설치가 가능하므로 단순 CCTV에 비해서 상대적으로 설치 장소의 제약을 받지 않는다. 또한 자동화된 영상분석 기술을 이용함에 따라서 실시간으로 전송되어 오는 영상을 보안관리자가 24시간 직접 감시하는 불편함을 극복할 수 있다. 한편 물리보안 장치로 가장 많이 사용되고 있는 사무실 혹은 일반 가정집 도어록(door lock)과 같은 출입문 잠금장치의 경우, 과거 단순한 잠금장치 기능을 탈피해 RFID 보안칩 (스마트 카드) 사용, 네트워크를 통한 원격 감시 및 지원, 복잡한 지문인식, 홍채인식 그리고 얼굴인식과 같은 첨단기술을 제공하는 수준에 이르렀다[6,7,8,14]. 따라서 오늘날 대부분 물리보안 장치는 네트워크를 통해 관리되며 이들 장치로부터 지리적으로 떨어진 독립된 보안관제실에서 물리보안 장치가 제공하는 다양한 보안이벤트를 수신하여 실시간 방어 수단을 제공할 수 있는 여건이 마련되어 있다[11].

본 논문에서 제안될 PSTM은 물리보안 장치가 제공하는 다양한 보안이벤트들을 활용해 해당 보안영역의 위협레벨을 결정한다. 이때 발생된 물리보안 이벤트의 가중치(이벤트의 중요도)와 서로 다른 복수의 보안이벤트 발생에 따른 물리보안 위험 수준의 변화를 감지해 일반 사용자들에게 공지하게

된다. 따라서 일반 사용자들은 PSTM이 제공하는 물리보안 위협레벨에 따라 각 단계별로 대응할 수 있다. 즉 정상레벨에서는 무시되었던 물리보안 영역 내 몇몇 행위들은 위협레벨이 높은 단계에서는 심각하게 고려되고 처리되어야 한다. 예를 들어, 물리보안 장치가 인가 받지 않은 외부인의 침입을 탐지하는 극단적인 경우 일시적으로 자산이동을 금지하는 조치를 취하게 된다. 뿐만 아니라, 발생된 물리보안 이벤트가 매우 극단적인 위험이 아니라 할지라도 여러 개의 보안이벤트가 동시 다발적으로 발생할 경우 적절한 위협레벨을 공지한다. 본 논문에서는 PSTM을 어떻게 활용할 것인지에 대한 구체적인 논의는 하지 않는다. 다만 정보통신 기술을 이용하여 PSTM을 어떻게 구현할 것인지에 대해 초점을 맞춘다.

서론에 이어, 제2장에서는 정보보안에서 사용하고 있는 위협레벨 기술에 대해 간략히 언급하고, 제3장에서는 본 논문에서 사용할 가장 일반적인 물리보안 장치와 관련 물리보안 이벤트를 기술한다. 제4장에서는 PSTM을 구현하기 위한 핵심 컴포넌트를 대상으로 가상코드와 구체적인 블록도를 제시한다. 제5장에서는 PSTM을 구현하는 실제 예를 설명하고 세 가지 실험 시나리오를 기준으로 제안된 PSTM이 어떻게 동작하는지 그 결과를 기술하였다. 마지막으로 제6장에서 결론 및 향후 연구 방향에 대해 기술하였다.

II. 관련 연구

서론에서 언급한 바와 같이, 본 논문은 물리보안장치에 의한 해당 보안영역 내 위협레벨을 자동으로 공지하기 위한 PSTM을 구현하는 것이다. 이러한 아이디어는 기존의 정보보안 업체들이 자신의 웹사이트를 통해 실시간으로 인터넷 위협레벨을 공지함으로써 일반 사용자들의 보안 경계심을 고취시키는 것과 동일하다. 즉 사이버 위험레벨이 올라가면 일반 사용자들은 자신의 컴퓨터를 보다 안전하게 사용하기 위해 최신 보안 패치 등의 사전 조치들을 하게 된다.

정보보안 기업들이 제공하는 위협레벨은 기업마다 약간의 차이가 있으며 위협레벨을 판단하는 기준 또한 기업 자체 기준에 의해 결정되는 것으로 조사되었다. 국내 A 업체 경우, 위협레벨을 네 단계로 나누어 1단계 '안전', 2단계 '대비', 3단계 '주의', 그리고 4단계 '긴급'으로 분류하고 있다. 이와 유사하게 외국 S 업체 역시 위협레벨을 레벨 1 'Low : Basic network posture', 레벨 2 'Medium : Increased alertness', 레벨 3 'High : Known threat', 레벨 4 'Extreme : Full alert'로 분류한다. 한편 위협레벨의 각 단계는 외부의 위협 수준을 판단할 수 있는 객관적이며 다양한 지표에 의해 결정되며, 얼마나 많은 이용자들이 바이러스 등 보안 위협으로 인한 피해를 겪고 있는지를 확인할 수 있는 고객 문의건수와 긴급엔진 제작 여부, 신종 바이러스 분석정보 제작 여부 등 외부 보안 위협에 대응하는 회사 내부의 다양한 판단 지표에 근거하여 설정된다. 이와 같이 기업들 마다 자신들의 고유한 위협 단계를 설정하고 실시간 위협레벨을 공지하고 있으나, 구체적으로 어떤 기준으로 위협레벨을 결정하는지는 자세히 공개하지 않고 있다. 그러나 대부분의 경우는 국내 A 업체와 동일하게 사용자들이 제공하는 각종 사건 사고 접수와 처리과정에서 획득되는 정보와 운영체제 및 응용 소프트웨어 제작사들이 제공하는 보안 패치 등을 근거로 위협레벨이 결정된다. 그림 1은 국내 기업과 기관 그리고 외국 기업과 기관이 동일한 시간대에 공지하고 있는 정보보안 위협레벨을 보여준다. 그림 1에서 보듯이, 국내와 국외가 서로 다른 위협레벨을 공지하고 있으며 국내의 경우 기업과 기관이 상당히 다른 위협레벨을 공지하고 있음을 확인할 수 있다. 이러한 현상은 앞에서 언급한 바와 같이 실시간으로 접수되는 사건 사고 접수 상황이 서로 다르며, 또한 자신들의 고유한 방법으로 위협레벨을 결정하기 때문이다. 본 논문에서 제안될 PSTM 역시 해당 물리보안 영역 내에서 발생된 다양한 물리보안 이벤트들을 기준으로 물리보안 위협레벨을 결정하게 될 것이다. 한편, 참고문헌[9]는 계층분석과정(AHP : Analytic Hierarchy Process)[12]을 이용해 물리보안 이벤트의 중요도(가중치)를 결정하는 방법을 제안하였다. 본 논문에서 사용할 물리보안 이벤트의 가중치 결정은 참고문헌[9]에서 제시한 참조 모델(reference model)을 이용한다.

그림 1. 정보보안 위협레벨 공지(위쪽 왼쪽으로부터 국내 기관, 국내 기업, 외국 기업, 그리고 외국기관)
Fig. 1. The announcement of Information Security Threat Level (From Upper Left, A Domestic Institute, A Domestic Company, A Foreign Company, and A Foreign Institute)

III. 물리보안 장치와 관련 보안이벤트

오늘날 물리보안의 중요성이 한층 강조됨에 따라 매우 다양한 보안 장치들이 출시되고 있다. 그러나 가장 흔히 우리들이 사용하고 있는 장치는 사무실 혹은 회사 출입문 등을 관리하는 출입문 제어기와 영상감시 등을 목적으로 사용하는 감시용 카메라가 대표적이다[5,6]. 이러한 물리보안 장치들은 TCP/IP 기반 인터넷 기술을 사용하여 더 이상 거리 혹은 공간의 제약을 받지 않고 있다. 즉 특정 보안 영역을 출입하는 사람들을 감시하고 추적하여 원격지 보안관제 센터까지 실시간으로 관련 물리보안 이벤트를 전송하고 보안관제 센터에서는 물리보안 장치로부터 수신된 다양한 보안이벤트를 통합 관리할 수 있는 환경을 마련하였다. 영상 감시시스템의 경우, 보안 담당자에 의해 24시간 실시간 영상을 감시하고 대응하는 것이 사실상 불가능하기 때문에 지능화된 영상감시 기술이 매우 중요하다.

물리보안 장치가 더욱 지능화되고 고도화됨에 따라, 이들 장치에서 발생되는 물리보안 이벤트 역시 매우 다양하다. 다음 표1은 이들 두 종류의 물리보안 장치에서 발생되는 일부 물리보안 이벤트를 나타내었다. 물리보안 장치에서 발생하는 보안 이벤트는 제품관련 매뉴얼을 참고하면 최소 20 ~ 30개 이상을 정의하고 있다. 그러나 본 논문에서는 설명의 편의성을 위해 표 1에 나타난 물리보안 이벤트만 다루기로 한다.

표 1. 물리보안 이벤트 예
Table 1. Example of Physical Security Events

항목	이벤트	설명
출입문 제어기	AC1	정상적인 문 열림
	AC2	일정횟수 이상 문 열림 실패
	AC3	강제 문 열림
	AC4	일정시간 문 열림 지속
	AC5	경보 기능 해제
	AC6	네트워크 연결 실패
지능형 영상감시기	IV1	정상적인 물체 인식
	IV2	침입탐지
	IV3	위장 물체 인식
	IV4	위험지역 배회자 인식
	IV5	시그널 혹은 네트워크 문제

표 1로부터 물리보안 이벤트는 보안 위험도 측면에서 크게 두 가지 타입 - 긍정적 효과를 주는 이벤트 혹은 부정적 효과를 주는 이벤트 - 으로 구분할 수 있다. 예를 들어, 이벤트 AC1과 IV1은 정상적인 사용자에 의한 문 열림 혹은 정상적인 물체 인식으로 인한 보안 영역 내 보안성을 높이는 긍정적인 효과를 가져 온다. 즉 보안 영역 내 허가 받은 다 수의 사람들이 존재할 경우, 외부로부터 물리적 침입 가능성은 훨씬 낮아지는 것이다. 이와 반대로 이들 두 이벤트를 제외한 표 1에 나타난 모든 물리보안 이벤트들은 보안영역의 위험도를 증가시키는 부정적 효과를 주는 이벤트들이다. 그러나 부정적 효과를 가져 오는 이들 보안이벤트들은 표 1에서 보듯이 서로 다른 위험 강도가 예상된다. 즉 강제 문 열림(AC3) 혹은 침입탐지(IV2)와 같은 매우 극단적이며 심각한 보안이벤트가 있는 반면, 문 열림 실패(AC2) 혹은 배회자 발견(IV4) 등과 같은 의심스러운 정도의 보안이벤트들도 존재한다. 따라서 체계적인 방법을 이용해 물리보안 위협에 영향을 미치는 이들 물리보안 이벤트의 가중치를 결정할 수 있어야 한다.

한편 물리보안 이벤트들은 이들 이벤트들 간의 상관관계에 의한 시너지 효과 혹은 Ringelmann 효과[13]를 예상할 수 있다. 시너지 효과는 두 개 이상의 이벤트 발생 시, 이들 이벤트의 긍정적 혹은 부정적 효과를 극대화시키는 것이고 Ringelmann 효과는 이와 반대로 서로의 영향력을 감쇄시키는 것을 의미한다. 시너지 효과의 예로서, 이벤트 AC2 발생 후 이벤트 AC4가 일어난다면, 이벤트 AC4는 훨씬 위험도가 강한 이벤트로 해석되어야 한다. 즉 여러 번의 문 열림 실패 이후 일정 시간 문 열림 지속 이벤트가 연이어 발생했다는 것은 외부로부터 해당 보안 영역으로 불법 침입자가 들어 올 확률이 이벤트 AC4가 단독으로 발생했을 경우보다는 훨씬 높다는 것을 쉽게 예상할 수 있다. 이와 반대로 Ringelmann 효과의 예는, 이벤트 AC1 발생 후 이벤트 AC2가 발생한다면, 이벤트 AC2의 부정적 효과는 이전에 발생된 이벤트 AC1의 긍정적 효과로 인해 중요도가 상대적으로 감쇄하게 된다. 즉 보안 영역 내에 존재하는 정상적인 사용자들에 의해 외부로부터 침입의 징후는 상대적으로 줄어들게 된다.

IV. 물리보안 위협 계수기 (PSTM: Physical Security Threat Meter)

1. 물리보안 이벤트 가중치 결정

보안 관리자는 발생된 각 물리보안 이벤트의 성격에 따라 심각성 혹은 긴급성 등을 고려해 서로 다르게 처리하기 원한다. 따라서 이들 보안이벤트들의 가중치(중요도)를 결정할 필요가 있다. 특히 이들 보안이벤트들은 서로 다른 이벤트들과 시간 연관성 (temporal relationship) 관계를 가질 수 있기

때문에 매우 다양한 이벤트 조합을 고려해야 한다. 예를 들어, 전체 n개의 물리보안 이벤트가 존재한다고 가정하면 발생 가능한 이벤트 조합은 2^n이 된다. 이때 시간 연관성 즉 발생 순서까지 고려하면 발생 이벤트 조합 당 $k!$ 만큼 이벤트 조합이 존재 한다 (여기서, 발생된 하나의 이벤트 조합 내에는 k개의 물리보안 이벤트가 발생되었다고 가정). 이렇게 많은 이벤트 조합을 고려하기 위해서는 체계적인 방법이 필요하며 본 논문에서는 참고문헌[9]에서 제안한 참조모델을 이용해 각 이벤트의 가중치를 결정하였다.

결정이론(decision theory)에서 가장 중요한 문제는 중요도에 따라 집합 내 각 행위의 가중치를 어떻게 결정할 것인가에 있다. 본 논문에서는 앞에서 언급한 바와 같이 이벤트의 가중치를 결정하기 위해 계층분석과정 기법을 사용한다. 기본적으로 AHP는 쌍대비교(a pair-wise comparison) 과정을 이용해 대안(alternatives) 집합 내 선호도에 대한 수치적 스케일을 결정하는 다목적 다중척도 결정 기법(multi-objective multi-criteria decision making approach)이다[12].

2. 다중 이벤트 발생에 따른 위협지수 변화

본 논문에서는 s개의 서로 다른 물리보안 장치로부터 n개의 물리보안 이벤트가 발생되는 것을 가정하며, 따라서 이벤트 집합 $E=\{e_1,e_2,\cdots,e_n\}$와 같다. 물리보안 이벤트 발생은 어느 시점에 일시적으로 발생하지만 대부분의 이벤트는 타임윈도우(time window)의 개념을 가진다. 즉 보안이벤트는 발생과 해제의 개념을 가진다. 표 1에서, 정상적인 문 열림(AC1) 이벤트는 인증절차를 거쳐 보안영역에 들어온 사용자(이벤트 발생)가 해당 영역을 빠져 나갈 때(이벤트 해제)까지 긍정적 효과 이벤트의 역할을 지속하고 있는 것이다. 표 1의 이벤트 AC2는 인증절차의 실패로 인한 어느 시점 일시적으로 발생하는 보안 이벤트이지만, 이러한 부정적 효과 이벤트를 충분히 보안영역에 반영하기 위해서는 일정시간 유지할 필요가 있다. 즉 타이머(timer)를 활용해 예약된 타이머가 종료할 때까지 일정시간 충분히 이벤트 발생 영향을 고려하는 것이다. 표 1의 이벤트 AC3(강제 문 열림)의 경우, 보안 관리자에 의해 해당 이벤트가 적절히 처리될 때까지는 계속 부정적 효과의 이벤트가 지속되는 것을 기본으로 한다. 표 1의 AC4(일정시간 문 열림 지속) 이벤트는 열려있는 문이 다시 닫히는 순간까지 부정적 효과의 이벤트는 지속되는 것이며, 표 1의 AC5(알람 해제) 이벤트는 보안 관리자에 의해 다시 알람 설정될 때까지 지속된다. 표 1의 AC5(네트워크 연결 실패) 이벤트는 네트워크가 정상상태로 되돌아 올 때까지 지속된다. 따라서 앞에서 언급한 바와 같이 물리보안 이벤트는 타임윈도우(time window) 개념을 가지며 다음 그림 2는 세 개 이벤트 발생과 해제에 따른 이벤트 타임윈도우 개념을 보여준다. 결론적으로, 임의의 어느 시점에는 복수의 물리보안 이벤트가 발생할 것이며 우리는 이러한 현상을 적절히 고려하여야 한다.

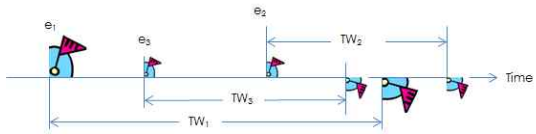

그림 2. 복수의 보안이벤트 발생
Fig. 2. Multiple Security Events

여러 개의 보안이벤트가 동시에 발생하면 PSTM은 이들 이벤트의 가중치 합을 이용해 단순하게 반응할 수도 있으나 앞에서 언급한 시너지 효과 혹은 Ringelmann 효과에 의해 가중치가 확장되거나 축소되어 반응할 수도 있다. 본 논문에서는 문제를 단순화하기 위해 이벤트 집합에서 쌍대 관계(pair-wise relationship)만 고려한다. 예를 들어, 그림 2와 같이 세 개의 이벤트 e_1, e_2, 그리고 e_3가 존재할 경우, 위협레벨 변화는 (e_1,e_2), (e_2,e_3), 그리고 (e_1,e_3)의 시간 연관성만 고려한다.

발생순서 조건(temporal order condition)을 고려하기 위해, 이벤트 e_i는 이벤트 e_j 이전에 발생했으며 임의의 시간 t에 동시에 존재한다고 가정한다. 이전 사건 e_i에 의해 최근에 발생한 사건 e_j의 중요도가 영향을 받으면 $e_i \rightarrow e_j$로 표현하고, 반대로 사건 e_j에 의해 이전 이벤트 e_i의 가중치가 영향을 받으면 $e_i \leftarrow e_j$로 표현한다. 본 논문에서는 임의의 두 이벤트 $e_i, e_j (i,j=1,\cdots n)$ 사이의 가중치 변화를 다음과 같은 $n \times n$ 시간 연관성 쌍대 행렬 (TPRM : temporal pair-wise relationship matrix)로 나타낸다.

$$\Gamma(i,j)=\begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ -1 & 0 & \cdots & 0 \end{pmatrix} \quad (1)$$

여기서, 행렬의 요소 (i,j)가 1이면 $e_i \rightarrow e_j$ 관계를 나타내고 -1이면 $e_i \leftarrow e_j$ 관계를 각각 나타낸다. 즉 TPRM은 두 이벤트사이 시간 연관성을 표현하는 행렬이다.

3. 물리보안 위협레벨 결정

어느 시점에 발생된 물리보안 이벤트 조합 $E_c, E_c \subseteq E$,에 대해 다음과 같이 물리보안 위협지수 $S(E_c)$를 계산한다.

$$S(E_c)=\sum_{e_i \in E_c} \delta_i w_i + \sum_{e_i,e_j \in E_c} f(w_i,w_j) \quad (2)$$

여기서, w_i와 w_j는 각각 보안이벤트 e_i와 e_j의 가중치이며, 이벤트 e_i가 부정적 효과를 주는 이벤트이면 $\delta_i = 1$, 반대로 긍정적 효과를 주는 이벤트이면 $\delta_i = -1$ 값을 가진다. 따라서 식 2의 오른쪽 첫 번째 항은 현재 발생된 보안이벤트의 단순 가중치 합이 되며, 이 값이 크다는 것은 발생된 보안이벤트들의 전체 위험 수준이 높다는 것을 의미한다. 식 2의 오른쪽 두 번째 항은 두 보안이벤트 사이 연관관계(식 1의 TPRM)에 의한 가중치 변화를 고려하기 위한 것이다. 식 2의 가중치 변화를 위한 함수 f 는 매우 다양하게 실험할 수 있으나 본 논문에서는 다음 식 3과 같이 단순 ON/OFF 함수를 사용하였다. 예를 들어, 표 1의 보안이벤트 AC1이 발생 후 보안이벤트 AC2가 발생했다면 TPRM으로부터 시간 연관성 관계를 확인하여 만약 '-1' 이면 AC2의 가중치를 무시한다. 이것의 의미는 정상적인 출입자가 해당 보안영역에 존재하면 이후에 발생된 문 열림 실패와 같은 보안이벤트는 무시될 수 있음을 의미한다. 만약 시간 연관성 관계를 확인하여 '1' 이면 이전에 발생된 보안이벤트의 영향을 무시하게 된다.

$$f(w_i,w_j)=\begin{cases} -w_j, & \text{if } e_i \rightarrow e_j \\ -w_i, & \text{if } e_i \leftarrow e_j \\ 0, & \text{if } otherwise \end{cases} \quad (3)$$

PSTM의 물리보안 위협레벨은 정보보안과 동일하게 4단계 위협레벨(정상, 주의, 위험, 심각)로 설정하였다. 본 논문에서는 식 2에서 계산된 위협지수 값 $S(E_c)$를 3개의 참고 기준 값(reference threshold value) R_a (주의레벨), R_d (위험레벨), 그리고 R_s (심각레벨) 과 비교해 해당 위협레벨을 결정한다. 예를 들어, $S(E_c)$ 값이 R_a이하이면 위협레벨은 '정상', R_a와 R_d 사이에 존재하면 '주의', R_d와 R_s 사이에 존재하면 '위험', 그리고 R_s 이상이면 '심각' 으로 각각 결정된다.

판단(classification) 문제를 풀기위해 기준 값을 이용할 때, 기준 값을 결정하는 방법은 일종의 magic number와 같다. 즉 기준 값을 어떻게 설정하는지에 따라 판단 문제의 결과는 엄청난 변화를 보인다. 본 논문에서는 몇몇 중요 물리보안 이벤트의 가중치를 기준 값으로 사용하는 방법을 채택하였다. 예를 들어, 최상위 위협레벨을 결정하는 기준 값 R_s는 표 1의 이벤트 AC3 (혹은 IV2) 같이 실질적인 침입이 탐지되는 극단적인 보안이벤트 가중치를 기준으로 결정했다. 그러나 이와 같이 매우 심각한 단일 보안이벤트가 발생하지 않아도 상대적으로 덜 민감한 여러 개의 보안이벤트 발생에 따른 식 2에 의해 계산된 위협지수 값 $S(E_c)$가 AC3의 가중치를 넘어서면 위협레벨은 심각레벨로 결정된다. 한편 기준 값 R_d 는 표 1의 이벤트 AC4 (혹은 IV4)와 같이 침입이 의심되거나 혹은 예상되는 이벤트 가중치를 기준으로 결정했으며 R_a 의 기준 값은 '0'으로 설정하였다. 제 3장에서 설명한 바와 같이, 일부 보안이벤트는 보안영역 내 긍정적인 효과를 미치기 때문에 위협지수 값 $S(E_c)$는 음수 값(negative value)을 유지할 수 있다.

4. 물리보안 위협 계수기 구현

그림 3은 본 논문에서 제안한 PSTM을 구성하는 주요 컴포넌트들과 이들 사이의 상호 연결을 보여준다. PSTM은 물리보안 장치에서 발생된 보안 이벤트를 수신하거나 (그림 3의 하위 왼쪽 부분) 혹은 PSTM과 물리보안 장치를 관리할 목적으로 보안 관리자로부터 제어 메시지를 제공 받는다 (그림 3의 상위 왼쪽 부분). 한편, PSTM은 물리보안 장치를 제어하기 위한 제어신호를 송신하거나 (그림 3의 하위 오른쪽 부분) 혹은 PSTM에서 결정된 위협레벨을 보안 관리자에게 알려주기 위한 메시지를 전송 한다 (그림 3의 상위 오른쪽 부분). 그림 3에서 보듯이, PSTM은 입력 이벤트를 처리하기 위한 입력처리 모듈(Input Processing Module)과 위협레벨을 결정하기 위한 메인 모듈(Main Module), 그리고 보안장치를 제어하기 위한 제어신호를 출력하는 출력처리 모듈(Output Processing Module)로 구성된다. 입력처리 모듈과 연결된 이벤트 테이블(event table)은 현재 발생되어 있는 물리보안 이벤트를 실시간 기록하고, 타이머(timer)는 제2장에서 설명한 바와 같이 발생된 몇 몇 물리보안 이벤트들을 일정 시간 경과 후 자동 해제하기 위한 것이다. 한편, 그림 3의 메인 모듈에 연결된 이벤트 가중치 테이블(event weight table)과 TPRM 테이블은 메인 모듈이 위협지수 값을 계산할 때 필요한 각 물리보안 이벤트의 가중치 값과 시간 연관성

관계를 나타내는 식 1의 값이 각각 저장되어 있다. 그림 4와 그림 5는 입력처리 모듈과 메인 모듈의 주요기능을 가상코드(pseudocode)를 사용해 나타내었다.

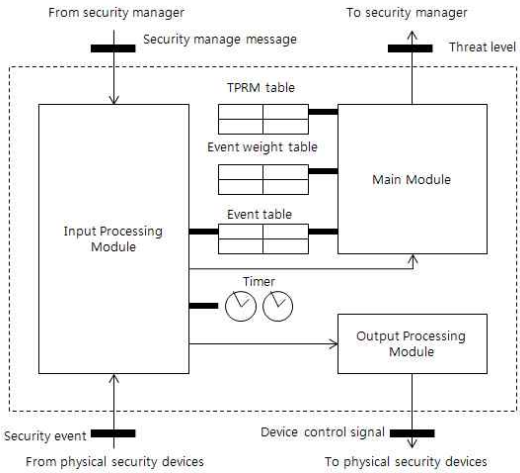

그림 3. 물리보안 위협 계수기 시스템 구조
Fig. 3. Physical Security Threat Meter System Architecture

입력처리 모듈은 앞에서 언급한 바와 같이 물리보안 장치, 보안 관리자, 혹은 타이머로부터 이벤트를 받을 때까지 대기 상태에 머문다. 보안 관리자로부터 수신된 메시지는 발생된 물리보안 이벤트를 처리 후 해제하기 위한 것이거나 혹은 특정 물리보안 장치를 제어하기 위한 메시지이다. 만약 발생된 보안이벤트를 해제하기 위한 메시지이면 이벤트 테이블에서 해당 이벤트를 제거하고 메인모듈로 갱신요구(update request)를 전송하여 현재상태의 위협지수 값을 다시 계산하도록 요청한다. 입력처리 모듈이 보안장치로부터 수신하는 메시지는 물리보안 이벤트의 발생 혹은 해제가 된다. 보안이벤트 발생의 경우, 먼저 해당 이벤트가 타이머를 필요로 하는지 판단하여 타이머를 설정하고 이벤트 테이블에 발생된 이벤트를 등록한다. 또한 메인 모듈로 위협지수 값을 계산하기 위한 갱신요구 메시지를 전송한다. 한편 보안이벤트가 해제 이벤트이거나 혹은 타이머 종료 이벤트이면 해당 보안이벤트를 이벤트 테이블에서 삭제하고 메인모듈로 위협지수 값을 다시 계산할 것을 요청한다.

메인 모듈은 입력처리 모듈로부터 위협지수 갱신요구가 수신되면 물리보안 이벤트의 발생 혹은 해제에 따른 현 위협지수 (식 2)를 다시 계산하고 기준 값과 비교해 위협레벨을 결정해 보안 관리자에게 통보한다. 그림 5에서 보이는 변수 Symptom은 식 2의 위협지수 값 $S(E_c)$에 해당된다.

```
Input_Processing_Module() {
  Sleep until an event is received;
  If (event from security manager) {
    If (the event is 'RELEASING' a security event i) {
      Delete the corresponding entry in EVENT table;
      Send a update request (i, delete) to the
      MAIN module;
      Return;
    }
    If (the event is 'CONTROLING' a security device) {
      Send a control request to the OUTPUT
      processing module;
      Return;
    }
  }
  If (event from security devices) {
    If (the event is 'OCCURING' a security event i) {
      if (the event needs to set the timer)
        Set the timer;
      Insert the corresponding entry in EVENT table;
      Send a update request (i, add) to the MAIN
      module;
      Return;
    }
    If (the event is 'RELEASING' a security event i) {
      If (the event has a timer)
        Expire the timer;
      Delete the corresponding entry in EVENT table;
      Send a update request (i, delete) to the MAIN
      module;
      Return;
    }
  }
  If (event from the timer i) {
    Delete an entry in EVENT table corresponding of
    the expired timer;
    Send a update request (i, delete) to the MAIN
    module;
    Return;
  }
}
```

그림 4. PSTM 입력처리 모듈
Fig. 4. Input Processing Module of the PSTM

V. 실험

본 장에서는 그림 6과 같이 출입문제어장치(access controller)와 CCTV를 포함한 지능형 영상감시 장치를 이용해 서버 컴퓨팅 시스템을 보호하는 보안 영역을 가정하고 제 4장에서 제안한 PSTM을 적용한 실험 시나리오를 구성하는 과정과 시뮬레이션 결과를 설명한다.

1. 물리 보안이벤트 가중치 결정

그림 7은 두 가지 보안 목적 - 불법적 서버 컴퓨팅 로그인 행위 방지와 서버 컴퓨팅 도난 방지 - 에 영향을 미치는 물리 보안이벤트의 가중치를 결정하기 위한 AHP 모델을 나타낸다. 보안 목적을 위한 기준(criteria)으로 네 가지 요소(심각성(severity), 정확성(accuracy), 공간적 영향(spatial impact), 그리고 시간적 영향(temporal impact)를 선택하였다. 공간적 영향은 보안이벤트가 보안영역 내 미치는 범위를 반영한다. 즉 어떤 보안이벤트는 보안영역 전체에 영향을 주는 반면, 다른 보안이벤트는 제한적인 영역 내에서 영향을 미친다. 시간적 영향의 경우, 어떤 보안이벤트는 발생시점에만 심각한 영향을 미치는 반면, 다른 보안이벤트는 일정시간 동안 지속적으로 그 영향을 미치는 경우도 있다.

```
// Initially, Symptom = 0
// The TPRM table and the Event weight table are
// already set-up for this module
Main_Module() {
  Sleep until a update is received;
  If (update is 'add' with event i) {
    Symptom += w_i;
    If (the number of entry in EVENT table is more
        than one)
      Change Symptom in associate with TPRM table;
  }
  If (update is delete with event i) {
    Symptom -= w_i;
    If (the EVENT table is not empty)
      Change Symptom in associate with TPRM table;
  }
  If (Symptom > Threshold level) // set three different
                                 // threshold levels
    Generate a threat level;
  Return;
}
```

그림 5. PSTM 메인 모듈
Fig. 5. Main Module of the PSTM

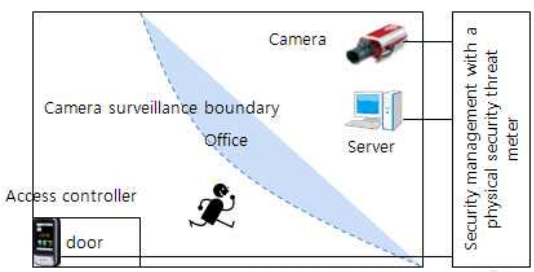

그림 6. 실험을 위한 시나리오 구성도
Fig. 6. Experimental Scenario

표 2는 불법적 서버 컴퓨팅 로그인 행위 방지(보안 목적)에 대한 중요도에 따른 출입문제어기의 보안이벤트의 각 기준별 쌍대-비교를 보여준다. 여기서, 쌍대-비교 값은 9단계로 (1은 동일한 중요도, 9는 매우 중요) 나누고 두 보안이벤트 사이의 상대적인 중요도를 판단하였다. 이러한 쌍대-비교 판

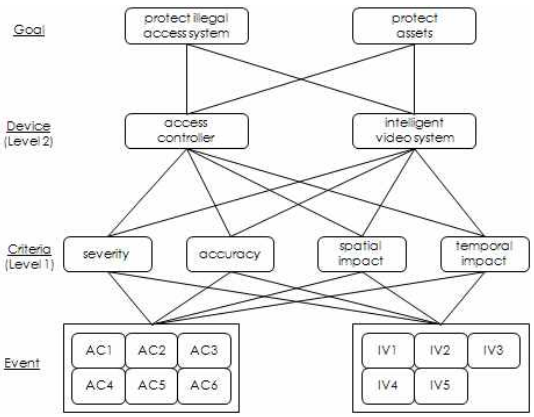

그림 7. 출입문제어기와 지능형영상 감시기(표 1 기준)의 보안이벤트 가중치 결정을 위한 AHP 모델
Fig. 7. AHP Model for Access Controller and Intelligent Video Camera (Table 1)

표 2. 기준 (S : 심각성, A : 정확성, SI : 공간적 영향, TI : 시간적 영향) 별 출입문제어기의 보안이벤트 쌍대-비교 및 가중치 결정 값
Table 2. Comparisons of Events of the Access Control with respect to Criteria (S : Severity, A : Accuracy, SI : Spatial Impact, TI : Temporal Impact)

기준	이벤트	AC1	AC2	AC3	AC4	AC5	AC6	가중치
S	AC1	1	3	1/7	1/5	1/3	1/5	0.044
	AC2	1/3	1	1/7	1/5	1/3	1/7	0.028
	AC3	7	7	1	5	5	3	0.439
	AC4	5	5	1/5	1	3	1/3	0.149
	AC5	3	3	1/5	1/3	1	1/5	0.076
	AC6	5	7	1/3	3	5	1	0.265
A	AC1	1	3	1	3	1	3	0.245
	AC2	1/3	1	1/3	1	1/5	1	0.075
	AC3	1	3	1	3	1	3	0.245
	AC4	1/3	1	1/3	1	1/3	1	0.082
	AC5	1	5	1	3	1	3	0.271
	AC6	1/3	1	1/3	1	1/3	1	0.082
SI	AC1	1	1/3	1/5	1/5	1/5	1/5	0.036
	AC2	3	1	1/7	1/7	1/7	1/5	0.036
	AC3	5	7	1	1	1	1	0.230
	AC4	5	7	1	1	1	1	0.230
	AC5	5	7	1	1	1	1	0.230
	AC6	5	7	1	1	1	1	0.230
TI	AC1	1	1/3	1/9	1/5	1	1	0.043
	AC2	3	1	1/7	1/3	3	3	0.107
	AC3	9	7	1	5	9	9	0.568
	AC4	5	3	1/5	1	3	3	0.187
	AC5	1	1/3	1/9	1/3	1	1	0.047
	AC6	1	1/3	1/9	1/3	1	1	0.047

단 지수는 전적으로 보안 관리자의 결정에 의존하게 된다. 지능형영상 감시기에 대한 가중치 결정도 동일한 방법으로 진행할 수 있다. 본 논문에서는 참고문헌[9]에서 사용한 AHP 모델링 방법에 의해 각 물리보안 이벤트 가중치를 결정하였으며, 표 2와 같이 출입문제어기의 보안이벤트의 가중치를 결정하였다.

표 3은 물리보안 장치의 가중치를 결정하기 위한 쌍대-비교 행렬을 나타내었다. 표 3에서 보듯이, 출입문제어기(AC)는 심각성(S) 가중치를 높게 부여하고 지능형영상감시기(IVS)는 정확성(A) 가중치를 높게 부여하였다. 일반적으로 IVS와 비교해 AC는 훨씬 간단한 구조와 대부분 하드웨어 집합체로 구성되어 있어 안정적으로 운영될 수 있다. 따라서 그림 7의 AHP 레벨 2에서 IVS의 가중치는 0.4, 그리고 AC의 가중치는 0.6으로 각각 설정하였다. 한편, 표 4는 실험 시나리오에서 사용한 출입문제어기의 TPRM을 보여준다. 실험을 위한 보안이벤트 가중치 설정은 AHP 모델을 이용한 체계적인 방법을 사용하였으나 이 과정에서 사용되는 물리보안 이벤트 상호 간의 쌍대비교 파라미터 값들은 전적으로 보안 관리자의 판단에 의존한다. 즉 보호해야할 보안영역 종류에 따라 물리보안 이벤트 상호 간의 중요도 결정은 관리자의 역할이다. 따라서 표 2, 표 3, 그리고 표 4와 같이 본 실험에서 사용된 파라미터 값들은 하나의 예로 볼 수 있다. 한편, 지능형영상 감시기를 위한 관련 파라미터 결정도 앞에서 설명한 출입문제어기와 동일한 방법으로 결정할 수 있으며 본 논문에서는 설명을 생략한다. 최종적으로 각 물리보안 이벤트의 가중치 0.065 (AC1), 0.028 (AC2), 0.218 (AC3), 0.08 (AC4), 0.09 (AC5), 0.115 (AC6), 0.046 (IV1), 0.168 (IV2), 0.074 (IV3), 0.058 (IV4), 그리고 0.052 (IV5)로 결정하였다.

표 3. 보안장치(AC : 출입문제어기, IVS : 지능형영상감시) 별 기준 비교 (S : 심각성, A : 정확성, SI : 공간적 영향, TI : 시간적 영향) 및 가중치 결정 값

Table 3. Comparisons of Criteria (S : Severity, A : Accuracy, SI : Spatial Impact, TI : Temporal Impact) with respect to Devices (AC : Access Control, IVS : Intelligent Video System)

장치	기준	S	A	SI	TI	가중치
AC	S	1	3	7	7	0.555
	A	1/3	1	7	7	0.33
	SI	1/7	1/7	1	3	0.073
	TI	1/7	1/7	1/3	1	0.041
IVS	S	1	3	6	7	0.325
	A	3	1	6	7	0.551
	SI	1/6	1/6	1	3	0.082
	TI	1/7	1/7	1/3	1	0.043

표 4. 출입문제어기 보안이벤트의 시간 연관성 쌍대 행렬 (TPRM)

Table 4. Temporal pair-wise relationship matrix (TPRM) for the security events of access control

	AC1	AC2	AC3	AC4	AC5	AC6
AC1	0	0	0	0	-1	-1
AC2	0	0	0	0	0	0
AC3	0	1	0	1	0	0
AC4	0	1	1	0	0	0
AC5	1	1	1	1	0	0
AC6	1	1	1	1	1	0

2. 시나리오 실험 결과

본 절에서는 표 1에 설명한 물리보안 이벤트를 대상으로 다음과 같은 세 가지 가상 시나리오를 구성하고 본 논문에서 제안한 PSTM이 어떻게 반응하는지 조사하였다.

(i) AC2 - IV4

(ii) AC1 - AC2 - AC4 - IV4

(iii) AC2 - AC5 - IV4

첫 번째 실험 시나리오는 누군가에 의한 문 열림 시도 실패 이벤트 이후 지능형영상감시기에 의해 해당 보안영역 내 배회자를 발견한 이벤트를 고려하였다. 두 번째와 세 번째 실험 시나리오는 첫 번째 시나리오에 긍정적 효과를 가진 이벤트 혹은 부정적 효과를 가진 이벤트가 함께 존재할 경우 PSTM은 어떻게 반응하는지 조사하여 첫 번째 실험 시나리오 결과와 비교 분석하였다.

그림 8은 시뮬레이션 단위시간(time unit) 1부터 시작하여 매 시뮬레이션 단위시간마다 시나리오에 구성된 순서대로 물리보안 이벤트가 발생하는 것을 가정하고, 각 실험 시나리오에 대해 PSTM이 제공하는 위협레벨을 보여준다. 그림 8의 실선은 첫 번째 실험 시나리오의 결과로서, 보안이벤트 IV4가 먼저 발생된 보안이벤트 AC2의 해제 이벤트(AC2의 경우 해제 이벤트는 타이머의 종료에 의해 발생)가 발생하기 전에 발생되는 경우 (그림 8의 시뮬레이션 시간 = 2의 화살표(1)), 위협레벨은 세 번째 단계인 위험레벨이 된다. 하지만, 첫 번째 실험 시나리오에서 AC2의 해제 이벤트가 발생되고 난 후, IV4가 발생되면 (그림 8의 시뮬레이션 시간 = 3의 화살표(2)) PSTM의 위협레벨은 한 단계 낮은 주의레벨이 된다. 따라서 첫 번째 보안이벤트가 발생되고 일정 시간 내에 또 다른 보안이벤트가 발생되면 상대적으로 보안영역 내 위협레벨은 재조정되는 결과를 확인할 수 있다.

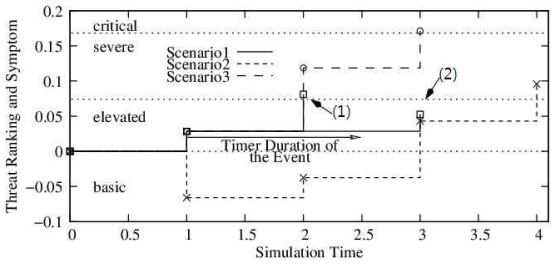

그림 8. 세 가지 실험 시나리오에 대한 시뮬레이션 결과. 실험 시나리오1에서 2개 화살표((1),(2))는 보안이벤트 IV4가 시뮬레이션 시간 2 (화살표(1)) 혹은 3 (화살표(2)) 에서 발생된 경우를 표현
Fig. 8. Simulation Results of three experimental scenarios. The two arrow points of the Scenario 1 represent the vent IV4 is occurred at simulation time 2 or 3

그림 8의 가는 점선은 두 번째 실험 시나리오 결과를 보여준다. 그림에서 보듯이 첫 번째 발생한 긍정적 효과의 보안이벤트 영향으로 위협지수가 '0' 이하로 일정시간 계속 유지되고 있음을 확인할 수 있다. 즉 정상적인 보안이벤트는 해당 보안영역 내에 위협지수를 상대적으로 낮추어 전체 위협레벨을 안정화시키는 효과를 보여준다. 그림 8의 굵은 점선은 세 번째 실험 시나리오 결과를 보여준다. 그림에서 보듯이 침입검출과 같은 극단적인 보안이벤트가 발생하지 않은 상황에서도 일정 수준 이상의 보안이벤트가 여러 개 발생될 경우, 최상위 위험수준인 심각레벨로 결정될 수 있음을 보여준다. 이상의 세 가지 실험 시나리오 결과로부터 본 논문에서 제안한 PSTM이 물리보안 이벤트의 다양한 발생 조건에 따라 우리가 원하는 각 단계별 위협레벨을 적절히 공지함을 확인할 수 있었다.

VI. 결 론

본 논문에서는 정보보안 기관이나 업체에서 매일 실시간으로 공지하는 위협레벨과 동일한 목적으로 물리보안 영역에서 물리적 공격 가능성을 위협레벨로 나타내는 위협 계수기(Threat Meter)를 제안하였다. 이와 같이 보안 분야에 있어서 위험수준을 단계별로 설정하고 각 단계별 대응책을 마련하여 적절히 대응하는 전략은 매우 일반화된 개념이다. 그러나 일반 기업과 같은 생산 현장이나 혹은 관공서 혹은 대학 캠퍼스와 같은 건물 단위의 물리보안 분야에 있어서는 이와 같은 전략이 적용되지 않고 있다. 오늘날 물리보안 장치는 정보통신 기술을 융합하여 네트워킹 기술이 적용되고 지능화된 인식 기술을 접목하여 실시간 원격에서 자동으로 침입을 검출하고 의심스러운 상황을 감지하는 기능을 보유하게 되었다. 따라서 정보보안 분야에서와 같이 물리보안 관제 시스템에서도 실시간으로 각종 물리보안 장치로부터 발생되는 보안이벤트를 수집할 수 있으며 이들 이벤트를 체계적으로 관리·분석하여 위협레벨을 자동으로 알려주는 물리보안 위협 계수기의 필요성이 절실하다.

본 논문에서는 계층분석과정 모델을 이용해 각 물리보안 이벤트의 가중치를 결정하고 복수의 이벤트 발생 시 이들 이벤트사이 연관성을 고려한 가중치 변화를 고려하였다. 한편 물리보안 위협레벨 계수기 구현을 위한 블록도를 제시하였고 블록도 내 주요 구성 모듈의 동작 원리를 자세히 기술하였다. 또한 위협레벨 결정을 위한 기준 값 설정을 위한 방법을 제시하였고 몇 가지 실험 시나리오를 설정하고 물리보안 위협 계수기의 동작 과정을 검증하였으며 각종 보안이벤트에 적절히 반응하고 있음을 확인하였다. 비록 본 논문에서 제안된 물리보안 위협 계수기가 시뮬레이션 수준에서 검증되기는 하였으나, 실제적으로 현재의 정보통신 기술 수준으로 충분히 구현 가능하며 따라서 본 연구진은 가까운 시일 내에 실제 현장에서 검증된 연구 결과를 발표할 예정이다.

참고문헌

[1] McAfee, Security Advice: Threat Meter Levels, http://home.mcafee.com
[2] Symantec Corporation, DeepSight Threat Management System, http://www.symantec.com/security_response/threatconlearn.jsp
[3] AhnLab, Security Alert, http://ahnlab.co.kr
[4] Korea Emergency Response Team Coordination Center, KrCERT Internet Threat http://www.krcert.or.kr/kor/main/main.jsp
[5] DVTtel Inc, Intelligent Video System Technology, DVTEL White Paper, http://info.dvtel.com/WhitePaper.html, 2006
[6] Suprema, Introduction of Bio Star Lite, Technical Columns, http://supremainc.com, June 2001
[7] B. Shin, "Study on Technical trend of physical security and future service," Journal of the Korea Industrial Information System Society, Vol. 15, No. 5, pp. 159-166, Dec. 2009.
[8] Y. Mehdizadeh, "Convergence of Logical and Physical Security," SANS Institute InfoSec Reading Room, 2010. 12.

[9] K. Kang, D. Kang, J. Na, and I. Kim, "Utilization of Physical Events for the Converged Security using Analytic Hierarchy Process: focus on Information Security," Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 3, pp. 553-564, June 2012.
[10] J. Han, and H. Jo, "Technical Trends of Image Security System," Review of Korean Institute of Information Security and Cryptology, Vol. 9, No. 5, pp. 29-37, Oct. 2009.
[11] J. Kim, G. Kim, and Y. Lee, "The Concept and Approach of the Converged Security," Review of Korean Institute of Information Security and Cryptology, Vol. 19, No. 6, pp. 68-73, Dec. 2009.
[12] T.L. Saaty, and L.G. Vargas, "*Prediction Projection and Forecasting*" Kluwer Academic Publishers, 1991.
[13] D.A. Kravitz, and B. Martin, "Ringelmann rediscovered: The original article" Journal of Personality and Social Psychology, Vol. 50, No. 5, pp. 936-941, May 1986.
[14] Y. An, "Security Analysis and Improvements of a Biometrics-based User Authentication Scheme Using Smart Cards" Journal of the Korea Society of Computer and Information, Vol. 17, No. 2, pp. 159-166, Feb. 2012.

저 자 소 개

강 구 홍
1985: 경북대학교
전자공학과 공학사.
1990: 충남대학교
전자공학과 공학석사.
1998: 포항공과대학교
전자계산학과 공학박사
현 재: 서원대학교
정보통신공학과 교수
관심분야: 네트워크 보안
Email : khkang@seowon.ac.kr