한국항행학회 논문지 제11권 제2호 2007년 6월

중요 정보시스템 위협원에 대한 분석

Analysis of Threat Agent for Important Information Systems

김태훈*, 김석수*, 박길철*

Tai-hoon Kim*, Seok-soo Kim*, Gil-cheol Park*

요 약

정보시스템에서 다루는 정보 및 정보시스템은 조직의 기능을 유지함과 동시에 임무를 완수하는데 필요한 중요 자원이므로, 정보의 비인가된 누출, 변경, 손실 혹은 정보시스템의 침해로부터 파생되는 문제점은 경제적 손실뿐만 아니라 조직의 지속성 차원에서도 중요한 의미를 갖게 된다. 경쟁관계에서의 생존을 위해 신속성, 정확성 측면에서 중요한 역할을 수행하여 온 정보시스템에 치명적 오류 혹은 침해가 발생하는 경우, 해당 정보시스템에 의존하고 있는 조직의 생존성은 지대한 영향을 받을 수 있다. 따라서 각 조직은 중요 정보시스템을 안전하게 보호하기 위해 상당한 투자를 아끼지 않고 있으며, 이러한 노력은 몇 가지 특징들을 나타내면서 발전되어 왔다.이러한 중요 정보시스템을 보호하기 위해서는, 먼저 누가 정보시스템에 대해 위협을 가할 수 있는지를 파악하여야 하며, 위협을 야기하는 위협원의 특징에 따라 보안대책을 수립하여야 한다. 본 논문에서는 중요 정보시스템에 위협을 가할 수 있는 위협원들을 식별하고, 이들의 특징을 정리하였으며, 위협원의 위험성을 가시적으로 표시하기 위해 가중치를 부여하는 방법을 제안하였다.

Abstract

Because the networks and systems become more complex, the implementation of the security countermeasures for important Information Systems becomes more critical consideration. The designers and developers of the security policy should recognize the importance of building security countermeasures by using both technical and non-technical methods, such as personnel and operational facts. Security countermeasures may be made for formulating an effective overall security solution to address threats at all layers of the information infrastructure. But all these works can be done after assuming who is the threat agent. In this paper we identify the treat agents for information systems, summarize the characteristics of threat agents, and apply weighting factors to them.

Key words : Information Systems, Threat Agents, Threat Motivation

Ⅰ. 서 론

정보시스템에서 다루는 정보 및 정보시스템은 조직의 기능을 유지함과 동시에 임무를 완수하는데 필요한 중요 자원이므로, 정보의 비인가된 누출, 변경, 손실 혹은 정보시스템의 침해로부터 파생되는 문제점은 경제적 손실뿐만 아니라 조직의 지속성 차원에서도 중요한 의미를 갖게 된다.

경쟁관계에서의 생존을 위해 신속성, 정확성 측면에서 중요한 역할을 수행하여 온 정보시스템에 치명적 오류 혹은 침해가 발생하는 경우, 해당 정보시스템에 의존하고 있는 조직의 생존성에 지대한 영향을 미칠 수 있다. 따라서 각 조직은 정보시스템을 안전하게 보호하기 위해 상당한 투자를 아끼지 않고 있으

* 한남대학교 멀티미디어학부
· 제1저자 (First Author) : 김태훈
· 접수일자 : 2007년 5월 16일

며, 이러한 노력은 몇 가지 특징들을 나타내면서 발전되어 왔다.

가장 보편화되어 있는 보안 관련 투자는, 정보시스템과 정보를 보호하기 위해 정보보호 관련 기능만을 담당하는 정보보호 제품을 구입하여 정보시스템에 추가하는 것이다. 이러한 투자는 상대적으로 간단한 조치이며, 예산에 여유가 있는 경우 더 다양하고 더 많은 정보보호 제품을 구매하여 탑재할수록 정보시스템이 안전할 것이라는 가정에 기반을 두고 있다. 대표적인 정보보호 제품으로는 침입차단제품(Firewall Systems)이나 침입탐지제품(IDS, Intrusion Detection Systems) 등이 있으며, 이러한 방식은 성능의 향상과 효율성의 달성에 중점을 두고 개발된 레거시 시스템이 많이 포함된 정보시스템의 경우에 아주 효과적일 수 있다.

정보와 정보시스템을 안전하게 지키기 위한 시도가 다양한 방식으로 발전, 체계화되면서, 정보시스템의 특성에 따라 적절한 보안대책을 구현할 필요성이 대두되고 있으며, 실제로 정보보호라는 대명제를 만족시키기 위해 과도한 투자를 집행하는 경우가 발생하고 있다.

정보와 정보시스템을 안전하게 보호하는 것은 물론 중요하지만, 정보와 정보시스템의 중요도를 고려하지 않고 일률적인 보안대책을 구현하는 것은 바람직하기 않다. 정보시스템은 사용 및 구축 목적에 따라 각기 다른 중요도를 가질 수 있으며, 일부 정보시스템은 다른 정보시스템에 비해 낮은 중요도를 가질 수도 있다. 심지어는 한 사무공간에 배치된 시스템 사이에도 중요도의 차이가 있을 수 있다. 다시 말하면, 공격자의 공격이 발생했을 경우, 절대로 침해되어서는 안 되는 시스템이 있는 반면, 침해되더라도 별다른 피해가 없는 시스템이 있을 수 있는 것이다.

이러한 다양한 경우의 수는 위협을 야기하는 주체가 누구인가에 따라 많은 영향을 받게 된다. 위협의 주체가 누구인지 파악되면, 위협에 사용될 수 있는 자원의 양과 사용될 도구를 짐작할 수 있게 된다.

본 논문에서는 중요 정보시스템에 위협을 야기할 가능성이 있는 위협원을 식별하고, 이들의 특징을 정리하였으며, 위협원의 위험성을 가시적으로 표시하기 위해 가중치를 부여하는 방법을 제안하였다.

Ⅱ. 정보시스템 보안의 개념

정보시스템 보안의 개념은 국제표준으로 제정된 공통평가기준(Common Criteria, ISO/IEC 18045)에 잘 표시되어 있으며, 자산 소유자와 자산, 위협, 보안대책, 취약성 등의 상관관계를 도식화하면 그림 1처럼 표시할 수 있다 [1].

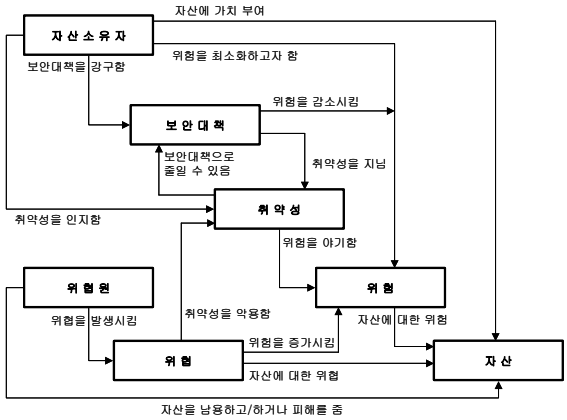

그림 1. 자산을 중심으로 한 보안개념 및 관계
Fig1. Security concept and relation in asset

공통평가기준은 정보기술 제품의 보안성을 평가하는 데 사용되는 기준이지만, 보안과 관련된 개념은 이를 확장하여 정보시스템에 적용하는 것이 가능하다.

자산 소유자는 자신의 환경에서 발생 가능한 위협을 분석하고, 분석의 결과를 위험으로 변환하여 보안대책을 선택함으로써 허용 가능한 수준까지 위험을 줄일 수 있다. 보안대책은 직접 혹은 간접으로 지침을 제공하여 취약점을 감소시키고, 자산 소유자의 보안 정책을 충족시킬 수 있어야 한다. 하지만 보안대책이 적용된 후에도 취약점은 여전히 잔존할 수 있으며, 이러한 취약점은 당연히 위협원에 의해 악용될 수 있다. 따라서 자산 소유자는 다른 제약을 가함으로써 이러한 위험을 최소화하기 위해 노력할 것이다.

그림 1에 표시된 많은 요소들 중, 정보시스템의 보안수준(SL, Security Level) 결정에 가장 중요한 영향을 미치는 요소는 위협(Threat)과 자산(Asset)이며, 나머지 요소들은 위협과 자산에 영향을 주거나 받음으로써 간접적으로 보안수준에 영향을 미치게 된다.

Ⅲ. 위협원에 대한 분석

3-1 위협원 식별

보편적인 의미에서, 위협원은 실제 공격을 수행하는 주체와 잠재적으로 공격을 가할 수 있는 주체를 모두 포함한다고 할 수 있다. 또한 공격을 가한다고 하여도, 공격을 수행하는 주체는 악의를 가지고 있을 수도 있고, 혹은 특별히 악의를 가지고 있지는 않으나 호기심 혹은 다른 단순한 이유만을 가지고 있을 수도 있다.

하지만 본 논문에서는 특정한 의도와 악의를 갖고 시스템에 위해를 가하려고 하는 주체를 위협원으로 정의한다.

다음의 표 1은 다양한 위협원을 표시한 것이며, 위협원은 개인일 수도 있고 특정한 조직의 형태를 나타낼 수도 있다. 표 1은 '위협의 대상'에 의해 분류된 것이 아니기 때문에, 각 위협원에 대한 가중치를 부여하는 것은 무의미하다. 일부 위협원은 시스템 자원을 사용하기 위해 관리자의 권한을 획득하는 것이 목적일 수도 있고, 또한 일부 위협원은 시스템 자체나 시스템의 정보를 파괴하는 것이 목적일 수도 있는데, 이러한 목적은 위협의 대상이 무엇인지 식별되는 순간 명확해 진다.

따라서 위협원을 식별하고 위협원에 대해 가중치를 부여하는 경우, 위협원이 가지고 있을 것으로 예상되는 힘의 범위를 함께 고민할 필요가 있다.

예를 들어, 만일 식별된 위협원이 사이버테러리스트였다면, 이들은 폭탄을 이용하여 정보시스템을 파괴할 수 도 있으므로, 사이버테러리스트가 가진 '위협력(위협을 가할 수 있는 잠재적인 힘의 크기)'은 관리

표 1. 잠재적인 위협원

자의 아이디나 패스워드를 획득함으로써 정보시스템에 침입할 수 있는 해커들보다 크다고 할 수 있다.

다음의 표 2는 식별된 위협원에게 부여할 수 있는 가중치의 예이다. 가중치는 정보시스템의 종류, 운영

표 1. 잠재적인 위협원
Table 1. Latent threat agents

위협원	설명
악의적인 경우	
적성 국가	잘 조직화되고 재정도 충분함. 경제적, 군사적, 정치적 이익을 위해 혹은 적성으로 판단되는 국가의 비빌 또는 중요한 정보를 모으기 위해 외부 전문기관을 사용할 수 있음
해커	운영 체제나 혹은 다른 결함을 이용하기 위해 시스템이나 네트워크에 위협을 가하는 그룹 혹은 개인 (예를 들어, 해커, 프랙커, 크랙커 등)
사이버테러리스트	자신들의 요구를 관철시키기 위해 정부나 사회에 폭력적인 위해를 가하려고 하는, 국지적 혹은 국제적으로 활동하는 개인들 혹은 그룹
범죄 조직	도박, 공갈, 마약 등 다양한 범죄 활동을 시도하기 위해 조직화되고 정비된 범죄 조직
국제 출판 매체	불법적으로 정보를 수집, 배포하거나 다른 출판 혹은 방송 매체에 서비스를 제공하는 조직
산업 경쟁 기관	국내 및 국제 경쟁 환경에서 운영중인 상태이며, 경쟁사나 혹은 외국 정부로부터 스파이 활동을 통해 종종 불법적인 정보를 수집하는 기관
불만이 쌓인 내부 직원	로컬 네트워크나 시스템에 위해를 가할 수 있는 불만이 쌓인 개인들로서, 현재의 고용 상태나 시스템에 대한 접근 권한에 따라 내부 위협원으로 발전될 수 있음
비 악의적인 경우	
부주의하거나 훈련이 부족한 사용자	훈련의 부족, 관심의 부족, 혹은 주의의 부족으로 정보 및 정보시스템에 위협을 가하는 사용자들로서, 또 다른 내부 위협원의 일종임

목적, 환경에 따라 달라질 수 있다.

표 2. 식별된 위협원의 위협력에 대한 가중치 예
Table 2. The example against weight for threat level of identified threat agents

항목	위협력의 수준	가중치	비고
위협원의 위협력	내부 침투 시도	1	
	침입 성공	3	
	무력화 성공	5	
	시스템 파괴	7	

3-2 위협원의 동기

'위협'의 개별적인 동기들은 다양하고 복잡하다. 일반적인 경우에 있어서는, 정보시스템에 의해 처리되는 정보에만 관심을 두기 때문에, 위협원의 동기는 내부 침입 및 관리자 권한 획득이라고 생각하기 쉽다.

본 논문에서는 이미 위협원들을 표 1과 같이 식별하였고, 위협원들의 위협력을 구분하였으며, 이에 대한 가중치를 부여하였다. 이러한 경우, 악의를 가지는 위협원들은 상업적, 군사적, 개인적 이익을 취하려고 시도하는 것으로 볼 수 있다.

위협원 분류의 반대방향의 종점에는 의도하지 않았으나 자신도 모르게 정보시스템에 위협을 가하게 되는 사용자들이 위치하게 된다. 해커들은 실무 경험이 없는 학생이나 스크립트 키디로부터 고도의 기술을 확보하고 있는 전문가까지 다양하게 분포하고 있다.

대부분의 해커들은 정보시스템을 파괴하거나 위해를 가하지 않고 단순히 관리자 권한을 획득하는 기술에 대하여 자부심을 가지고 있으며, 이러한 방식에 대하여 꾸준히 연구하고 있다.

하지만 이러한 의도 역시 정보시스템에 대한 위협이 되기에는 충분하므로, 현실적으로 구체화되는 모든 시도는 위협으로 간주되고, 이를 실행하는 해커들은 모두 위협원이 된다.

다음은 일반적으로 위협원들이 특정 목표물에 대하여 위협을 가하는 이유를 명세한 것이다.

o 중요하거나 민감한 정보에 대하여 접근을 획득함(단, 여기에서 말하는 중요성은 개인이나 조직의 성향에 따라 달라지는 것으로서, 절대적인 것은 아님)
o 목표 시스템의 운영을 추적하거나 모니터함
o 목표 시스템의 운영을 방해함
o 금전, 재물, 서비스를 탈취함
o 시스템 자원의 무료 사용권을 획득함(예를 들어, 컴퓨터 자원이나 네트워크를 자유롭게 사용함)
o 목표 시스템을 혼란스럽게 만듦
o 보안 메커니즘을 무력하게 만듦으로서 성취감을 느낌

정보시스템의 관점에서 볼 때, 이들 동기들은 세 개의 기본 목표를 달성하기 위한 것으로 분류하여 정리할 수 있다.

o 정보에 대한 접근
o 정보 혹은 시스템 프로세스의 수정 혹은 파괴
o 정보에 대한 접근 방해

정보 처리 시스템을 공격할 때, 위협원은 자신이 처할 수 있는 위험에 대하여 충분히 알고 있는 경우가 많다. 이 위험은 시간 의존적 요소이며, 경우에 따라서는 이 위험이 공격 성공으로 얻을 수 있는 이익을 넘어서기도 한다.

이러한 위험 요소에는 다음과 같은 내용들이 포함될 수 있다.

o 다른 유형의 공격을 수행하기 위한 공격자의 능력을 확인함
o 얻을 수 있는 이익이 커질 때, 미래의 공격 성공을 막을 수 있는 대응 방안을 촉발함
o 공격이 발각되었을 때의 손해(예를 들어, 벌금, 투옥, 재정장애 등)
o 생명의 위태로움

이러한 위험성에도 불구하고, 위협원이 감내하려고 결심하는 위험의 수준은 위협원의 동기에 의해 결정된다. 만일 어떤 테러리스트가 다른 조직의 정보

시스템을 파괴하기로 마음먹었다면, 테러리스트들은 자신들의 정체가 노출되는 것을 별로 두려워하지 않을 것이다. 이것은 또 다른 종류의 동기가 되기도 하며, 가장 위험한 종류로 분류될 수 있다.

다음의 표 3은 위협원의 동기에 가중치를 부여한 예이다.

표 3. 위협원 공격 동기에 대한 가중치 예
Table 3. The example against weight about Threat Motivation

항목	분류	가중치	비고
위협원의 동기	혼란스러움 야기	1	
	자원 획득	2	
	자산 침탈	3	
	서비스 거부	4	
	시스템 파괴	5	

위협원의 위협력과 동기는 동일한 개념으로 보기는 어렵다. 위협원이 높은 위협력을 보유하고 있더라도, 위협원이 정보시스템에 대한 강한 공격 동기를 가지고 있다고 볼 수 없기 때문이다.

따라서 [표 3]의 내용을 실제 정보시스템에 그대로 적용하는 것은 바람직하지 않을 수 있으며, 사전에 반드시 정보시스템의 환경을 확인하고 위협원의 동기를 예측하여야 가중치를 적용하여야 한다.

Ⅳ. 결론 및 향후 연구과제

정보시스템은 다양한 형태로 변형되어 활용되고 있으며, 정보화 시대를 지탱해 주는 핵심 인프라로 자리매김하고 있다. 중요한 역할을 수행하는 정보시스템을 보호하기 위해서는, 먼저 누가 정보시스템에 대해 위협을 가할 수 있는지를 파악하여야 하며, 위협을 야기하는 위협원의 특징에 따라 보안대책을 수립하여야 한다.

이에 따라 본 논문에서는 중요 정보시스템에 위협을 가할 수 있는 위협원들을 식별하여 이들의 특징을 정리하였으며, 위협원의 위험성을 가시적으로 표시하기 위해 가중치를 부여하는 방법을 제안하였다.

또한 위협원의 위협력과 함께 위협원의 동기를 식별하여 가중치를 부여하는 방법을 제안함으로써 무형적 요소를 유형적 요소로 변환하는 방안을 도입하였다.

참 고 문 헌

[1] ISO/IEC 21827, Information technology Systems Security Engineering Capability Maturity Model (SSE-CMM)

[2] ISO/IEC 15408-1:1999, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[3] Tai-hoon Kim, Tae-seung Lee, Kyu-min Cho, Koung-goo Lee, The Comparison Between The Level of Process Model and The Evaluation Assurance Level, *The Journal of The Information Assurance,* Vol.2, No.2, KIAS.

[4] Sangkyun Kim, Hong Joo Lee, Choon Seong Leem, Applying the ISO17799 Baseline Controls as a Security Engineering Principle under the Sarbanes-Oxley Act, ICCMSE 2004

[5] Tai-hoon Kim, Yune-gie Sung, Kyu-min Cho, Sang-ho Kim, Byung-gyu No, A Study on The Efficiency Elevation Method of IT Security System Evaluation via Process Improvement, *The Journal of The Information Assurance*, Vol.3, No.1, KIAS.

[6] Tai-hoon Kim, Tae-seung Lee, Min-chul Kim, Sun-mi Kim, Relationship between Assurance Class of CC and Product Development Process, The 6th Conference on Software Engineering Technology, SETC 2003

김 태 훈(金泰勳)

1995년 성균관대학교 공학사
1997년 성균관대학교 공학석사
1999년 (주)신도리코 기술연구소 연구원
2002년 성균관대학교 공학박사
2004년 한국정보보호진흥원 선임연구원
2006년 국군기무사령부 사무관
2007년 이화여자대학교 연구교수
2007년~현재한남대학교 멀티미디어학부 조교수
관심분야 : DRM, Security, Assurance, HW/SW Design

박 길 철(朴吉綴)

1983년 한남대학교 공학사
1986년 숭실대학교 공학석사
1988년 성균관대학교 공학박사
1998년~현재 한남대학교 멀티미디어학부 정교수
관심분야 : Communication, HCI,VR

김 석 수(金錫洙)

1989년 경남대학교 이학사
1991년 성균관대학교 공학석사
1991년 정풍물산(주)중앙연구소 주임연구원
1997년 한국 탑웨어 책임연구원
1998년 경남 도립 거창전문대학교 교수
2000년 동양대학교 컴퓨터공학부 교수
2002년 성균관대학교 공학박사
2003년~현재 한남대학교 멀티미디어공학 교수
관심분야 : Ubiquitous, Healthcare, Multimedia Authoring