2005 한국경영과학회/대한산업공학회 춘계공동학술대회
2005년 5월 13일~14일, 충북대학교

UML을 적용한 ERP 보안 프레임워크 구현

UML with ERP Security Framework implementation

원치성, 임상환, 엄완섭
Won Chi Sung, Leem Sang Hwan,Um wan sub
강원도 강릉시 지변동 123 강릉대학교 산업시스템 공학과

Abstract

ERP(Enterprise Resource Planning) 시스템은 급여, 회계, 인사, 생산, 판매, 물류 등을 포함한 핵심 비즈니스 프로세스를 담고 있는 소프트웨어이다. 인터넷의 등장으로 ERP 시스템이 WEB 기반으로 전환되었고 ERP의 영역도 기업내부에 국한된 것이 아니라 기업간의 거래를 모두 포함하기에 이르렀다. 그러나 ERP 시스템은 회사의 중요한 의사결정 데이터들과 한 Application 안에서 일어나는 Transaction 처리 등의 정보 보안에 대한 취약성을 가지고 있다. 이에 ERP 시스템에도 보안에 대한 필요성이 대두되었으나 ERP 업체들의 대다수는 아직도 구체적인 보안에 대한 방안을 제시하지 않고 있는 실정이다. 결국 비즈니스의 성공도 취약한 기업의 자원을 인증되지 않은 다른 사용자로부터 보호하는 능력에 달려 있으며, 이 연구의 목적은 ERP 시스템의 보안 이슈를 어떻게 다룰 것이며, ERP 보안 요구 사항을 어떻게 모델링 할 것인가에 대한 연구 이다. 현재 나와있는 SAP R/3와 EAGLE ERP의 제품 보안 모델을 비교함으로써 외산 제품과 국산 제품의 보안 요구 사항을 분석 하고, ERP시스템 보안에 대한 고려사항 및 접근 방법을 모델링 할 것이다. 본 연구에서는 UML을 이용하여 ERP 시스템 안에서 찾을 수 있는 모든 보안 사항을 점검 하고, UML의 물리적 요소와 논리적 요소를 이용함으로써 ERP 보안을 모델링 하고자 한다. 이 논문을 통하여 ERP 시스템의 각 분야의 담당자가 ERP 보안을 개념적으로 접근 할 수 있도록 할 것이다. 차후 연구 과제는 좀더 구체적인 모델링을 통한 ERP 보안 solution 개발이다.

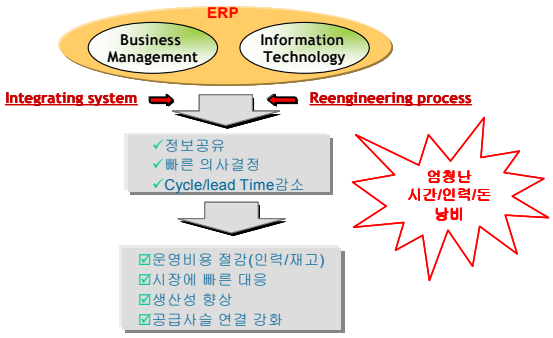
1. 소개

ERP(Enterprise Resource Planning) 시스템은 모든 비즈니스 프로세스와 기능의 전체적인 통합을 목표로 한 선진 업무 모델이 내장된 S/W 패키지이다. 이 시스템은 비즈니스 프로세스의 시각적인 모형을 제공하고 비즈니스 프로세스에 대한 S/W 요소간의 연결과 멀티 S/W 플랫폼 상에서 쉽게 이룰 수 없는 데이터의 무결성, 보안 등의 중요한

기능을 가지고 있다. 1990년대 말,IT 발전으로 인해 기업들은 인터넷과 웹 기반의 기술들을 이룩하게 되었고, ERP S/W를 통하여 비즈니스 프로세스 정보의 전사적 관리와 거래 파트너간의 정확한 정보 공유가 가능하게 되었다. 대부분의 회사는 ERP 시스템이 Corporate Backbone 이라고 생각 한다. ERP 시스템은 전체 비즈니스에서 사용되는 데이터(예:Enterprises Key Business Data)를 위한 Central Repository를 제공한다. 때문에 기업은 ERP Project에 중요한 인력 자원과 ERP Process 자원을 제공해야만 한다. ERP 자원이 잘 정의되지 않는다면, ERP 시스템은 허가받지 않은 사용자에게 치명적인 공격을 당할 것이다. 이를 위해 보안의 목적, 보안 위협의 종류, ERP system의 취약성과 ERP S/W를 위한 보안 요구 사항에 관련된 연구가 필요하다. ERP 시스템의 보안을 위한 ERP S/W에 요구되어 지는 보안사항을 개념적 측면, 시스템 구성 측면, 기술적 구성 측면의 관점에서 연구 할 것이다. 마지막으로 이러한 관점 들을 UML을 적용하여 모델링 한다.

1.1 ERP (Enterprise Resource Planning)

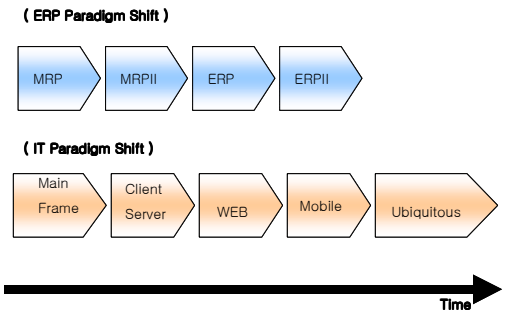
ERP(Enterprise Resource Planning)는 우리말로 전사적 자원계획이라 한다. 그야말로 기업에 존재하는 모든 리소스(통상 경영자원)에 대해서 최적의 활용방안을 제시하는 프로그램이라 할 수 있다. 통상, 인사/급여/생산/자재/무역/영업/회계/원가 시스템의 유기적인 집합체(또는 통합체)라고 하면 금방 이해가 갈 것이다. 해서, 통상 업무 패키지라든가 통합 기간업무시스템으로 불려지고 있다.



[그림 1.] ERP 개요

2. ERP 보안의 필요성 및 취약성

ERP는 지금껏 기술환경 변화에 민감하지 않았다. 이유로는 ERP가 회사입장에서 직접 고객을 상대하는 Front Office업무이기 보다는 내부직원에 의해서만 사용되는 Back Office업무이기 때문에 유행에 민감하지 않고 폐쇄적이었으며, ERP 제품이 IT적인 측면보다는 경영적인 측면이 더욱 강조되었기 때문이다.



[그림 2.] 기술 변화에 따른 ERP의 변화

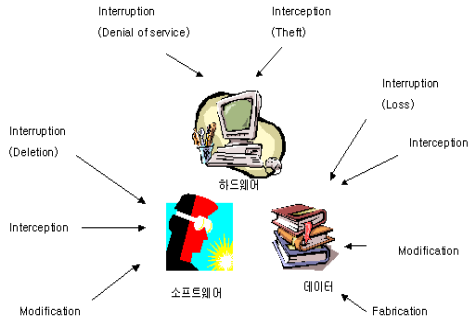
하지만 WEB, Mobile등의 새로운 개념의 환경이 도래 하였고, Business 측면에서도 ERP II 라고 하는 새로운 개념이 대두된 것이 촉매재가 되었다.
최근의 갑작스런 기술변화에 대해 사용자의 요구를 받아들이지 않을 수 없기에 개방적인 측면으로의 상당히 많은 변화를 겪고 있다. 이에, ERP 제품에 대해서도 예전보다 많은 보안적인 허점이 생기게 되므로 복합적이고 다각적인 관점에서의 보안적용 방안이 필요하게 되었다.

2.1 보안의 특성

컴퓨터의 보안은 중요한 세 가지 특성으로 구성 된다 : 기밀성, 무결성, 이용성
기밀성은 컴퓨터 시스템에 권한을 부분적으로 위임해 주는 방식으로 접근이 허용될 수 있는 것을 의미한다. 접근 Type은 Read-Type Access : Object Existence의 Reading, viewing, printing 과 knowing 이다.
무결성은 정보의 부적절한 변경을 예방, 감지 및 제지하는 것을 의미 하는 것으로, 권한을 위임 받아야지만 정보의 수정이 이루어 질 수 는 것을 의미한다.
이러한 관계에 있어서, 변경은 writing, changing, changing status, deleting, creating을 말한다. 이용성은 권한을 부여 받은 부분은 접근 할 수 있는 것을 의미한다.

2.2 보안 결함의 종류

Computing 시스템의 중요한 Asset은 하드웨어, S/W, 데이터로 이루어진다.
보안에 대한 4가지 위협 요인 :
Interruption, Interception, Modification, Fabrication.
위의 네 가지의 위협 요소는 Computing 시스템의 취약성을 이용한다. Interruption 은 시스템 Asset을 사용할 수 없게, 이용할 수 없게 하는 것을 의미한다. Interception은 권한부여 없이 시스템의 Asset에 접근 하는 것을 의미 한다. Modification은 누군가 데이터베이스의 값을 변경하고 부가적인 컴퓨터 사용의 실행이나 전자적으로 전송되는 데이터를 변경하는 것을 의미 한다. Fabrication은 권한위임 없이 Computing시스템의 Object를 복사 하는 것을 의미 한다.



[그림 3.] 컴퓨터 시스템의 취약성

2.3 ERP S/W의 취약성

ERP S/W의 취약성은 시스템의 자원의 세 가지 범주로 적용 되어 진다.
=> 하드웨어, S/W, 데이터

서로 연결되어 있는 이 세 가지 Assets 는 모두 취약한 점을 내포 하고 있다. 하드웨어는 Interruption과 Interception 의 결점을 가지고 있다. S/W는 Interruption, Interception, Modification의 결점을 가지고 있다. 마지막으로 데이터는 모든 가능한 결점 : Interruption, Interception, Modification, Fabrication을 가지고 있다.

3. ERP S/W에 필요한 보안 요구 사항 및 접근 방법

3.1 ERP 보안 요구 사항

ERP S/W의 보안 요구사항은 허가된 사용자의 접근, S/W 데이터의 보호,네트워크 보호, 백업과 치료, 위협요소로부터의 차단, 바이러스의 경계 등이 있다. 접근 사용자의 종류로는 시스템 개발자, 최종사용자, 시스템 관리자, 데이터베이스 관리자, ERP S/W에 대한 네트워크 관리자가 있다. 보호의 종류로는 데이터/S/W 보호, 네트워크 보호, 백업/복구, 위협요소로부터의 차단, ERP S/W에 대한 바이러스 경계 등이 있다. 데이터/S/W 보호는 시스템 개발자에 의해, 시스템 관리자, 네트워크 관리자에 의하여 가능하게 된다. 이유는 이러한 보호는 데이터의 관리를 필요로 하기 때문이다. 하지만 End_user와 네트워크 관리자는 데이터를 수정 할 수 없다. 그래서 End_user 와 네트워크 사용자는 단지 데이터에 대한 읽기 권한 만을 요구한다. 시스템 관리자, 데이터베이스 관리자, 네트워크 관리자는 네트워크 보호를 필요로 한다. 이렇게 함으로써 관리자의 힘을 갖게 된다. 백업/복구는 전체의 object와 전체의 자원을 필요로 한다. 그렇게 시스템 관리자는 전체적인 object에 관한 관리적인 힘을 가지게 되고 데이터베이스 관리자는 네트워크 보호를 제외한 전체적인 Resource에 대한 관리적인 힘을 가지게 된다. 위협의 차단과 바이러스 경계의 필요성은 ERP S/W와 데이터베이스에 필요할 뿐만 아니라 또한 근거리 Resource 간에도 필요하다.

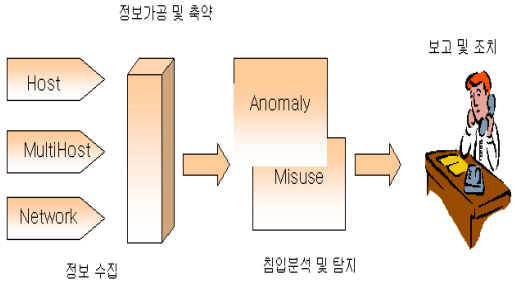
	System Developer	End User	System Admin	DBA	Network Admin
Data/Software Protection	R/W	R	R/W	R/W	R
Network Protection	NA	NA	EN	EN	EN
Backup Recovery	NA	NA	EN	NA	NA
Cut Off for Threats	EN	EN	EN	EN	EN
Virus Alert	EN	EN	EN	EN	EN

(R : Read, W:Write, NA:Not Active, EN:Enable)

[그림 4.] ERP S/W 보안 요구 사항

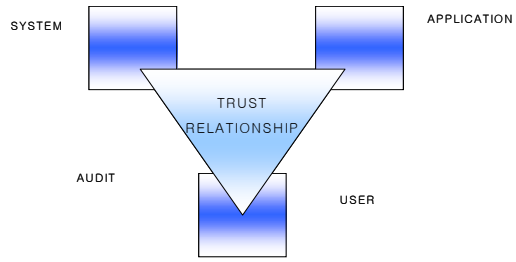
이러한 요구 사항은 침입탐지시스템과 차단시스템으로

해결 될 수 있다. 침입차단시스템은 보안이 보장되지 않는 외부네트워크와 보안이 요구되는 내부 네트워크 간의 중간에 설치되며, 접근 통제, 사용자 인증, 등의 기능을 통하여 보안을 수행 한다.



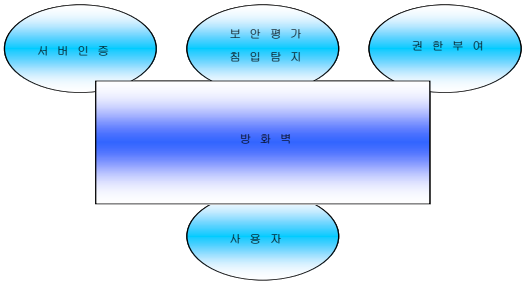
[그림 5.] 침입 탐지시스템의 수행 과정
* 정보수집(Data Collection) : 호스트나 네트워크로부터 정보를 수집 한다.
* 정보가공 및 축약(Data Reduction) : 시스템 설정과 패턴 데이터베이스 설정에 따라 정보 분석기에서 수행.
* 침입 분석 및 탐지(Analysis & Detection) : 기존의 가공된 정보와 축약을 거친 데이터를 기반으로 침입 여부를 결정하는 단계
* 보고 및 조치(Report & Response) : 침입으로 규정된 행위가 발생할 경우 수행되어지는 것
-> 침입 탐지를 통하여 조사한 후 침입차단 시스템을 통하여 제어한다.

3.2 외산 ERP S/W와 국산 ERP S/W

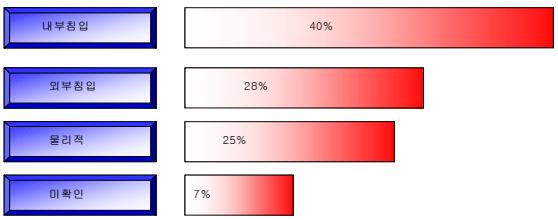


[그림 6.] SAP R/3 의 보안모델

위의 그림은 세계 대기업에서 가장 많이 사용하는 ERP S/W로 ISO 77498-2에서 정의한 5가지 보안 서비스를 잘 활용 하고 있는 SAP사의 R3라는 제품의 보안 모델을 보여준 것이다.
- SYSTEM : SNC(Secure Network Communications) 서버와 클라이언트, 서버와 서버간의 암호화를 말함.
- APPLICATION : SSF(Secure Store & Forward) 매카니즘. 전자서명 및 보안 포맷을 사용한 저장 및 전달.
- USERS : 권한관리. 사용자는 자신의 역할에 따라 자동으로 정보와 어플리케이션, 서비스에 대한 Acess를 부여 받음.
- TRUST RELATIONSHIP : 다양한 사용자 인증. SSO, PKI, Smart Card, X.509의 인증서 등
- AUDIT : AIS(Audit Information System). 로그온 시도 및 트랜잭션 개시 등의 이벤트를 기록.



[그림 7.] EAGLE ERP 의 보안모델
위의 그림은 코인택사의 EAGLE ERP 라는 제품의 보안 모델을 보여준 것이다.
- 서버인증 : 서버에 접속한 클라이언트 사용자의 인증을 서버 간 통신을 통하여 주고받음.
- 보안평가, 침입탐지 : 시스템의 비 정상적인 사용과 오남용을 탐지.
- 권한부여 : 내용보호, 암호저장, 바이러스 검출
- 방화벽 : 내부 네트워크에 대한 접근 통제, 사용자 신분 확인, 감사추적 및 보안관리, 기밀성 및 무결성
- 사용자 : 권한관리. 사용자는 자신의 역할에 따라 자동으로 정보와 어플리케이션, 서비스에 대한 Access를 부여 받음.
SAP R3는 세계적인 회사 답게 여러 가지 방면에 대한 보안 방안을 제시하고 있음을 알 수 있다. 하지만 보안영역의 각 항목이 ERP제품에 따른 보안 분류라기 보다는 보안 제품을 염두에 둔 분류에 가깝다. 이것은 SAP R3제품이 보안부분을 자체적으로 해결하는 것보다는 보안회사의 제품을 손쉽게 적용할 수 있다는 것에 무게중심을 두었다고 생각 할 수 있다. 이와 유사하게 EAGLE ERP 또한 PKI 인증, 서버 간 USB-key, Token 인증 방식 등 효율적인 보안 방안을 제시하고 있다. EAGLE ERP의 특징 중 하나는 침입탐지와 침입차단시스템(Firewall)을 함께 사용함으로써 보안의 효율성을 높였다.
두 회사 모두 효율적인 보안 방안을 제시 하고 있으나, 공통적으로 문제 되는 것은 허가된 사용자의 내부 정보유출의 경우에 대한 내부 감사가 부족하다는 것이다.



[그림 8.] 네트웍 보안 사고 유형

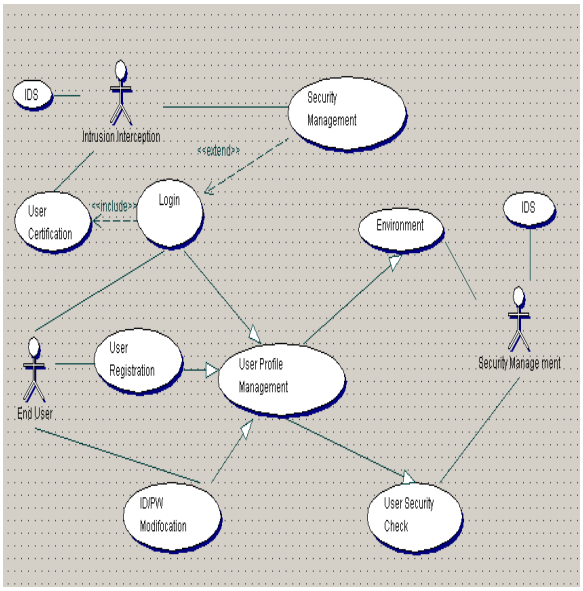
네트웍 보안사고 유형을 보면 외부 침입 보다는 내부 침입에 의한 피해가 더 큰 것을 알 수 있다.
ERP 시스템에 있어서 유출방지 방안은 다음의 두 가지로 요약할 수 있다. 첫째, ERP시스템에서 중요한 정보에 대해 출력을 하거나 파일을 생성하는 작업 하는 행위에 대하여 log로 생성하여 관리자가 항시 모니터링을 할 수 있는 IDS를 사용. 둘째, 허가되지 않은 사용자에 대한 암호화 기법 사용.

4. 보안 모델

4.1 설명

ERP 시스템의 유출방지 방안 중 내부 감사에 사용하는 IDS를 중심으로 UML을 적용하여 보안 사항을 모델링 한다. 두 회사의 보안 모델을 참조하여 내부 감사에 대한 보안 방안으로 다중 IDS와 실시간 해킹 탐지 기술인 자율적인 에이전트(autonomous agent)를 사용한 보안 모델을 고려하여 보았다.
다중 IDS란 ERP 시스템 밖과 안에 방화벽과 함께 각각의 IDS를 설치하여 내/외부 감사를 하는 것을 말하며, 자율적인 에이전트란 시스템과 독립적으로 에이전트들끼리 가장 높은 침입 패턴을 규정하여 서로 도움을 주며 시스템 내의 비정상적인 행위를 감시하는 것을 말한다.

4.2 Use Case View

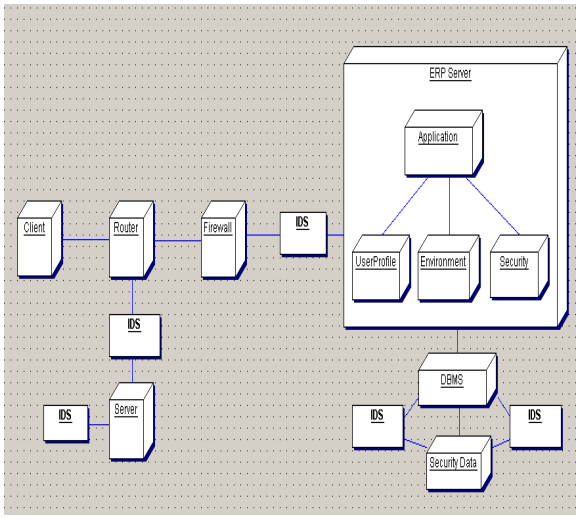


[그림 9.] ERP 보안 Use Case 다이어그램.

Use Case View는 ERP 시스템에 할당되어진 다른 View의 시나리오 뿐 아니라 정확하고 완전한 소프트웨어 구조를 증명하는 방법을 제공한다. IDS를 외부에 내부에 두어 효율적인 보안 감사가 이루어 지도록 한다.

4.5 Deployment View

Deployment View는 시스템 실행에 대한 시스템 하드웨어 토폴로지 형식의 노드를 포함한다. Deployment View는 시스템에 요구되는 (신뢰성,이용성,실행성,측정성과 같은..) 비 기능적인 중요한 관계의 개념을 포함한다. 클라이언트가 ERP 서버에 접속하기 위해서는 사용자 인증을 통한 보안처리 과정이 필요하다.
이를 위하여 침입 탐지 시스템에서 보안사항을 검사 하고 다음으로 침입차단 시스템을 두어 사용자 인증 과정을 처리 한다. 데이터베이스 서버를 따로 설치하여 좀더 강력한 보안환경을 구축 한다. 침입 차단 시스템을 통과한 후 발생할 수 있는 보안 문제는, 서버내부에 침입탐지 시스템을 각



[그림 10.] ERP 보안 Deployment 다이어그램

각 연결 시켜 보안 사항을 점검 하고 내부 사용자에 의한 불법 행위 또한 감시 한다.

5. 결론

ERP의 도입으로 기업은 최적의 업무 프로세스 구축하게 되었다. 기업의 모든 자원을 하나의 통합 개념으로 전사적 관리가 가능해진 것이다. 하지만 IT 기술의 진보로 C/S 환경에서 개발된 ERP 소프트웨어는 여러 가지 보안 사항에 취약성을 보이고 있다. ERP 시스템 내에서의 가장 중요한 보안 사항은 사용자에 대하여 올바른 권한 부여와 불법적인 사용자로부터 데이터를 보호하는 것이다. 많은 ERP S/W 개발 업체들이 각각의 보안 모델을 바탕으로 보안 방안을 제시 하고 있으나, 표준화된 구체적인 방안을 제시 하지 못하고 있는 실정이고, 외부 보안에 대하여 방화벽 사용 등의 대책을 세운 반면 내부 보안 감사에는 미흡한 것이 현실이다. 그 해결책 중 하나로 침입탐지 시스템과 보안관리 시스템을 내부에 두어 실시간 검사 가능하도록 한다. 좀더 구체적인 침입탐지 기법의 연구와 보안 요구사항과 사용자 요구사항을 적절히 만족시켜 주는 보안 정책에 대한 연구는 앞으로 남은 과제이다.

6. 참고 문헌

[1] Lee Sung Ho. Design of Security Architecture for e-business Collaboration.
[2] UML과 Rational Rose 비주얼 모델링 김덕화 역. Wendy Boggs , Michael Boggs 저
[3] Specialist on Information Security- III Application Security
[4]Specialist on Information Security- IIV Information Security
[5] Mark Denning, Kate Hill, Bernard Dodd, Jonathan Lingard, Gray Elkingon, Eric Matthews, Wendy Hewson, Jonathon R. Tate, *using SAP R/3*, QUE 1996, 743~753
[6] Kruchten, P. The 4+1 view of architecture. *IEEE Software* 12(Nov.1995),45-50

[7] JDEdwards, *System Foundation*, JEDdwards Enterprise soft ware, 73~99, 1999
[8] Jung Chang Ho. Conceptual Security Model For by "4+1" Views of UML
[9] 알기 쉬운 ERP Plus, 신철 저
[10] Nam Do Hyeon Implementation of Web Based ERP Securit y Framework