침입감내 시스템의 분류

김기한[0] 조현철 윤영태
한국전자통신연구원 부설 국가보안기술연구소
{ghkim1[0], hccho, ytyun}@etri.re.kr

Classify of Intrusion Tolerant System

GiHan Kim[0], HyenChul Cho, YoungTae Yun
NSRI in ETRI

요 약

현재의 보안활동은 침입방지, 침입탐지 및 패치 제공과 같은 수동적인 보안이 주로 수행된다. 그러나 소프트웨어에서 취약성이 존재하지 않는다는 것을 증명하는 것은 불가능한 일이다. 침입감내 시스템은 수동적인 보안이 아닌 적극적인 보안의 개념으로 침입이 발생하더라도 시스템이 제공하는 서비스를 지속적으로 제공하는 것을 목표로 하고 무결성과 가용성을 강조하는 개념이다. 본 논문에서는 현재 진행 중인 침입감내 시스템에 대한 프로젝트에 대해 알아보고 침입감내 시스템에 대해 계층기반과 복제기반으로 분류를 수행한다. 그리고 계층기반과 복제기반은 프로그램과 데이터의 관점에서 나누어 분류하고 각 4가지 분류에서 고려해야할 기술적 기능적 특징을 알아본다.

1. 서론

침입감내 시스템은 침입이 성공하였다고 하더라도 시스템의 중요 서비스의 지속적인 제공을 목표로, 무결성과 가용성을 강조한다. 즉, 침입감내 시스템은 침입에 저항성을 가지고 결함을 허용하는 시스템의 개념, 설계, 개발, 검증 아키텍처, 방법론에 대한 기술을 개발하는 것이다. 또한 시스템 상위 계층에서 성공한 공격을 탐지하여 중요한 어플리케이션의 올바른 수행을 지속적으로 보장하기 위한 행위를 수행한다. 이러한 행위는 의심스러운 코드의 잠금과 하드웨어의 재설정과 소프트웨어 자원에 대한 잠금을 의미한다.

본 논문에서는 침입감내 시스템을 프로그램과 데이터 관점, 복제기반(replica-based) 침입감내와 계층기반(layered-based) 침입감내 관점에서의 분류를 수행한다. 복제기반 침입감내 시스템과 계층기반 침입감내 시스템의 관점에서 중요한 보호 대상인 프로그램과 데이터를 중심으로 침입감내 시스템을 분류하고 각 분류에서 필요한 기술적인 고려사항을 계층적으로 제시한다.

이러한 기술적 고려사항이 계층적 구조로 제시함으로 인해 다양한 침입감내 메커니즘을 구축하려고 할 때 특정 업무 도메인 환경에 따라 침입감내 메커니즘을 선택적으로 이용할 수 있도록 설계하는데 도움을 줄 수 있다.

본 논문은 2장에서 DARPA에서 진행되어온 침입감내 시스템 관련 연구를 소개하고, 3장에서 복제기반과 계층기반의 침입탐지 시스템을 프로그램과 데이터관점에서 분류하고 각 분류에서 고려해야할 기술적인 요소를 설명하고, 4장에서 결론을 맺는 구성이다.

2. DARPA의 침입감내 프로젝트

DARPA의 IA&S(Information Assurance and Survivability) 프로젝트는 정보전에 대응하기 위한 정보보증 및 생존 기술 개발을 주도하고 있다. 그 주요 내용은 여덟 가지 영역에 걸쳐 전략적 침입평가(Strategic Intrusion Assessment), 침입감내 시스템(Intrusion Tolerant Systems), 결함허용 네트워크(Fault Tolerant Networks), 동적협동(Dynamic Coalitions), 정보 보증(Information Assurance), 정보 보증 과학 및 공학 도구(Information Assurance Science and Engineering Tools), 자율적 정보 보증(Autonomic Information Assurance), 그리고 사이버 지휘 통제(Cyber Command and Control) 기술을 개발하는 것이다[1].

IA&S 프로젝트의 후속 프로젝트인 OASIS 프로젝트[2]는 3세대 보안 메커니즘(3GS:*Generation Security* mechanism)을 제공한다. 1세대 보안 메커니즘은 신뢰 컴퓨팅 환경, 암호화, 인증과 접근제어와 같은 기술이고, 2세대 보안 메커니즘은 경계 제어, 침입탐지 시스템, PKI, 생체인식과 같은 기술이다. 3GS는 1세대와 2세대 메커니즘을 보완하고 저항을 다중 계층 형태로 제공한다. 첫번째 저항 계층은 실시간 실행 모니터 부분으로 보안 정책을 위반하는 코드의 실행을 방지한다. 그러나 만약 그런 코드가 실행된 경우 다음 저항 계층이 에러의 탐지와 전파를 통해 피해를 방지한다. 추가적인 메커니즘으로 에러 상쇄와 피해 복구, 자원의 재설정과 같은 기능을 수행한다. 그리고 이미 성공적으로 구현된 침입감내기술을 결함허용 시스템에 적용하는 범위까지 포함한다.

OASIS는 몇 가지 과정으로 나누어진 프로그램이다. 첫번째 과정은 특정 익스플로이트에 대한 해결을 강조하는 단계이다. 개발된 기술이 충분히 만들어진 후 다음단계로 나아가기 전에 검증을 받는다. 두 번째 단계는 OASIS에서 개발된 여러 기술을 통합하는 단계이다. 추가적으로 DARPA에서 추진되었고 추진 중에 있는 IS(Information Survivability)와 IA&S에서 개발된 결과의 통합에 대한 연구도 수행하고 있다.

DARPA의 OASIS 프로젝트와 관계된 프로젝트로 OASIS DEM/VAL(Integration, Demonstration and Validation) 프로젝트는 이러한 1세대, 2세대 보안 기술과 OASIS 기술의 통합에 대한 연구를 수행하고 있다.

OASIS DEM/VAL 프로젝트는 2002년 8월에 시작하고, 2년안에 필드 테스트 가능한 프로토타입을 개발하여 군 정보시스템에 설치하여 모니터링과 제어 능력을 통합시키는 것을 목표로 한다.

3. 침입감내시스템의 분류

이 장에서는 침입감내 시스템을 침입으로부터 보호해야할 프로그램과 데이터의 관점, 계층 기반과 복제 기반 관점에서 현재 연구 중인 침입감내 시스템에 대해서 분류를 수행한다.

복제기반은 예전부터 연구되어진 결함허용 기술에서 꾸준히 연구되었고 현재도 지속적으로 연구되는 분야이다. 단순한 복제의 증가는 기밀성에 대한 위협을 증가하므로 기존의 복제기반에 보안요소를 포함하는 방향에 대한 모색이 필요하다.

계층기반을 분류의 기준으로 제시하는 이유는 침입에 저항을 가지는 아키텍처는 계층구조로 생각할 수 있다. 또한 모든 상황에 모든 계층을 적용하는 것이 아니라 성능과 기능성, 적용성을 고려를 하여 각 계층을 설정할 수 있기 때문이다.

복제기반과 계층기반을 프로그램과 데이터로 다시 분류하는 이유는 프로그램과 데이터관점에서 필요로 하는 기술적 요구사항이 상이하기 때문에 프로그램과 데이터 관점에서 분류를 수행하고 각 분류에 맞는 기술적 요구사항을 기술한다.

3.1 복제기반 침입감내 시스템 분류

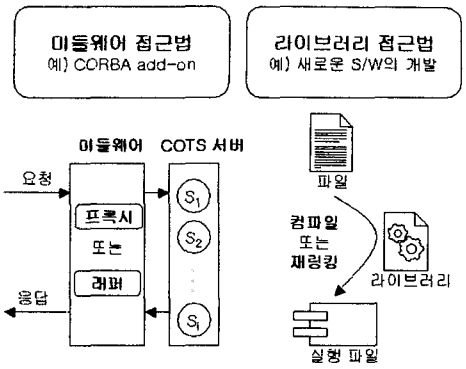
복제기반 침입감내 시스템은 결함허용 기술과 유사하게 분산 컴퓨팅 환경에서 침입이 발생하더라도 지속적인 시스템의 서비스를 제공하기위한 가용성 확대를 위해 접근하고 있는 시스템이다. 이 복제기반 침입감내 시스템은 프로그램과 데이터로 다시 분류할 수 있다.

3.1.1 프로그램을 위한 복제기반 침입감내 시스템

프로그램의 복제는 결함허용을 위한 연구자에게서 로드 밸런싱, 분산 컴퓨팅의 최적화 등으로 많이 연구되었고 보안 연구자에게는 서비스 거부 공격에 저항력 있는 서비스 제공 관점에서 지속적으로 연구되었던 부분이다.

프로그램을 위한 복제기반 침입감내 시스템은 대부분의 분산 컴퓨팅 환경을 지원하는 미들웨어에서 COTS 소프트웨어를 지원하기 위한 미들웨어에 새로운 계층을 포함하는 접근방법과 새로운 소프트웨어 개발에 침입감내 특성을 포함할 수 있는 라이브러리의 개발로 분류할 수 있다. 그러므로 프로그램을 위한 복제기반 침입감내 시스템은 기존의 COTS 소프트웨어에 침입감내 특성을 지원하기위해 미들웨어 차원에서의 래퍼 기술과, 새로운 결함허용 분산 프로그램의 제작을 위한 침입감내 특성을 지원하기 위한 라이브러리에 의한 접근으로 분류할 수 있다.

그림 1에서 프로그램을 위한 복제기반 침입감내 시스템에서 분산 컴퓨팅의 환경의 미들웨어에 대한 레퍼 접근법과 라이브러리 접근법에 대한 구성이 표현되어 있다.



(그림 1) 프로그램을 위한 복제기반 침입감내 시스템

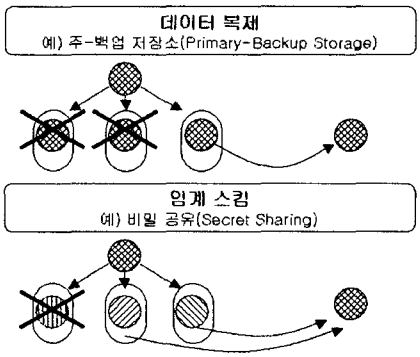
3.1.2 데이터를 위한 복제기반 침입감내 시스템

데이터의 복제는 현재의 데이터베이스나 파일 시스템에서 널리 사용되고 있다. 데이터를 위한 복제기반 침입감내 시스템에서는 기존의 안전한 스토리지 기술에서 사용되는 단순한 주-백업 저장서버의 경우보다 향상된 보안성을 가지기 위해 저장 서버 중 하나를 공격자가 침입하더라도 데이터를 알아내지 못하게 하는 임계 개념(threshold scheme)이 필요하다. 이런 임계 개념은 데이터를 위한 복제기반 침입감내 시스템 뿐만 아니라 프로그램을 위한 복제기반 침입감내 시스템에서도 적용하여 공격자가 하나의 서버에 침입을 성공하더라도 적절한 서비스를 제공받지 못하게 보안성을 향상시킬 수 있다.

본 논문에서는 단순한 결함허용을 위한 데이터 복제와 단순 데이터 복제보다 좀더 보안 관점을 강조할 수 있는 임계 개념을 포함한 데이터 복제로 분류한다.

그림 2에서 데이터에 대한 복제기반 침입감내 시스템을 분류하고 있다. 데이터 복제를 위해서는 단순 복제와 향상된 보안을 지원하는 임계 개념을 포함하는 비밀공유(secret sharing)가 표현되어 있다.

비밀공유의 개념은 중요한 정보를 여러 조각으로 나누어 여러 사람이 관리하여 비밀 정보를 복원하기 위해서는 다수의 정보조각이 모여지지 않으면 비밀정보를 복원할 수 없게 하는 개념이다.



(그림 2) 데이터를 위한 복제기반의 침입감내 시스템

3.2 계층기반 침입감내 시스템 분류

복제기반 침입감내 시스템이 분산 컴퓨팅 환경을 묵시적으로 가지고 있는 것에 비해 계층기반 침입감내 시스템은 호스트 자체 내에서의 프로그램, 데이터에 대한 침입에 대한 대응에 관한 접근법이다.

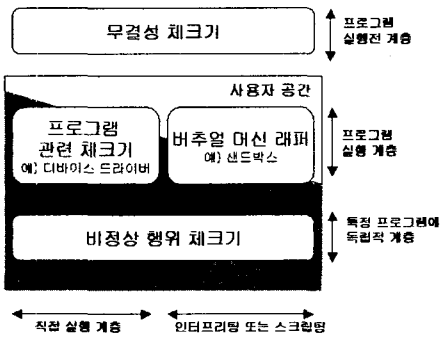
3.2.1 프로그램을 위한 계층기반 침입감내 시스템

계층 기반 침입 감내 시스템에서는 전략적 침입 평가 기술이 강조된다. 왜냐하면 침입의 위협에 따라 계층적으로 대응 방법이 달라지기 때문에 현재 진행중인 침입에 대한 정확한 평가가 필수적이다.

프로그램을 위한 계층기반 침입감내 시스템에서는 세 부분의 계층으로 나누어질 수 있다. 첫 번째 계층은 프로그램의 실행이 이루어지기 전에 실행 파일의 무결성을 체크하는 실행 전처리 부분이고 두 번째 계층은 실제 프로그램이 동작 중인 순간에 적합한 동작을 하는 지와 비정상적인 행위에 대한 중지 및 대응을 담당하는 프로그램 실행 모니터링 계층이고, 세 번째 계층은 특정 프로그램 실행과 관계없이 현재 시스템 상태를 보고 자원의 재할당과 자원에 대한 접근을 제한하는 비정상 행위 탐지 계층이다.

실행 모니터링 계층은 프로그램의 실행시의 침입탐지 기능, 프로그램 실행시의 프로세스 문맥에 대한 파악 기능, 구체적인 프로세스 실행 시 각 침입 상태에 따른 대응을 표현할 수 있는 명세 기능 등이 필요하다. 특히 프로그램 실행에서 프로세스 문맥을 파악하기 위해서는 직접적으로 실행되는 프로그램의 경우 운영체제에서의 시스템 콜을 가로챌 수 있는 기능이 필수적이고, 인터프리터 형태로 실행되는 프로그램을 위해서는 샌드박스를 제공해주는 기능이 필요하다. 시스템 콜을 가로채거나 프로그램 실행에 독립적으로 운영체제의 상태에 따라 자원의 재설정을 위해서는 운영체제 내부에 해당 기능이 포함되어야 한다.

그림 3에 프로그램을 위한 계층기반 침입감내 시스템이 도식화되어 있다. 프로그램을 위한 계층기반 침입감내 시스템은 세로축으로 실행 전처리, 실행 때의 처리, 프로그램과 실행과 관계없이 커널 내부에서의 처리로 나누어지게 된다. 이때 특정 프로그램 실행에 관계된 처리는 가로축으로는 실행 파일이 직접 실행되는 경우와 인터프리터/스크립트로 동작하는 경우로 나누어진다.

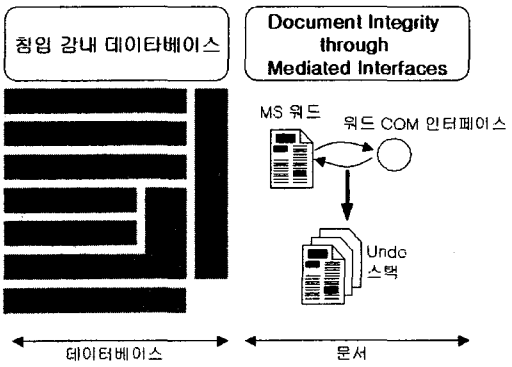


(그림 3) 프로그램을 위한 계층기반의 침입감내 시스템

3.2.2 데이터를 위한 계층기반 침입감내 시스템

데이터를 위한 계층기반 침입감내 시스템은 프로그램을 위한 계층기반 침입감내 시스템에 비해서는 그리 활발하게 진행되고 있지 않지만 데이터베이스에 계층적 침입 감내 기법을 도입하여 악의적인 트랜잭션에 대응할 수 있는 방법에 대한 연구와 문서에서의 무결성을 보장하기 위한 감사 기록을 남기는 연구도 이루어지고 있다.

그림 4에 데이터를 위한 계층기반 침입감내 시스템이 분류되어 있다.



(그림 4) 계층기반의 침입감내 시스템 - 프로그램

4. 결론

프로그램을 위한 복제기반 침입탐지 시스템은 기존 COTS 소프트웨어 보호를 위하여, 침입감내 특성을 래핑한 미들웨어나 침입감내 특성을 포함한 라이브러리의 개발에 초점이 맞추어지고 있다. 데이터를 위한 복제기반 침입탐지 시스템은 기존의 결함허용 기술 연구의 결과인 단순한 주-백업 스토리지 기술 외에 좀더 나은 기밀성을 제공하는 임계 개념을 도입한 스토리지에 대한 기술과 개발이 진행 중이다.

이에 반하여 프로그램을 위한 계층기반 침입탐지 시스템은 가장 연구가 활발히 되고 있으며 프로그램의 실행시에 동적으로 침입 상황에 맞는 대응을 목표로 접근하고 있다. 그리고 일부에서는 데이터을 위한 계층기반 침입감내 시스템에 관한 연구로서 데이터베이스와 문서 파일에 대한 무결성을 강조하는 계층기반에 대한 연구도 이루어지고 있다.

이러한 침입 감내 시스템은 한가지 관점으로는 침입 감내 특성을 모두 제공할 수 없으므로 계층기반과 복제기반 침입감내 시스템의 통합과 복제기반에 필요한 동적 협동 기술과 계층기반에 필요한 전략적 침입 평가기술과의 이들의 유기적인 통합에 대한 연구가 필수적이다.

참 고 문 헌

[1] 박상서, 정보전 대응체계 구축 현황, WISC2000 튜토리얼 자료집, 2000. 9.

[2] DARPA OASIS project home page. http://www.darpa.mil/ipto/research/oasis/