보호 도메인 정보를 이용한 통합 보안 관리 시스템의 침입경보 감소 기법

박용철*, 이성호**, 이형효***, 노봉남**
*전남대학교 정보보호협동과정
**전남대학교 전산학과
***원광대학교 정보·전자상거래학부
e-mail:yoch76@athena.jnu.ac.kr

An Intrusion Alert Reduction Method for an Integrated Security Management System using Protected Domain Information

Yong-Cheol Park*, Seong-Ho Lee**, Hyung-Hyo Lee***, Bong-Nam Noh**
*Interdisciplinary Program of Information Security, Chonnam National Univ.
**Dept. of Computer Science, Chonnam National Univ.
***Division of Information and Electronic Commerce, Wonkwang Univ.

요 약

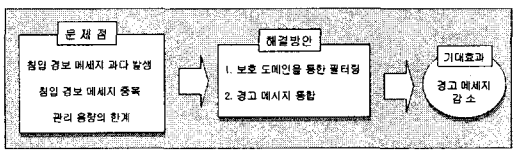
주요 정보통신기반 시설에 대한 분산화되고 지능화되는 침해 행위 및 위협이 급속도록 증가하고 있다. 따라서 여러 보안 제품을 연동하여 해커의 침입 탐지, 차단, 대응 및 역 추적을 위한 통합 보안 관리의 필요성이 대두되고 있다. 그러나 통합 보안 관리의 특성상 다양한 보안 제품에서 전송된 이벤트와 침입 경보의 양이 많아 분석이 어려워 서버에 부담이 되고 있다. 본 연구에서는 이러한 문제를 해결하고자 보호 도메인 정보를 초기에 에이전트에 설정하여 침입경보 중복 발생을 감소시켰다. 도메인 정보를 이용한 침입경보 감소 기법은 개발중인 통합 보안 관리 시스템과 침입경보 연관성 연구를 위해 사용된다.

1. 서론

주요 정보통신기반 시설에 대한 분산화 되고 지능화 되는 침해 행위 및 위협이 급속도록 증가하고 있다[1]. 따라서 여러 보안 제품을 연동하여 해커의 침입 탐지, 차단, 대응 및 역 추적을 위한 통합 보안 관리의 필요성은 대두되고 있다. 통합 관리 제품들은 초창기 단순히 이벤트를 직접받아 모니터링하는 것을 벗어났다. 검색엔진을 추가해 관리자로 하여금 보안 로그를 손쉽게 확인 할 수 있도록 기능이 확장되었다. 특히, 인가 받지 않은 외부 침입자를 실시간으로 탐지, 침입에 대한 즉각적인 대응, 역 추적까지 할 수 있는 보안 통합 개념의 관제 서비스로 발전되고 있다[2].

그러나 다양한 보안 제품을 활용하기 때문에 전송되는 이벤트 및 침입 경보의 양이 많아 분석이 어렵고 서버의 부담이 되고 있다.

본 연구에서는 이러한 문제를 해결하고자 보호 도메인 정보와 시간정보에 의한 침입경보 축약기법을 적용해 중복 메시지가 발생하지 않도록 해결하였다. 전송되는 메시지 규격은 IDWG(Intrusion Detection Working Group)에서 제안한 IDMEF(Intrusion Detection Message Exchange Format) XML(Extensible Markup Language)을 사용한다. 이는 국제 표준이 유력한 요구사항, 공통 언어, 통신 프로토콜을 따르고자 함이다[3].



[그림 1] 통합 관리 시스템의 문제점 및 해결방안

본 논문의 구성은 다음과 같다. 2장은 관련연구로 침입경보 메시지 축약을 위한 세 가지 기법에 대해 설명한다. 3장은 제시하고자 하는 내용으로 보호 도메인 정보를 이용한 침입경보 감소기법과 과정에 대해 기술한다. 4장은 구현 및 실험, 마지막으로 본문 내용을 요약하고 향후 연구방향에 대해 기술한다.

본 연구는 대학 IT 연구센터 육성/지원사업의 연구결과로 수행되었음.

2. 관련연구

경고메시지 축약에 대한 기존 연구는 침입 탐지 시스템간 경고메시지 통합이 대부분이며, 대표적인 방법으론 확률론적 방법, ACC(Aggregation and Correlation Component) 및 CRIM 모듈등이 있다.

2.1 확률론적 침입경보 통합방법

침입경보 메시지 간 유사성을 평가하여 이들을 하나로 묶는다. 침입탐지에 의해 생성된 침입경보는 표준화된 기준에 따라 재 분류되며 이를 확률적인 방법으로 통합한다[4]. 통합 방법으로는 새로운 침입경보 발생시 이전의 침입경보들간 유사성을 평가 근접되는 그룹과 통합을 이루는 방법과, 일치하는 침입경보가 없을 경우엔 새로운 그룹을 생성하는 방법을 사용한다. 확률적인 방법에 의한 경고메시지 통합공식은 그림 2와 같다.

이 방법은 유사성을 평가하기 위한 환경변수를 정의하기가 어렵고, 경고메시지간 인과관계를 찾아내기가 어렵다.

$$SIM(X,Y) = \frac{\sum_j E_j SIM(X_j, Y_j)}{\sum_j E_j}$$

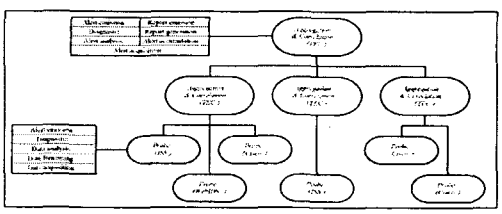
X = Candidate meta alert for matching
Y = New alert
j = Index over the alert features
E_j = Expectation of similarity for feature j
X_j, Y_j = Values for feature j in alerts X and Y, respectively (may be list valued)

[그림 2] 확률론적 침입경보 메시지 통합 공식

2.2 ACC(Alert Correlation Component)

침입 경보 메시지의 전후 동일성 및 순서, 상황별 유사성을 가지는 경우로 나누어 통합을 수행한다. 계층화된 분산 구조를 지원하며 모든 침입경보 메시지를 표준화된 IDMEF의 형태로 맞추어 통합한다[5].

이 방법은 미리 정의된 상황에 들지 않는 유사한 침입경보 메시지들에 대해 그룹화가 어렵다. 또한 순서가 고정되어 있고, 연관된 모든 침입경보 통합을 제공하기 위한 선행 정보가 충분하지 않다.

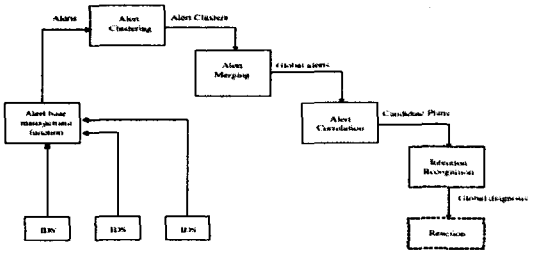


[그림 3] ACC 시스템 구조

2.3 CRIM 모듈

CRIM 모듈[6,7]은 MIRADOR 프로젝트 내에서 개발된 IDS 협동(cooperation) 모듈이다. MIRADOR 프로젝트는 협동적이고 적응적인 IDS 플랫폼을 구축하기 위하여 French Defense Agency에 의하여 시작됐다. CRIM 모듈의 구성은 그림 4와 같다. 수집된 침입경보은 전처리 과정을 거친 후 연관성 분석을 시도한다. 전처리 과정은 클러스터링과 통합 과정으로 이루어지는데, 여러 IDS에서 생성한 침입경보들을 전송받아 분석을 위해 데이터베이스에 저장한다. 침입경보의 전송형태로는 IDMEF를 사용하며, 데이터베이스는 프롤로그를 이용하였다. 시스템이 초기화되었을 때는 삽입되는 튜플의 수가 많지만, 시스템이 진행됨에 따라 그 수는 낮아지게 되며 시스템의 성능에 큰 영향을 주지 않는다.

침입경보 연관성 검사에 대한 접근방법은 LAMBDA로 명세된 공격에 기반하고 있다. 공격은 LAMBDA에서 Attack Pre-condition, Attack Post-condition, Attack scenario, Detection scenario, Verification scenario의 5개 필드로 구성되어 있다.

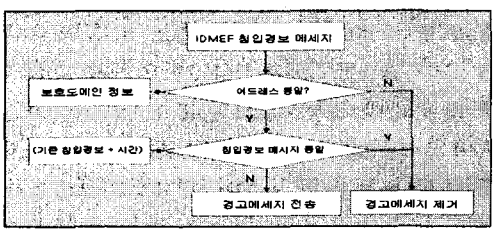


[그림 4] CRIM 모듈의 구성

3. 침입 경보 감소 기법

통합 보안 관리를 하기 위한 시스템의 한계점은 다양한 보안 시스템의 연동에 따른 침입경보 메시지 과다 발생과 중복이다. 예를 들면, 공격형태가 복잡해짐에 따라 하나의 공격이라도 한개 이상의 침입경보 메시지를 발생시키고, 세부화된 네트워크 구성에 의해 침입경보가 중복되게 나타날 수 있다.

기존의 축약 기법은 축약을 담당하는 모듈이 통합 관리시스템 내에 존재하여 과다한 침입경보 발생시 성능저하와 연관성 검사 수행의 어려움이 있었다.



[그림 5] 침입경보 감소 기법 적용 알고리즘

본 연구에서는 에이전트에 보호 도메인 정보(Protected

Domain Information)와 시간정보에 의한 침입경보 축약 기법을 적용해 문제를 해결하였다.

3.1 보호 도메인 정보를 이용한 침입경보 감소기법

보호 도메인 정보란 외부 또는 내부의 네트워크 자산 가치를 기준으로 보호 되어야할 도메인 정보를 일컫는다. '99 DARPA 침입탐지 평가 데이터 셋을 기준으로 정의한 보호 도메인 정보는 표 1과 같으며, 보호 도메인 정보는 서브넷 내의 보호할 IP 또는 보호할 도메인 명으로 구성된다.

침입경보의 내용이 보호 도메인 내의 자원이 아니라면 에이전트 시스템은 새로운 침입경보를 제거한다. 이는 경보 메시지가 보호 시스템 내의 경보로 감소되는 것과 서로 다른 이종의 시스템으로부터 오는 경보 메시지가 독립적이게 한다.

본 연구에서는 에이전트 시스템에 표 1의 보호 도메인 정보를 삽입해 침입경보를 감소하였다.

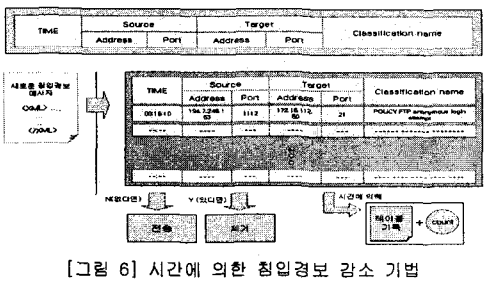
<표 1> Simulation Network 99에서의 보호 도메인 정보

NO	호스트명	호스트 주소
1	pascal	172.16.112.50
2	zeno	172.16.113.50
3	marx	172.16.114.50
4	hume	172.16.112.100
5	kant	172.16.112.110

3.2 시간에 의한 침입경보 감소 기법

시스템의 취약성을 탐침하기 위한 스캔 공격의 경우 일정 시간동안 침입 정보를 유지함으로써 침입경보의 축약이 가능하다. 이 밖에 DoS나 DDoS 공격의 경우도 근원지나 목적지 주소정보를 토대로 침입경보의 축약이 가능하다.

본 연구에서는 침입경보 정보를 에이전트 시스템에 유지하기 위해 그림 6과 같은 테이블 구조를 만들었다. 이 테이블은 큐를 이용해 시간에 의해 정보가 삭제되도록 구현되었으며 침입경보를 삭제후에도 정보 유지를 위해 카운터 정보와 함께 파일로 기록된다.



[그림 6] 시간에 의한 침입경보 감소 기법

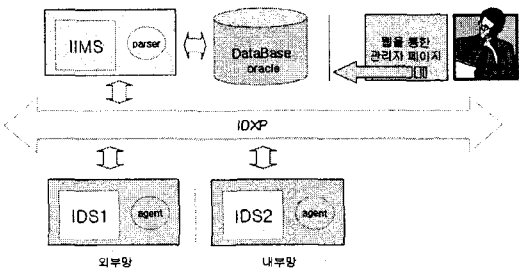
4. 구현 및 실험

침입탐지 시스템 테스트를 위해 널리 사용되고 있는 '99 DARPA 데이터를 실험 데이터로 사용한다. 본 데이터는 '99 DARPA Intrusion Detection Evaluation Program에 의해 표준 데이터 집합을 얻기 위하여 미국 군사 네트웍(military network) 상에서 시뮬레이션을 통해 만들어진 데이터이다.

사용되어질 패킷은 외부망에 대한 tcpdump파일과 내부망에 대한 tcpdump파일이다. 실험을 위해 같은 IDS에 외부망과 내부망에 대한 패킷을 읽어들어 침입경보를 생성하도록 하였다.

4.1 구현

전체 동작과정은 다음과 같다. 먼저, 단위 IDS가 생성한 침입정보를 표준화된 IDMEF 형태로 변환해 에이전트 시스템에 전달한다. 에이전트는 생성된 침입경보 메시지가 보호도메인 내의 정보인가를 판단한뒤 신뢰경로 IDXP 채널을 통해 안전하게 서버측으로 전달한다. 마지막으로, 통합 관리자는 전송받은 침입정보 메시지를 파싱하여 DB에 저장한다. 전체 시스템 구성도는 그림 7과 같다.



[그림 7] 전체 시스템 구성도

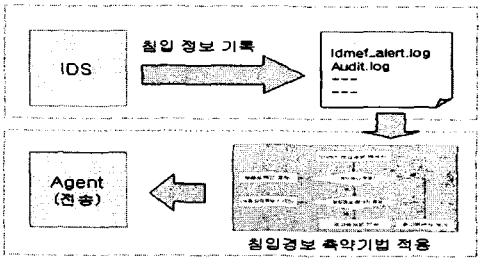
가. 침입경보 감소를 위한 전송 에어전트

단위 IDS에서 탐지된 침입경보는 침입경보 축약 기법에 의해 축약되고 서버측으로 암호화 되어 전달된다. 이때 침입경보는 커널기반 메시지 큐를 사용해 내부에서 IDS와 에이전트간 정보 교환이 이룬다. 암호화는 RoadRunner 라이브러리에서 제공하는 암호화 프로파일인 RRTLS를 사용한다. 그림 8은 클라이언트 측의 침입경보 메시지 전달 과정이다.

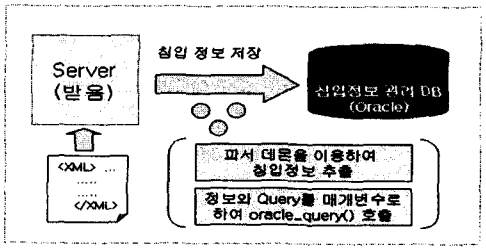
나. 침입경보 저장

침입경보 저장을 위한 서버는 암호화된 IDMEF 형태의 침입경보 메시지를 복호화해 의미 있는 정보단위로 파싱한다. 이 의미 있는 정보는 커널기반 메시지

큐를 이용해 침입경보 저장 모듈에 전달되며, 적절한 질의어와 침입정보 매개변수를 이용해 DB인 Oracle에 저장된다. 그림 9는 침입정보 통합 관리자 내에서 침입정보를 저장하는 과정이다.



[그림 8] 침입경보 축약 메시지 전달과정



[그림 9] 침입경보 저장 과정

4.2 실험

'99 DARPA 데이터 셋을 통하여 IDS를 외부망의 IDS1, 내부망의 IDS2를 구분하여 실험을 진행하였다. 첫 번째로 IDS1과 IDS2에 별도의 보호 도메인 정보를 두지 않은 상태에서 패킷을 생성시켜 침입경보를 발생시킨다. 두 번째로 보호 도메인 정보를 초기화한 상태에서 패킷을 생성시킨다. 마지막으로 시간정보에 의한 침입경보 감소 기법을 적용한 후 패킷을 생성시킨다.

가. 보호 도메인 정보를 통한 침입경보 감소 기법 적용

Simulation Network 99 데이타를 기준으로 내부망과 외부망 tcpdump 파일을 사용해 침입경보를 발생시킨 결과 320,287건이었다. 이 중 보호 도메인 정보를 적용해 침입경보를 제거한 결과 침입경보가 185,362건으로 42% 감소하였다. 아래의 표 2는 침입경보 발생건수이다.

<표 2> 침입경보 발생 건수

침입경보 통합	보호 도메인 정보 적용	비 고
320,287	185,362	42% (감소)

나. 시간정보에 의한 침입경보 감소 기법 적용

테이블 유지 설정 시간은 1분이며 테이블이 다 채워질 경우엔 순서대로 비워진다. 침입경보 유지 테이블의 내용 중 침입경보명이 "POLICY FTP anonymous login attempt"의 경우, 기법 적용 전 침입경보 1,272건이었으나, 기법 적용후 860건으로 32% 감소하였다.

<표 3> 시간정보에 의한 침입경보 감소율

NO	Target address	통합 전 Alert 수	통합 후 Alert 수	감소비율
1	172.16.112.50	14	8	43%
2	172.16.113.50	0	0	-
3	172.16.114.50	5	3	40%
4	172.16.112.100	1,253	849	32%
5	172.16.112.110	0	0	-
합계		1,272	860	32%

5. 결론 및 향후 연구방향

본 논문에서는 통합 보안 관리로 인해 일어날 수 있는 침입경보 과다발생과 중복 메시지 발생에 대한 해법으로 보호 도메인 정보를 이용한 메시지 축약 기법을 제안하였다. 테스트 환경은 '99 DARPA 침입탐지 평가 데이터 셋을 이용해 침입경보 메시지를 통합, 적용, 분석해 보았다. 실험결과 침입경보가 첫 번째 기법 적용시 43%, 두 번째 기법 적용시 32% 감소효과를 얻었다.

향후에는 보호 도메인 정보와 시간에 의한 침입경보 통합에 나타난 문제점을 보완하고, 수집된 침입정보에 대한 연관성 분석을 통해 침입 탐지율을 개선하고자 한다.

참고문헌

[1] 2002년 해킹·바이러스 통계 분석, 정보통신부, Jan. 2003

[2] 이영석, 나중찬, 손승원, ESM 개발 동향: 이기종 보안 시스템 연동을 중심으로, 한국전자통신연구원, May. 2003

[3] 이성호, 박용철, 이형효, 노봉남, 침입정보 통합관리시스템을 위한 테스트베드 구축, 한국정보처리학회, May. 2003

[4] A. Valdes and K. Skinner. Probabilistic alert correlation. In Proc. of the 4th Int'l Symposium on Recent Advances in Intrusion Detection (RAID 2001), pages 54--68, 2001.

[5] H. Debar and A. Wespi. Aggregation and correlation of intrusion-detection alerts. In Recent Advances in Intrusion Detection, number 2212 in Lecture Notes in Computer Science, pages 85 -- 103, 2001.

[6] F. Cuppens, "Managing Alerts in a Multi-Intrusion Detection Environment", In Proc. of Annual Computer Security Applications Conference (ACSAC 2001), Dec. 10-14, 2001, New Orleans, Louisiana

[7] F. Cuppens, A. Miege, "Alert Correlation in a Cooperative Intrusion Detection Framework," In Proc. of the 2002 IEEE Symposium on Security and Privacy, May 2002