보안경보 검증을 확장한 다단계 상호연관 분석에 관한 연구

최대수*, 이용균*
*이글루시큐리티 인터넷보안연구소
e-mail : {dschoi,spider}@igloosec.com

A Study on Multi-Level Correlation Technique extended Security Alert Verification

Dae-Soo Choi*, Yong-Kyun Lee*
*Internet Security Lab., IGLOO Security

요 약

보안위협은 갈수록 심각해지고 다양한 정보보호시스템들을 통합하는 통합보안관리시스템에 관한 연구 개발도 활발히 진행 중이다. 이기종 정보보호시스템에서 발생하는 다량의 경보와 이벤트를 효과적으로 수집, 통합하고 상호연관 분석할 수 있는 방법이 절실하다. 현재 연구되고 있는 상호연관분석 방법들에 대해서 조사 분류하고 각 분류별로 장단점을 분석하여 이기종 통합보안관리에 적합한 상호연관분석 방법을 제안한다. 보안 경보 검증과정과 분산화된 경보처리방법으로 실시간 상호연관분석이 가능하도록 설계하였다.

1. 서론

갈수록 심각해지는 보안위협에 대응하기 위하여 정부, 기업 및 학교에서는 다양한 정보보호제품을 도입하고 운영한다. 특히 침입탐지시스템(Intrusion Detection System) 은 대부분 도입하고 있으며 침입을 감시하고 침입경보가 발생하면 대응한다. 침입을 탐지하기 위한 설정에 따라 다량의 경보가 발생될 수 있으며 현재 침입탐지시스템은 많은 오탐(false alarm)경보를 발생시킨다. 보안관리자는 오탐 경보에 대응을 하게 된다. 그 외 다른 정보보호제품들도 마찬가지로 다양한 경보들을 발생시키고 보안관리자는 대응을 한다.

다양한 이기종 정보보호시스템을 운영하고 효과적으로 통합관리하기 위하여 통합보안관리시스템(ESM:Enterprise Security Management)을 운영한다.

현재 연구 개발되어 있는 대부분의 통합보안관리시스템은 동종 혹은 이기종의 정보보호시스템 이벤트와 경보를 수집하고 필터링하고 리포팅 해주는 기능과 사후 이벤트 상호연관분석기능으로 되어 있다. 그래서 오탐 경보가 발생되면 통합보안관리시스템에서는 오탐 경보 상호연관분석을 하게 된다.

그래서 개별 이기종 단위보안제품에서 발생되는 수많은 이벤트와 경보들을 효과적으로 분석, 침입을 추론할 수 있는 기술이 요구되고 있다.

본 논문에서는 지금까지의 상호연관분석 방법에 관한 연구를 조사하고 분류한다. 그리고 경보검증에 관한 연구를 조사한다. 통합보안관리시스템에서 이기종 정보보호시스템의 이벤트를 효과적으로 실시간 상호연관분석하여 침입을 추론하기 위한 다단계 구조의 상호연관분석 방법에 관하여 제안한다.

2. 상호연관분석 방법론

지금까지 연구되어온 침입탐지시스템 상호연관분석 방법들을 조사하고 분류하였다. 상호연관분석은 분류기준에 따라 다양해 질 수 있는데 본 논문에서는 분석하는 모듈구조, 기능 등을 기준으로 종합하여 분류하였고 최근 업계의 분류방법에 대해서도 조사하였다.

2.1 경보 클러스터링 방법(Alert Clustering) [1][2]

첫번째 분류로 SRI International 의 Valdes 는 경보간의 연계성(probabilism) 에 비중을 두고 유사한 경보들을 그룹화하는 방법을 사용하였다. 하나의 경보 쓰레

드는 하나의 공격과 연관되는 경보들의 그룹이다. 새로운 공격을 탐지했을 때 경보들을 비교하여 유사그룹이 있으면 해당그룹에 포함시키고 그렇지 않으면 새로운 경보 쓰레드를 생성한다. 이때 유사도(Similarity) 를 평가하는 방법은 두 경보간의 특징(feature)을 비교하는 것이다. 예를 들면 두 공격간 공격자 ip, 공격대상 ip, 공격대상 포트, 공격클래스, 시간 등을 비교한다.

Valdes 가 사용한 개념은 메타경보(Meta-alert)와 경보템플릿(Alert Template) 을 정의하여 사용하였다. 메타경보는 다양한 경보를 쓰레드별로 분류하기 위한 분류 경보이고 경보템플릿은 경보를 처리하기 위한 통합 정규화 형태이다. 침입을 추론하기 위한 경보융합(Alert fusion) 방법은 특징의 일치, 특징의 유사도, 최소한의 유사도등의 개념를 이용한다. 그리고 자체적으로 공격분류 클래스를 가지고 분류한 유사도 matrix 를 이용한다. 그리고 각각 다른 상황마다 다른 특징들을 이용하기 위해서 유사도의 특징에 다른 가중치를 부여하도록 한다.

현재 통합보안관리시스템과 비교해보면 메타경보 즉 시나리오에 기반한 방법과 유사하다. 그러나 이 개념은 다양한 환경과 상황에 따라 유사도 기대치와 가중치를 다르게 부여해야 하는데 방법이 현실적으로 어렵고 하나의 메타경보에 대해서도 상태별로 여러 쓰레드가 처리하게 되기 때문에 실제 구현시 한계가 있다. 많은 비교와 클러스터링이 필요하기 때문에 실시간 처리에도 부적합하다.

2.2 공격시나리오 비교방법[4][5]

두 번째 분류는 '사전에 정의한 공격시나리오에 적합한가' 로 분류하는 방법이다. Debar 와 Wespi 는 IBM Tivoli Enterprise Console(TEC) 에 구현된 방법으로 ACC (Aggregation and Correlation Component) 의 개념을 소개한다. 여러 IDS 센서에 해당되는 Probe 에서 경보를 보내면 ACC 모듈 에서 유사한 경보들을 모으고 분석한다. 기본 개념은 유사공격동향을 집합화하는 것이고 속성이 연관된 경보들을 묶어 Security Level 을 평가하고 추론한다. 경보를 집합화할 때 공격자 ip, 공격대상 ip, 공격클래스 3 가지 속성을 기준으로 하며 다음과 같은 시나리오를 이용할 수 있다.

(시나리오 1) 한 공격자가 한 공격대상을 공격할 때 (같은 공격자 ip, 공격대상 ip, 공격클래스) 항목이 동일하다.

(시나리오 2) 한 공격자가 한 공격대상을 여러 방법으로 공격할 때 (같은 공격자 ip, 공격대상 ip) 항목이 동일하다.

(시나리오 3) 한 공격대상에 분산된 공격할 때 (같은 공격대상 ip, 공격클래스) 항목이 동일하다.

(시나리오 4) 한 공격자가 여러공격대상에 같은 공격을 할 때 (같은 공격자 ip, 공격클래스) 항목이 동일하다.

일련의 경보들은 시간대별로 제약조건을 가지고 연관되어진다. 통합보안관리시스템에서 룰기반의 방법과 유사하다. 분석 구조에서는 다단계의 계층적 구조로 볼 수 있다. 제약된 시나리오별 침입탐지를 추론할 수 있다.

2.3 선행조건과 결과조건비교방법[6]

세번째 분류는 경보가 발생하기 위해 필요한 조건(Prerequisites)과 공격으로 인해 발생 가능한 결과(Consequences)를 선행관계(Prepare-For)로 연결하는 방법이다. 단지 AND 와 OR 형태의 논리식으로 표현될 수 있다. 상호연관 분석 그래프를 이용하여 선행조건과 결과를 표현할 수도 있다.

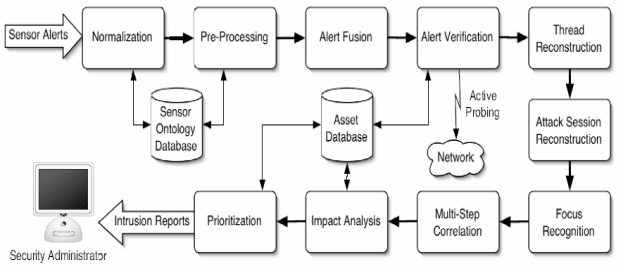
이 분류는 조건별로 제약을 주어 단순화 시켜야 한다. 그렇지 않으면 선행조건에 따라서 결과가 방대해질 수 있고 이 방대한 결과들을 모두 표현하기 위해서는 현실적으로 구현이 어려워진다.

이 분류은 선행관계에 따라 결과가 달라지기 때문에 이기종정보보호 시스템간의 시간동기화가 필수적이다.

2.4 포괄적인 구조 [7]

네 번째 분류로 Valeur 는 다양한 경보분석 구조들을 모두 통합한 포괄적인 구조를 제안하였다. 경보를 연관시키는 방법은 동일 시간대에 발생하고 여러 센서에서 발생한 유사 속성이 있는 경보들을 분류하여 융합하는 방법이다.

(그림 1)은 통합된 상호연관분석 프로세스를 표현한 것이다. 센서에서 발생한 경보는 정규화되고 경보 속성별로 분류하게 된다. 그리고 시간,공간적인 요소를 기준으로 융합과정을 거친다. 그리고 경보검증과정으로 공격의 성공여부를 판단한다. Thread reconstruction 은 동일 공격자가 동일 공격 대상에 공격하는 경보를 연관시킨다. Attack session reconstruction 은 네트웍 기반 경보와 호스트기반 경보를 연관시킨다. Focus recognition 는 실재 공격의 공격지와 공격대상 호스트를 식별한다. Multi-step correlation 에서 공격패턴을 식별하고 마지막으로 Impact Analysis 은 탐지된 공격의 영향을 평가한다.



(그림 1) Valeur 가 제안한 상호연관분석 프로세스

모든 상호연관분석 방법들을 통합하다 보니 너무 많은 단계를 갖게 되고 복잡해진 경향이 있다. 지금까지 제안된 여러 방법론들을 컴포넌트로 구성하여 결합시켰고 각 컴포넌트별로 탐지하게 하였다. 구현시 많은 오버헤드가 발생할 수 있고 실시간 분석은 어려워질 수 있다. 그리고 모든 분석이 통합서버에서 구현

되기 때문에 부하는 증가하게 된다.

2.5 통합보안관리 상호연관분석 방법론

이글루시큐리티[9]에서는 상호연관분석방법을 분석 시점에 따라 실시간 상호연관분석 방법과 배치 상호연관분석 방법으로 구분하였다. 그리고 분석할 수 있는 센서 종류에 따라서 다음과 같이 구분하였다. 동기종 정보보호제품 기준으로 분석할 때 Single Level 상호연관분석 방법, 이기종 정보보호제품을 분석할 때는 Multi Level 상호연관분석 방법으로 분류하여 연구 개발하였다. (그림 2) 는 이기종 정보보호시스템에서 수집된 데이터를 상호연관분석 요소들을 구분한 것이다.

Common Factors Source IP, Dest IP, Port, Protocol	IDS	Type	Category	Priority	Signature	
		Information Gathering, Intrusion Attack, Denial of Service, Others	Vulnerability Probing, Access Attempts, Etc.	High, Medium, Low Information	Signature Lists	
	Firewall	Action	Accept, Drop, Close, NAT, Proxy, Exchange, Encrypt, Decrypt, Error, Warning, Information			
Causation Factors Date, IP, Duration, Scenerios, Impact	Access Control	Status	Invalid Password, Access Denied, Account, Disable Account, Update Fail, Logout, Start/Shutdown, Permit, Update Success, Trace, Sexuid Changed, Insufficient Auth			
	System Event	Log-on / off	User Right Change	FTP	System	Application
		Success, Fail, Logout	User->User, User->Root	Conn, Discon	Error, Warning, Information	
	System Resources	CPU	Memory	DISK	Process	Network(Inbound)	Network(Outbound)	Total Bandwidth	Session
		Threshold, Duration, Count							
	Web Server	Status	Bad Request, Unauthorized, Not Found, Forbidden, URI too Long, Internal Server Error, Others			
Statistical Factors Data, Time, Duration	Anti-Virus	Status	Clean files only, Clean/treated files only, Keep infected files, Delete infected files, Remedless Virus			
		Virus List	Virus Name Lists			
	File Integrity	Status	Create, Delete, Update			

(그림 2) 통합보안관리 상호연관분석 구성요소

3. 침입탐지시스템 경보검증(Alert Verification) [8]

침입탐지시스템에서는 설정에 따라 많은 경보를 발생시킨다. 발생한 경보들은 올바른 경보도 있지만 오탐경보도 많이 발생한다. 공격이 아닌데 공격으로 오판하는 False positives 와 성공하지 못한 공격 (non-relevant positives)이 있다. 침입탐지시스템을 튜닝하고 환경설정을 알맞게 해서 False positive 를 줄인다고 해도 정확한 경보와 오탐경보 사이의 오차가 있다.

이러한 문제 때문에 Kuregel 은 침입탐지시스템에서 경보 검증 방법을 연구하였다. Snort 개발자 Marty Roesch 는 경보의 False-positive 를 감소하기 위해 RNA(Real-time Network Awareness)를 이용한 적이 있다. 하지만 이 정보만으로는 많이 부족하다.

Kuregel 은 경보를 3 가지 타입으로 구분하였다.

(Type 1) True Positive : 센서가 올바르게 성공한 공격으로 구분한 경우

(Type 2) Non-Relevant Positive: 센서가 올바르게 공격으로 구분했지만, 공격이 실패한 경우

(Type 3) False Positive : 센서가 잘못 공격으로 구분한경우

경보검증의 핵심은 3 가지 타입중 성공과 실패를 구분하는 것이고 경보검증은 성공한 경보를 검증하는 프로세스로 정의할 수 있다. 이 때 검증을 하기 위해서는 부가적인 정보가 필요하다.

예를 들면 공격대상시스템에 Code Red 웜이 발생하였다. 이때 Code Red 는 Microsoft IIS Server 에 대해서 동작한다. 공격대상시스템이 Linux 인지, MS-Windows 인지 OS 정보와 IIS Server 동작유무정보와 패치정보가 필요하다. 이러한 정보를 이용해서 경보가 성공했는지 실패했는지 구분할 수 있다. 침입탐지시스템에서 발생한 경보 검증과정을 수행하기 위해서는 공격대상시스템에 대한 정보를 이용하여 판단할 수 있다.

첫째, OS, 실행중인 서비스, 서비스별 버전, 패치버전 등의 환경정보를 비교하는 것 이다. 해당 시스템이 특정공격에 대한 취약점이 없다면 경보는 실패로 기록된다. 둘째, 피해시스템에 공격결과로 발생될 수 있는 정보를 추적해서 경보의 성공/실패여부를 판단한다. 공격에 사용되는 임시파일이나 특정 네트웍 연결 정보 등을 추적한다.

경보 검증 메커니즘은 경보검증정보를 얻는 시점에 따라 2 가지로 구분할 수 있다. 첫째 Active 검증 메커니즘은 경보발생 후 환경정보와 포렌식 추적을 하는 방법이다. 둘째 Passive 검증 메커니즘은 스케줄에 의해 경보발생 전 수집된 정보를 이용한다.

경보검증절차에서 가장 중요한 것은 정확성 (accuracy) 이다. 수집된 데이터의 품질과 시간 그리고 검증프로세스의 비용이 검증절차에서 정확성을 높이는 요소이다.

Passive 방법은 공격발생 후, 이전에 수집된 정보를 이용해서 검증과정을 거치기 때문에 성능관련 추가 비용이 없다. 대신 공격 후 발생한 정보와 달라서 정확성에서 떨어질 수 있다. 그리고 수집되는 정보에도 제한이 있다.

Active 방법은 공격발생 후 취약점 스캐너를 이용해서 정보를 수집하고 netstat, ps, lsof 등의 정보등으로 많은 데이터를 수집할 수 있다. 하지만 많은 비용이 들어 서비스에 이상을 줄 수 있다. 리소스사용 즉 비용과 정확성 사이의 절충(trade-off)이 필요하다.

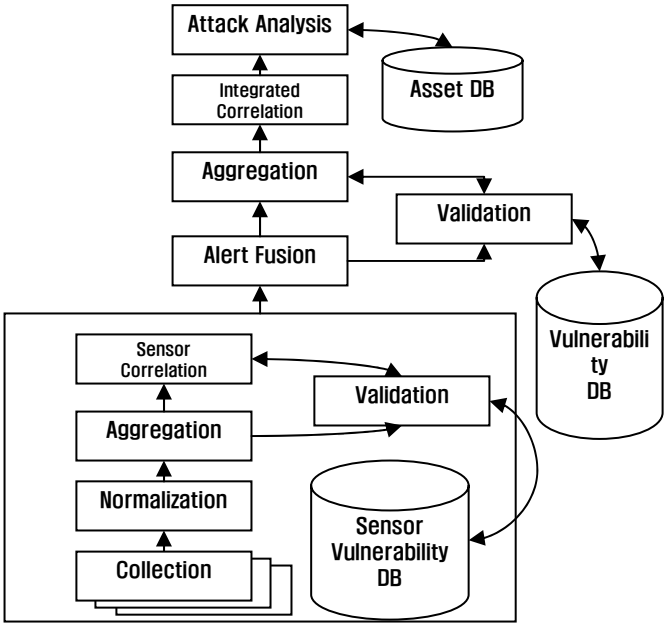
Kuregel 은 Snort 에서 경보검증을 실험하였다. 실험데이타 99.64%의 False Positives 를 0%로 줄여서 경보검증의 필요성을 증명하였다. Kuregel 은 경보의 상호연관분석에서 입력으로 사용되는 경보가 전체 상호연관분석시스템의 품질을 결정한다고 주장한다. 실패한 경보가 입력으로 주어진 상호연관분석 시스템은 연관경보들을 집합(aggregation)하고 전체 탐지 시나리오에 따라 분석하면 결과적으로 연관성이 없는 잘못된 결과를 탐지할 수 있다는 것이다. 오탐 경보를 사전에 감소시킨다면 결과적으로 우수한 상호연관분석 결과를 기대할 수 있다.

4. 다단계 상호연관분석 시스템 제안

대부분의 통합보안관리 시스템에서는 경보검증과정 없이 단위보안제품의 결과에 의해 상호연관분석을 처리한다. 상호연관분석에서 Kuregel 이 분류한 3 가지 경보타입 중 Non-Relevant Positive 와 False Positive 를 감소시킬수 있다면 정확한 연관분석결과를 도출할 수 있다. 또한 Valeur 가 제안한 포괄적인 상호연관 분석

구조를 분산화시켜 운영한다면 처리성능도 향상 시킬 수 있다.

본 논문에서는 통합보안관리시스템의 분산화된 다단계 상호연관분석 모듈을 제안한다. 제안한 구조는 보다 정확한 결과를 도출할 수 있고 실시간으로 처리 가능하도록 처리는 분산화 시켰다.



(그림 3) 다단계 상호연관분석 구조

4.1 센서 상호연관분석

(그림 3)에서 아래 네모 상자가 센서에서 동작하는 상호연관분석 모듈이다. 통합보안관리시스템은 각 단위정보보호시스템에 이벤트 및 경보를 수집하기 위해 에이전트를 설치하거나 그 외 여러가지 방법으로 데이터를 수집하는데 이 부분이 센서가 되고 데이터 수집과 동시에 경보검증과정을 수행하고 일차적인 센서 상호연관분석 동작을 한다. 서버에서 모든 데이타를 통합해서 상호연관분석할 때의 부하를 줄 일수 있다. 일차적으로 검증된 경보만 필터링되어 서버에서 통합되어지기 때문에 본 구조가 실시간 처리가 적합하다.

수집모듈은 각 단위시스템에서 수집 가능한 다양한 정보들이 된다. 이 정보들을 처리 가능한 형태로 바꾸는 정규화 과정이 있고 경보조건에 알맞은 데이터를 찾기 위해 개별 데이터 별로 비교 분석한다. 그리고 단위시스템에서 분석된 개별 경보 및 이벤트들을 일차적으로 상호연관분석 한다. 이 시점에서 발생된 경보를 검증하게 된다. 이때 경보검증은 단위시스템 취약점 DB 를 참조하게 되는데 취약점은 Active 와 Passive 방법으로 나누어 수집할 수 있다. 제안한 방법에서도 처리 비용과 결과의 정확성 사이에 절충과정이 필요하다. 이러한 과정 후 검증된 경보들만 서버로 통합하게 된다.

4.2 서버통합 상호연관분석

(그림 3)에서 윗부분이 서버의 처리과정이다. 센서들의 경보들을 모두 받아서 융합(Alert Fusion)하게 된다. 그리고 전체 상호연관분석 경보조건에 맞도록 경보들을 분류하고 집합시킨다. 이때 융합하고 경보별로 나누는 시점에 경보검증과정을 수행한다. 센서에서 경보검증이 호스트기반경보 검증이었다면 이 때의 경보검증은 네트웍기반 경보검증으로 분류할 수 있다. 이 시점에도 마찬가지로 Active 와 Passive 방법의 절충과정이 필요하다. 모든 경보검증을 거친 후 통합 상호연관분석을 하게 되고 공격에 대한 영향을 분석하게 된다. 이때 영향분석은 자산별로 위험도를 산정할 수 있다.

5. 결론 및 향후연구방향

현재 통합보안관리시스템에서 상호연관분석방법은 단위보안제품에서 발생한 경보들을 모두 수집하고 통합해서 분석한다. 이때 경보분석과정이 없기 때문에 오탐경보와 성공하지 못한 경보들 모두 연관분석하게 된다. 또한 모든 경보를 통합서버에서 처리하기 때문에 처리과정에서 많은 부하가 있다.

본 논문에서는 센서레벨에서 일단계 경보처리를 하고 경보 검증과정을 거친다. 통합서버에서는 센서레벨에서 검증된 경보만을 통합하여 처리하고 다시 경보검증과정을 수행한다.

통합처리구조를 다단계로 나누었기 때문에 부하를 분산시킬수 있어서 실시간 상호연관분석 및 침입추론에 적합하다. 또한 단계별로 경보검증과정을 수행하기 때문에 상호연관분석결과의 정확도가 높아진다.

향후 연구방향으로는 구현시 어느 정도의 성능과 처리정확도를 보장할 수 있는지 증명이 필요하고 실제 운영시 경보양에 따라 달라질 수 있는 동적 처리 방법연구도 필요하다.

참고문헌

[1] A. Valdes, K. Skinner, “Probabilistic Alert Correlation”, RAID 2001

[2] O. Dain, R. Cunningham, “Building Scenarios from a Heterogeneous Alert Stream”, IEEE Workshop on Information Assurance and Security, 2001

[3] http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt

[4] H. Debar, A. Wespi, “Aggregation and Correlation of Intrusion-Detection Alerts”, RAID 2001

[5] B. Morin, H. Debar, “Correlation of Intrusion Symptoms : an Application of Chronicles”,RAID 2003

[6] F. Cuppens, A. Miege, “Alert Correlation in a Cooperative Intrusion Detection Framework”,
In IEEE Symposium on Security and Privacy, 2002

[7] F. Valeur, G. Vigna, C. Kruegel, R. Kemmerer,
"A Comprehensive Approach to Intrusion Detection Alert Correlation", In IEEE Transactions on Dependable and Secure Computing, 2004

[8] C.Kruegel, W.Robertson, "Alert Verification: Determining the Success of Intrusion Attempts", In the Proceedings of the 1st Workshop on the Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). July 2004, Dortmund, Germany

[9] http://www.igloosec.com/

[10] http://www.netforensic.com