침입정보분석을 위한 침입탐지 Extrator구현

조정민*, 이은영*,이현우*, 이홍규*,임채호*,이광형*,최명렬**,이진석**

*한국과학기술원 전산학과, **국가보안연구소

Implementation of Intrusion Detection Extractor for Intrusion Analysis

Cho Jung Min* ,Eun Young Lee* ,Hyun Woo Lee ,Heung-Kyu Lee* ,Cheho Lim* ,Kwang H.Lee* ,Myung Ryul Choi**, Jin Suk Lee**

*Department of Computer Science, KAIST,**National Security Research Institute

요 약

인터넷의 확장과 함께 더 나은 보안 도구가 요구되고 있다. 최근 몇 년간 많은 기업에서 보안 전문가를 위한 제품을 출시했다. 그러나 새로운 도구가 나올 때 마다 새로운 위협이 발생했다. 이와 함께 새로운 개념의 보안 시스템이 필요하게 되었다. 인터넷 위협 관리 시스템은 실시간으로 보안 경보를 중앙서버에서 수집하고 분석하여 실시간 분석 , 경보 및 대응을 하는 시스템이다. 인터넷 위협 관리 시스템은 보안 관리자에게 전체 시스템들 간에 무슨 일이 일어났는지를 한눈에 볼 수 있게 해준다. 결과적으로 보안제품과 시스템을 감시하는데 투자되는 시간이 그만큼 줄여준다

I. 서론

인터넷의 폭발적인 성장과 더불어 해킹기법 또한 다양해지고 있다. 그리고 새로워지는 해킹기법에 대응하여 보안기술도 새로워지고 있다. 일반적으로 새로운 인터넷 위협요소가 나타나면 newsgroup 이나 보안 회사에서 그것을 감지하고 분석하여 보안시스템이나 백신시스템의 패치를 발표하고 사용자들이 받아서 사용하는 방식을 주로 사용해왔다 .그러나 최근의 해킹이나 Virus, Internet Worm 등과 같은 기법들이 지능적, 자동화되어지면서 전통적인 방식의 보안기법으로 Internet worm을 미처 탐지하기도 전에 전 세계의 서버들을 감염시켜 무력화시킴으로써 적절한 대응을 하기 힘들어지고 있다. 이러한 급속도로 번져나가는 형태의 새로운 패러다임의 해킹기법들은 앞으로 더욱 발전하게 될 전망인데 이것을 미연에 탐지하고 방지하기 위해서 새로운 개념의 보안시스템인 인터넷 위협 관리 시스템의 개념이 출현하였다. 이 보안 네트워크는 전 세계에 흩어져 있는 개별적인 보안 단위에 깔려있는 추출기를 통해 필요한 정보를 IDS나 firewall로부터 추출하여 중앙의 서버에서 수집하고 이를 분석하여 실시간 분석, 경보 및 대응을 하는 시스템이다. 전 세계에서 모이는 정보를 수집하여 분석하기 때문에 급속도로 퍼지는 바이러스나 인터넷 웜의 공격을 실시간으로 감지할 수 있고 이에 대한 경보 등의 적절한 대응을 하여 시스템의 사용자가 좀더 빠른 시간에 대응을 할 수 있도록 도와 줄 수 있으며, 개별 사용자의 정보를 잘 분석하고 관리하여 복잡하지 않게 유지 보수 작업을 할 수 있도록 도와 줄 수 있게 되었다.

본 논문에서는 이러한 인터넷 위협 관리 시스템을 구현하여 Internet Attack Map system이라고 호칭하였고 이 시스템을 더욱 효율적으로 사용하기 위하여 더욱 효율적인 추출기를 고안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 Internet Attack Map System에 대해서 알아보고 문제점을 분석한다. 3장에서는 제기된 문제점을 해결하기 위해 제안한 효율적인 추출엔진에 대하여 설명한다. 4장에서는 제안된 추출엔진이 사용된 시스템과 실험결과를 보여주며, 그리고 5장에서는 결론 및 앞으로의 연구 방향을 제시한다

II. Internet Attack Map System

Internet Attack Map System(이하 IAM system)은 본 논문에서 구현한 광범위한 인터넷에서 개별적인 보안시스템의 정보를 모아서 분석하고 대응하는 시스템이다. 이 시스템은 크게 개별 보안시스템에서 정보를 수집하여서 보내어주는 역할을 하는 클라이언트와 수집된 정보를 모아서 분석하여 대응하는 서버의 구조로 나누어진다. 이 시스템의 구조는 그림 2.1 과 같다

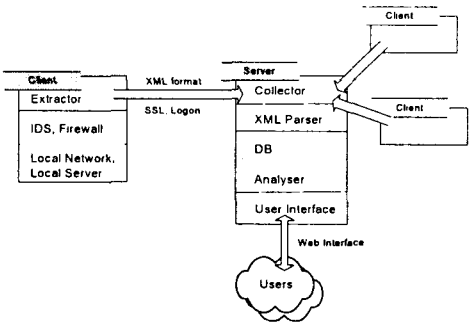

그림 2.1

위의 그림에서 살펴보면 클라이언트의 추출기(Extractor)는 사용자의 개별적인 Local Network나 Local Server위에서 돌아가는 IDS시스템이나 firewall의 정보를 사용한다. 개별적인 보안시스템의 정보를 추출하여 필요한 정보를 서버에 보내는 기능을 담당하게 된다. 이때 추출기는 IDS에서 탐지한 공격이나 portscan의 event에서 공격자 ip address, port, 공격받는 ip address, port, 알려진 공격기법, 공격이 이루어진 시각, protocol, event의 Log등의 정보를 수집하여 보내게 된다. 전송의 경우에도 위협탐지 시스템 자체에 대한 공격으로 거짓 공격 패킷을 보내 혼란하게 하거나 디스크를 고갈시키는 여지를 최소화하기 위하여 SSL을 사용한 http protocol을 사용하였으며 사용자마다 로그온을 하도록 고안하여서 사용자에 대한 개별적인 서비스가 가능하도록 고려하였다. [3]

전 세계의 인터넷에서 수집되어 보내어진 정보를 서버에서는 collector를 통해서 수집하고 분석하게 된다. 각 extractor에서 사용자별로 로그 온하여 이 정보는 데이터베이스에 저장되어 지고, 저장되어진 정보를 기반으로 여러 가지 분석을 통하여서 웹이나 메일 등의 방식으로 사용자들에게 정보를 제공하고 공격자들에게는 경고메일 등을 발송하게 된다. 또한 서버에서 다음과 같은 서비스를 제공함으로서 단순한 분석에 그치지 않고 공격에 대한 억제력을 가질 수 있게 된다. 첫째로 가장 활발한 공격을 하고 있는 top 10 IP를 실시간으로 공개한다. 이것은 공격자 주소를 공개함으로 사용자들이 공격자의 ip에서의 접속을 미리 차단할 수 있게 해줄 뿐만 아니라 공격자들에게 주소 공개에 대한 두려움 때문에 공격을 사전에 억제하는 효과를 가져온다. 둘째로 가장 활발한 상위 10개 공격 protocol을 공개한다. 이 서비스는 단순히 protocol 만을 공개하는 것이 아니라 그에 관련된 취약성 데이터 베이스와 대처법을 같이 공개를 한다. [8] 특히 특정 protocol의 공격이 급격히 증가되는 경우에는 경보를 발효하고 사용자들에게 경보메일을 발송하여 조기에 대응할 수 있도록 도움을 줄 수 있다. 또한 부가적으로 공격자에 대한 자동적인 대응메일 발송을 통해서 공격을 억지 시킬 수 있으며 사용자의 시스템에 대한 공격 로그를 사용자 별로 정리해서 보여주기도 한다

III. IAM추출기(Extrator) 구조설계

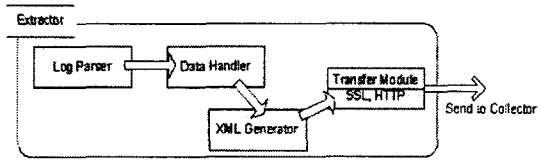

그림 3.1

IAM 추출기란 IAM시스템에서 클라이언트에 해당하는 agent로서 사용자의 security sensor의 정보를 수집하는 프로그램이다. IAM 추출기의 역할은 일정 시간마다 반복적으로 개별 보안 시스템의 로그를 분석하여서 이중 필요한 정보를 추출하고 정형화된 포맷으로 변환시켜서 안전하게 서버의 수집기(Collector)로 보내는 역할을 수행한다.

이 프로세스들은 Log Parsing, Data Handling, XML Report Generating, Transferring의 4가지 모듈로 나누어져 수행된다. 이것을 그림으로 나타낸다면 위의 그림 3.1과 같다.

Log Parser 모듈은 방화벽, 침입 탐지 시스템, Host Log 등과 같은 보안 기기의 Log를 분석하여서 정보를 해석하는 모듈이다. Log Parser는 아래 그림과 같이 계층적 구조를 가져 특정 제품의 보안 기기나 상품만을 지원하지 않고 확장될 수 있는 특징을 가진다.

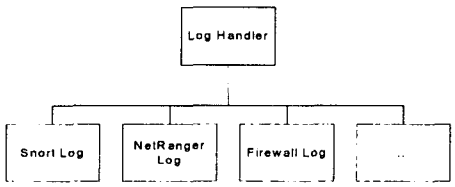

그림 3.2

Data Handler는 Log Parser에서 추출되어진 정보를 넘겨받아서 가공을 하게 된다. 이 모듈은 주로 필요 없는 데이터의 screening과 데이터 압축에 관련한 역할을 수행한다. 사용자에게 부담이 가지 않도록 최소한의 CPU를 사용하면서 효율적인 데이터 압축을 위해 History Queue를 이용한다. History Queue는 counting 기능이 첨가된 aging queue 라고 생각하면 된다. 새로운 사고 데이터가 있을 때 동일한 사고 데이터가 queue 안에 이미 있는지를 살펴보고 존재하지 않는다면 처음 일어난 사건이므로 일단 보고를 하고, 가장 오래된 사건을 queue 밖으로 밀어내면서 최근의

사건으로 등록을 한다. 이는 반복적으로 일어나는 사건을 효율적으로 압축하여 보고할 수 있는 구조이다.

XML generator는 Data Handler가 가공한 정보를 넘겨받아서 미리 약속된 DTD의 형식으로 XML format으로 정보를 재가공 하는 모듈이다. 다른 인터넷 위협 관리 시스템과 그리고 내부 시스템의 다른 버전의 시스템간의 데이터의 호환성을 위해서 XML format을 사용하였다

Transfer Module은 XML format으로 가공되어진 report를 IAM system의 collector에게 안정적으로 보내어주는 역할을 수행한다. 본 시스템에서는 Http 프로토콜을 사용하여 사용자가 시스템에 보안 로그온 하여 정보를 업로드 하는 방식을 사용하였고 이 과정 전체를 SSL을 사용하여 보호하였다.

IV. 구현 및 실험

본 장에서는 제안된 인터넷 위협 관리 시스템의 추출기의 성능 평가하기 위해서 실험을 통해 얻은 결과를 비교, 분석한다

인터넷 위협 관리 시스템을 위한 추출엔진이 효과적이 되기 위해서는 확장성과 호환성과 데이터 압축성능이 필요하다. 이 중에서 확장성과 호환성의 경우 실험적으로 보일 수 있는 방법은 없으므로 3장에서의 설명과 운영되고 있는 시험 시스템의 모습으로 이를 대처한다. 따라서 이 장에서는 데이터 압축 성능으로 추출기를 평가한다.

실험의 평가는 2가지로 나누어서 평가하였다. 첫 번째는 네트워크를 통해서 서버로 보내는 report file의 size를 직접 비교하였다. 두 번째는 데이터베이스에 update되는 event 개체의 개수 차이로 평가하였다. 2가지 평가에 있어서 2가지 버전의 추출기를 2가지 종류의 Log와 병행해서 사용하여 결과를 얻었다. 데이터 압축성의 평가를 위해 실험한 실험의 결과는 아래의 도표 4.1, 4.2와 같다

bytes	A)기존의 추출기	B) IAM 추출기	Ratio (B/A)
평상시 1일 Report file 크기	9616	3430	0.36
nimda 공격시 1일 Report file 크기	9167460	94004	0.01

표 4.1

개	A)기존의 추출기	B) IAM 추출기	Ratio (B/A)
평상시1일 DB Update 개수	9	3	0.30
nimda 공격시 1일 DB Update 개수	4742	51	0.011

표 4.2

표 4.1을 살펴보면 History Queue의 기능을 제외한 기존의 추출기가 평상시 생성하는 Report 파일의 평균 크기가 9616 byte 인 것에 비해서 History Queue의 기능이 추가된 추출기에서는 평균 3430byte 정도를 만들어내는 것을 볼 수 있다. 이것은 평상시에는 IAM 추출기가 report 파일의 크기를 1/3정도로 압축해서 보내는 것으로 볼 수 있다.

표 4.2의 경우를 살펴보면 평상시에 일반 추출기가 database에 update 하는 개체의 수보다 IAM 추출기가 1/3 정도 적게 update하는 것을 살펴볼 수 있으며 nimda virus가 공격을 하는 날들의 경우에는 표 4.1의 결과와 비슷하게 1/100정도의 차이를 보였다.

인터넷 위협 관리 시스템의 목적 중 하나는 급격한 인터넷 공격증가 원인을 빨리 진단하고 판별하는 것에 있다. 즉 가장 공격이 활발하게 일어날 때 서버가 실시간으로 사건을 처리할 수 있어야 진단이 가능해진다. IAM system은 이 차이를 줄여 주기 때문에 일반 추출기로 운영해야 하는 서버보다 훨씬 저 사양의 서버로 적절한 운영을 할 수 있도록 도움을 줄 수 있다.

V. 결론 및 향후 연구 방향

본 논문의 인터넷 위협 관리 시스템을 위한 추출기는 효율적인 정보의 수집을 위해서 제안되었다. 효율적이고 신뢰할만한 기능을 제공하기 위해서 많은 보안 제품들을 지원하여 풍부한 데이터를 인터넷에서 가져올 수 있도록 해야 하며, 다른 인터넷 위협관리 시스템들과 데이터의 호환도 가능하도록 해야 하며, 강력한 데이터 압축기능을 제공해야 한다. 이를 위하여 계층적인 구조로 쉽게 보안 제품의 지원을 추가할 수 있도록 디자인하였고, XML format을 사용한 reporting module을 구현하여 데이터의 호환과 내부 시스템의 일치성을 확보하였다. 마지막으로 history queue module으로 가볍지만 강력한 데이터 압축이 가능하도록 설계하였다. 실제 시스템이 현재 시험 운영중이며, 보안업체인 일본 secom의 데이터를 받아와서 협력하는 시험 시스템이 운영중이다

제안된 시스템이 안정적으로 수행되어지기 위해서는 더 보강되어야 할 점들이 있다. 우선 더욱

많은 보안 제품에 대한 지원을 할 수 있도록 Log parser를 보강해야만 한다. 그리고 사고 대응이 자동적으로 실행되어야 시스템의 효과가 극대화 될 수 있지만 아직 사건 분석의 정확성 부족으로 대응메일을 보내는 것에 대한 관리자의 결정이 필요하며, 그리고 대응메일에 대한 담장관리와 사후 관리 등의 서비스가 필요하다. 표준화 단계에 있는 자동사고 대응 정보교환을 위한 IDEF 규약을 따라서 수행되도록 하여 표준화작업에 대응해야만 하며 그리고 실시간으로 데이터의 분석이 이루어지고 있기는 하지만 데이터베이스 처리에 대한 시간적인 한계로 기초적인 분석만을 제공하고 있는 수준에 머물러 있다. 여러 가지 방법의 데이터의 분석으로 많은 사건을 더욱 신속하고 효과적으로 파악할 수 있도록 하기 위한 연구가 좀 더 진행되어야 할 것이다.

참고문헌

[1] Fyodor, "The Art of Port Scanning", Phrack Magazine Volume 7 Issue 51, 1997.

[2] V. Paxson, "Bro:A System for Detecting Network Intruders in Real-Time", 7th USENIX Security Symposium, San Antonio, TX, 1998.

[3] H.Y. Chang, P. Chen, A. Hayatnagarkar, R. Narayan, P.Sheth, N. Vo, C.L. Wu, S.F. Wu, L. Zhang, X. Zhang, F. Gong, F. Jou, C. Sargor, X. Wu, "Design and Implementation of A Real-Time Decentralized Source Identification System for Untrusted IP Packeets", Proceedings of the DARPA Information Survivability Conference & Exposition, January 2000.

[4] Real-Time Security Awareness(RTSA)-SANS http://www.sans.org

[5] Internet Security Systems - Product : SAFEsuite Decisions http://www.iss.net

[6] e-Security, Inc - Product : Open e-Security Platform http://www.esecurityinc.com

[7] Tivoli - Product : SecureWay Risk Manager

http://www.tivoli.com

[8] Common Vulnerabilities and Exposures(CVE)

http://www.cve.mitre.org