상관분석을 활용한 웹방화벽 정책 적용 방안 연구

김창홍* · 최대영** · 이정현***· 김종배****°

*,**,***,****°숭실대학교

A Study of Security Policy Adaptation to WAF using Correlation Analysis

Chang-hong Kim* · Dae-young Choi** · Jeong-hyun Yi***· Jong-bae Kim****

*,**,***,****°Soong-sil University

E-mail : *chkim@nextup.kr, **choidy219@naver.com, ***jhyi@ssu.ac.kr, ****°kjb123@ssu.ac.kr

요 약

이제 국내에서 IT서비스는 웹을 통하지 않고서는 불가능할 정도까지 일반화 되었다. 반면, 이러한 웹에 대한 보안 문제가 이슈가 되면서 웹서버에 대한 안전한 코팅이 2012년부터 안전행정부를 통하여 강제적인 지시사항으로까지 된 상황이다. 기존에는 이러한 요구를 해결하고자 보안 장비인 웹 방화벽이 국내 시장에서 많은 탄력을 받으며 판매가 되어 왔다. 본 연구에서는 이러한 웹 방화벽의 보안 정책을 운영자가 능동적으로 설정할 수 있는 방안을 제시하여, 보다 안전한 웹서비스를 가능하게 하는 방안을 제시하고자 한다.

ABSTRACT

The public services without going through the web is now about to become impossible. To solve these kinds of security issues about the web, the government announced that a secure coding for web server is mandatory since 2012. In the domestic market, the web firewall has been promoted and widely sold as one of the best solutions for the existing web problems. In this study, with providing the effective way operator can apply security policies for the web firewall, more stable web services can be presented.

키워드

웹 방화벽, 보안 정책, 시큐어 코딩, 웹 어플리케이션 보안

Ⅰ. 서 론

기업에서 가장 많이 활용하는 것이 웹사이트를 이용한 웹서비스이다. 최근 스마트폰이 활성화 됨에 따라 이러한 웹사이트의 활용은 더욱 더 많아지고 있다. 이에 비례하여 웹사이트에 대해서 해킹사고가 많아지고 있으며 이를 방어하기 위한 보안장비들도 많이 사용되고 있는데 이러한 장비 중의 하나가 WAF(Web Application Firewall)이다. 그러나 WAF의 특성상 세밀한 정책이 설정되지 않으면 일부 서비스가 안되는 문제가 발생할 수 있기 때문에 대부분의 경우 세부적인 설정을 하지 못하고 이로 인하여 경로우회 및 해킹 사고가 많이 발생하여 WAF의 장점에도 불구하고 많은 기업에서 활용을 제대로 못하고 있는 상황이다.

본 연구에서는 이러한 WAF의 세부적인 설정을 보다 쉽게 하기 위하여 기존에 해킹 탐지에 가장 많이 사용되는 IPS를 이용하여 IPS와 WAF에서 발생하는 탐지 이벤트를 가지고 상관분석을 통해 차단 정책을 적용할 수 있는 방법을 제시하여 보다 안전한 웹 서비스를 제공할 수 있도록 하게 위함이며, 또한 WAF의 활용도를 더 높게 할 수 있도록 하는데 목적을 두고 있다.

II. 본 론

본 연구에서 사용한 가장 기본적인 로직은 IPS와 WAF에서 발생되는 탐지 이벤트를 가지고 상호 연관 시킬 수 있는 키값으로 공격자 IP, 목적지 IP, 이벤트를 탐지한 시간, 그리고 IPS와 WAF에서 탐지되는 이벤트의 공격 분류를 키값으로 맞추어 동일하게 적용될 경우 하나의 인시턴트(incident)로 정리하게 된다.

2.1. 웹 어플리케이션 공격

웹 어플리케이션 공격은 웹서비스에서 개발자 및 운영자가 어플리케이션들의 설정 오류나 소스코드의 문제점으로 인하여 웹 서버 내부의 정보를 유출하거나 변조, 혹은 서버의 권한을 획득하기 위한 것으로 국내에서는 국정원의 분류 및 해외에서는 OWASP 10의 분류에 따라서 가장 많이 발생된 웹공격의 유형을 10개로 나누고 있다.

국내에서는 안전행정부에서 공공기관에서 활용되는 웹페이지에 대해서 Secure coding guide로 프로그래밍 자체에서 취약한 코드를 사용하지 않도록 하여 보안 문제점을 해결하고자 하고 있다. 이러한 해킹시도에 대해서 국내외로 많이 사용되는 보안장비로는 IPS와 WAF가 주종을 이루고 있으며 최근의 대응 방법에는 IPS에서 공격 패턴을 등록하여 탐지하고 WAF는 알려진 공격에 대해서 차단하도록 rule을 설정하여 웹에 대한 공격을 방어하고 있다. 그러나, 두 가지 장비 모두 각각의 한계를 가지고 있으며 모든 보안 장비가 그러하듯이 많은 공격 부분에 대하여 대응하고 있으나 완벽하게 대응하지는 못하고 있다.

2.2. IPS의 한계

IPS는 네트워크를 지나는 패킷을 개봉하여 헤더부분의 비정상적인 부분이나 미리 정해져 있는 탐지 패턴으로 공격을 탐지하는 것으로 웹에 관련된 공격에는 아래와 같은 공격에는 탐지할 수 없다.

① SSL : 웹서버에서는 중요한 데이터의 sniffing을 막기 위하여 네트워크 구간에서 암호화를 진행한다. 이 경우 IPS에서는 암호화된 내용을 복호화 할 수 없기 때문에 탐지가 불가능하다.

② 패턴이 없는 공격 : 과거 anomaly기법으로 만들어진 IPS가 존재하였으나 오탐이 많이 발생하여 최근에는 거의 모든 IPS가 misuse방식을 활용하고 있다. 이에 따라 패턴이 없는 신종 공격에 대해서는 탐지가 불가능하다.

2.3. WAF의 한계점

WAF는 해킹 공격에 대한 차단에 주요 목적을 두고 있다. 그러나, 현재처럼 계속 새로운 공격이 나오고 있는 상황에서 단순 IP, port단위의 3계층에 대한 대응이 아닌 source code, logic에 대한 문제점으로 취약점이 발생하고 있는 상황에서 쉽게 공격에 대응하기는 어렵게 되었다.

이에 통상 WAF의 rule 설정을 위하여

① Learning mode의 활용 : WAF의 차단 정책을 설정하는 것이 아닌 탐지 정책을 설정하여 몇 개월간 탐지되는 이벤트를 파악하여 실제 정상 서비스 인것과 공격을 분류하는 방법으로 대규모의 영역에서 사용한다. 그러나, 세부적인 정책 적용은 불가한 상황이다.

② 웹스캐너로 취약점 분석 : 웹 취약점을 스캐너를 활용하여 분석하고 이에 대한 내용을 WAF에 적용하는 방법이나 웹스캐너와 WAF의 제조사가 다를 경우 해당 공격에 대한 정확한 대응방법을 찾기 어렵고, 또한 웹 스캐너로 찾을 수 있는 취약점이 한계가 있어서 최근에는 잘 사용하지 않고 있다.

③ 운영 모드에 의한 차단 룰 설정 : 서비스가 크게 많이 사용되지 않는 상황에서 모든 공격유형에 대하여 우선 차단을 하고 사용자 입장에서 막히는 서비스에 대하여 차단을 해제하는 방법이 있으나 실 사이트에 적용하기는 서비스 중단이 발생할 여지가 있어 위험한 상황이다.

크게 위와 같이 3가지 형태로 룰을 적용하는 방식이 있으며 세부적으로는 다른 방법도 있으나 실제 서비스를 하고 있는 웹 사이트에 적용하거나 적용 이후 룰을 신규로 추가하기가 쉽지 않아 많은 기업에서는 WAF의 활용도가 떨어지는 상황이 발생한다. 이와 같이 WAF는 정확한 룰을 설정할 경우 많은 도움을 받을 수 있으나 실제 룰 적용에 많은 어려움이 있기 때문에 기존의 생각과 달리 기업에서는 적용되었던 WAF가 기존의 룰 그대로 되어 있거나 혹은 WAF를 빼어 버리고 모의 해킹을 통하여 소스코드에서 취약점을 찾아내어 제거하는 방식을 많이 사용하고 있다. 즉, 장비의 기본 기능이 아닌 활용 방법에서 한계가 발생하기 때문에 WAF가 기대했던 것 보다는 적게 사용되고 있는 것으로 판별이 된다. 본 연구는 이러한 WAF의 활용도를 높이기 위하여 시작되었으며 테스트 과정에서 어느 정도 그 결과를 도출하였다.

2.4. WAF와 IPS의 연동

2.4.1. 기본 개념 및 연동 방안

위에서 언급한 바와 같이 IPS는 주로 공격에 대한 탐지를 위하여 많이 사용하고 있으며 WAF는 이러한 공격을 차단하기 위하여 사용하고 있다. 즉, IPS로는 웹공격에 대한 차단보다는 신규 공격 유형에 대한 탐지 형태로 많이 사용되고 WAF는 알려진 공격에 대한 차단을 위주로 가고 있다. 그렇다면, IPS에서 탐지된 신규 공격을 WAF를 통하여 차단할 수 있는 체계가 된다면 현재의 WAF를 잘 활용할 수 있을 것이다. 본 연구에서는 IPS와 WAF의 보안 탐지율을 서로 상승시키기 위한 목적으로 상호간의 룰을 검증한다.

이를 위하여 연구에 사용된 장비에 설정을 보면

① IPS : 웹에 관련된 공격을 탐지하도록 하고

탐지 이벤트 로그는 통합로그관리시스템으로 전송한다.

② WAF : 웹 공격을 탐지하거나 차단한 이벤트 로그에 대해서는 통합로그관리시스템에서 이벤트 로그를 받게 한다.

③ 통합로그관리시스템 : IPS와 WAF에서 탐지된 탐지 이벤트를 가지고 연계시키기 위하여 두 개의 장비에서 들어온 이벤트를 1분이내 발생된 동일한 IP(공격자, 대상자)를 서로 매칭시켜 상관분석시키도록 설정한다.

단, 개개별 이벤트로써 정리하면 세부적으로 공격별로 탐지되는 이벤트가 다를 수 있으므로 공격 이벤트를 분류하여 정리하고 탐지 이벤트는 분류된 유형으로 한정 짓는다.

2.4.2. 공격에 대한 탐지 결과

연구에서 테스트한 네트워크는 IPS에서 탐지를 하고 WAF에서 차단을 하는 방식으로 하였다. 즉, IPS에서 네트워크 구간에서 탐지를 하였더라도 WAF에서 차단을 했다면 IPS에서 잘못 된 정보를 내 보낼 수 있기 때문에 IPS의 탐지 이벤트와 WAF의 탐지 이벤트가 명확하게 맞아 들어가거나 WAF가 차단하지 않고 탐지하였다는 탐지 이벤트가 나타날 경우에만 공격으로 판단할 수 있도록 하였다. 즉, 수많은 이벤트에서 많은 수의 공격이 제거되어 실 상황에서 탐지 되는 이벤트 중 많은 수를 제거하여 실제 공격을 탐지 할 수 있는 시간적인 여유를 가지게 하는 것이 된다.

실제 테스트에서 1개의 victim ip에 대해서 공격 테스트를 해 본 결과

① IPS탐지 이벤트 : 6000 여건
② WAF차단 및 탐지 이벤트 : 600여건
③ WAF미탐지 이벤트 : 20여건
④ IPS미탐지 이벤트 : 100여건
⑤ IPS 및 WAF탐지 이벤트 : 580여건

으로 결과가 발생되었다. 물론 공격에 대해서 각 장비별로 탐지 및 처리 로직이 다르기 때문에 정확한 이벤트수가 적용되지는 않으나 언급한 바와 같이 개별 공격으로 적용한 것이 아닌 공격을 유형별로 나누어 적용하였기 때문에 이러한 부분은 IPS:WAF가 N:M으로 적용되어 탐지 되었다. 즉, 기존의 방식대로 따랐을 때에 비하여 IPS입장에서는 6000개의 이벤트 중 580개의 의미있는 이벤트를 추출 한 것 이고 WAF의 입장에서도 미탐지 공격에 대한 결론을 추출할 수 있었기 때문에 향후 실 시스템에서 적용되는 경우 더 많은 부분에 대해서 활용이 가능할 것으로 보인다.

테스트 결과의 정확도를 향상하기 위해서는 공격분류를 조금 더 세부적으로 분류하고 IPS, WAF의 공격을 세부화한다면 테스트 결과보다 더 정확한 내용이 나올 것으로 예상되나 이 부분은 추후과제로 남겨 두는 것으로 한다.

Ⅲ. 결 론

본 연구를 통하여 웹 공격의 경우 수없이 많이 발생되는 탐지 이벤트에 대하여 탐지 이벤트를 정제할 수 있는 방안이 제시되었고 WAF입장에서도 미탐지 및 차단된 이벤트를 파악할 수 있었다. 이에 대한 대응 방안으로 더 세밀한 탐지 공격을 적용할 수 있었으며 기존의 신공격에 대한 WAF 적용이 어려웠던 부분에서 IPS에서 탐지된 이벤트에 대하여 적용이 가능하였기 때문에 WAF정책 적용이 더 용이하게 될 수 있었다. 물론 제한적인 환경이기 때문에 실 환경에서 적용할 때 다른 문제점이 발생할 수 있으리라 보이지만 이론적인 환경에서는 큰 문제는 없을 것으로 보인다. 향후 이 방법을 활용하여 과다하게 탐지되는 이벤트 중 실제 공격으로 파악되는 최소한의 공격을 제거할 수 있고 WAF의 차단 수준을 향상하여 새로운 공격에 대한 WAF의 수준을 향상 시켜 사용할 수 있으리라 예상된다. 향후 제품별, 네트워크 구조별로 달라 질수 있을 것이므로 실제 상황에서 연계하여 가장 적합한 수치를 검토해야 할 것으로 보인다.

참고문헌

[1] IBM, "X-Force 2010 Trend and Risk, Report", March 2011.
[2] ArcSight, Inc., Common Event Format Revision 15, 2009.7
[3] OWASP, OWASP 2013, 2013.
[4] 유종호, 김종현, 나중찬, "통합보안관리 및 사이버 역추적 기술 표준화 현황", TTA Journal No.118, pp.66-74, 2008.
[5] C. Abad, J. Taylor, Y. Zhou, C. Sengul, K. Rowe and W. Yurcik, "Log Correlation for Intrusion Detection: A Proof of Concept", Proceedings of the 19th Annual Computer Security Applications Conference, 2003.
[6] W. Chen, W.h Kuo, and Y. Wang, "Building IDS Log Analysis System on Novel Grid Computing Architecture", CloudSlam 09 Conference, 2009.
[7] Barracuda Networks, Barracuda Web Application Firewall Manual, 2010