김일성종합대학학보
(정보과학)
주체107(2018)년
제64권 제1호

전자도서비법내리적재검출에 대한 한가지 방법

김하경, 허철만

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《통신망의 보안능력을 결정적으로 높여야 합니다.》

오늘 전자도서관은 전자도서수집, 목록화, 도서열람 등을 주요기능으로 하여 과학교육사업을 위한 다양한 정보자원봉사를 제공하고있다. 그런데 일부 사용자들은 흔히 비법적인 방법으로 혹은 비법내리적재도구를 리용하여 전자도서관에 구축된 전자자료에 대한 다량의 내리적재를 진행하는데 이것은 곧 비법적인 내리적재로 된다.[1]

론문에서는 침입검출프로그람 Snort와 모호추론을 리용한 비법적인 내리적재를 검출하는 체계를 연구하여 전자도서관망을 비롯한 자료봉사단위들의 정상적인 운영과 보안을 보장하는 한가지 방법을 제안하였다.

1. 체계구조설계

다음의 그림에서 보여준 체계구조는 기능모듈의 각도에서 자료수집, 이상분석, 해석, 반응 등의 모듈로 나눌수 있다.(그림) 자료수집모듈은 주요하게 지정된 망자료를 수집하여 이상분석모듈에 제공하여 분석을 진행하게 한다. 이상분석모듈은 기본망흐름의 이상행위를 분석하고 이상행위의 이상도를 계산하여 이상도가 설정된 턱값보다 크면 곧 해석모듈에 경보를 보낸다. 해석모듈은 이상분석모듈의 이상경보를 분석하고 일정한 알고리듬에 기초하여 그것이 비법적인 내리적재행위인가를 판단한다. 반응모듈은 해석모듈에서 보내온 정보를 수집하고 현시 및 경보를 울리거나 기타 처리를 진행한다.

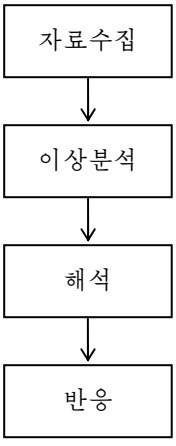

그림. 체계구조

① 자료수집

망사건자료의 원천은 콤퓨터망에서 전송되는 망자료파케트이다. Snort를 리용하여 망대면부를 《혼잡방식》으로 설정하고 목표한 대상의 모든 자료파케트를 획득한다.

② 이상분석

시간차와 IP주소의 우연분포특성을 특징인자로 하고 모호추론방법에 기초하여 비법적인 내리적재와 같은 이상행위를 판단한다.[2]

③ 해석

해석모듈은 이상분석모듈로부터 접수한 경보정보를 루적하여 실지 이상흐름인가 아닌가를 판단한다.

④ 반응기구

일반적인 경우의 반응방법은 공격을 자동적으로 방지하는것이다. 구체적인 방법은 망

자원을 다시 구성하거나 관리조종대에 창문형식으로 알리거나 전자우편의 형식으로 체계 보안관리자에게 통지하여 사건의 발생을 적발하거나 사건자료(날자, 시간, 원천주소, 목적주소 및 사건과 관련되는 초기자료 등)를 기록하고 TCP련결을 차단하여 즉시 현재대화를 닫는것 그리고 미리 정의한 프로그람을 실행하는것 혹은 기타 보안제품 례하면 방화벽과의 협동 등이다.

공격차단방식에는 일반적으로 두가지 방식 즉 대화차단과 련결요청거절방식이 있다.

TCP대화에 대해 보면 체계는 대화통신의 량쪽에 TCP RESET파케트를 보낸다. 이때 통신쌍방은 이 RESET파케트를 다른 한쪽의 응답으로 해석하고 전체 통신과정을 중단한다.

망공격의 원천추적은 망공격사건이 발생한 원천지를 찾아서 공격자의 IP주소와 MAC주소를 얻어 공격자의 신분을 확정하는것이다.

망공격을 추적하는데서 고려해야 할 문제는 IP주소가 가상주소이지 물리주소는 아니라는것이다.

IP주소는 아주 쉽게 위조될수 있으며 대부분의 망공격자들은 IP주소속임기술을 쓴다. 이렇게 하면 공격원천지를 추적하는것이 불정확하게 되며 IP주소를 기술로 하여 공격자를 밝히는것은 보다 더 어렵게 된다.

2. 이상분석모듈설계

1) 특징인자의 선택

론문에서는 2개의 검출하려는 특징인자를 선택하였는데 하나는 시간차를 선택하고 다른 하나는 IP주소의 통계적분포특성을 선택한다.

① 요청파케트의 시간차

비법내리적재행위에 대하여 분석해보면 요청자는 반드시 대량의 SYN자료파케트를 봉사기에 보내게 된다. 그러므로 요청시 SYN파케트가 빈번하고 시간간격이 상대적으로 짧은 특성에 기초하여 첫번째 특징인자로 시간차 DT를 선택한다.

② IP주소의 통계적분포

전자도서관봉사기로 전송되는 파케트의 IP주소들은 어떤 통계적특성을 만족시킨다. 대량의 요청이 발생할 때 요청파케트는 위조IP주소 혹은 유한개의 IP주소에 기초하므로 원래IP주소의 통계적특성은 파괴될수 있다. 정보엔트로피 DH로 이러한 우연분포특성을 표시한다.

엔트로피는 다음과 같이 구한다.

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

그러므로 어떤 련속적인 파케트흐름의 단일원천IP주소의 출현확률을 그 IP주소의 발생확률로 하고 웃식을 리용하여 원천IP주소분포에 기초한 파케트흐름의 엔트로피값을 얻는다. 이 엔트로피값은 일종의 원천IP주소의 우연분포특성을 제공한다. 엔트로피가 크면 클수록 IP주소분포가 우연특성을 가진다는것을 보여주며 반대로 엔트로피값이 작으면 IP주소의 분포범위가 작고 일련의 주소의 출현확률이 높다는것을 보여준다.

2) 2개의 특징인자를 리용한 모호추론

론문에서는 모호추론방법을 리용하여 비법적인 내리적재를 판단한다. 콤퓨터망에서 비법적인 행위가 발생할 때 정상파케트와 이상파케트가 동시에 전송되며 정상파케트와 이상파케트를 판별할수 없는 경우가 조성되며 동시에 엔트로피값과 시간차 역시 믿을수 있는 정확한 값이 아니다.

콤퓨터망의 정보는 전송과정에 여러가지 인자의 영향을 받기때문에 오유가 발생할수 있다. 그러므로 공격검출과정에 오경보가 발생할수 있고 어느것이 이상이고 어느것이 정상인지 판단할수 없게 한다. 때문에 론문에서는 모호추론을 리용하여 이러한 문제를 해결하며 작은 규칙을 가지고 여러가지 경우를 처리하고 검출을 진행한다.

모호추론체계는 특징인자(엔트로피값, 시간차)의 입력값에 의하여 결과를 판단하며 련속적으로 공격가능성이 큰 결과가 출현하고 턱값을 초과하면 비법적인 내리적재행위로 판단한다.

3) 이상분석모듈의 실현

분석모듈은 4개의 부분 즉 모호발생부분, 모호규칙기지, 모호추론부분, 이상결정부분으로 이루어진다. 모호발생부분은 이상검출부분의 입력과 출력을 확정한 후에 이상행위의 주요인자인 DH(엔트로피값)와 DT(시간차)의 성원함수를 정의한다. 여기서 2개의 인자는 5개의 모호모임으로 나누어진다. 모호모임은 L+, L, M, H, H+로 표시한다. 이것들의 의미는 《더 작다》, 《작다》, 《중간》, 《크다》, 《더 크다》이다.

이상의 모호모임과 규칙기지에 따라 모호추론을 진행하고 이상가능성은 DH, DT의 변화에 따라 결과를 얻는다. 모호규칙기지는 모호추론규칙으로 구성되고 규칙의 새로운 입력정보가 들어오면 1개의 결론을 낸다.

이상행위분석에 대한 모호추론규칙은 다음의 표와 같다.

표. 이상행위분석에 대한 모호추론규칙

	DH=H+	DH=H	DH=M	DH=L	DH=L+
DT=L+	R=H+	R=H	R=H+	R=H	R=H+
DT=L	R=H	R=H	R=H	R=H	R=H
DT=M	R=H	R=M	R=M	R=M	R=H
DT=H	R=M	R=M	R=L+	R=M	R=M
DT=H+	R=M	R=L	R=L+	R=L	R=M

모호추론규칙에서 R는 이상가능성을 의미하고 규칙은 실험과 경험을 통하여 얻어지며 조건에 따라 수정할수 있다. 모호추론부분은 추론규칙과 입력값에 따르는 모호추론을 리용하여 그것의 이상가능성을 결정한다. 모호모임 H+, H, M, L, L+가 대표하는 이상도값의 초기값은 1, 0.8, 0.6, 0.4, 0.2로 한다.

이상도값 R는 시간차의 증가에 따라 작아지며 엔트로피의 값이 중간에 있을 때 이상가능성이 비교적 작으며 엔트로피의 값이 너무 작거나 크면 이상가능성이 비교적 크다.

이상결정부분은 이상가능성결정부분과 판단부분으로 나누어진다. 가능성은 실험분석을 통하여 결정하며 0.7(턱값)(수정가능)이상의 파케트는 이상가능성이 큰 파케트로 여긴다. 판단부분은 검출한 파케트에 대하여 판단을 진행하고 이상가능성이 큰 파케트수가 규

정한 개수의 턱값을 초과하면 비법적인 상태라고 본다.

Snort규칙은 2개의 부분으로 이루어진다. 즉 규칙머리부와 규칙선택으로 이루어진다. 규칙머리부는 규칙의 동작, 규약, 원천지주소와 목적지주소, 원천포구와 목적지포구를 포함한다. 규칙선택은 1개의 경보정보와 자료파케트관련부분의 정보를 포함한다.

론문에서는 모호추론에 기초한 검출규칙을 다음과 같이 추가하였다.

alert tcp any any －> $HOME_NET any (msg: "Attack attempt"; attack:2, 0.7, 100, 200;)

규칙에서 괄호앞의 부분은 규칙머리부에 속하며 괄호내부의 부분은 규칙선택에 속한다. 규칙머리부에서 규칙의 동작은 규칙이 기동된 후에 사건에서 무엇을 하는가를 보여준다. 괄호안의 모든 내용은 규칙선택부분이다. 공격이 검출되면 msg의 내용이 출력된다.

실험에서 리용한 미끄럼창문의 크기는 100이다. 요청수의 증가에 따라 실험이 진행되였다. 실험콤퓨터의 장치적조건은 Intel(R) Pentium(R) 4 CPU 1.70GHz이고 기억기는 2GB이다. 실험결과는 제기한 방법이 1.4s안에 비법행위가능성을 검출하며 이러한 행위가 일정한 시간동안 루적되면 비법적인 내리적재요소자와 공격콤퓨터를 검출할수 있다는것을 보여주었다.

맺 는 말

비법적인 내리적재검출방법을 연구하고 원천코드공개형침입검출체계 Snort 및 그것의 확장성을 리용하여 개발을 진행하고 Snort에서 실행하여 가능성을 검출하였다. 실험은 요청개수의 증가에 따라 정확히 검출한다는것을 보여주고 여러가지 응용분야에 적용할수 있다는것을 보여주었다.

참 고 문 헌

[1] Sanjay Sharma et al.; International Journal of Security and Its Applications, 9, 5, 69, 2015.

[2] HO Cholman et al.; IEEE Computer Society, IPTC 2010, 297, 2010.

주체106(2017)년 11월 5일 원고접수

A Method of Malicious Downloads Detection System on Electronic Book

Kim Ha Gyong, *Ho Chol Man*

In this paper, using open source intrusion detection software of Snort, we proposed the library malicious downloads detection system. Test results explained that the proposed method was effective on library malicious downloads detection.

Key words: malicious downloads, Snort, library