김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제1호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 1 JUCHE105(2016).

망보안중계기에서 로그분석체계에 대한 연구

염성호, 김성훈

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《정보기술발전을 위한 과학연구사업을 앞세워야 합니다.》(《**김정일**선집》 증보판 제20권 380페지)

오늘날 콤퓨터망기술의 급속한 발전으로 사용자들이 대용량자료를 고속으로 아무런 지장없이 봉사받을수 있게 되면서 콤퓨터망보안과 관리는 중요한 문제로 나서고있으며 이를 위한 여러가지 방법들과 수단들이 출현하여 응용되고있다.

그러한 방법과 수단들중에서 대표적인것이 콤퓨터망설비나 봉사기들, 콤퓨터들의 동작상태로그를 분석하는 수법이다. 로그는 프로그람이 동작하는동안 기록되는 단순한 자료로서 사용자료, 성능자료, 오유/경고 및 운영자료들을 포함한다. 로그분석은 방대한 량의 로그자료로부터 필요한 정보를 추출하여 외부침입자흔적탐색, 체계취약점발견, 보안관리자의 결심채택지원, 체계장애원인분석 등에 리용된다. 따라서 이것은 망보안관리와 운영을 보다 과학적인 자료에 기초하여 진행할수 있게 하며 이러한 체계를 로그분석체계라고 한다.

선행연구[2]에서는 망보안중계기의 로그분석체계를 중계자료들에 대한 수동검사, 체계설정들에 대한 관리 등 사용자기능에 따른 정의만을 하였을뿐 정보보안의 기본요구항목에 기초하여 구체적인 기능정의와 그 실현방법에 대하여 서술하지 않고있다.

우리는 자료중계체계, 보안검사체계, 로그분석체계로 구성되는 망보안중계기에서 로그분석체계가 수행하여야 할 기능을 정보보안의 기본요구항목에 기초하여 정의하고 그 실현을 위한 한가지 방법을 제기하였다.

1. 로그분석체계의 기능정의

① 조사자료의 제공

로그분석체계는 자료중계과정에 제기되는 보안문제들에 대한 조사자료를 제공하기 위하여 망보안중계기안의 매개 부분체계들의 로그들을 수집하여 저장할수 있어야 한다.

이러한 로그들에는 내부망과 외부망사이의 자료중계를 담당하는 자료중계체계의 로그, 중계되는 자료들에 대한 보안검사를 담당하는 보안검사체계의 로그, 우의 체계들의 동작을 지원하는 조작체계로그들이 포함된다.

② 기초적인 심사수단의 제공

로그분석체계는 자료중계과정에 제기되는 보안문제들에 대한 기초적인 심사수단을 제공하기 위하여 망보안중계기의 저장된 로그들을 관리자의 분석요구에 따라 검색할수 있어야 한다.

관리자는 자료중계체계의 로그에 대한 검색을 통하여 중계체계에 대한 감시 및 관리(자료중계단계, 통로차단여부), 보안검사체계에 대한 감시 및 관리(승인, 차단)를 할수 있다. 또한 조작체계로그에 대한 검색을 통하여 조작체계의 성능검사 및 관리(CPU사용량, 기억기사용량, 하드디스크사용량)를 진행할수 있다.

③ 종합적인 심사수단의 제공

로그분석체계는 자료중계과정에 제기되는 망보안문제들에 대한 종합적인 심사수단을 제공하기 위하여 관리자가 망보안중계기의 전반동작을 분석할수 있도록 보고서를 추출할수 있어야 한다.

그러한 보고서에는 사용자리용통계에 기초한 보고서, 기능별리용통계에 기초한 보고서, 특정부분의 성능리용통계에 기초한 보고서, 오유/경고정보에 기초한 보고서들이 있다.

2. 로그분석체계의 실현

1) 로그정보의 자바스크립트객체표시(JSON - JavaScript Object Notation)에로의 형식화 및 저장실현

론문에서는 망보안중계기의 특성상 매 부분체계들에서 각이한 형식과 내용으로 로그들이 생성되는 조건에서 다양한 류형의 자료들을 형식화하고 저장하기 위하여 표준자료교환형식의 하나인 JSON방식을 선정하였다.

로그의 형식화 및 저장과정은 그림 1과 같다.

그림 1. 로그의 형식화 및 저장과정

부분체계들로부터 수집된 로그는 JSON형식으로 변환된 후에 로그식별정보의 추가 등 표준화과정을 걸친다. 표준화된 로그는 JSON을 자료형으로 지원하고있는 PostgreSQL(판본 9.0이상)을 리용하여 대응한 저장질문으로 변화되고 실행되며 결과 로그분석에 필요한 조사자료를 제공할수 있다.[1]

실례로 보안검사체계의 로그저장을 위한 SQL은 다음과 같다.

```
INSERT INTO log_datas VALUES (
1, // 식별자
0, // 검사류형 – 수동
0, // 검사결과 – 보류
15, // 검사자
    '214-12-25 21:56:12', // 검사날자
1, // 규칙갱신여부 – 갱신
'위험한 자료', //검사자의견
// 로그자료
{
checktype: "viruscheck",  // 검사류형정보－비루스검사
```

checktarget: { // 검사대상정보
filename : “1.exe”, // 화일이름
fileowner: “김모”, // 화일소유자
filesize: “100kb” // 화일용량
}
checkresult: { //검사결과정보
virustype: “worm”, //비루스류형
virusresult: “success” //성공
}})

2）JSON형식의 검색어에 의한 로그검색실현

각이한 류형의 로그자료들에 대하여 한정된 검색항목들과 그 조합에 의한 검색으로는 만족한 결과를 얻을수 없으며 이것은 검색열쇠와 검색어를 조합한 JSON형식의 검색어에 의한 검색으로 해결할수 있다.

관리자의 분석요구에 따라 입력된 검색열쇠 및 검색어는 JSON형식으로 변환된 후에 PostgreSQL(판본 9.0이상)의 JSON자료의 유효검사 및 관련함수를 리용하여 대응한 질문으로 변환되고 실행된다. 현시되는 질문실행결과를 가지고 관리자는 로그자료에 대한 기초적인 심사를 진행할수 있다.

로그검색의 동작과정은 그림 2와 같다.

그림 2. 로그검색의 동작과정

화일 test.exe의 비루스검사결과를 얻기 위한 검색어실례는 다음과 같다.

{checktype:virus filename: ‘test.exe’}

이때 여기에 대응한 SQL질문은 다음과 같다.

SELECT * FROM log_datas
WHERE data->>‘checktype’ = ‘viruscheck’ and data ->> ‘filename’ = ‘test.exe’

3）JSON형식의 자료들로부터 보고서추출의 실현

로그분석체계가 얻어내는 로그자료는 JSON형식인것으로 하여 그 자료로부터 직접 보고서를 추출하는것은 어려우며 이로부터 그것을 일반 SQL질문결과형식으로 변환하면 쉽게 추출할수 있다.

관리자의 분석요구에 따라 선택된 보고서형식은 질문으로 변환되여 실행되며 추출된 질문실행결과는 PostgreSQL(판본 9.0이상)의 JSON에 의한 질문결과를 일반형식으로 변환하는 기능을 리용하여 형식을 변환한다. 변환된 자료는 선택된 보고서형식으로 현시되고 이 보고서를 가지고 관리자는 로그자료에 대한 종합적인 심사를 진행할수 있다.

보고서추출과정은 그림 3과 같다.

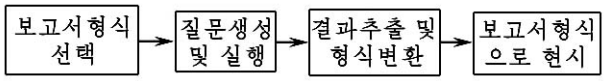

그림 3. 보고서추출의 동작흐름

2014년 3월 비루스검사결과보고서추출을 위한 SQL실례는 다음과 같다.

```
SELECT
 data->>'virustype'as  Virustype,
 data->>'virusresult'as  Virusresult
 data->>'filename'as  Filename
 FROM  log_datas
WHERE   data->>'checktype'='viruscheck'  and   checkdate >= '2014-3-1' and checkdate <= '2014-3-31'
```

이때 추출된 보고서형식은 표와 같다.

표. 추출된 보고서의 형식

Virustype	Virusresult	Filename
Worm	success	1.exe
⋮	⋮	⋮

맺 는 말

망보안문제들에 대한 조사자료와 심사수단을 제공하는 망보안중계기의 로그분석체계를 정의하고 실현함으로써 정보보안설비로서의 망보안중계기가 정보보안의 심사가능성을 만족시킬수 있도록 하였다.

참 고 문 헌

[1] L. K. Joshila Grace; International Journal of Network Security & Its Applications(IJNSA), 3, 1, 102, 2011.

[2] Mahdi Sahlabadi; Journal of Computer Science, 10, 3, 393, 2014.

주체104(2015)년 9월 5일 원고접수

On Log Analysis Subsystem in Gap System

Yom Song Ho, *Kim Song Hun*

We define and implement the log analysis subsystem which can be examinable with analysis data and tool.

The suggested method shows that gap system can be examinable according to information system's security policy.

Key words: log analysis subsystem, security policy