



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0009811
(43) 공개일자 2011년01월31일

(51) Int. Cl.

H04L 12/22 (2006.01) H04L 12/26 (2006.01)

G06F 11/30 (2006.01) G06F 21/00 (2006.01)

(21) 출원번호 10-2009-0067205

(22) 출원일자 2009년07월23일

심사청구일자 2009년07월23일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 공동 220번지 충남대학교

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블
3101동 501호

한신대학교 산학협력단

경기 오산시 양산동 한신대학교내

(72) 발명자

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블
3101동 501호

김태수

경기도 가평군 가평읍 읍내9리 445-2번지

(뒷면에 계속)

(74) 대리인

특허법인태동

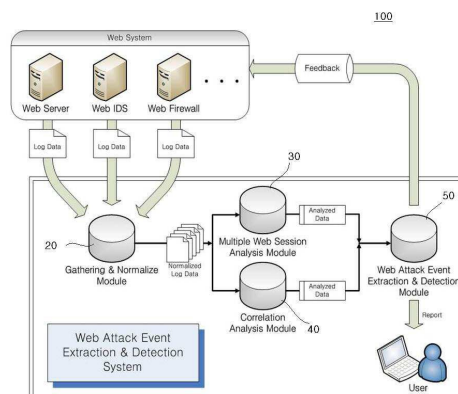
전체 청구항 수 : 총 16 항

(54) 감사자료 기반의 웹공격 이벤트 추출 시스템 및 방법

(57) 요약

본 발명은 감사자료 기반의 웹 공격 이벤트 추출 시스템에 관한 것으로, 웹IDS를 통해 웹 로그를 분석하여 공격을 탐지하는 웹 공격 이벤트 추출시스템에 있어서, 웹 로그, 방화벽 로그, 시스템 로그 정보를 수집하여 통합로그정보를 생성하는 통합로그 생성 및 생성된 통합로그정보를 정규화하는 통합로그 수집 및 정규화모듈과, 정규화된 통합로그정보를 분석하는 다중 웹 세션분석모듈과, 정규화된 통합로그정보의 상관관계를 분석하는 상관분석모듈과, 상기 다중 웹 세션 분석모듈과 상관분석모듈로부터 분석된 데이터를 토대로 웹 공격이벤트를 탐지 및 추출하는 웹 공격탐지 및 추출모듈을 포함하여 이루어진 것을 특징으로 한다.

대표도 - 도28



(72) 발명자

김득용

경기도 수원시 권선구 평동 14-5

윤하나

경기도 오산시 양산동 286-2 한신오피스텔 C동 20
5호

특허청구의 범위

청구항 1

웹IDS를 통해 웹 로그를 분석하여 공격을 탐지하는 웹 공격 이벤트 추출시스템에 있어서,
 웹 로그, 방화벽 로그, 시스템 로그 정보를 수집하여 통합로그정보를 생성하는 통합로그 생성 및 생성된 통합로그정보를 정규화하는 통합로그 수집 및 정규화모듈과,
 정규화된 통합로그정보를 분석하는 다중웹세션분석모듈과,
 정규화된 통합로그정보의 상관관계를 분석하는 상관분석모듈과,
 상기 다중웹세션 분석모듈과 상관분석모듈로부터 분석된 데이터를 토대로 웹 공격이벤트를 탐지 및 추출하는 웹공격탐지 및 추출모듈을 포함하여 이루어진 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 시스템.

청구항 2

제 1 항에 있어서,
 상기 상관분석모듈은 정규화된 통합로그정보의 상관관계를 분석하여 상관관계 가중치 값을 계산하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 시스템.

청구항 3

제1 항의 감사자료 기반의 웹공격 이벤트 추출 방법을 이용한 감사자료 기반의 웹공격 이벤트 추출방법에 있어서,
 웹 로그, 방화벽 로그, 시스템 로그 정보를 수집하여 통합로그정보를 생성하는 제1 단계와,
 생성된 통합로그정보를 정규화하는 제2 단계와,
 정규화된 통합로그정보의 상관관계를 분석하여 웹 공격 이벤트를 추출하는 제3단계를 포함하여 이루어진 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 4

제 3 항에 있어서,
 상기 제3 단계에서 정규화된 통합로그정보의 상관관계를 분석하여 상관관계 가중치 값을 계산하는 제4 단계를 더 포함하여 이루어진 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출방법.

청구항 5

제 3 항에 있어서, 상관 관계 분석은 시간정보, 근원지 IP, 근원지 접속 환경 등에 대한 정보와 목적지 IP 및 URI 정보 등이 기록되어 있는 통합 로그내 시간 정보, 근원지 IP 정보, URL 정보를 중심으로 웹 로그와 웹 IDS 로그간 상관관계 분석하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출방법.

청구항 6

제 3 항에 있어서,
 상관관계를 분석하는 과정은
 웹 서버에 대한 DoS 공격 패턴 및 공격 이벤트를 추출하는 과정을 수행하는 것으로, 통합 로그내 웹 로그, 웹 IDS 및 방화벽 로그에 대한 분석을 통해 웹 서버에 대한 DoS 공격 이벤트를 추출하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 7

제 3 항에 있어서,
 통합 로그 정보를 대상으로 근원지 IP 및 목적지 IP를 분석하여 일정한 시간대에 폭주 형태로 발생한 공격을

탐지하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 8

제 3 항에 있어서,

상관 관계를 분석하는 과정은 통합 로그 정보를 토대로 상호 연관성을 분석하고, 세션내 로그 정보를 대상으로 SQL Injection 및 Parameter Injection 공격 등에 해당하는 이벤트를 추출하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 9

제 3 항에 있어서,

상관 관계 분석은

전체 통합 로그 정보에 대한 근원지 IP와 목적지 IP 간의 상관관계 분석

웹 IDS 시스템에 기록된 Alert 정보와의 상관관계 분석

세션내 근원지/목적지 IP 간 연관성 분석을 통해 DoS 공격 탐지

Injection 공격 상관관계 분석

근원지 IP와 사용자 접속 환경을 중심으로 동일 사용자에 대한 행위 분석

동일 사용자에 의해 기록/저장된 로그 정보에 대한 키워드 검색

동일 사용자에 의한 Injection 공격 탐지를 포함하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 10

제 3 항에 있어서,

통합 로그를 생성하는 과정은 각 로그 정보에서 공통적으로 가지고 있는 시간 정보, 클라이언트 IP 주소 값 및 URI 값을 선택적으로 비교하여 동일한 필드값을 가지고 있는 것을 하나의 통합 로그 정보로 생성하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 11

제 3 항에 있어서,

생성된 통합로그 정보는 크게 다음과 같이 두가지 형태로 구성되되,

- 웹 로그, 웹 방화벽 및 IDS 로그가 모두 연관성을 가지고 있어서 하나의 로그로 통합 생성되는 경우
- 웹 로그와 방화벽 로그만이 연관성을 가지고 하나의 로그로 통합되는 경우
- 웹 로그와 IDS 로그만이 연관성을 가지고 하나의 로그로 통합되는 경우
- 웹 로그는 방화벽 및 IDS와 연관성을 찾을 수 없어서 웹 로그만이 생성되는 경우

이와 같은 경우의 수에 따라서 각각의 로그 정보는 가중치 값을 다르게 설정하는 것을 특징으로 하며,

세가지 형태의 로그 모두 관련성이 있어서 하나의 로그로 통합된 경우라면 연관성 부분의 가중치 값을 상당히 높게 설정할 수 있는 반면, 웹 로그가 방화벽 또는 IDS와 연관성을 갖는 경우에는 중간 정도의 가중치를 갖게 되고, 마지막으로 웹 로그가 방화벽 및 IDS 로그와 연관성이 없는 경우 낮은 가중치를 갖게 되는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 12

제 3 항에 있어서,

상기 제3 단계에서 각각의 로그에 대해 개별적으로 가중치를 계산한 후에 각 개인별 세션을 중심으로 세션내 가중치 합을 다시 계산하면 하나의 세션에 대한 통합 가중치 값을 구하는 것을 특징으로 하는 감사자료 기반의

웹공격 이벤트 추출 방법.

청구항 13

제 3 항에 있어서,

DoS 공격인 경우 특정 시간대를 중심으로 각 통합 로그의 생성 회수를 측정하여 일정 임계치를 넘어설 경우 대량의 접속로그가 발생한 것이기 때문에 DoS 공격으로 간주하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 14

제 3 항에 있어서,

통합로그에 대한 DoS 공격은 특정 시간대를 중심으로 발생한 로그의 빈도수를 측정하여 일정 임계치 이상에 해당하는 트래픽이 도착하였을 경우 이를 검출하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 15

제 3 항에 있어서,

웹 서버에서의 SQL 및 파라미터 삽입 공격인 경우 통합 로그에서 우선 IDS 로그에서 탐지된 SQL 부분 관련 가중치 값을 상대적으로 높게 책정하여 이를 중심으로 공격을 탐지하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

청구항 16

제 3 항에 있어서,

다중 세션에 대해 우선 각각의 세션별로 SQL 공격 로그에 대한 탐지 과정을 수행하고 이를 토대로 SQL 공격에 대한 가중치 조정 과정을 수행하고,

다시 최종적으로 각 세션내 가중치 값을 다시 재계산하여 최종적으로 SQL 공격에 대한 검출 및 공격 탐지 기능을 수행하는 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 감사자료 기반의 웹 공격 이벤트 추출 시스템 및 방법에 관한 것으로, 더욱 상세하게는 웹 서버에서 생성되는 웹 로그 정보와 웹 방화벽 또는 웹 IDS에서 생성되는 Alert 정보, 시스템 로그 정보 등을 이용하여 종합적으로 웹 공격에 대응할 수 있는 감사자료 기반의 웹 공격 이벤트 추출 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 웹 사용자가 급증하면서 다양한 형태의 웹 서비스 공격이 발생하고 있다. 이에 대응하기 위해 웹 방화벽, 웹 IDS 등의 시스템이 도입되고 있으나 웹 공격에 대해 개별적인 탐지 및 대응 체계만을 제공하고 있다.

[0003] 웹 공격 기술의 발달로 인하여 기존 웹 로그 분석에 통한 공격 탐지 기술뿐만 아니라 웹 방화벽, 웹 IDS, 시스템 로그 등과 같은 감사 자료에 기반한 웹 공격 이벤트 추출 기술과 로그 상관관계 분석을 통한 웹 비정상 행위 탐지 기술이 요구되는 실정이다.

[0004] 기존 기법은 웹 방화벽, 웹 IDS, 시스템 공격 탐지가 개별적으로 처리되며, 로그 저장 및 공격 탐지 기능을 통한 탐지 규칙의 업데이트 과정이 부족한 문제점이 있다. 또한 감사 정보 등에 대한 활용 및 상관관계 분석이 이루어지지 않아 공격 이벤트 추출에 비효율적인 구조를 보이는 문제점이 있다.

[0005] 도 1은 종래기술에 따른 웹 로그 분석 시스템의 개략적인 구성도이고, 도 2는 종래의 웹 로그파일의 종류와 옵션을 나타낸 표이고, 도 3은 종래의 웹 방화벽에서의 차단정책 내용의 예를 나타낸 표이고, 도 4는 종래의 웹

침입탐지시스템(IDS)의 기능을 개략적으로 나타내는 구성도이고, 도 5는 종래의 웹 로그수집 기법인 클러스터링 기법을 나타낸 도면이고, 도 6은 종래의 웹 로그 전처리기법을 설명하는 시스템 구성도이고, 도 7은 종래의 웹 로그 정보기반 상관처리과정을 나타낸 시스템 구성도이고, 도 8은 종래의 공격 시나리오 기반 정보(ALERT) 상관(CORRELATION) 과정을 나타낸 도면이다.

[0006] 기존 웹 로그 분석 시스템 구조

[0007] 웹 로그 분석 기법은 웹 서버에서 생성된 로그와 추가 정보에 대하여 정제 및 사전처리 절차를 수행하고 이를 토대로 웹 로그에 대한 분석 결과를 제시하는 방법이다. 도 1은 기존의 웹 로그 분석 시스템의 개략적인 시스템 구성도이다. 도 1을 참조하면, 기존의 웹 로그 분석 시스템 구조는 웹 서버가 서비스를 제공하면서 생성되는 로그파일(LogFile)을 분석하여 웹 서버의 트래픽(Traffic) 및 에러상태, 그리고 방문경로 등 기본적인 분석을 수행한다. 웹 로그 분석 시스템은 전처리 과정을 수행한 후 생성/가공된 웹 로그 정보를 일정한 주기로 분석하여 그 결과를 관리자에게 전송한다.

[0008] 기존 웹 로그 포맷 분석

[0009] 웹서비스에 대한 로그는 콘텐츠의 사용을 분석하는데 있어 일반적인 통계자료로 이용될 수 있다. 도 2는 로그 파일의 종류와 옵션에 대한 설명을 나타낸 표이다.

[0010] 이외에 다양한 로그 파일들은 각각의 설정이 있으며 대부분 옵션으로 존재 한다. 가장 많이 쓰이는 것은 AccessLogFile과 ErrorLogFile이다. httpd를 관리하는 입장에서 접속정보와 오류정보만으로도 웹 분석에 충분한 정보를 얻을 수 있기 때문이다. 그렇기에 시스템의 자원을 더 사용할 필요 없이 두개의 파일만을 저장한다.

[0011] 기존 웹 방화벽 로그 분석

[0012] 방화벽은 외부망과 연동하는 유일한 창구로서 외부로부터 내부망을 보호하기위해 각 서비스별로 서비스를 요구한 시스템의 IP 주소 및 port 번호를 이용하여 외부의 접속을 차단하거나 또는 사용자 인증에 기반을 두고 외부접속을 차단한다. 또한 상호 접속된 내외부 네트워크에 대한 트래픽을 감시하고 기록하는 기능을 수행한다.

[0013] 방화벽에서는 외부로부터 불법적인 접근이나 해커의 공격으로부터 내부 네트워크를 방어하기 위해 내부 네트워크와 외부 네트워크 사이의 통로에 설치하여 두 네트워크간의 트래픽을 제어하는 기능을 제공한다. 방화벽에서는 패킷의 IP 헤더 정보에 대한 분석을 통해 비인가된 서비스 접속에 대한 허용 또는 차단 정책을 설정하고, 내/외부간 네트워크 사용자에게 대한 통제 및 트래픽 감시 기능을 제공하게 된다.

[0014] 도 3은 방화벽에서의 차단정책 내용 예시표를 나타낸 도면이다. 도 3을 참조하면, 일반적인 차단 정책은 출발지 IP 및 포트, 도착지 IP/포트, 프로토콜 및 허용여부, 허용 시간 정보와 같은 8가지 정보로 구성된다. 방화벽 관리자는 아래와 같은 설정을 통해 정책을 설정하고 이를 기반으로 방화벽 시스템에서는 각 패킷에 대해 정책 부분을 적용하게 된다.

[0015] 기존 웹 IDS 로그 분석

[0016] 가. 침입탐지(Intruduction Detection System : IDS) 기술

[0017] IDS는 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다.

[0018] 침입탐지시스템은 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그파일 분석에서부터 복잡한 실시간 침입탐지시스템까지 다양한 소프트웨어가 존재한다. 침입탐지 기법은 크게 비정상적인 침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다.

[0019] 즉, 침입탐지 시스템이라는 것은 허가를 받지 않은 침입자가 비정상적인 방법으로 접근을 시도하거나 네트워크를 마비시키려는 시도, 혹은 시스템 전체를 장악하려는 프로세스등을 감시하고 찾아 내는 시스템이다. 따라서 이미 네트워크에 침입했거나 침입하려는 시도를 검출하고 그 자료를 기록하거나 역추적, 혹은 세션을 종료하는 등의 기능을 할 수 있다.

- [0020] 도 4는 침입탐지시스템의 기능을 설명하기 위한 개념도이다
- [0021] 나. 침입탐지시스템의 기능(도 4 참조)
- [0022] 데이터 수집 : 대상 시스템에서 제공하는 사용 내역 및 네트워크상의 패킷등 탐지 대상에서 생산되는 데이터 수집한다.
- [0023] 가공 및 축약 : 수집된 감시 데이터를 침입 판정에 사용할 수 있도록 의미 있는 정보로 전환하고, 새로운 침입 패턴의 기록 관리 및 분석 결과에 대한 LOG 기록, DB 생성한다.
- [0024] 분석 및 탐지 : 가공된 데이터를 이용 침입 여부를 판정, 비정상 행위 탐지 기술과 오용 탐지 기술로 분류한다. 이는 IDS의 핵심단계라고 할 수 있다.
- [0025] 보고 및 대응 : 침입 판정시 자동으로 적절한 대응을 하거나 관리자에게 보고 하여 조치를 취하도록 한다.
- [0026] 다. 공격 탐지 방식
- [0027] 비정상 침입 탐지 : 이는 감시되는 시스템의 일반적인 행위를 분석하고, 패턴을 생성하여 이로부터 벗어나는 행위를 침입으로 분류하는 방식이다.
- [0028] 오용탐지 : 알려진 침입행위를 분석 패턴화하여 이와 유사하거나 동일한 행위를 침입으로 간주하는 방식이다.
- [0029] **기존 웹 로그 수집 및 분석 기법**
- [0030] □ 기존 웹 로그 전처리 기법(도 6 참조)
- [0031] Clustering 기반 전처리 기법: 유사한 성격을 가지는 item을 그룹화 하는 기법으로 User Clusters, Page Clusters로 구분 할 수 있음(도 5 참조).
- [0032] Classification 기반 전처리 기법 : 다양한 데이터를 사전에 정해진 Class로 분류하는 과정. Decision Tree, Neural Network 기법을 사용함.
- [0033] Sequential Patterns 전처리 기법 : 시간을 중심으로 item 또는 페이지 이동 패턴을 분류하기 위한 과정. Trend Analysis, Change Pont Detection Similarity Analysis 기법이 이용됨.
- [0034] Association Rule 전처리 기법 : 웹 사이트의 페이지 간에 연관 규칙을 탐색하기 위한 기법. Market Basket Analysis, Neural Network 기법이 이용됨
- [0035] **기존 상관관계 분석 기법**
- [0036] □ 기존 상관관계 분석 기법
- [0037] 가. Alert Correlation 방법
- [0038] Alert Correlation 과정은 도 7과 같이 일반화할 수 있다. 도 7에 도시된 바와 같이 다양한 형태의 네트워크 장비로부터 생성되는 로그 정보 등에 대해 IDMEF 형태로 전송하면 이를 수집하여 전처리 과정을 수행하게 된다. 전처리 과정에서는 Logical predicate 모듈을 수행하고 이를 기반으로 다음 단계에서는 Alarm analysis 과정을 수행하게 된다. 이 과정에서는 유사도 측정, 클러스터링 및 퓨전 기반 통합 과정을 거쳐 최종적으로 단 일화된 형태의 Alarm 메시지를 생성하게 된다. 마지막 세 번째 단계에서는 상관관계를 분석하게 되고 이를 토 대로 공격 이벤트를 추출하게 된다.
- [0039] 나. Rule 기반 Alert Correlation 방법
- [0040] 본 방식은 많은 관심과 주목을 받았던 방식으로 룰 생성 과정을 토대로한 전문가 시스템에서 참조한 방식이다. 구체적으로 본 방식에서는 if-then 룰을 개발하여 특정 영역에 해당하는 지식 정보를 룰 집합(rule set)으로 생성하고 이를 DB에 저장하게 된다. 룰 집합 내에는 형식 언어 형태로 정보를 표시하고 이를 연결하여 두 정보 간 관계성을 표현하게 된다. 사전요구사항 들로 구성된 정보에 대해 룰 기반으로 추론 과정을 수행하게 된다. 구체적으로 추론 엔진, 지식 DB 정보, 작업 메모리 정보들로 구성된다.
- [0041] 이와 같은 정보들을 이용하여 룰 추론(Rule induction) 과정을 수행하고 최적의 룰 값을 찾아가는 과정(Rule matching)을 수행한다.
- [0042] 다. Attack 시나리오 기반 Alert Correlation 방법

- [0043] 이 방식은 지식 기반 상호연관성 추출 방식으로, 룰 정보를 공격 시나리오에 기초하여 보다 상세한 내용으로 표기하여 연관성을 검출한다. 따라서 공격 시나리오에 대해 보다 명시적으로 구성하기 위해 LAMBDA와 ADeLE와 같이 특정 형태의 언어를 사용하게 되며 최근 많은 관심을 보이는 분야이기도 하다. LAMBDA 언어는 모든 Alert 값을 IDMEF 포맷을 이용하여 모델링하며 각 공격에 대해 아래와 같은 다섯가지 필드 값으로 정의하게 된다.
- [0044] - Attack pre-condition : 공격이 성공하기 위해 필요로하는 조건 등을 명시하는 논리적 요구사항을 정의한다.
- [0045] - Attack post-condition : 공격이 성공하였을 경우 발생하는 효과 등에 관해 명시적으로 논리적 요구사항을 정의한다.
- [0046] - Attack scenario : 공격이 수행될 경우 침입자에 의해 수행되는 이벤트 들의 조합을 정의한다.
- [0047] - Detection scenario : 공격이 발생하였을 경우 이를 검출하는데 필요한 이벤트들의 조합을 정의한다.
- [0048] - Verification scenario : 공격이 성공하였을 경우 이를 확인하기 위한 이벤트 들의 조합을 정의한다.
- [0049] 라. Alert Correlation을 위한 표현 언어
- [0050] 공격의 pre-condition 및 post-condition 부분은 시스템 상태 정보와 관련된 사항들로 구성된다. 따라서 LAMBDA 언어에서는 공격에 대한 논리적 요구사항 및 관련 필요 사항들을 정의하게 된다.
- [0051] 도 8에 도시된 바와 같이 다수의 보안 시스템으로부터 수집된 Alert 정보들을 종합적으로 관리할 수 있는 시스템을 구축하고 이를 기반으로 Clustering 과정을 수행한다.

[0052] □ 기존 기법의 문제점

- [0053] 앞에서 제시한 기존 기법은 다중 IDS 시스템으로부터 Alert 메시지를 수집하여 그들간 연계성을 파악하는 기법이지만, 실제 공격 대상 웹 서버에 접속한 사용자에게 대한 Access 정보 등을 활용하지 않은채로 공격 위험도를 측정한다는 문제점이 존재한다. 즉, 기존 기법인 경우 IDS를 통해 공격 등이 탐지되었으나, 실제로 80포트를 통해 공격 대상 웹 서버에 접속한 공격자에 대해 단순히 IDS 시스템을 통해 탐지된 Alert 메시지만을 가지고 이상현상 및 공격 패턴을 추출하고자 한다는 점이다. 공격자의 접속에 대해 이상 현상 등이 있을 경우 단순히 IDS에서는 차단 기능을 수행하지 않고 단순히 Alert 메시지만을 제공하기 때문에 실제 공격자는 해당 웹 서버에서 다양한 형태의 공격을 수행할 수 있다. 이 경우 웹 서버에 대한 DoS 공격인 경우 기존 IDS Alert에서는 발견되지 않게 되므로 웹 서비스와 관련하여 새로운 관점에서 상관관계를 분석할 필요가 있다.

발명의 내용

해결 하고자하는 과제

- [0054] 본 발명의 목적은 웹 로그를 중심으로 IDS 및 방화벽으로부터 생성된 Alert 메시지를 같이 분석하는 시스템 및 방법을 제공하는데 있다.
- [0055] 본 발명의 또 다른 목적은 웹 서버에 대한 공격 패턴 중에서 DoS 공격, SQL Injection 및 명령어 Injection 공격인 경우 이를 탐지하고 공격 이벤트를 추출하기 위해 웹 로그와 웹 방화벽 및 IDS 시스템에서 발생하는 Alert 로그에 대해 통합된 형태의 로그를 생성하고 이를 기반으로 웹 서비스에 대한 상관관계를 분석하는 감사자료 기반의 웹공격 이벤트 추출 시스템 및 방법을 제공하는 데 있다.

과제 해결수단

- [0056] 상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따르면, 웹IDS를 통해 웹 로그를 분석하여 공격을 탐지하는 웹 공격 이벤트 추출시스템에 있어서, 웹 로그, 방화벽 로그, 시스템 로그 정보를 수집하여 통합로그정보를 생성하는 통합로그 생성 및 생성된 통합로그정보를 정규화하는 통합로그 수집 및 정규화모듈과, 정규화된 통합로그정보를 분석하는 다중웹세션분석모듈과, 정규화된 통합로그정보의 상관관계를 분석하는 상관분석모듈과, 상기 다중웹세션 분석모듈과 상관분석모듈로부터 분석된 데이터를 토대로 웹 공격이벤트를 탐지 및 추출하는 웹공격탐지및 추출모듈을 포함하여 이루어진 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 시스템이 제공된다.
- [0057] 본 발명의 다른 측면에 따르면, 감사자료 기반의 웹공격 이벤트 추출 방법을 이용한 감사자료 기반의 웹공격 이벤트 추출방법에 있어서, 웹 로그, 방화벽 로그, 시스템 로그 정보를 수집하여 통합로그정보를 생성하는 제1

단계와, 생성된 통합로그정보를 정규화하는 제2 단계와, 정규화된 통합로그정보의 상관관계를 분석하여 웹 공격 이벤트를 추출하는 제3단계를 포함하여 이루어진 것을 특징으로 하는 감사자료 기반의 웹공격 이벤트 추출 방법이 제공된다.

- [0058] 바람직하게는, 상기 제3 단계에서 정규화된 통합로그정보의 상관관계를 분석하여 상관관계 가중치 값을 계산하는 제4 단계를 더 포함하여 이루어진 것을 특징으로 한다.

효 과

- [0059] 이상 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템 및 방법에 의하면, 웹 공격 기술의 발달로 인하여 기존 웹 로그 분석에 통한 공격 탐지 기술뿐만 아니라 웹 방화벽, 웹 IDS, 시스템 로그 등과 같은 감사자료에 기반한 웹 공격 이벤트 추출 기술과 로그 상관관계 분석을 통한 웹 비정상 행위 탐지 할 수 있는 효과가 있다.

- [0060] 본 발명을 통해 개발된 감사 정보에 기반한 웹 공격 이벤트 탐지 기법을 이용할 경우 다중 웹 사용자 환경에서 생성되는 대용량의 웹 로그 및 웹 방화벽/IDS 기반 로그 정보를 대상으로 효율적 상관관계 분석 기능을 제공하여 능동적이고 효율적인 웹 로그 공격 이벤트 분석과 개선된 웹 공격 탐지/대응 기술을 제시할 수 있을 것으로 기대된다.

발명의 실시를 위한 구체적인 내용

- [0061] 이하, 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템 및 방법에 대하여 첨부도면을 참조로 상세히 설명한다.

- [0062] 도 9는 본 발명에 따른 감사자료 기반 웹관련 통합로그의 필드의 예를 나타낸 표이고, 도 10은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 통합로그 추출 및 생성과정의 일예를 나타낸 도면이고, 도 11은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그 정보 수집 알고리즘의 통합로그 생성과정을 나타낸 도면이고, 도 12는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그 형식 지정의 예를 나타낸 도면이고, 도 13은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그형식 지정방식의 일예를 나타낸 도면이고, 도 14는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 시간정보 형식지정이 항목의 예를 나타낸 도면이고, 도 15는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그 로드 과정을 개략적으로 나타낸 도면이고, 도 16은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 연관성을 이용한 로그 통합과정을 나타낸 도면이고, 도 17 및 도 18은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 문자열 처리를 위한 비-트리(B-TREE)와 인덱싱 과정을 나타낸 도면이고, 도 19는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 비-트리를 이용한 통합로그 인덱싱 과정을 나타낸 도면이고, 도 20은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 사용자 구분결과를 나타낸 도면이고, 도 21은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 웹 공격 이벤트 추출과정을 나타낸 도면이고, 도 22는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 공격에 대한 가중치를 계산하는 과정을 나타낸 도면이고, 도 23은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 프로그램 수행절차를 개략적으로 나타낸 도면이고, 도 24는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템을 구현하는 개발 프로그램의 그래픽화면의 일예를 나타낸 도면이고, 도 25는 도 24에서 세션분류결과를 나타낸 도면이고, 도 26은 도 24에서 상관관계 분석의 예를 나타낸 도면이고, 도 27은 도 24에서 프로그램 작업내역을 나타낸 도면이고, 도 28은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템을 개략적으로 나타낸 도면이고, 도 29는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서 다양한 웹관련로그를 통해 웹 공격 이벤트를 추출하는 과정을 개략적으로 나타낸 도면이고, 도 30은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 다중세션 분석과정의 일예를 나타낸 도면이고, 도 31은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 상관관계 분석 기반 공격탐지모듈 및 시스템 통합과정을 개략적으로 나타낸 도면이다.

- [0063] 본 발명에서는 다음과 같은 발명을 수행하고자 한다. 우선 다중 웹 세션 및 로그 상관분석 기법을 개발하고자 하며, 다중 웹 세션 분석을 통한 공격 탐지 알고리즘을 개발한다. 다중 웹 세션 분석과 로그의 상관분석 기법을 설계/구현하여 최신 웹 공격에 대한 신속한 웹 공격 이벤트 추출 기술을 개발하고자 한다. 그 결과 웹 관련 정보를 토대로 공격 이벤트 추출 기술을 개발하고자 한다.

- [0064] 이하 본 발명에 관한 설명에 있어서, 이 분야에서 잘알려진 용어를 그대로 사용하며 그에 대한 개념정의 등 자세한 설명은 생략하기로 한다.
- [0065] □ 웹 관련 로그 정보 수집 알고리즘
- [0066] 통합된 로그 생성
- [0067] 본 발명에서는 형식이 다른 여러 로그들에서 정보를 추출하기에 웹 공격 이벤트 추출을 위해 필요한 정보들로 이루어진 통합된 로그를 제안한다. 각 로그들에서 추출된 정보들은 통합 로그에서 지정한 항목들로 저장되고 이렇게 여러 로그가 통합된 새로운 로그가 생성된다. 웹 로그, 웹 IDS 로그, 웹 방화벽 로그 등 서로 다른 형식의 로그들에서 통합 로그에 필드에 해당하는 정보를 추출하고 중복된 필드 정보의 연관성을 통해 로그를 통합시킨다.
- [0068] 도 9는 통합 로그 필드의 예를 나타낸 표이다.
- [0069] 도 10은 웹 로그, 방화벽 및 IDS 로그로부터 시간 정보, IP 및 URI 정보 등 공통적인 필드 특성을 기반으로 통합 로그를 생성하는 과정을 보인다.
- [0070] 제안한 웹 관련 로그 정보 수집 알고리즘의 모듈 구성
- [0071] 본 발명에서는 로그를 로드할 때, 다양한 형식의 로그들을 처리하기 위하여 사용자가 로그의 형식을 지정하고, 로그 모듈은 지정된 형식에 따라 로그를 불러옴과 동시에 처리하며, 처리된 정보를 이용하여 통합 로그의 각 필드들에 정보를 저장하고, 필드들의 연관성을 이용하여 로그를 통합시킨다.
- [0072] 가. 로그 형식 지정
- [0073] 텍스트로 이루어진 로그의 특성을 이용하여 불러올 로그 형식을 지정할 수 있다. 도 12는 로그 형식을 지정하는 예이다.
- [0074] 로그 형식 지정하는 방식은 도 13에 도시한 바와 같이, 로그가 텍스트로 이루어져있다는 특징을 이용한다. 로그 형식은 먼저 로그 텍스트의 시작 문자열을 의미하는 'Prefix' 와 로그에서 추출할 정보를 의미하는 'Feature' , 그리고 각 필드들의 뒤에 위치하는 고유 문자열을 의미하는 'Postfix' 로 이루어진다.
- [0075] 'Feature' 와 'Postfix' 는 하나의 쌍이며, 'Prefix' 와는 달리 여러 개가 존재할 수 있다.
- [0076] 로그 형식 지정의 요인들인 도 14에 도시한 바와 같이, 'Feature' 는 통합 로그에서 지정한 필드들이다. 로그의 'Feature' 설정을 시작함을 알리는 문자로 '[' 를 사용하고, 끝남을 알리는 문자로 ']' 를 사용한다. 로그 형식을 처리할 때, '[' 문자가 나오게 되면, 다음 ']' 문자가 나올 때까지의 문자열은 추출하고자 하는 정보를 의미한다. 지정된 로그 형식에서 'Feature' 로 지정된 문자열이 통합 로그에 필드 정보로 적용된다. 'Feature' 는 통합 로그에서 지정된 필드 외의 다른 정보는 필요치 않는다. 그런 항목들이 로그에 있을 때, 그 값은 필요 없는 정보를 의미하는 'Garbage' 로 지정한다. 'Garbage' 는 문자열로 '-' 로 표현한다.
- [0077] 'Postfix' 는 'Feature' 뒤에 붙은 고유 문자열로, 다음 'Feature' 와 구분하기 위해 사용된다. 로그는 하나의 텍스트이므로 정보를 추출하기 위해 적당한 구분자가 필요하다. 'Postfix' 는 바로 이 부분을 의미한다. 그러므로 'Postfix' 는 필히 지정되어야 한다.
- [0078] 통합 로그의 정보 중 필수 항목인 시간 정보는 날짜와 시간을 포함한 정보로, 로그마다 시간을 표현하는 방식이 다르기 때문에 추가적인 형식 지정 정보가 필요하다. 시간 정보의 형식 지정은 시간 정보를 문자열로 표현하는 C 표준 함수 'strftime' 와 같다. 'strftime' 은 시간 정보를 문자열로 생성하지만, 그에 반대되는 처리를 하는 함수가 없기에 시간 형식을 처리할 수 있는 새로운 클래스를 구현하여 처리하였다.
- [0079] 나. 로그 형식에 따른 로그 로드
- [0080] 본 발명에서는 다양한 형식의 로그들을 로드하기 때문에, 각 로그마다 설정된 로그 형식을 이용하여 로드한다 (도 15 참조).
- [0081] 로그 파일에서 로드한 텍스트 형식의 로그는 지정된 로그 형식과 시간 형식을 이용하여 처리한다. 하나의 긴 문자열인 하나의 로그는 지정된 로그 형식을 참조하여 필요한 정보를 가지고 있는 문자열들만 추출한다. 추출된 문자열들은 통합 로그 필드의 성격에 맞게 변환한다. 시간 정보일 경우 시간 형식에 맞게 처리하여 하나의

정수 값으로 변환한다. 다른 정보들 역시 정수로 변환하거나 문자열 값의 경우 B-Tree에 넣어 인덱스 값으로 변환한다. 이런 과정을 거쳐 텍스트로 이루어진 로그는 컴퓨터로 연산하는데 문자열보다 빠른 속도를 보이는 숫자 값들로 변환된 로그로 만들어진다.

[0082] 로드하는 모든 로그들은 같은 작업을 통해 변환된 로그들로 생성된다. 변환된 로그들은 통합 로그의 필드 형식과 같은 구조로 이루어져 있다. 각 로그들은 시간 정보를 이용하여 정렬한다. 정렬에 경우 같은 시간이라면 로그가 생성된 순서도 중요하기 때문에 안정 정렬을 이용하였다.

[0083] 다. 연관성을 이용한 로그 통합(도 16 참조)

[0084] 로그 형식에 맞게 로드하여 변환된 로그들은 서로 목적이 다른 로그들에서 정보를 추출한 로그들이기 때문에, 같은 통합 로그 형식이라 해도 저장한 필드가 있고 저장하지 않은 필드 형식이 있다. 그리고 하나의 작업에 의해 각 시스템에서 중복되어 생성된 로그들도 있다. 이런 로그들은 하나의 로그로 통합할 필요가 있다.

[0085] 로그 통합의 기본적인 연관성 필드들은 시간 필드와 IP 필드가 있다. 시간 순서를 기준으로 로그를 비교하면서 로그에서 추출한 정보 중에 IP가 같은 경우 다른 필드들의 연관성을 검사한다. 연관성의 예로 요청한 URI나 Port 번호 등이 될 수 있다.

[0086] 연관성을 이용한 로그 통합의 과정을 통해, 몇 개의 로그들을 로드해도, 하나의 통합된 로그들을 생성한다. 다양한 목적과 형식의 로그들은 웹 공격 이벤트 추출을 위한 필요한 정보들만 가지는 하나의 통합된 로그로 변환된다.

[0087] 웹 관련 로그 정보 정규화 알고리즘

[0088] □ 제안한 웹 관련 로그 정보 정규화 알고리즘

[0089] 가. 숫자 항목 정규화

[0090] 숫자 항목의 경우는 웹 로그에서 클라이언트 요청에 대한 상태 코드인 'Status' 등이 있다. 로그에서 숫자로 저장해야 하는 정보들은 텍스트로 이루어져 있다고 해도 숫자 문자로만 이루어진 텍스트이다. 이 숫자 문자들은 단순한 연산을 통해 간단히 숫자로 변환할 수 있다. 숫자 문자는 아스키 코드로 되어 있어 간단한 뺄셈 연산으로 해당 숫자로 변환할 수 있고, 곱셈을 통해 자릿수를 판단하여 계산한다.

[0091] 나. IP 항목 정규화

[0092] IP 항목은 클라이언트를 판단하는 중요한 항목이다. 서버 IP, 클라이언트 IP 등이 IP 항목에 해당한다. IP의 경우는 32비트 주소체계인 IPv4와 128비트 주소체계인 IPv6가 있다. IPv4의 정보를 저장하기 위해서는 4Byte크기의 메모리 공간이 필요하며, IPv6의 정보를 저장하기 위해서는 16Byte크기의 메모리 공간이 필요하다.

[0093] Windows 개발환경에서 'WindSock2'를 이용해서 주소변환을 할 수 있다. 'WindSock2'에서 제공하는 함수 'WSAStringToAddress()'와 'WSAAddressToString()'를 이용한다. 'WSAStringToAddress()' 함수는 문자열로 이루어진 IP 주소를 소켓 통신을 위한 주소 정보로 변환한다. 이 주소 정보는 숫자로 이루어진 정보이기 때문에 변환된 값으로 이용할 수 있다.

[0094] 다. 문자열 항목 정규화

[0095] 로그가 텍스트로 이루어진 만큼 문자열로 이루어진 정보는 다양하다. 가장 기본적인 항목으로는 URI 항목이 있다. 이런 문자열들은 문자열 자체가 의미를 가지고 있기 때문에 특정 수치로 변환할 수 없다. 하지만 문자열을 그대로 처리하기에는 많은 문제점이 있다. 로그의 특성상 중복되는 문자열이 있을 수 있으며, 중복 문자열을 감안하지 않더라도 문자열이 차지하는 메모리 공간은 일반적으로 숫자 값보다 크다. 그리고 문자열 연산에 소요되는 비용 역시 숫자 값보다 높다. 이런 문제점을 해결하기 위해 인덱스 기법과 B-Tree 구조를 이용하였다(도 17참조).

[0096] 본 발명에서 제안한 B-Tree 구조는 Key와 Value를 가지고 있고, Key를 이용해서 B-트리를 구성하며, Key는 고유한 값을 가져야 한다. 이때 Key로 사용되는 것이 로그에서 추출된 문자열 항목들이고, Value는 Key에 부여된 인덱스 값이다.

[0097] 문자열 항목을 Key로써 B-Tree 구조에 삽입하면, B-Tree 내부에서 Key가 위치할 적당한 위치를 찾는 연산을 수행한다. 만일 Key가 B-Tree 내부에 이미 존재하게 되면 그 Key가 가지고 있는 인덱스 값인 Value를 반환하게 된다. 삽입된 Key가 B-Tree 내부에 없는 새로운 Key라면 해당 Key의 Value에 중복되지 않은 인덱스를 부여하고

인덱스 리스트에 추가한다. 위와 같은 연산을 통해, 각 문자열 항목들은 자동으로 중복되는 문자열에 대한 문제를 해결하며 고유 인덱스를 부여받게 된다(도 18참조).

[0098] 처리하고자 하는 문자열은 대수시간의 비교를 통해 인덱스 값을 변환할 수 있고, 인덱스 리스트에서 직접적인 접근으로 인덱스에 해당하는 문자열을 바로 가져올 수 있다. 문자열 항목에 인덱스를 부여함으로써 검색 및 연산, 상관관계 분석 등에 문자열 연산을 수치 연산으로 대체할 수 있어서 문자열 처리의 문제점을 해결할 수 있기에 문자열 처리에 드는 비용을 감소시킬 수 있다(도 19 참조).

[0099] 라. URL 항목 정규화

[0100] 본 발명에서 기반이 되는 로그는 웹 로그이다. 웹 로그에서는 필수적인 정보로 URL 정보가 있다. URL 정보는 기본적으로 문자열 항목의 처리와 마찬가지로 B-Tree와 인덱싱 기법을 사용한다. 하지만 웹 로그의 경우 IIS 웹 로그와 같이 URL 정보와 Query 정보가 필드로 나뉘어진 경우와 아파치 로그와 같이 URL 정보와 Query 정보가 URL 정보로 하나의 문자열로 이루어진 경우가 있다. URL과 Query는 다르게 처리하기 때문에, 두 정보가 분리되어 로깅되는 경우는 특별한 처리를 할 필요가 없지만 하나의 정보로 이루어진 경우 추가적인 작업을 수행해야 한다.

[0101] 본 발명에서는 URL 정보 부분을 URI라 정의하고 Query 정보 부분을 Query라 정의하였다. 그리고 두 정보가 통합된 부분을 URL이라 정의하였다. 이렇게 정의하여 로그 정보에 맞는 처리를 할 수 있도록 구현하였다.

[0102] **정보 정규화의 수행**

[0103] 로그 정보의 정규화는 지정된 로그 형식에 따라 로그를 로드함과 동시에 수행된다. 로그의 양은 방대하기 때문에, 전체 로그를 대상을 정보들을 문자열로 추출한 이후에 추출된 전체 문자열에 대해 정규화 작업을 실행시키게 되면 텍스트로 추출된 정보를 임시로 저장하는 공간만큼의 메모리 비효율을 가지게 되며, 두 번의 순차작업이 수행되기 때문에 로그의 양이 많아질수록 시간적으로 비효율적이다. 그래서 정보가 문자열로 추출됨과 동시에 각 정보의 특성에 맞는 정규화 작업을 즉시 수행한다.

[0104] **□ 다중 웹 세션 분석 알고리즘**

[0105] 제안한 다중 웹 세션 분석 알고리즘

[0106] 가. 세션 분류 기법

[0107] 본 발명에서는 사용자의 세션을 분류하기 위해 웹 로그에서 다음과 같은 특정 필드 정보만을 이용하였다.

[0108] - IP Address : 클라이언트 IP 주소

[0109] - User Agent : 클라이언트 Agent 정보

[0110] - Date & Time : 클라이언트가 요청한 시간

[0111] 세션을 분류하기 위해 위의 로그 정보들을 이용하여 다음과 같은 조건을 모두 만족시키는 로그들을 하나의 세션으로 분류하였다.

[0112] - 같은 IP Address와 User Agent 정보를 가지는 로그

[0113] - 인접한 로그와의 시간적 인터벌이 15분 이하인 로그

[0114] 앞서 설명하였듯이, 본 발명에서는 기본 세션 분류 기법 중, 사용자 분류 기법으로 'IP Address & Agent Method'를 사용하고, 같은 사용자 내의 세션 분류 기법으로 세션 인터벌을 15분으로 지정한 'Standard Timeout Method'를 사용하여 세션을 분류하였다.

[0115] 나. 세션 분류 기법의 효율성

[0116] 본 발명에서 제안하는 웹 로그 처리 알고리즘은 대용량 웹 로그를 필드 단위로 분할하며, 탐색에 최적화된 알고리즘을 이용하는 검증된 방법이다. 현재 대용량화되고 있는 웹 로그에서 세션을 탐지하기 위해 웹 로그 정보의 문자열을 순차적으로 탐색하여 세션을 분류하고 있다. 그러나 본 발명에서는 웹 로그 세션 분류에 이용된 특정 필드의 추출과 함께 정규화 및 인덱스, B-Tree 구성을 통해 시간적인 비용을 감소시키는 개선된 세션 분류 알고리즘을 제공하고 있다.

[0117] 동일한 IP정보만으로 사용자를 분류하는 것은 정확한 User Identification 방법이 아니다. Proxy 서버를 사용

하거나 ISP업체의 비용 절감을 위한 유동 IP를 사용한다면 사용자의 IP만으로 사용자를 분류하기는 불가능하다. 실제 본 발명에서 실험한 웹 로그에서 같은 IP를 가지고 있지만 다른 User Agent를 가지고 있는 세션을 볼 수 있다.

- [0118] 도 20의 사용자 구분 결과를 보면 ‘210.122.170.6’의 IP 주소는 4개의 다른 Agent를 가지고 있다. 그러므로 다른 사용자로 분류가 된 것을 볼 수 있다. 이처럼 세션 분류 과정에서 사용되는 검색 기법은 필드 단위의 검색이며, 정규화된 IP 주소의 비교와 인덱스가 부여된 Agent 비교를 통해 수행되므로 문자열에 대한 순차적인 처리보다 훨씬 효율적이다.
- [0119] □ 통합로그 기반 상관관계 분석 알고리즘
- [0120] 제안한 상관관계 분석 기법
- [0121] 본 발명에서는 우선적으로 웹 로그, 방화벽 및 웹 IDS 로그를 대상으로 통합 로그로 생성하도록 하였다. 따라서 통합된 로그 정보를 분석하게 되면 웹 시스템의 이상 현상 등을 파악할 수 있게 된다. 결국 통합 로그에 기록된 웹 로그 정보와 웹 IDS, 방화벽에 의해 생성된 Alert 로그간 상관관계를 분석하게 된다.
- [0122] 즉, 웹 공격이 발생하였을 경우 웹 IDS에 의해 이를 탐지하게 되고 이는 해당 사용자에 대한 웹 로그 정보가 기록되게 된다. 따라서 일차적으로 웹 로그 정보와 웹 IDS 정보간의 연관성을 분석하여 상관관계 가중치 값을 계산하도록 하였다.
- [0123] 구체적으로 다음과 같은 세가지 조건을 중심으로 상관관계를 분석하도록 하였다.
- [0124] - 통합 로그내 시간 정보를 중심으로 웹 로그와 웹 IDS 로그간 상관관계 분석
- [0125] - 통합된 로그에서 동일 시간에 생성된 웹 로그, 웹 IDS Alert 정보를 이용하여 공격 이벤트를 추출하고, 또한 이 시간대 전후로 생성된 통합 로그 정보간 연관성을 분석한다.
- [0126] - 통합 로그내 근원지 IP 정보를 중심으로 웹 로그와 웹 IDS 로그간 상관관계 분석
- [0127] - 통합 로그내 근원지 IP 정보를 중심으로 동일 IP에서 접속한 사용자에 대한 웹 로그, 웹 IDS 로그 및 기타 방화벽 로그간의 연관성을 분석하고 이를 통해 웹 이상 현상을 판별한다.
- [0128] - 통합 로그내 URI 정보를 중심으로 웹 로그와 웹 IDS 로그간 상관관계 분석
- [0129] - 마찬가지로 통합 로그내 유사 또는 동일한 URI 정보를 갖는 웹 로그, 웹 IDS 로그에 대한 상호 연관성 분석을 통해 웹 서비스의 이상 유무를 판별하고 공격 이벤트를 추출한다.
- [0130] 위 세가지 조건에 대한 상관관계 분석 결과를 그래프 형태로 제시하여 연관성 정도를 손쉽게 확인할 수 있도록 하였으며 최종적으로 다중 세션을 분류하는 과정에 적용할 수 있었다.
- [0131] 웹 공격 이벤트 추출을 위한 상관관계 분석
- [0132] 가. 공격 이벤트 추출 대상 선정
- [0133] 웹 관련 서비스 환경에서 발생 가능한 공격을 분류하면 크게 웹 서버에 대한 공격과 웹 클라이언트에 대한 공격으로 나눌 수 있다. 클라이언트에 대한 공격 방법으로는 입력선택 제한을 회피하는 방법, 클라이언트에서의 검증을 회피하는 방법 등이 있으며, XSS 등과 같이 각종 스크립트 언어 등에 악성 코드를 삽입하여 전송하는 방법 등이 있다. 서버에 대한 공격은 버퍼 오버플로우 기반 공격, 널 문자열 공격, SQL 삽입 및 파라미터 삽입 공격 그리고 DoS 공격 등이 있다.
- [0134] 이와 같이 크게 두 가지 방식으로 나눌 수 있는 공격 패턴 중에서 웹 서버 로그, 웹 IDS 및 방화벽 등에 로그로 남겨지는 경우는 대부분 웹 서버에 대한 공격일 경우이다. 클라이언트에 대한 공격 기법인 경우 웹 서버 로그에는 관련 기록 등이 남아 있지 않기 때문에 본 발명에서 목적으로 하는 감사정보 기반 공격 이벤트 추출 등에는 해당되지 않는 것이라고 할 수 있다.
- [0135] 따라서 본 발명에서는 웹 공격 중에서 웹 서버에 대한 공격 기법을 대상으로 이에 대해 상관관계를 분석하고 공격 이벤트를 추출하는 기법을 제시하고자 하였다(도 21 참조). 특히 SQL 삽입, 파라미터 삽입 및 서버에 대한 DoS 공격에 대해 웹 로그 정보, 방화벽 및 IDS 로그 정보를 분석하고 공격 이벤트를 추출하는 기법을 제시하였다.
- [0136] 다중 세션 정보를 이용하여 각 세션간 상관관계를 분석하고 웹 공격 이벤트를 추출할 수 있는 기술을 발명하였

다. 현재 통합 로그 정보에는 시간정보, 근원지 IP, 근원지 접속 환경 등에 대한 정보와 목적지 IP 및 URI 정보 등이 기록되어 있다. 따라서 세션 정보를 토대로 상관관계를 분석하는 과정에서 우선 크게 두가지 형태의 공격 탐지를 목적으로 분석하였다.

- [0137] - 웹 서버에 대한 DoS 공격 수행
- [0138] - 웹 서버에 대한 DoS 공격 패턴 및 공격 이벤트를 추출하는 과정을 수행하는 것으로, 통합 로그내 웹 로그, 웹 IDS 및 방화벽 로그에 대한 분석을 통해 웹 서버에 대한 DoS 공격 이벤트를 추출한다.
- [0139] - 통합 로그 정보를 대상으로 근원지 IP 및 목적지 IP를 분석하여 일정한 시간대에 폭주 형태로 발생한 공격을 탐지하고 해당 이벤트에 대한 분석 기능을 제공한다.
- [0140] - 웹 서버에 대한 SQL 및 Parameter Injection 공격 등 수행
- [0141] - 통합 로그 정보를 토대로 상호 연관성을 분석하였고, 세션내 로그 정보를 대상으로 SQL Injection 및 Parameter Injection 공격 등에 해당하는 이벤트를 추출한다.
- [0142] 따라서 위 두 가지 공격 형태에 대한 이벤트 추출을 위해 우선 다음과 같은 과정을 수행하였다.
- [0143] - DoS 공격 상관관계 분석
- [0144] - 전체 통합 로그 정보에 대한 근원지 IP와 목적지 IP 간의 상관관계 분석
- [0145] - 웹 IDS 시스템에 기록된 Alert 정보와의 상관관계 분석
- [0146] - 세션내 근원지/목적지 IP 간 연관성 분석을 통해 DoS 공격 탐지
- [0147] - Injection 공격 상관관계 분석
- [0148] - 근원지 IP와 사용자 접속 환경을 중심으로 동일 사용자에 대한 행위 분석
- [0149] - 동일 사용자에 의해 기록/저장된 로그 정보에 대한 키워드 검색
- [0150] - 동일 사용자에 의한 Injection 공격 탐지
- [0151] 나. 웹 DoS 공격 이벤트 추출 방법
- [0152] 웹 서버에 대한 DoS 공격 이벤트를 추출하기 위해 우선 웹 로그, 웹 방화벽 및 IDS 시스템 로그를 대상으로 통합 로그를 생성하였다. 통합 로그를 생성하는 과정은 앞에서 제시한 것처럼 각 로그 정보에서 공통적으로 가지고 있는 시간 정보, 클라이언트 IP 주소 값 및 URI 값을 선택적으로 비교하여 동일한 필드값을 가지고 있는 것을 하나의 통합 로그 정보로 생성하였다. 이때 생성된 통합로그 정보는 크게 다음과 같이 두가지 형태로 구성된다.
- [0153] - 웹 로그, 웹 방화벽 및 IDS 로그가 모두 연관성을 가지고 있어서 하나의 로그로 통합 생성되는 경우
- [0154] - 웹 로그와 방화벽 로그만이 연관성을 가지고 하나의 로그로 통합되는 경우
- [0155] - 웹 로그와 IDS 로그만이 연관성을 가지고 하나의 로그로 통합되는 경우
- [0156] - 웹 로그는 방화벽 및 IDS와 연관성을 찾을 수 없어서 웹 로그만이 생성되는 경우
- [0157] 따라서 이와 같은 경우의 수에 따라서 각각의 로그 정보는 가중치 값을 다르게 설정할 수 있다. 즉 세가지 형태의 로그 모두 관련성이 있어서 하나의 로그로 통합된 경우라면 연관성 부분의 가중치 값을 상당히 높게 설정할 수 있는 반면, 웹 로그가 방화벽 또는 IDS와 연관성을 갖는 경우에는 중간 정도의 가중치를 갖게된다. 마지막으로 웹 로그가 방화벽 및 IDS 로그와 연관성이 없는 경우 낮은 가중치를 갖게 된다.
- [0158] 이렇게 각각의 로그에 대해 개별적으로 가중치를 계산한 후에 각 개인별 세션을 중심으로 세션내 가중치 합을 다시 계산하면 하나의 세션에 대한 통합 가중치 값을 구할 수 있다.
- [0159] DoS 공격인 경우 특정 시간대를 중심으로 각 통합 로그의 생성 회수를 측정하여 일정 임계치를 넘어설 경우 대량의 접속로그가 발생한 것이기 때문에 DoS 공격으로 생각할 수 있다.
- [0160] 따라서, 통합로그에 대한 DoS 공격은 특정 시간대를 중심으로 발생한 로그의 빈도수를 측정하여 일정 임계치 이상에 해당하는 트래픽이 도착하였을 경우 이를 검출하는 방식이다.

- [0161] 다. 웹 SQL 및 파라미터 삽입 공격 이벤트 추출 방법
- [0162] 웹 서버에서의 SQL 및 파라미터 삽입 공격인 경우 앞에서 제시한 통합 로그에서 우선 IDS 로그에서 탐지된 SQL 부분 관련 가중치 값을 상대적으로 높게 책정하여 이를 중심으로 공격을 탐지하게 된다.
- [0163] 다중 세션에 대해 우선 각각의 세션별로 SQL 공격 로그에 대한 탐지 과정을 수행하고 이를 토대로 SQL 공격에 대한 가중치 조정 과정을 수행한다. 다시 최종적으로 각 세션내 가중치 값을 다시 재계산하여 최종적으로 SQL 공격에 대한 검출 및 공격 탐지 기능을 수행하게 된다.
- [0164] 도 22에 도시된 바와 같이 통합로그 형태로 생성된 각각의 Alert 메시지에 대해 사용자가 설정한 공격 위험도 가중치 테이블의 값을 참조하여 각 필드별로 위험도를 계산하는 과정을 수행하게 된다. 통합로그에는 이미 기존의 IDS Alert 생성시 설정된 Priority 값이 있으나, 도 22에서와 같은 위험도 가중치값 재구성 과정을 통해 각 통합 Alert 메시지내 위험도 값을 계산하게 된다.
- [0165] 이렇게 각기 통합로그에 대해 Alert 값을 구하게 되면 다음단계에서는 로그 정보내 단일 세션에 대해 위험도 가중치 값을 제조정하거나 사용자별 위험도 가중치를 다시 얻는 과정을 수행하게 된다. 이와 같은 과정을 수행하게 되면 통합로그에 대한 공격 위험도 값을 객관적으로 얻을 수 있게 된다.
- [0166] **본 발명의 구현 결과 및 세부 모듈**
- [0167] **개발 시스템 구조**
- [0168] 프로그램 수행 절차(도 23 참조)
- [0169] 본 발명에서 제안한 알고리즘의 기능을 구현한 프로그램의 실행 주기는 다음과 같다. 1) 프로그램을 실행시키고, 2) 웹 로그 및 관련 로그들을 로드 시킨다. 3) 로드된 로그 정보를 이용하여, 관리자가 필요한 작업을 수행하고, 4) 프로그램을 종료한다.
- [0170] 로그를 로드하는 부분은 크게 두 가지로 나뉜다. 웹 로그를 로드하는 부분과 관련된 여러 로그들을 로드하는 부분이다. 로드하는 로그들은 지정된 로그 형식을 이용하여 필요한 정보를 추출하고 정규화 및 인덱싱 B-Tree를 이용하여 변환한다.
- [0171] 관리자는 로드된 정보를 이용하여, 로그에 접근한 사용자의 분류된 세션을 이용한 세션 분석과 상관관계 분석을 통한 공격 이벤트 추출 및 여러 통계적 정보를 그래프를 통해 시각적으로 분석할 수 있다.
- [0172] 일련의 작업들을 마치고 작업 결과 등을 저장하거나하는 작업을 거친 후 프로그램을 종료한다.
- [0173] 사용자 GUI 및 메뉴 구성(도 24내지 도 27참조)
- [0174] 본 개발 프로그램의 GUI는 (1) 기능별 메뉴, (2) 메뉴별 서브 메뉴, (3) 메인 작업 공간으로 크게 세 가지로 구분 할 수 있다. 그 외에는 로드한 로그에 대한 정보를 볼 수 있는 상태바와 선택한 메뉴에 대해 간단한 설명이 적힌 도움말 바가 있다. 도 24는 프로그램의 초기 화면이다.
- [0175] 가. 주요 기능별 메뉴
- [0176] 주요 기능별 메뉴를 살펴보면 ‘로그처리’, ‘세션분석’, ‘상관관계’, ‘정보’로 총 5개의 메뉴로 구성되어 있다.
- [0177] - 로그처리 메뉴 : 로그처리 메뉴의 주요 기능은 웹 로그 및 관련 로그들을 불러오거나, 불러오면서 전처리된 통합 로그를 저장하는 기능을 한다. 그리고 설정을 통해 로그 형식을 지정하거나 통합 로그의 필드 정보를 정의할 수 있다.
- [0178] - 세션분석 메뉴: 통합 로그 정보에서 세션 분석을 위한 정보를 추출해 사용자의 세션 정보를 추출 하여 동일한 세션의 로그를 분류할 수 있다. 세션 정보를 이용해 공격탐지에 적용해 한 세션에서 일어난 사용자의 행동 패턴 분석에 이용될 수 있으며, 기간별 세션의 접속 정보를 그래프 등의 방법으로 분석하여 보여준다.
- [0179] - 상관관계 메뉴: 통합된 로그에서 각 로그별 상관관계 분석, 사용자별 상관관계 분석, 세션별 상관관계 분석, 로그 필드 간의 상관관계 분석 등을 이용하여 웹 공격 이벤트를 추출하는 작업을 하는 메뉴이다. 현재 중간발표 단계에서는 상관관계 기법을 정립하고 있으며, 세션별 정보를 그래프로 표현하는 부분까지 구현되었다.
- [0180] - 정보 메뉴: 정보 메뉴는 프로그램 자체의 진행 사항 및 결과 등의 작업 내역을 볼 수 있으며, 통합된 로그의

정보를 볼 수 있다.

- [0181] 본 발명에서는 구체적으로 다중 웹 세션에 대한 분석 과정을 수행하고 세션과 웹 공격 관련 상관관계를 분석하는 기법을 제시하였다(도 28참조). 도 28을 참조하면, 감사자료 기반의 웹공격 이벤트 추출 시스템(100)은 웹 로그수집 및 정규화모듈(20)과, 다중웹세션 분석모듈(30)과, 상관관계 분석모듈(40)과, 웹 공격 이벤트탐지 및 추출모듈(50)로 구성된다. 상기 웹로그수집 및 정규화 모듈(20)은 웹로그를 수집하는 로그데이터수집부(21) 및 로그데이터 정규화부(22)를 포함한다.
- [0182] 이를 통해 대용량 웹 정보에 대한 공격 탐지 성능을 향상시키고 신속한 웹 공격 이벤트 추출 기능을 제공하였다(도 29참조). 본 발명을 통해 개발된 감사 정보에 기반한 웹 공격 이벤트 탐지 기법을 이용할 경우 대용량의 웹 로그 및 웹 IDS 정보에 대한 효율적 상관관계 분석 기능을 제공하여 능동적이고 효율적인 웹 로그 공격 이벤트 분석 및 웹 공격 탐지/대응 분야의 발전을 도모할 수 있을 것으로 기대된다.
- [0183] 구체적으로 본 발명에 따르면, 웹 공격 이벤트 추출 모듈의 세부 단계로 우선 다중 웹 세션 분류 알고리즘을 설계/구현하였다(도 30참조). 단일 서비스의 로그가 아닌 웹과 관련된 서비스들의 로그를 수집하고, 수집된 정보를 통합하고 필요한 정보를 추출하여 정규화 과정을 수행하였다. 이를 통해 정밀한 웹 세션 분류 기능을 제공한다.
- [0184] 또한 상관관계 분석 알고리즘을 설계/구현하였다. 각 웹 관련 서비스들에서 공격 로그 정보를 추출하고, 로그 정보들에 대한 상관관계 분석과정을 수행하여 다중 웹 세션과 상관관계 분석에 기반한 공격 탐지 기능을 제공하였다. 최종적으로 시스템 통합 과정을 통해 다중 웹 세션 분류와 상관관계 분석 모듈을 통합하고 웹 공격 이벤트 추출 모듈과 연동하였다(도 31 참조).

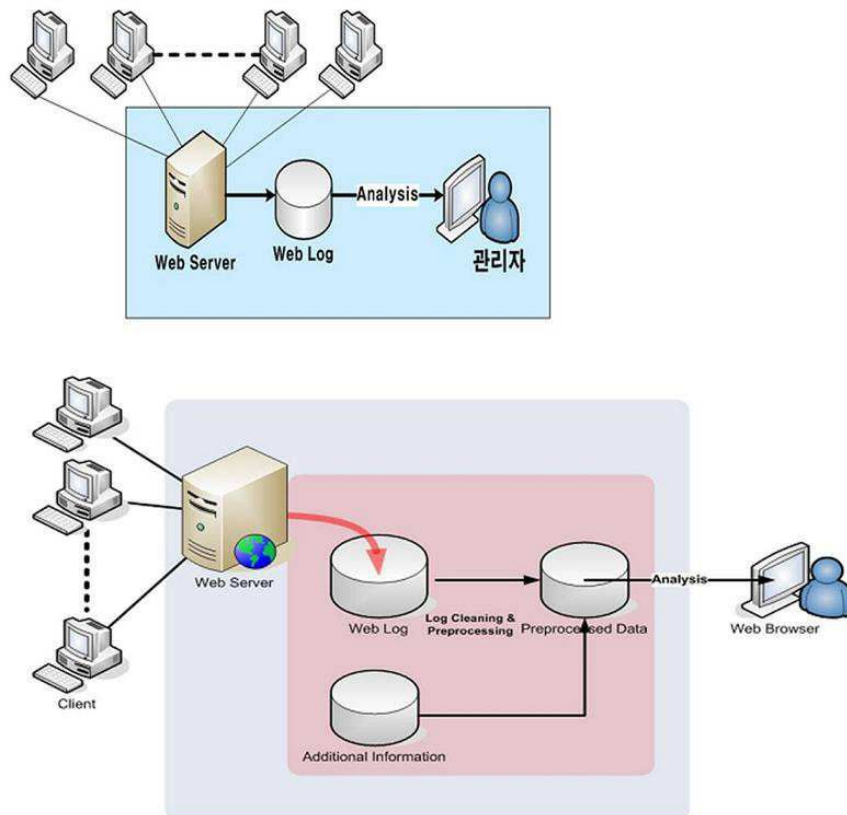
도면의 간단한 설명

- [0185] 도 1은 종래기술에 따른 웹 로그 분석 시스템의 개략적인 구성도이다.
- [0186] 도 2는 종래의 웹 로그파일의 종류와 옵션을 나타낸 표이다.
- [0187] 도 3은 종래의 웹 방화벽에서의 차단정책 내용의 예를 나타낸 표이다.
- [0188] 도 4는 종래의 웹 침입탐지시스템(IDS)의 기능을 개략적으로 나타내는 구성도이다.
- [0189] 도 5는 종래의 웹 로그수집 기법인 클러스터링 기법을 나타낸 도면이다.
- [0190] 도 6은 종래의 웹 로그 전처리기법을 설명하는 시스템 구성도이다.
- [0191] 도 7은 종래의 웹 로그 정보기반 상관처리과정을 나타낸 시스템 구성도이다.
- [0192] 도 8은 종래의 공격 시나리오 기반 경보(ALERT) 상관(CORRELATION) 과정을 나타낸 도면이다.
- [0193] 도 9는 본 발명에 따른 감사자료 기반 웹관련 통합로그의 필드의 예를 나타낸 표이다.
- [0194] 도 10은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 통합로그 추출 및 생성과정의 일례를 나타낸 도면이다.
- [0195] 도 11은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그 정보 수집 알고리즘의 통합로그 생성과정을 나타낸 도면이다.
- [0196] 도 12는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그형식 지정의 예를 나타낸 도면이다.
- [0197] 도 13은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그형식 지정방식의 일례를 나타낸 도면이다.
- [0198] 도 14는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 시간정보 형식지정이 항목의 예를 나타낸 도면이다.
- [0199] 도 15는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 로그 로드 과정을 개략적으로 나타낸 도면이다.

- [0200] 도 16은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 연관성을 이용한 로그 통합과정을 나타낸 도면이다.
- [0201] 도 17 및 도 18은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 문자열 처리를 위한 비-트리(B-TREE)와 인덱싱과정을 나타낸 도면이다.
- [0202] 도 19는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 비-트리를 이용한 통합로그 인덱싱과정을 나타낸 도면이다.
- [0203] 도 20은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 사용자 구분결과를 나타낸 도면이다.
- [0204] 도 21은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 웹 공격 이벤트 추출과정을 나타낸 도면이다.
- [0205] 도 22는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 공격에 대한 가중치를 계산하는 과정을 나타낸 도면이다.
- [0206] 도 23은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 프로그램 수행절차를 개략적으로 나타낸 도면이다.
- [0207] 도 24는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템을 구현하는 개발 프로그램의 그래픽화면의 일예를 나타낸 도면이다.
- [0208] 도 25는 도 24에서 세션분류결과를 나타낸 도면이다.
- [0209] 도 26은 도 24에서 상관관계 분석의 예를 나타낸 도면이다.
- [0210] 도 27은 도 24에서 프로그램 작업내역을 나타낸 도면이다.
- [0211] 도 28은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템을 개략적으로 나타낸 도면이다.
- [0212] 도 29는 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서 다양한 웹관련로그를 통해 웹 공격 이벤트를 추출하는 과정을 개략적으로 나타낸 도면이다.
- [0213] 도 30은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 다중세션 분석과정의 일예를 나타낸 도면이다.
- [0214] 도 31은 본 발명에 따른 감사자료 기반의 웹공격 이벤트 추출 시스템에서의 상관관계 분석 기반 공격탐지모듈 및 시스템 통합과정을 개략적으로 나타낸 도면이다.
- [0215] * 도면의 주요부분에 대한 부호의 설명 *
- [0216] 20: 로그데이터수집 및 정규화 모듈
- [0217] 21: 웹로그데이터 수집부
- [0218] 22: 웹로그데이터 정규화부
- [0219] 30: 다중웹세션 분석모듈
- [0220] 40: 상관관계 분석모듈
- [0221] 50: 웹 공격이벤트탐지 및 추출모듈
- [0222] 100: 감사자료 기반의 웹공격이벤트 추출시스템

도면

도면1



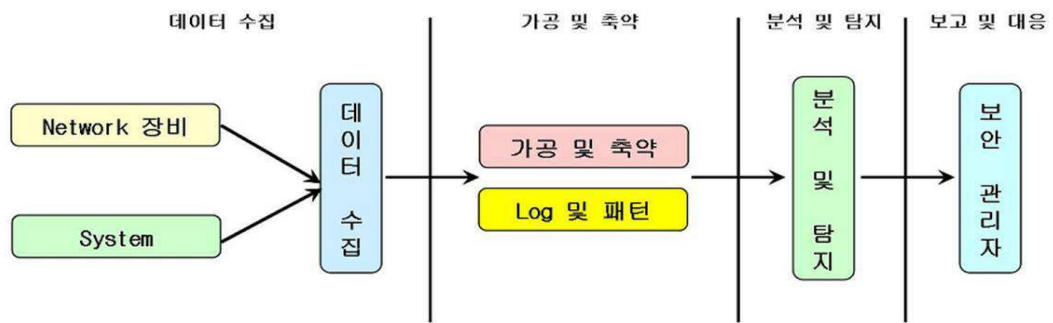
도면2

Log File & Option Type	Detail
Access Log	Set access log file name
ProxyAccessLog	Log proxy accesses to a different log file
CacheAccessLog	Log cache accesses to a different log file
ErrorLog	Set error log file name
LogFileDateExt	Common Time/Date extension to all log file names
LogFormat	Set access log file format
LogTime	Set time zone for log files
NoLog	No log entries for listed hosts/domains

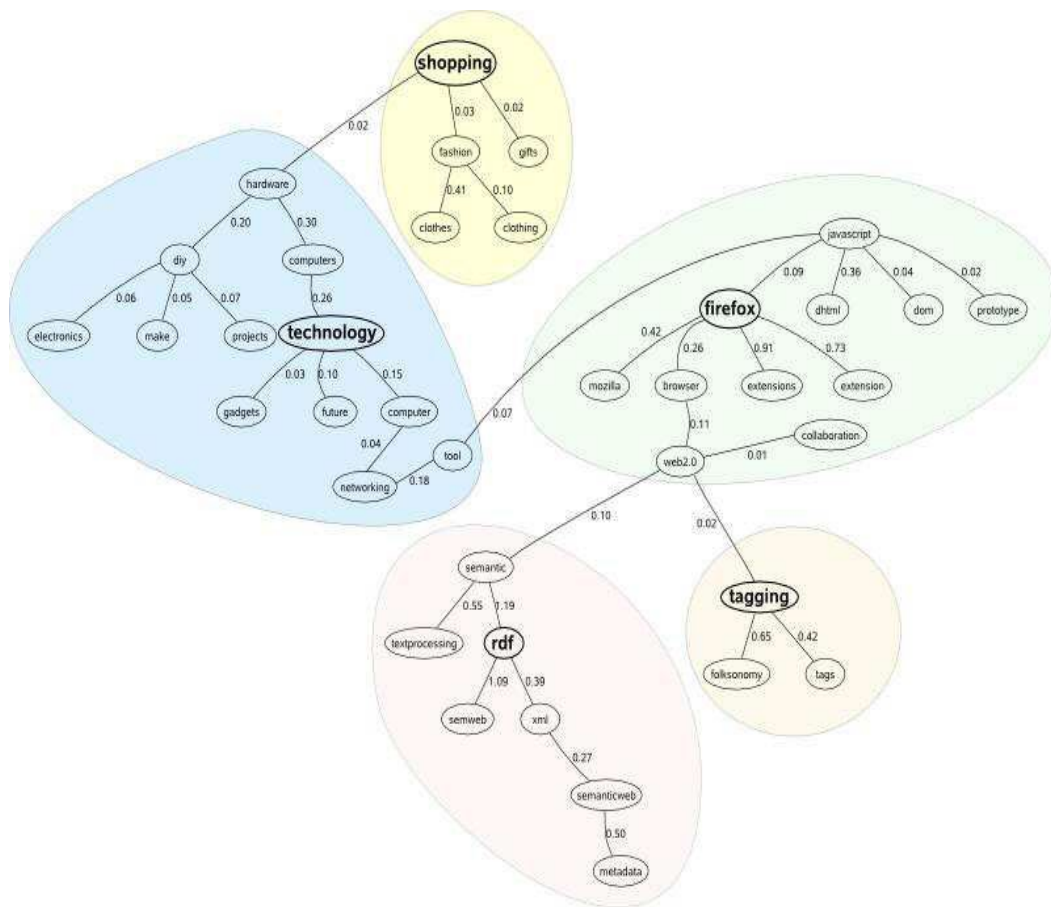
도면3

순번	출발지IP	출발지PORT	도착지IP	도착지PORT	프로토콜	허용여부	허용시간
1	any	any	1.1.1.1	80	TCP	허용	any
2	2.1.*.*	any	any	any	TCP	차단	any
3	3.1.*.*	any	any	any	TCP	허용	any
4	any	any	any	any	any	허용	any
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
99	any	any	any	any	any	차단	any

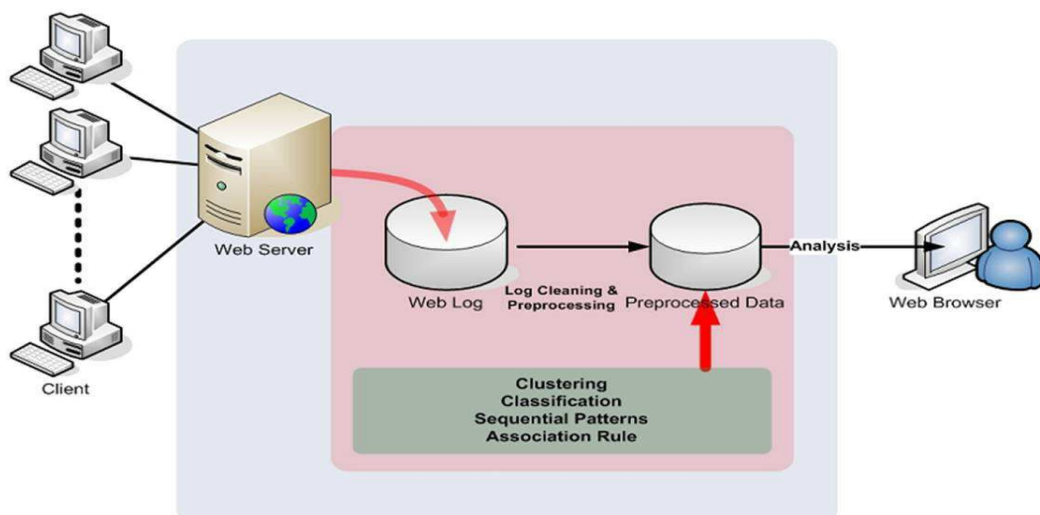
도면4



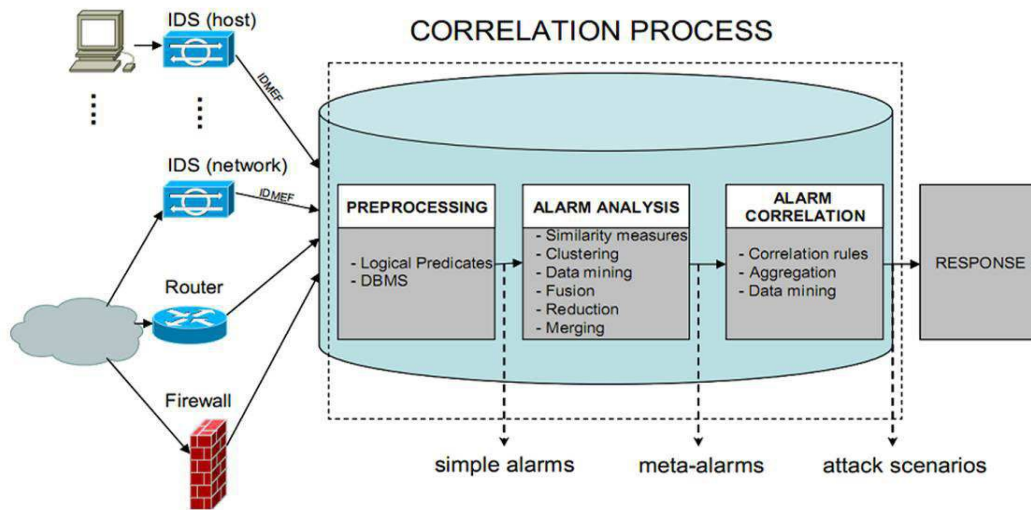
도면5



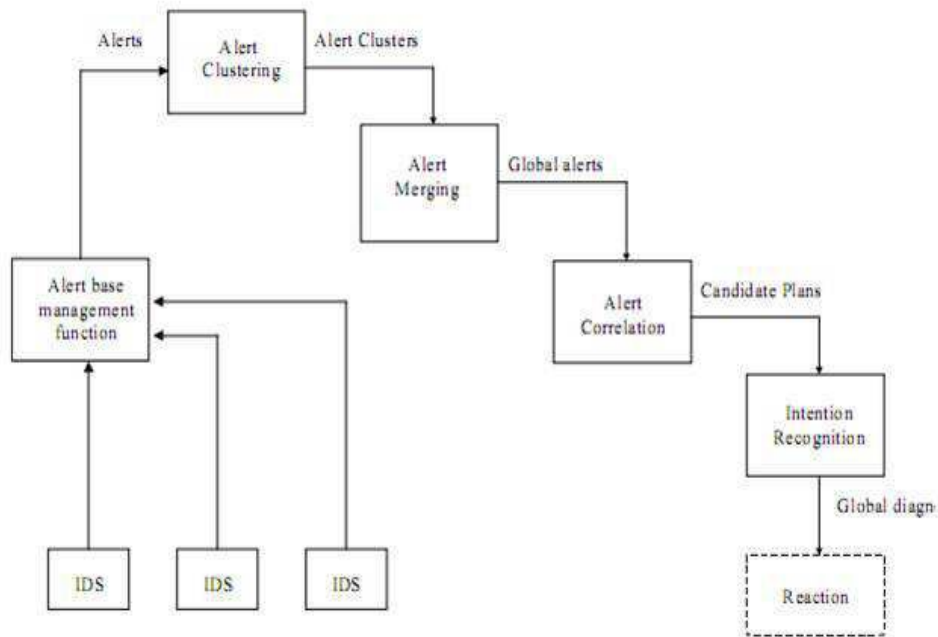
도면6



도면7



도면8



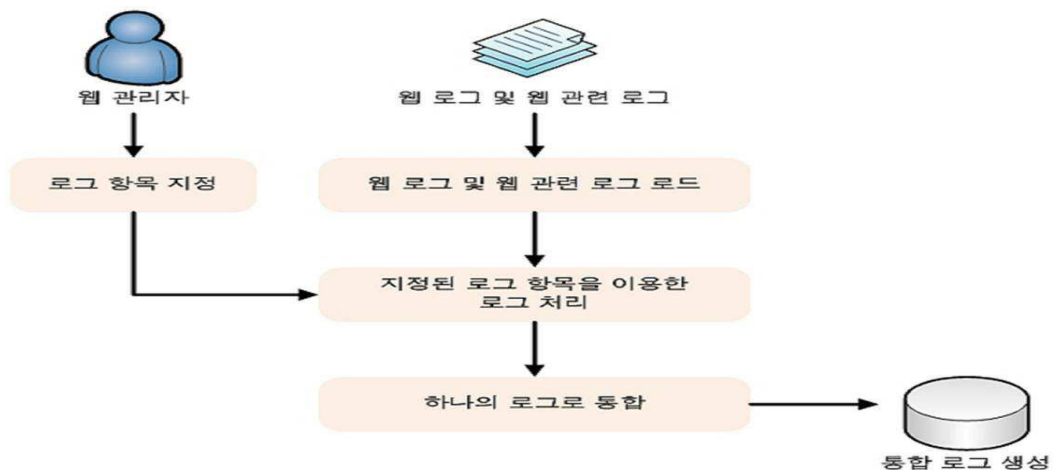
도면9

필드 이름	형식	의미	필드 이름	형식	의미
Time	Number	날짜, 시간	Agent	String	User Agent
Source IP	Number	IP 주소	URI	String	요청된 URI
Source Port	Number	Port 정보	Query	String	요청된 Query
Destination IP	Number	IP 주소	Status	Number	상태 코드
Destination Port	Number	Port 정보	Alert	Number	IDS의 경고

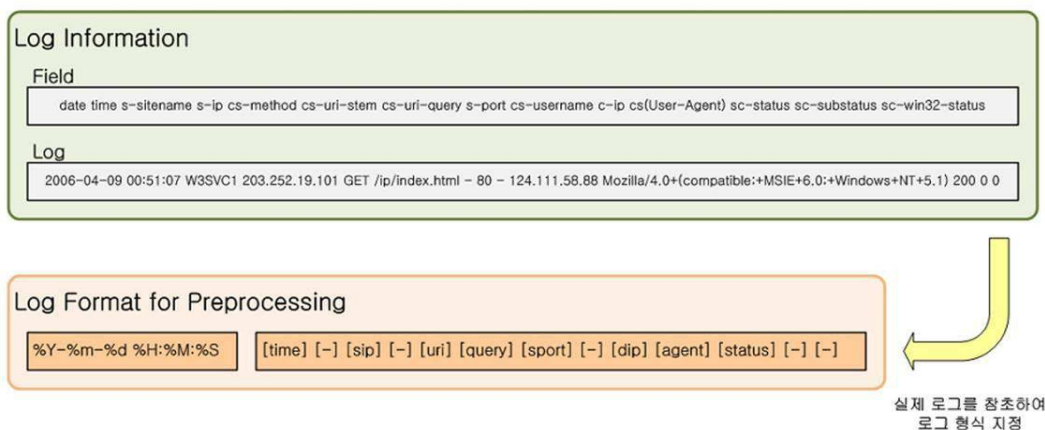
도면10



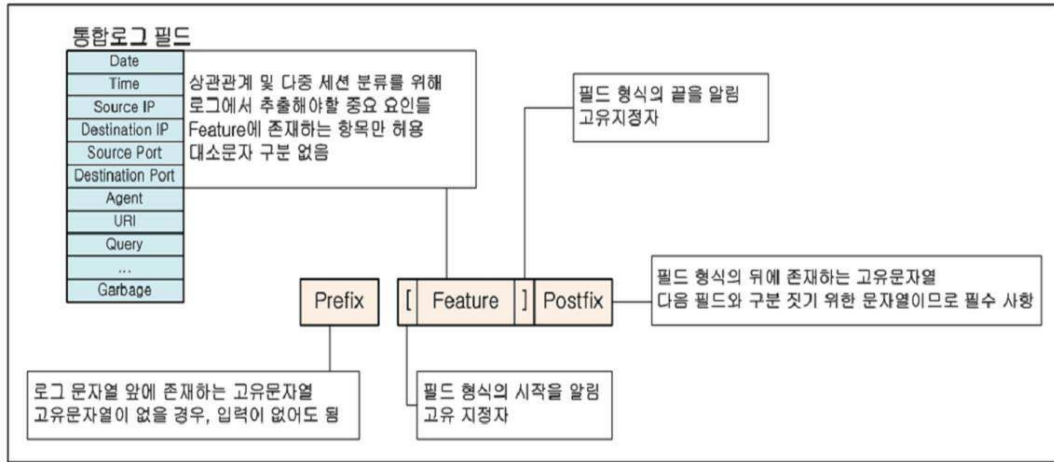
도면11



도면12



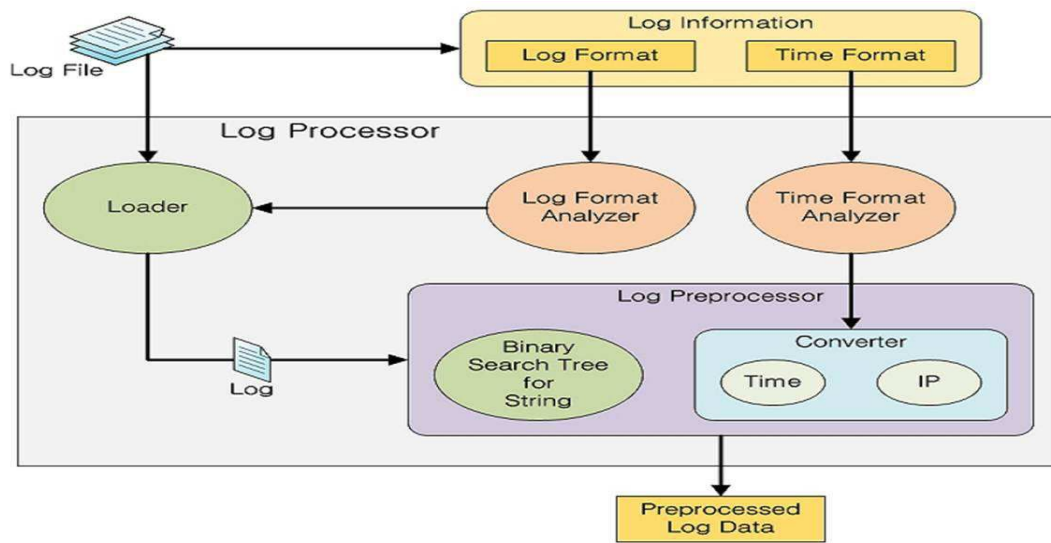
도면13



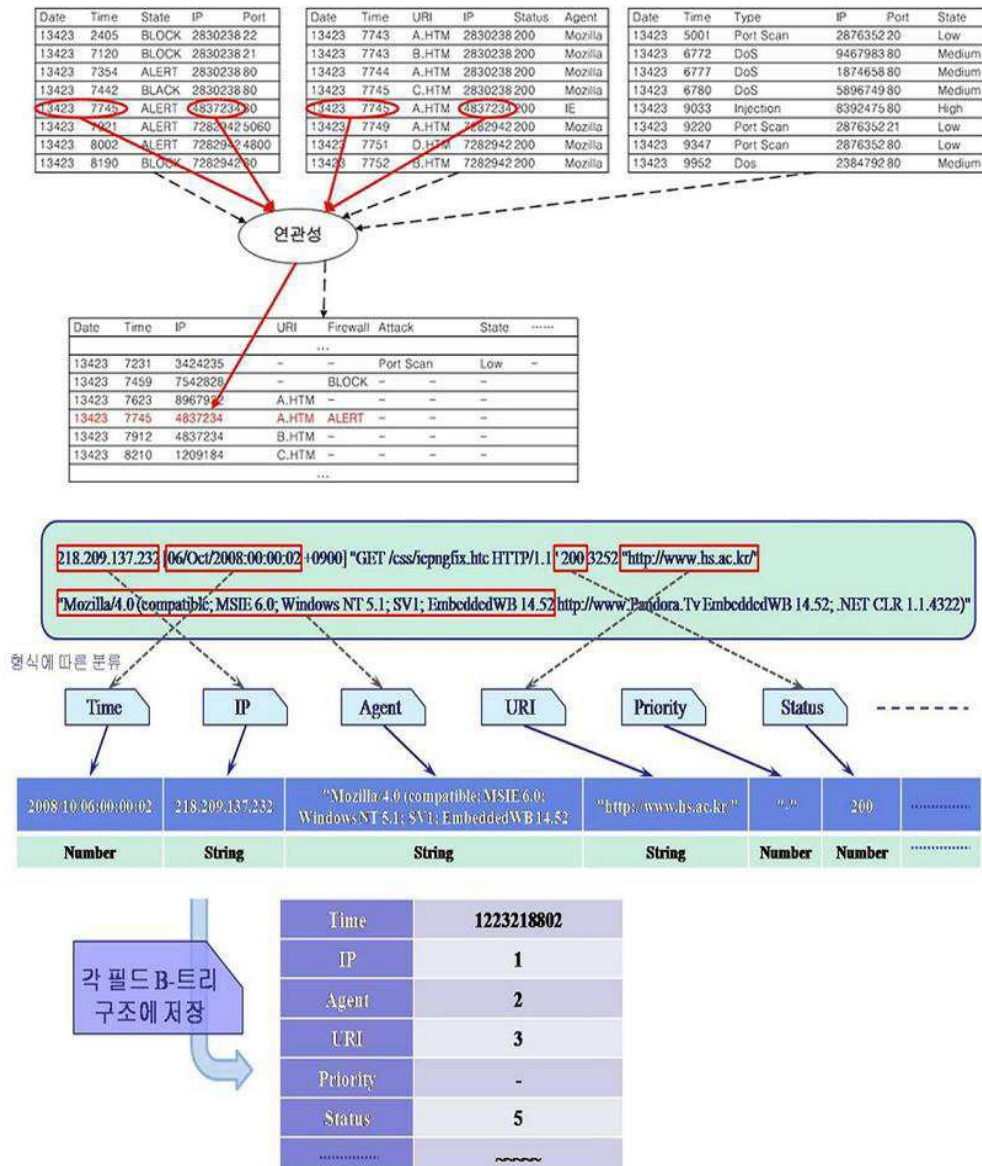
도면14

형식	설명	결과	예제
%a	요일	세 문자 영어 약어	Sun
%A	요일	영어 전체 이름	Sunday
%b	월	세 문자 영어 약어	Dec
%B	월	영어 전체 이름	December
%d	일	두 자리 (01-31)	10
%H	시	24시간 형식 두자리 (00-23)	00
%I	시	12시간 형식 두자리 (00-12)	12
%m	월	두 자리 (01-12)	12
%M	분	두 자리 (00-59)	39
%p	시	두 문자, AM 혹은 PM	AM
%S	초	두 자리 (00-59)	50
%y	년	두 자리 (00-99)	06
%Y	년	두 자리 (0000-9999)	2006
%%	%	한 문자, % 기호	%

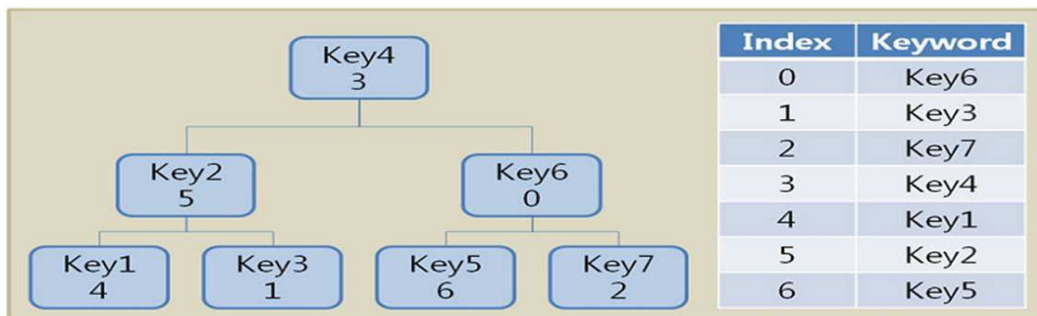
도면15



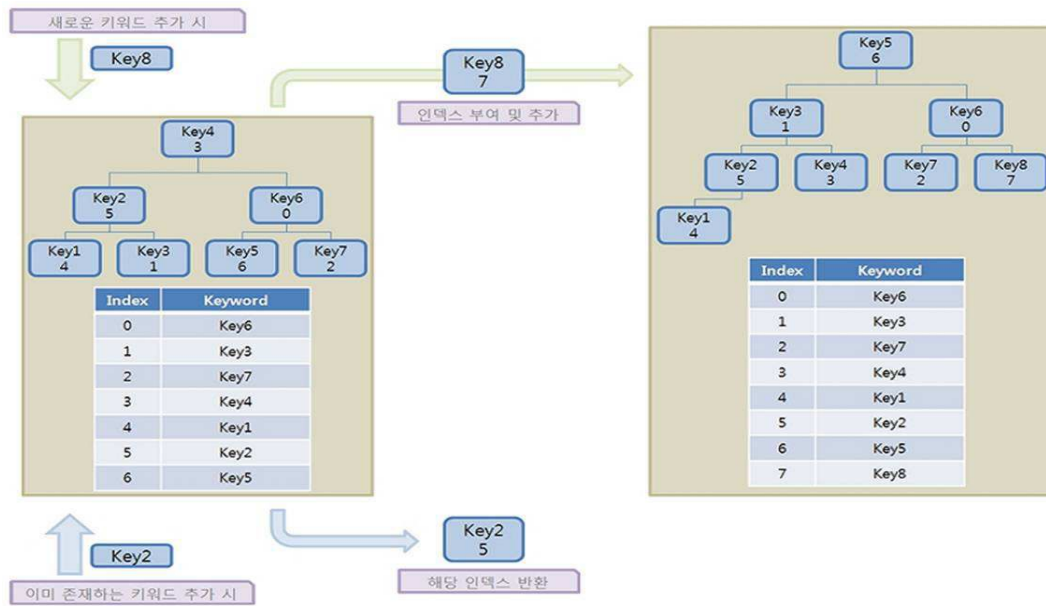
도면16



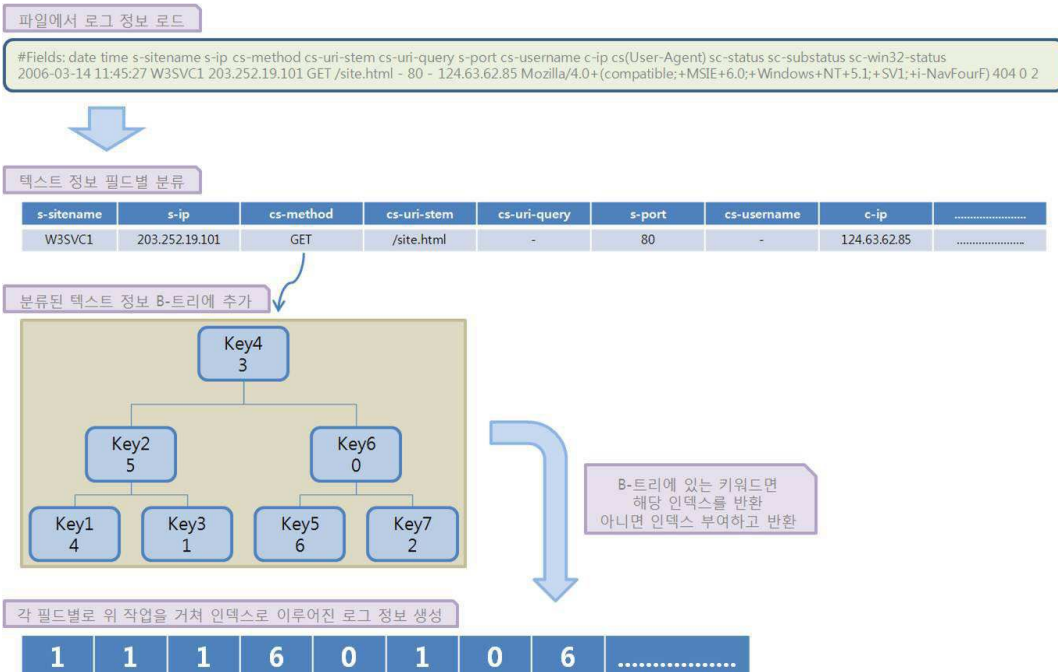
도면17



도면18



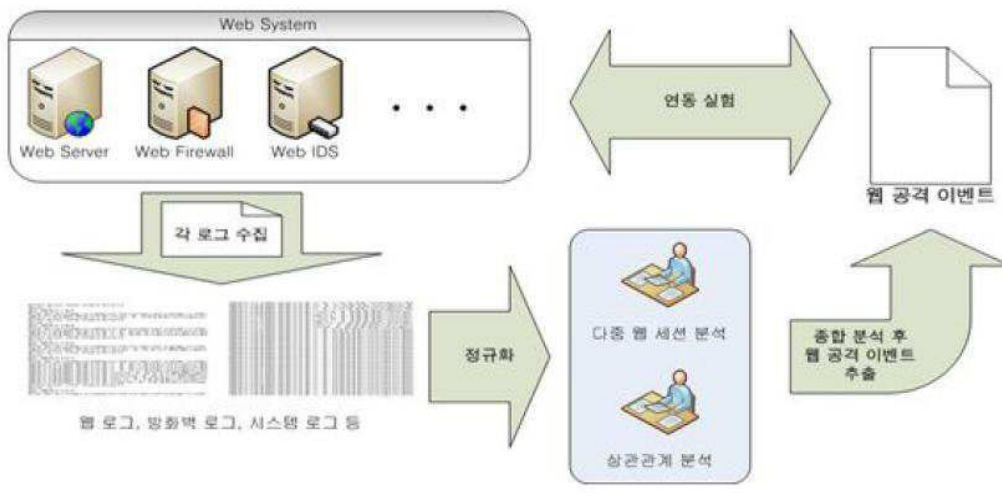
도면19



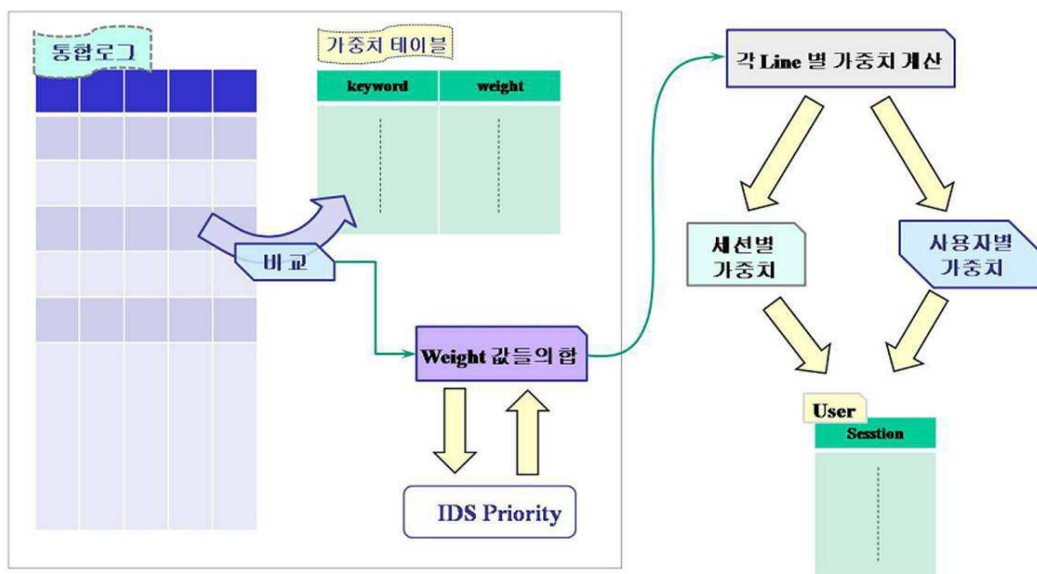
도면20

Index	IP	Agent
121	80.153.115.186	Mozilla/3.0 (compatible; Indy Library)
122	211.54.110.104	-
123	58.238.214.56	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
124	125.191.10.57	-
125	210.122.170.6	-
126	210.122.170.6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; NetClient_AA00A0C9DACA08)
127	210.122.170.6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; NetClient_AA00142246FBCD)
128	210.122.170.6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; NetClient_AA001143B2BB1A)
129	59.11.243.196	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
130	210.104.22.18	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
131	220.82.244.198	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
132	222.96.134.21	-
133	122.34.155.244	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

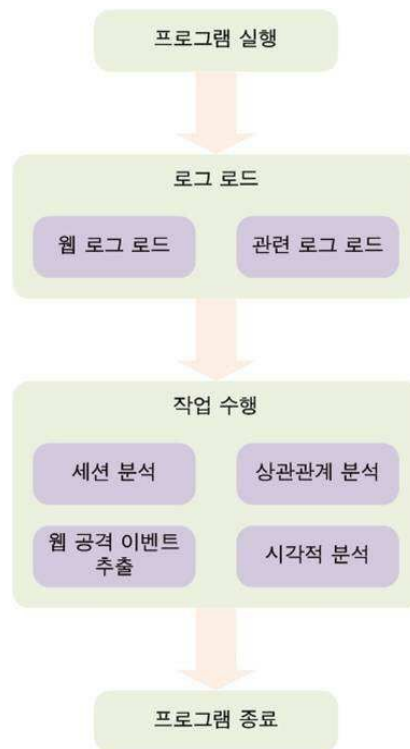
도면21



도면22



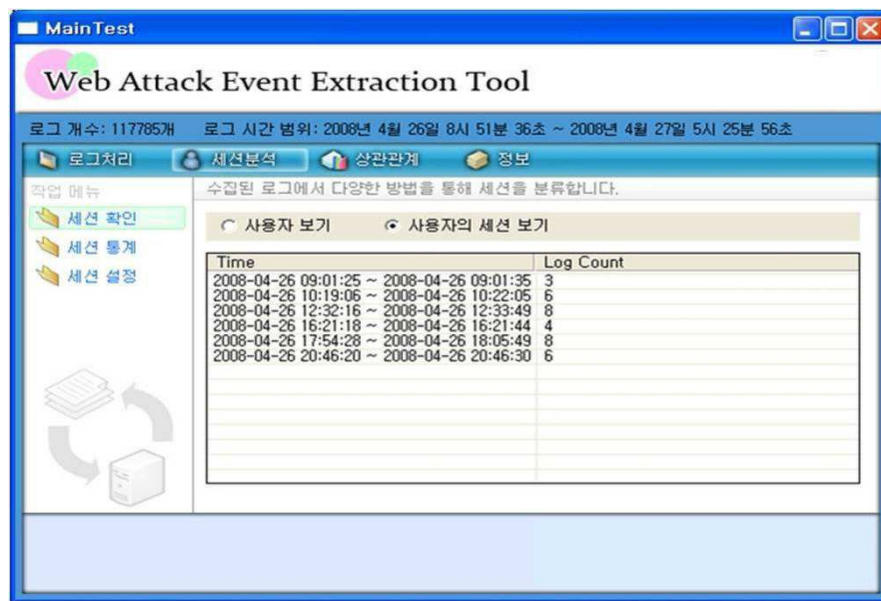
도면23



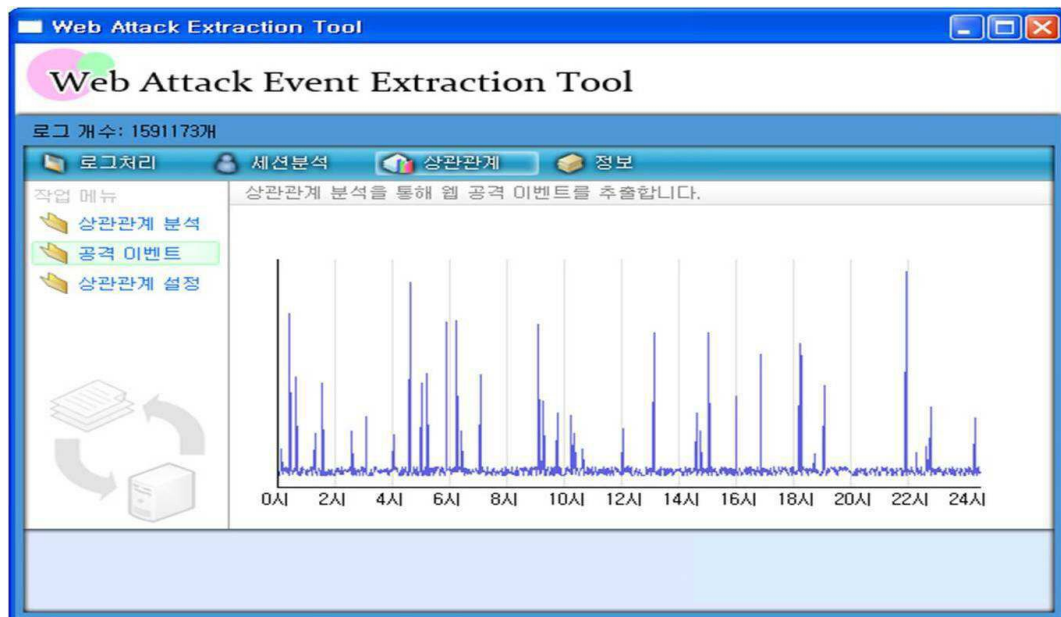
도면24



도면25



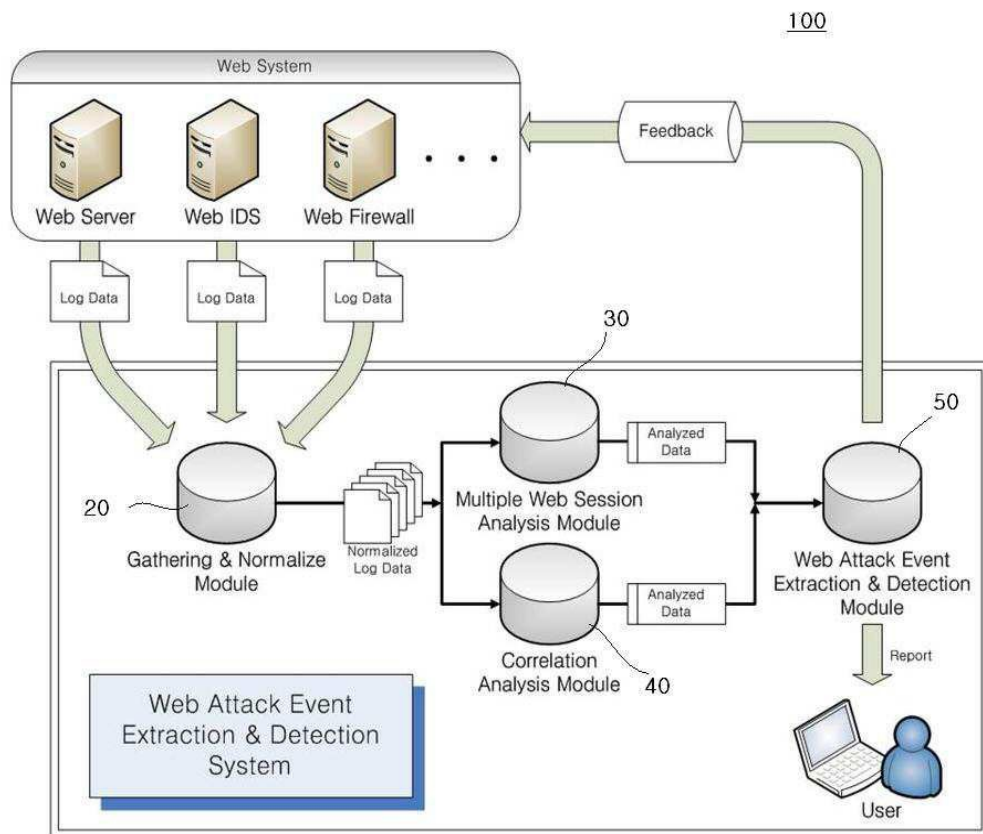
도면26



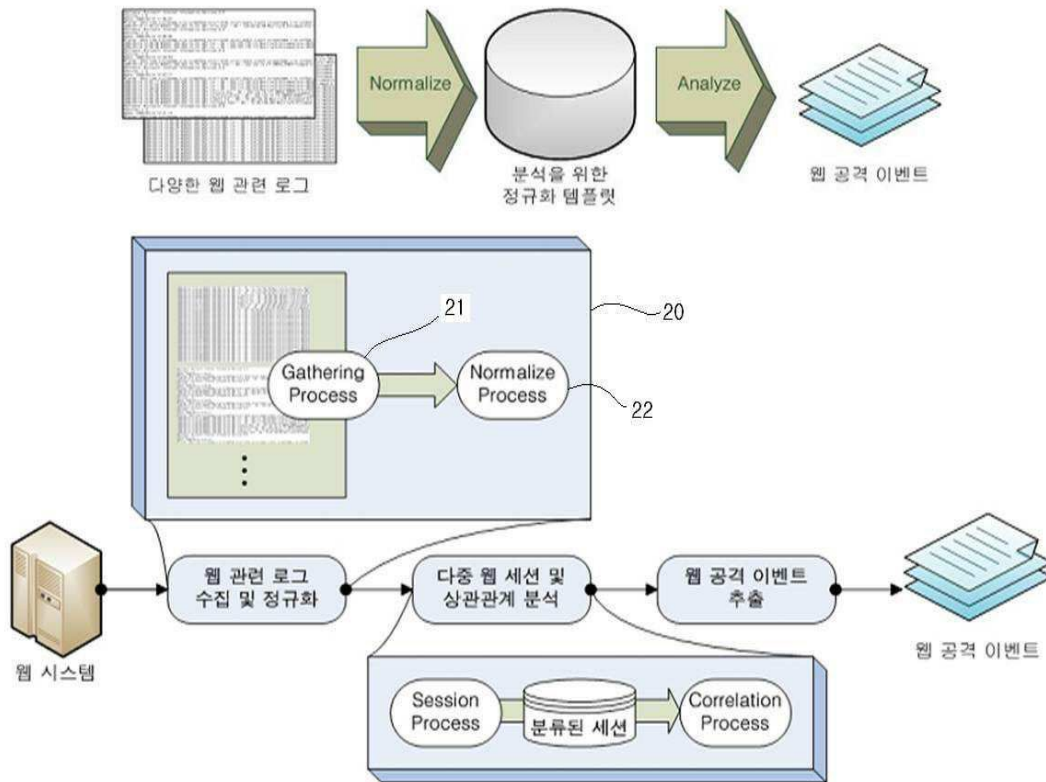
도면27

```
[2008-07-21/11:28:48] 프로그램 실행
[2008-07-21/11:28:55] 로그 파일들을 불러옵니다.
[2008-07-21/11:28:56] C:\Documents and Settings\win\바탕 화면\access_log_200
[2008-07-21/11:28:56] 로그 불러오기를 완료했습니다. < 0.922 sec >
[2008-07-21/11:28:56] 로그를 정렬했습니다. < 0 sec >
[2008-07-21/11:28:56] 사용자 정보를 가져왔습니다. < 0.015 sec >
```

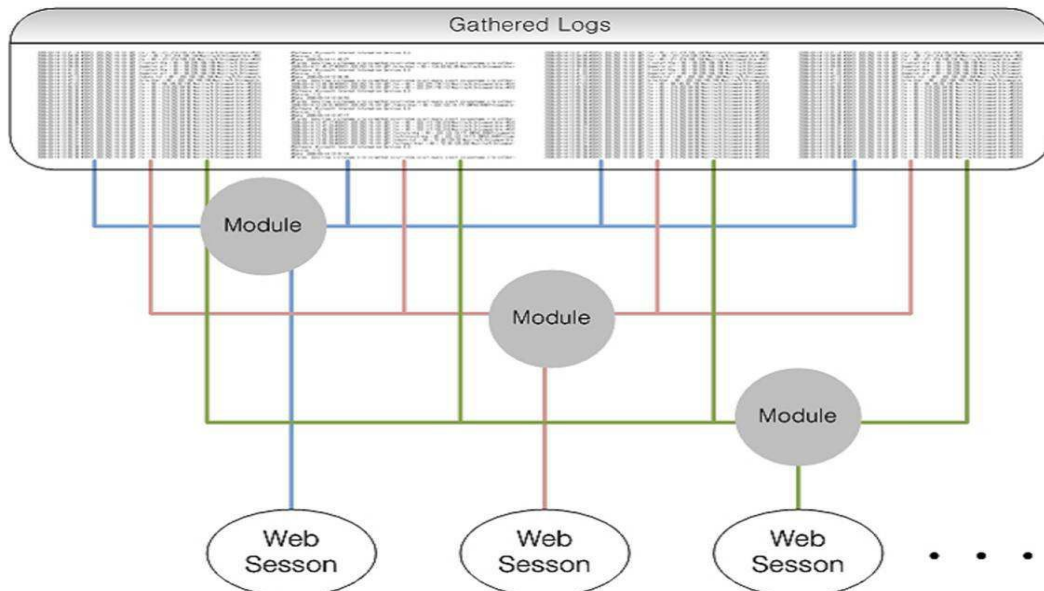
도면28



도면29



도면30



도면31

