침입탐지 시스템을 이용한 웹 스테고데이터 검출 시스템 설계 및 분석

도 경 화† · 전 문 석††

요 약

인터넷의 보편화로 인해 일반 정보뿐만 아니라 중요 정보의 전송도 인터넷을 통하여 이루어지고 있다. 그렇기 때문에, 비밀리에 중요 데이터의 전송이나 비밀문서 등의 유출도 증가되고 있다. 그러나 그에 따른 보안 방안은 매우 취약한 실정이다. 따라서 본 논문에서는 네트워크 기반의 침입탐지시스템 모듈을 사용하여 네트워크를 통한 중요 정보의 유출을 탐지하는 것을 목적으로 한다. 그리고 중요 데이터의 유출과 테러에 대한 비밀문서의 방지 및 검출하기 위한 은닉정보검출방법을 제안하고 설계한다. 이는 기존의 은닉정보검출방법을 분석하고 그 중 스테고데이터에 대한 검출 방법을 이용하여, JPG, WAVE 등의 웹 데이터나 이메일의 첨부 파일에 스테고데이터 검출 방법에 초점을 맞추어 제안하고 설계한다. 또한, 본 논문에서 제안한 스테고데이터 검출 시스템을 실험을 통하여 분석한다.

Design and Analysis of the Web Stegodata Detection Systems using the Intrusion Detection Systems

Kyoung-hwa Do† · Moon-Seog Jun††

ABSTRACT

It has been happening to transfer not only the general information but also the valuable information through the universal Internet. So security accidents as the expose of secret data and document increase. But we don't have stable structure for transmitting important data. Accordingly, in this paper we intend to use network based Intrusion Detection System modules and detect the extrusion of important data through the network, and propose and design the method for investigating concealment data to protect important data and investigate the secret document against the terrorism. We analyze the method for investigating concealment data, especially we use existing steganalysis techniques, so we propose and design the module emphasizing on the method for investigating stego-data in E-mail of attach files or Web-data of JPG, WAVE etc. Besides, we analyze the outcome through the experiment of the proposed stego-data detection system.

키워드 : 스테가노그래피(Steganography), 스테고디텍션(Stegodetection), 정보은닉(Information Hiding), 침입탐지시스템(IDS), 정보보호(Information Security)

1. 서 론

인터넷의 보편화는 정보화에 큰 역할을 하였다. 정보화는 일반 데이터 뿐만 아니라, 중요 정보의 전송도 인터넷을 통하여 전송하게 하였다. 뿐만 아니라, 회사나 연구소등의 기밀문서나 테러정보 등이 전송되기도 한다. 이때, 데이터를 일반적인 전송방식으로 전송하는 것 외에 비밀리에 전송하는 방법을 사용하기도 한다. 특히, 이러한 기밀문서의 유출이나 테러정보 등은 비밀리에 전송되기 때문에, 그 전송의 유무조차 확인할 수가 없는 경우가 있다. 또한, 디지털 데이터는 복제와 원본에 대한 조작이 용이하기 때문에, 더욱 위험하다. 비밀리에 전송하는 방법으로 정보은닉 기법을 볼 수 있다. 정보은닉으로는 은닉채널, 스테가노그래피, 익명성, 저작권 표시 등의 기법이 대표적이다. 특히, 스테가노그래피 방법은 최근 테러정보를 전송하는데 사용되고 있다. 이는, 비밀통신의 유무조차도 알 수 없는 매우 위험한 형태이다.

네트워크의 보호와 침입에 대한 방지를 위하여 침입차단 및 탐지 기술은 발전하고 있으나, 전송 시 데이터의 진실성에 대한 연구는 부족하다. 따라서 본 논문에서는 네트워크 기반 침입탐지 모듈을 사용하여 수집 저장된 패킷 정보를 통하여 웹페이지의 이미지와 오디오 혹은 이메일의 첨부화

※ 본 논문은 숭실대학교 교내 연구비 지원에 의한 것임.
† 준 회 원 : 숭실대학교 대학원 컴퓨터학과
†† 종신회원 : 숭실대학교 정보과학대학 교수
논문접수 : 2003년 6월 24일, 심사완료 : 2003년 9월 30일

일을 검사하여 스테가노그래피 유무를 검출하여 관리자에게 알리는 IDS/StegoDetector 시스템을 제안하고 설계한다.

논문의 2장에서는 관련연구를 통하여 네트워크기반 침입탐지모듈과 스테가노그래피시스템과 스테가노그래피 검출시스템에 대해 알아보고, 네트워크기반 침입탐지 모듈과 스테가노그래피 검출모듈을 연계한다. 3장에서는 본 논문에서 제안한 웹 스테고데이터 검출 시스템에 대해 구성도와 순서도를 통하여 제안하고 4장에서는 기본적인 시뮬레이션 결과를 통하여 본 시스템을 분석한다. 마지막으로 5장에서 결론을 내린다.

2. 관련 연구

2.1 IDS의 구조와 컴포넌트

IDS의 구조는 크게 3가지로 분류 할 수 있는데, 호스트기반 IDS, 네트워크기반 IDS, 그리고 하이브리드 IDS로 나눌 수 있다.

호스트 기반 IDS인 경우, 중요한 파일에 대한 접근확인, 접근 규칙의 변화, 프로세스 처리, 로그인 행위등과 같은 로그검사를 목적으로 하고 있다. 네트워크 기반 IDS인 경우, 네트워크 세그먼트에 대한 트래픽을 모니터하는 네트워크 스니퍼와 유사하며, 로컬 네트워크 세그먼트를 통과하는 모든 트래픽뿐만 아니라 관련된 모든 패킷을 처리하는 혼잡모드로 설정된 네트워크 인터페이스 카드를 사용하고, TCP/IP 스택을 구현하며, 스택과 인접하여 관련 트래픽 정보를 필터에게 제공한다. 하이브리드 IDS는 두 가지를 모두 겸하는 IDS 구조이다[1].

본 논문에서는 네트워크 기반 IDS를 기본 구조로 사용한다. 네트워크기반 침입탐지시스템에서는 네트워크로 유입되는 모든 패킷이 미리 정해져 있는 보안정책에 따라 방화벽을 통과하게 되며, 네트워크 패킷에 대한 모든 정보는 IDS의 로그로 저장 된다. 이때 여러 침입탐지 컴포넌트를 이용해 저장된 로그를 조사하여 침입 유무를 확인한다. IDS의 컴포넌트를 살펴보면 다음과 같다[2].

- 센서(Sensor) : 침입탐지를 위한 타깃 시스템의 정보를 제공한다.
- 프로세싱 엔진(알고리즘) : 반드시 필요한 구성요소이며, 통합된 프로세싱 알고리즘은 매우 중요하다. 데이터 단순화, 침입 증거 구별, 관련 임계값의 침입증거를 통한 의사결정, 특화된 침입 데이터 웨어하우스의 데이터마이닝, 초기대응 의사결정 등 여러 가지 기능을 제공한다.
- 감사/기록(Audit/archive) : 감사 로그와 데이터 집적소에서 타깃 시스템의 행위를 저장하는 문제는 정보보관 시간, 정보 보호방법, 저장과 검색을 위한 정보 암호화 형식 등 많은 요구사항들을 고려를 해야 한다.
- 시스템관리(System management) : 각 컴포넌트를 연결하여 모니터링, 환경설정, 업데이트, 경고의 감시를 수행한다.
- 침입 패턴 데이터베이스(Intrusion pattern DB) : 이미 발견된 패턴을 저장하며 새로운 패턴이 발생하면 갱신한다.

2.2 정보은닉과 스테가노그래피

정보은닉(Information Hiding)이란 정상적인 데이터에 정보를 숨기는 방법을 말한다. 다음과 같은 종류가 있다[3].

- 은닉 채널(covert channel) : 두 집단 사이의 은밀한 채널을 통하여 공격자가 통신자체를 알지 못하도록 한다.
- 스테가노그래피(steganography) : 커버텍스트, 커버이미지, 커버오디오와 같은 겉보기에는 일반적인 텍스트, 이미지, 오디오와 똑같이 보이면서, 스테고텍스트나 스테고오브젝트를 만들어내어 은밀한 정보를 전달하는 방법이다.
- 익명성(Anonymity) : 통신의 주체 자체를 숨기는 방법으로서, 보내는 사람이 누구인지 밝히지 않고 데이터를 전송하는 형식이다.
- 저작권 표시(copyright marking) : 스테가노그래피와 달리 정보의 은닉보다는 여러 가지의 공격에 대해서 견디어 낼 수 있는 강건성(robustness)이 요구된다.

스테가노그래피는 정보은닉 방법 중에 기밀문서를 보내는 방법으로 가장 많이 사용된다.

스테가노그래피는 정보가 은닉되어 있는 것을 숨기며 통신하는 방법이다. 다시 말해, 두 사람 간에 비밀메시지를 제 3자가 알지 못하도록 하는 방법이며 커버메시지와 삽입메시지로 구분된다. 커버메시지는 제 3자에게 아무런 의심없이 전달되어 실제 의미가 없는 메시지로 숨겨진 메시지인 삽입메시지를 포함하고 있는 데이터이며, 삽입 메시지는 두 집단간에 비밀스럽게 전달되는 실질적인 메시지이다.

2.3 기존 스테가노그래피 검출방법

2.3.1 기존 스테가노그래피 방법

이 장에서는 기존 스테가노그래피 방법을 이용한 여러 가지 툴에 대해서 분석한다.

기존의 스테가노그래피 툴은 이미지 도메인(Image Domain)툴과 변환 도메인(Transform Domain)툴로 나눌 수 있다[4, 10]. 이미지 도메인 툴은 비트 와이즈(bit-wise)방식을 사용하여 최하위 비트(LSB : Least Significant Bits) 삽입과 노이즈 수정 기법을 사용한다. 이러한 접근방법은 스

테가노그래피 같은 단순한 시스템에 적당하며 StegoDos, S-Tools, Mandelsteg, EzStego, Hide and Seek, Hide4PGP, Jpeg-Jsteg, White Noise Storm, Steganos등이 속한다. 사용되는 이미지 형식은 손실이 없으며 데이터가 직접 수정되고 복구 된다. 이미지에 원하는 정보를 삽입하기 위해 사용하는 마스크와 이미지 객체 같은 추가적인 컴포넌트를 포함하므로 이미지 형식에 다소 독립적이라 할 수 있다.

변환 도메인 툴은 알고리즘의 수정과 이산 코사인 변형(DCT : Discrete Cosine Transformation)과 같은 이미지 변형, 웨이브 변형 등을 사용한다. 이 방식은 커버의 최상위 비트(MSB : Most Significant Bits) 지역에 메시지를 숨기고 발광도와 같은 이미지 값을 수정할 수 있다. 따라서 워터마킹 툴은 이 분류에 적당하며 PictureMarc, JK-PGS, SysCop, SureSign등과 같은 툴이 이에 해당한다. 이 방식은 비트 와이즈 방식보다 강건하지만 이미지에 추가될 수 있는 정보의 양과 얻을 수 있는 강건함 사이에 장단점이 존재한다. 많은 변환 도메인 방법들은 이미지 형식이 독립적이며 무손실 포맷과 손실 포맷 사이에서 변환이 생긴다.

몇몇 기법들은 두 가지의 domain tool을 공유한다.

2.3.2 기존 스테고데이터 검출 방법

기존의 스테고데이터 검출 방식은 stego-only, known cover, known message, chosen stego, chosen message 검출 방식으로 나뉜다. stego-only detection은 ciphertext only 방식과 유사하며 분석과정에서 stego-medium 만이 사용된다. 원래 cover-media와 stego-media 둘 다 사용가능 하면 known cover 방법이 가능하다. 숨겨진 메시지를 통계적 기법으로 분석할 경우에 known message detection 방법을 사용한다. 또한, detector가 직접 미래의 용도로 stego-media를 분석할 수 있다. chosen stego 방식은 스테가노그래피 tool algorithm과 stego-media를 알고 있을 때 사용된다. chosen message 공격은 steganalyst가 스테가노그래피 tool을 통해 stego-media를 만들었거나 알려진 메시지로 알고리즘을 만들었을 때 사용된다. 이 detection 방식은 stego-media와 일치하는 형식을 찾아 사용된 특정 툴과 알고리즘을 알아내는 방법이다.

(1) 은닉 정보 검출 방식

- signature 검색 : stego-image의 숨겨진 메시지를 발견하는 기초적인 방법은 명백하고 반복적인 패턴을 찾는 것이며 이는 스테가노그래피 툴의 숨겨진 메시지 구별방법이나 시그니쳐로 볼 수 있다[4]. 이러한 방법은 stego-only 검출기법을 지원한다. 몇몇 툴 특히, 비트 와이즈(bit-wise) 방법은 이미지의 왜곡이 명백하여 쉽게 스테가노그래피의 존재가 발견되며 인접한 패턴 색상을 비교하여 이미지를 검사 한다.
- S-Tool[5] : 사용되는 커버 이미지의 고유색상 수가 256을 넘지 않으며 최소 32까지 가능하다. 이때 발광도에 따라 패턴을 정렬하여 블록단위에 색상들이 유사하게 보이지만 실제 값이 1bit씩 다르다. 인간의 눈이 가진 특성으로 인해 검출에는 어려움이 있지만 많은 이미지 비교를 통해 패턴이 부자연스럽다는 것을 알 수 있다. 패턴색의 변형방법은 일부를 제외하고 일반적이 아니다.
- SysCop : 8-bit 이미지를 수정할 때 S-tool과 유사한 패턴을 가진 유일한 변환 툴이다. 패턴색 변경 시 발생하는 시그니쳐는 S-Tool pattern보다 발견하기 어렵다. SysCop은 화상을 만들 때 쓰이는 점 방식의 수평선 집합인 raster 데이터가 생기기 전에 검정색 00 00 00 값을 가진 많은 패턴 색상을 버퍼에 올리는데 약 256색과 검정색 지역이 있는 사진에는 00 00 00의 패턴색 값을 갖지 않는 특성 때문에 검출이 가능하게 된다[6].
- Mandelsteg : Mandelsteg의 fractal 형태의 이미지는 패턴을 자세히 살피면 분별 할 수 있다. 존재하는 커버 이미지를 수정하지 않는 유일한 특성을 가지며 숨겨진 메시지를 보내기 위해 커버 이미지로써 Mandelbrot fractal 그래픽을 만들며 parameter에 따라 이미지의 색상과 크기가 다양하다. Mandelsteg가 만든 이미지는 색 인덱스에 256 palette색 값을 가지며 모든 이미지의 패턴은 각 색상에 두개의 palette 입력 값을 가진 128개의 고유 색상으로 만든 이미지 패턴이 존재한다[4].
- Hide4PGP : 8-bit와 24-bit BMP 이미지를 커버 이미지로 사용하며 8-bit 패턴 취급방법과 숨기는 데이터의 비트 결정에 여러 옵션을 제공한다. 숨겨진 정보의 디폴트 저장소는 24-bit 이미지의 4번째 LSB와 8bit의 LSB가 사용된다. 정보를 숨기기 위하여 선택하는 bit level 옵션은 LSB는 1, 두 번째 LSB는 2, 네 번째 LSB는 4, 8번째 LSB는 8이다. 옵션 모두가 8-bit 이미지에서 눈에 보이는 노이즈를 만들어 낸다[7]. 이러한 기법은 커버의 결과를 매우 좋게 만들지만 스테가노그래피의 독특한 특성을 첨가 하여 숨겨진 메시지의 존재를 알도록 한다.
- Jsteg-Jpeg : JPEG 이미지의 IDCT 공식을 통해 계수를 계산하면 이미지가 상대적으로 부드러우며 0 값이 아닌 그래프가 나타난다. 그러나 이 툴을 사용하여 이미지의 계수를 계산하면 약간 엉뚱한 그래프가 나타나며 숨겨진 정보를 저장할 때 보이는 과장된 선형 에러로 인해 중복된 계수 값이 발생하여 검출이 가능하다[8].

(2) 스테가노그래피와 워터마킹의 파괴

변형 툴을 사용할 때 비교할 본래의 이미지가 없으면 검출이 힘들다. 그러나 검출이 반드시 필요하지 않으며 스테가노그래피 데이터를 제거하는 것으로 목적을 달성할 수 있다. 숨겨진 정보를 사용하지 못하게 하는 방법은 반드시 스테고 데이터의 변화를 요구하며 작은 이미지 압축처리에도 쉽게 이미지가 변경되는 비트 와이즈 방식에서 쉽게 파괴할 수 있다. 숨겨진 메시지가 커버와 완전하게 통합된 변형 방식은 많은 노력이 필요하며 이를 제거하거나 사용하지 못하도록 하기위해서는 스테고 이미지를 파괴하여야 한다[9].

비트 와이즈 방식은 적은양의 이미지 처리에도 취약 하다. 이를 이용하여 숨겨진 많은 메시지를 빨리 파괴하는 방법은 JPEG과 같이 압축처리에 손실이 많은 포맷으로 변경하는 것이다. Jpeg-Jsteg로 처리된 JPG 이미지를 재압축하면 DCT 계수로 삽입된 메시지는 재 계산 시에 파괴된다. transformation, redundancy, masking 방법을 적용한 변형 방식은 숨겨진 정보가 이미지의 필수적인 부분으로 병합되기 때문에 비트 와이즈 방법보다 강건하지만 여전히 파괴에는 취약하다. 어떤 정보가 추가되어 숨겨진 정보를 발견할 수 없도록 하는 미디어가 존재한다면 같은 임계값내에서 삽입된 은밀한 정보를 덮어쓰거나 제거하면 된다.

적용 가능한 이미지 형식은 디지털 사진, 클립아트, 디지털 아트가 있으며 이들의 형식은 주로 24비트의 BMP, JPEG 혹은 8비트의 BMP, GIF이며 필요에 따라 스테가노그래피나 워터마킹 툴이 요구하는 형식으로 변경할 수 있다.

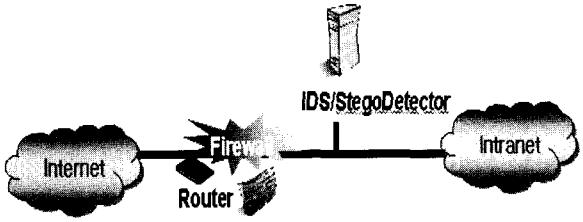
스테고 이미지는 다음과 같은 처리 기법으로 수정되거나 메시지 내용을 확인할 수 있다. 무손실 포맷과 손실 포맷사이의 변형, 비트 밀도 사이의 변형, 희미함, 스무딩, 노이즈 추가 혹은 제거, 샤프닝, 에지개선, 마킹, 로테이팅, 스케일링, 리어셈블링, 워핑, 디지털에서 아날로그의 변형, 프린팅과 스캐닝, 미러링, 플리핑, 비트 와이즈 메시지 추가, 변형 메시지 추가, unZign과 StirMark 툴등의 방법을 이용한다.

이러한 방법을 통해 비트 와이즈를 이용하는 툴은 숨겨진 메시지를 재생할 수 없고 변형 툴은 여러 가지 방법을 혼합하여 사용한다.

3. 제안한 웹 스테고데이터 검출시스템

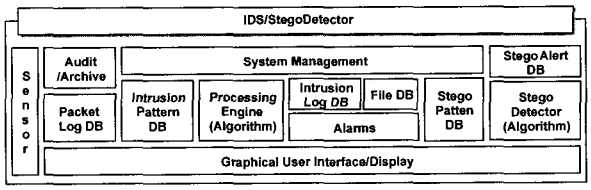
3.1 IDS를 이용한 웹 스테고 데이터 검출 시스템

외부에서 들어오면 패킷은 보안정책이 설정된 방화벽을 통하여 내부로 유입된다. 이때, 침입탐지시스템(IDS : Intrusion Detection System)이 패킷의 감사자료를 남겨 침입의 징후를 검사하게 된다. 본 논문에서는 침입의 징후를 검사하기 위하여 남긴 패킷의 로그를 통하여 스테고데이터인지 아닌지를 검사한다. 본 IDS/StegoDetector 시스템에서 비밀데이터가 검출될 경우, 기능을 사용하여 관리자에게 알린다(그림 3-1).



(그림 3-1) 웹 IDS/StegoDetector 검출 시스템 네트워크 구성도

본 IDS를 이용한 StegoDetector 시스템은 IDS의 Sensor, Audit/Archive, Log DB, System Management, Intrusion Pattern DB, Processing Engine(Algorithm), Intrusion Log DB에 스테고데이터를 검출하기 위한 부분인 스테고디텍터(알고리즘), Stego Pattern DB, Stego Log DB, Packet Log DB, Alarm 그리고 관리자가 관리를 수행하는 GUI(Graphical User Interface/Display)를 구성요소로 갖는다(그림 3-2).



(그림 3-2) 웹 IDS/StegoDetector 검출 시스템

IDS의 기본요소들에 대한 설명은 2장의 관련 연구의 2.1 IDS 시스템에 설명되어있기 때문에, 본 절에서는 StegoDetector의 구성요소에 관해 설명한다.

- Packet Log DB : Log DB에 패킷의 정보가 Full로 기록되어 있도록 저장하였기 때문에, StegoDetector에서는 Log DB에 있는 정보를 사용한다.
- System Management : IDS에서의 System Management의 역할은 각 컴포넌트를 연결하여 모니터링, 환경설정, 업데이트, 경고의 감시등을 수행하는 것이다. 본 IDS/StegoDetector에서는 재조합된 파일 헤더를 분석하여 jpg, audio, attach file이면 스테고디텍션 알고리즘 모듈로 넘겨주는 부분이 추가된다. 다른 System Management에 존재하는 모니터링, 환경설정, 업데이트, 경고 등의 모듈은 함께 쓰인다.
- Stego Detector(Algorithm) : System Management의 재

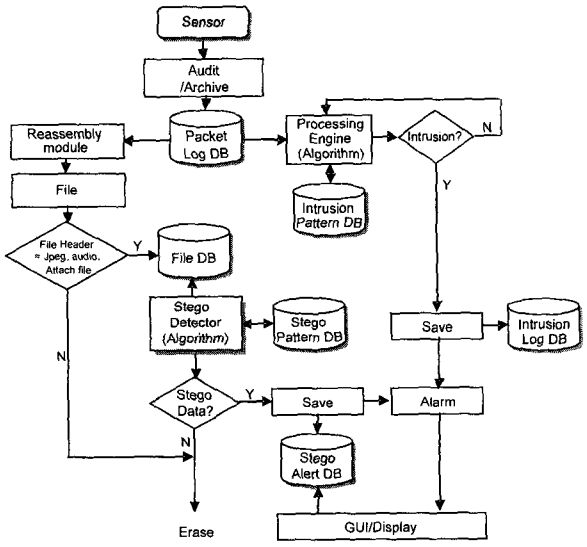
조합 모듈로부터 File로 추출된 데이터의 파일헤더를 검사하여 검출된 웹 데이터나 이메일의 첨부파일이 스테가노그래피가 된 스테고데이터인지를 검출하기 위한 알고리즘과 연결해주는 주 모듈이다. 이는 2.3.2절에서 설명한 기존의 여러 가지 툴들에서 사용하는 알고리즘들이 들어있어 이와 데이터를 연결하여 검출한다.

- Stego Pattern DB : 스테고디텍터(알고리즘)에서 참조 할 수 있는 여러 시그네쳐나 기존 알고리즘들에 대한 정보가 저장된다.
- Stego Log DB : 스테고디텍터를 통하여 스테고데이터로 검출된 경우 그에 대한 감사자료를 저장한다.
- Alarms : 스테고데이터를 검출했다는 것을 관리자에게 메일이나 호출기로 알린다.

3.2 제안한 웹 스테고데이터 검출시스템 설계

본 웹 스테고데이터 검출 시스템은 기존의 IDS 모듈에 스테고디텍션 모듈을 추가시킨 형태이다. 때문에, 패킷로그 DB에 저장되는 로그는 모두 패킷의 전체 내용을 저장해야 한다. 그래야 리어셈블링을 통하여 파일형태로 변경이 가능하며 파일형태로 변경한 연후에 분류를 통하여 스테고데이터인지 아닌지를 검사할 수 있다.

본 시스템의 센서로부터 감지된 패킷은 감사자료 형태로 패킷로그 DB에 저장된다. 저장된 데이터는 침입탐지 엔진을 통하여 침입탐지 패턴과 매칭하여 침입에 대한 로그인지 아닌지를 판별하고 침입인 경우 침입탐지로그 DB에 저장하고 관리자에게 알린다(그림 3-3).



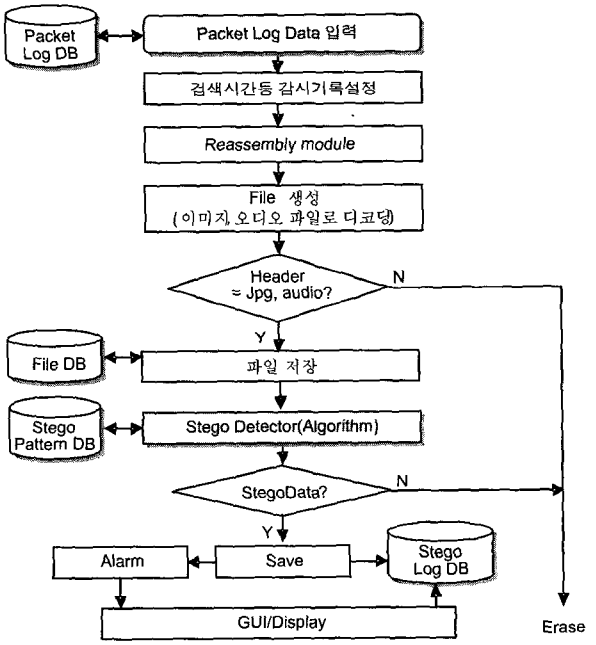
(그림 3-3) 웹 IDS/StegoDetector 시스템

패킷로그 DB에 저장된 패킷은 리어셈블링모듈을 통하여 파일형태로 변경되고 파일헤더부분을 분석하여 JPG, gif, audio, attach file 등의 파일 헤더포맷과 비교하여 맞으면 StegoDetector(Algorithm) 모듈로 보내고 그렇지 않으면 삭제한다. 본 모듈을 통하여 Stego Pattern DB의 내용과 매칭하여 스테고데이터이면 스테고 로그 DB에 저장하고 알람으로 관리자에게 알린다. 이렇게 저장된 데이터는 GUI를 통하여 관리자가 확인할 수 있도록 한다. 만약, 정상적인 데이터이면 전송한다. 관리자는 언제든지 스테고로그 DB를 통하여 GUI를 통하여 데이터를 확인할 수 있다.

본 IDS를 이용한 스테고디텍터 시스템은 웹페이지의 이미지와 오디오 그리고 이메일의 첨부메일에 대한 데이터를 중심으로 검출한다. 다음은, 본 모듈을 통하여 이미지와 오디오에 대한 스테고디텍터 모듈과 이메일에 대한 스테고디텍터 모듈의 상세 설계이다.

3.2.1 이미지와 오디오 데이터를 위한 스테고디텍터 모듈 설계

본 스테가노디텍션 모듈은 각 웹 이미지 및 오디오 파일이 원본 파일인지 은밀하게 변경된 파일인지 검사하는 모듈이다(그림 3-4). 다음 설계도에 대해 설명하면 다음과 같다.



(그림 3-4) 웹데이터 및 오디오에 관한 스테가노디텍션 모듈

본 모듈의 입력파일은 IDS 모듈의 Packet Log DB에 저장되어 있는 패킷정보를 파일로 디어셈블하여 웹 이미지와 오디오 데이터를 식별, 검출하여 사용한다. 먼저, 패킷 Log DB로부터 가져온 데이터를 검사하기 위하여 검사시간 등 감사기록을 설정한다. 다음은 리어셈블리 과정을 통하여 파

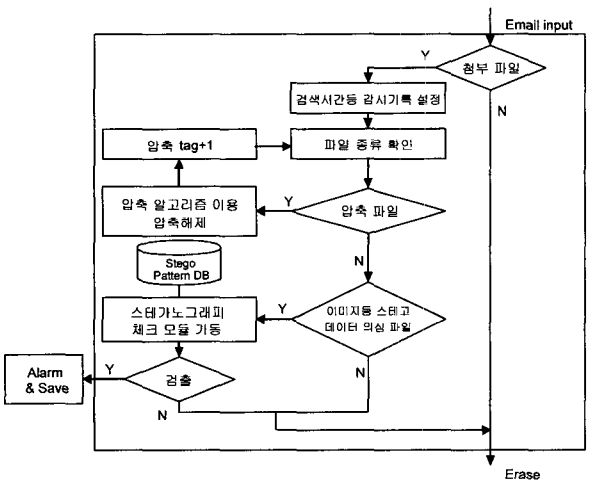
일로 변환하고 파일의 종류를 확인하여 웹 이미지와 오디오 파일의 데이터를 디코딩한다. 그리고 이러한 이미지와 오디오파일의 파일 헤더를 먼저 검사해서 jpg, gif, audio 파일이 아니면 삭제한다.

다시 말해, 입력된 파일의 처리에 대한 기본설정을 한 후, Files DB로부터 입력된 로그 데이터에 대해 공통적인 작업을 행한다. 즉 JPG, gif, MP3, wave와 같이 encoding된 이미지를 decoding하고 각 파일의 헤더를 탐색하여 임베디드 데이터가 들어 있는지 검사한다. 이때, 스테가노데이터가 없는 것으로 판별 된 이미지 혹은 오디오 파일은 검사를 종료하고, 양성으로 판정된 이미지는 파일 내에 스테고데이터로 의심되는 부분을 표시하여 세부적으로 검사하는 모듈로 넘겨준다.

세부적으로 검사하는 부분에서는 Jsteg, Out Guess, Jphide, Invisible Scret등 여러 알고리즘들이 저장된 스테고디텍터(알고리즘)의 스테가노 패턴 DB의 내용과 매치시킨다. 이 때, 이미지나 오디오의 히스토그램이나 파장을 분석하여, 최종적으로 어떤 파일이 스테가노 데이터를 담고 있으며, 어떤 툴로 생성되었는지, 임베디드된 데이터의 크기는 어느 정도인지 출력한다. 이때, 데이터베이스 내에 미리 포함되어 있지 않던 패턴은 관리자에게 알려 DB에 입력하도록 한다. 또한, 알람기능을 사용하여 관리자에게 스테고데이터의 발신자 주소와 내용 등을 확인하도록 한다.

3.2.2 이메일의 첨부화일에 대한 스테고디텍터 모듈 설계

위의 모듈과 같은 경로를 통하여 입력 파일인 e-mail을 Packet Log DB에서 가져온다. 위의 3.2.1 모듈에서와 같은 방식으로 파일로 변경하고 이때 그 파일이 e-mail의 첨부화일이 중요정보를 숨기고 있는 스테고데이터인지를 검사하게 된다(그림 3-5).



(그림 3-5) 이메일의 첨부파일에 관한 스테가노검출 모듈

먼저 이메일에 첨부파일이 없으면 검사 없이 전송하고, 있으면 다음의 모듈을 수행한다. 이때, 첨부화일을 검사해야 하는데, 일반적으로 첨부화일은 압축형태로 되어 있기 때문에, 압축을 풀고 스테가노그래피 검출 모듈을 가동하여 스테고 패턴 DB(알고리즘)을 사용하여 검사한 후, 이상이 없을 경우는 재압축하여 사용자에게 보내고, 이상이 있을 경우는 Stego DB에 저장하고 관리자에게 알린다.

4. 평가 및 실험

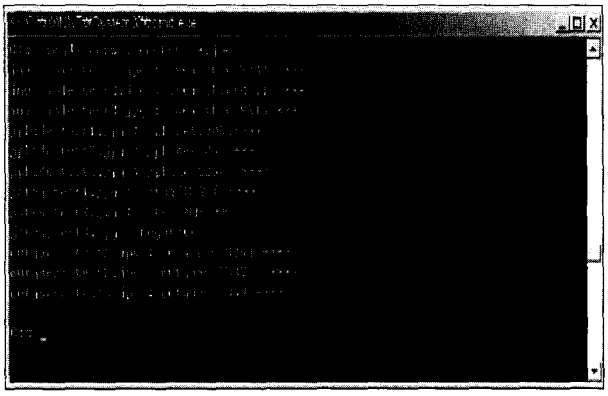
본 실험은 헤더의 내용을 통하여 스테고데이터를 검출하는 방법을 보인다. 또한, 검출 알고리즘을 사용한 프로그램을 만들어 검출하여 검출 내용을 보인다.

실험 환경인 운영체제는 공개용 침입탐지 시스템인 스노트가 수행중인 윈도우와 리눅스를 사용하였다. 다음은 실제 윈도우에서 IDS를 통하여 저장된 파일자료를 통하여 실험한 내용이다. 이때, 판별용 데이터로 JPG 파일을 사용하였다.

파일을 캡쳐하여 헤더 부분을 탐지하면, 은닉된 데이터가 있는지를 판별 할 수 있다. JPG와 같은 대부분의 이미지 파일은, 끝 부분에 필요 없는 데이터라도 넣어서 파일의 포맷을 유지해야 한다. 아래 그림에서 '20'을 채워 넣는 것이 그 예인데(그림4-1), 이 공간에 다른 데이터가 들어 있는 것만으로도 쉽게 스테고데이터가 있는지 판별해 볼 수 있다. 한편 이를 복호화할 수 있는 부분은 파일의 중간에 삽입되어 눈으로는 쉽게 찾아 볼 수 없게 되어 있으며 원본 이미지를 거의 손상시키지 않는다.

(그림 4-1) 패킷캡쳐에 의한 스테고데이터 판별

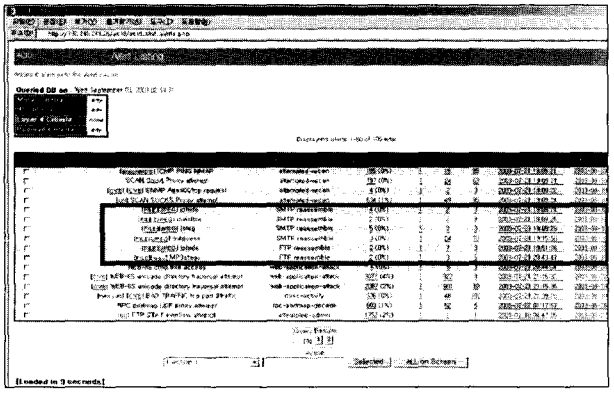
(그림 4-2)는 'stegdetect'를 여러 가지 스테가노그래피 알고리즘과 연결하여 만든 프로그램으로써, 윈도우 버전으로 jpg파일에 숨은 스테고데이터를 탐지한 모습이다(그림 4-2).



(그림 4-2) jpg 파일에 대한 스테가노디텍션

(그림 4-2)의 내용을 보면, invisibel, jphide, jsteg, outguess로 생성된 스테고데이터가 커버데이터에 숨겨 있는 걸 알 수 있다. 첫 번째, 칼럼은 원본데이터의 이름이고 두 번째 칼럼은 생성 알고리즘 이름이다. 여기서 괄호([ ])안은 stego data의 사이즈이다.

(그림 4-3)은 침입탐지시스템과 스테고디텍터의 연동에 대한 실험 결과이다. 이는 스노트를 리눅스에서 실행시키고 ACID(Analysis Console for Intrusion Database)[11]을 이용하여 스노트의 Alert 경고에 대한 내용과 스테고 검출을 수행한 내용을 함께 보여주고 있다. 굵은 사각체크 표시를 한 부분이 스테고디텍션으로 검출된 경고 부분이다. jphide, invisible, jsteg, outguess, mp3stego 등의 스테가노그래피 알고리즘을 통하여 생성된 파일들을 ftp와 메일로 전송하여 이를 검출하도록 하였다. 따라서 (그림 4-3)에서 보면, 검은색 체크부분을 보면 메일을 통하여 전송된 jpg 파일들과 FTP를 통하여 전송된 오디오 파일이 검출된 것을 볼 수 있다.



(그림 4-3) ACID에서의 스테고데이터 검출에 대한 알람

5. 결 론

인터넷이 일상화가 되면서 많은 데이터들이 웹을 통하여 전송되고 있으나, 데이터의 내용의 진실성에 대해서는 간과하고 있다. 침입에 대한 개념이 이제는 실제적인 해킹을 막기 위한 침입차단과 탐지에서 벗어나 데이터의 진실성에 의미를 두어야 할 것이다.

또한, 현재 까지는 'stegdetect'처럼 스테가노그래피 인지 여부와 임베디드 된 데이터의 크기, 사용 된 툴의 이름 정도만 알 수 있다는 단점이 있다. 또한 특별한 GUI를 지원하지 않고 검색 속도가 눈에 띄게 느리다는 단점이 있어서 실시간으로 사용되기에는 무리가 있다. 따라서 향후에는 스테가노디텍션 알고리즘과 모듈의 성능개선과 IDS에서 지원하는 GUI 툴과 별개의 스테가노디텍션에 알맞은 GUI를 추가하고자 한다.

본 IDS를 이용한 웹스테고디텍션 시스템을 통하여 침입탐지 뿐만 아니라 전송되는 데이터의 진실성도 판별하여 중요자료의 보호와 테러정보등도 알아 낼 수 있을 것으로 기대된다.

참 고 문 헌

[1] Brian Laing, How To Guide-Implementing a Network Based Intrusion Detection System, Brian Laing sovereigh House, 2000.

[2] Edward Amoroso, Intrusion Detection, Intrusion.net Books, pp.26-28, 1999.

[3] Fabien A. P. & Petitcoals, Ross J. Anderson & Markus G. Kuhn, "Information Hiding - A Survey," *Proceedings of the IEEE*, 1999.

[4] Neil F. Johnson & Sushil Jajodia, Steganalysis of Images Created Using Current Steganography Software, George Mason University, 1998.

[5] Andreas Westfeld & Andreas Pfitzmann, Attacks on Steganographic Systems, Dresden University, 1999.

[6] Jian Zhao, A Digital Watermarking System for Multimedia Copyright Protection, Fraunhofer Center, 1996.

[7] Jessica Fridrich & Miroslav Goljan, Practical Steganalysis of Digital Images, SUNY Binghamton, 2002.

[8] Neil F. Johnson & Sushil Jajodia, "Exploring Steganography : Seeing the Unseen," IEEE Computer, pp.26-34, 1998.

[9] Eugene T. Lin & Edward J. Delp, A Review of DataHiding in Digital Images, Purdue University, 1999.

[10] Qieng Cheng and Thomas S. Huang, "An Additive Aproach to Transform-Domain Information Hiding and Optimum Detectio Structure," *IEEE Transactions on Mutimedia*, Vol.3, No.3, September, 2001.

[11] Online, Avalable : http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html.

도 경 화

e-mail : khdo0905@dreamwiz.com

1997년 건양대학교 컴퓨터공학과(공학사)

1999년 숭실대학교 컴퓨터학과(공학석사)

2002년 숭실대학교 컴퓨터학과 수료(공학박사)

2001년~2003년 숭실대학교 생산기술연구소 연구원

관심분야 : 정보은닉, DRM, 네트워크보안, 데이터통신, 암호학

전 문 석

e-mail : mjun@comp.ssu.ac.kr

1980년 숭실대학교 컴퓨터공학과(공학사)

1986년 University of Maryland, 전산과(공학석사)

1989년 University of Maryland 전산과(공학박사)

1989년 Morgan State University 전산수학과 조교수

1989년~1991년 New Mexico State University 부설 Physical Science Lab. 책임연구원

1991년~현재 숭실대학교 정보과학대학 정교수

관심분야 : 네트워크보안, 컴퓨터알고리즘, 병렬처리, VLSI 설계, 암호학