실시간 저장장치 패킷분석을 통한 안전한 문서 유출 방지 시스템의 설계 및 구현1)

김현민, 김수현, 이선호, 이임영
순천향대학교 컴퓨터학부
e-mail : [yukylove, kimsh, sunho431, imylee]@sch.ac.kr

Design and Implementation of Secure Document Loss Prevention System by Real-Time Storage Device Packet Analysis

Hyun-Min Kim, Su-Hyun Kim, Sun-Ho Lee, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

휴대용 저장장치의 발달로 인하여 많은 보안상의 문제점들이 나타나고 있으며, 특히 공공기관 혹은 기업체 내에서 USB메모리 등 보조기억매체를 활용한 정보유출이 갈수록 증가하고 있다. 이에 따라 본 논문에서는 전송이 허가된 문서에 인증패킷의 삽입 후 실시간 패킷분석을 이용하여 휴대용 저장장치로 전송하는 문서의 이동경로 확인 및 허가되지 않은 문서들에 대한 제어가 가능하도록 시스템을 제안하게 되었다.

1. 서론

휴대용 저장장치는 필요에 따라 기술의 발달로 인하여 대용량화가 급격히 진행되었으며 휴대성 또한 점차 발전하게 되었다. 그 중 USB 메모리는 데이터의 전송속도가 빠르고 휴대가 간편하여 휴대용 저장장치로서 널리 사용되고 있다. 이와 같은 장점으로 인하여 휴대용 저장장치 사용자가 증가함에 따라 많은 보안상의 문제점들이 나타났다. 특히, 공공기관 및 기업들은 고속 네트워크와 모바일 컴퓨팅 등을 통해 보다 원활하게 정보를 공유하여 이용하고 있는데, 이와 같이 정보에 대해 개방된 업무 환경에서 최근 여러 가지 정보유출 사고가 발생하면서 기업은 중요 정보 유출방지에 대한 요구를 지속적으로 하고 있다. 이러한 정보 유출에 따른 사고는 해당 기업에 심각한 경제적 피해를 끼침에 따라 문제해결에 대해서 기업 경영진에서 직접적으로 요구하고 있다. 정보 손실은 외부로부터 악의적인 공격보다는 일반 직원들의 부주의, 기업 프로세스 위반, 내부자의 의도적인 유출 등으로 주로 발생함에 따라 보안 USB 메모리 도입을 의무화 하는 등 USB 메모리 관리기준을 강화해야 한다는 목소리가 높아지고 있다.

이와 같이 정보유출을 사전에 방지하기 위해 일반 휴대용 저장장치에도 손쉽게 사용할 수 있는 보안기능을 탑재한 문서관리 시스템을 제안하게 되었다.

2. 요구사항

본 논문에서 제안하고자 하는 실시간 패킷분석을 이용한 안전한 문서유출방지 시스템은 일반 기업체에서 휴대용 저장장치를 이용한 피해를 최소한으로 줄이기 위한 목적을 가진 시스템으로 다음의 요구사항을 가진다.

2.1. 사용자 인증

정당한 사용자만이 내부 문서에 접근 권한을 가질 수 있도록 해야 하며, 그 사용자의 신분이 거짓이 아닌 정당한 사용자라는 것을 증명할 수 있어야 한다.

2.2 기밀성

저장장치 사용 시 정당한 사용자만이 저장장치를 사용할 수 있어야 하며 저장장치로 문서 전송 시 문서는 정당한 사용자만이 전송할 수 있어야 한다.

2.3 무결성

사용자와 서버간의 송수신되는 사용자리스트 정보는 정상적인 사용자 인증을 위해 변조되지 않아야 한다.

반출허용 문서 변환 시 문서에 저장되는 인증패킷은 정상적인 파일 전송을 위하여 변조되지 않아야 한다. 만일 제 3자에 의해 위/변조가 되었다면 그 사실을 확인할 수 있어야 한다.

3. 기존방식 및 관련연구

본 논문에서 제안하는 실시간 패킷분석을 이용한 문서 유출방지에 대하여 유사한 방식인 문서관리 프로그램에 대한 특징 및 장/단점을 분석한다.

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0022607)

<표 1> 문서관리 프로그램 제조사별 분석결과

제조사 / 기술항목	SafePC Enterprise	G-Ware EDMS	Docu Share	Secu Print
사용자 인증	○	○	○	○
매체제어	○	X	○	○
서버 /에이전트	○	○	○	○
전송제어	X	X	X	X

3.1 내부정보 유출방지 시스템(Data Loss Prevention)

내부정보 유출방지 시스템은 기업 구성원, 프로세스, 기술의 결합을 통해 고객 또는 직원 기록 등의 개인정보, 재무재표, 마케팅 계획과 같은 기업정보, 제품 계획, 소스코드와 같은 지적 재산을 포함하는 기밀 정보 등이 기업 밖으로 유출되는 것을 방지하는 솔루션이다.

3.2 문서관리 프로그램

문서관리 프로그램 제품은 회사에서 주로 사용하는 제품으로 문서관리만을 사용하지 않고 주로 회사의 포탈과 웹메일, 기업용 메신저 등 여러 가지 복합적으로 되어있는 솔루션에서 같이 사용되는 프로그램이다. 제품의 사용방식은 회사 내 개인/부서별, 문서의 중요도에 따라 보안설정을 할 수 있으며 데이터베이스 형식으로 문서들이 관리되어 있다 (표 1 참조).

4. 제안방식

본 논문에서는 휴대용 저장장치에 이동하는 문서에 대한 제어기술로 패킷분석방식과 인증패킷방식, 매체제어방식을 사용한다.

4.1 패킷분석방식

패킷분석방식이란 저장장치에서 이동하는 신호들에 대하여 스니핑하는 방식으로 저장장치가 연결되었을 경우 컴퓨터와 저장장치 간 보내는 신호부터 파일의 전송에 관한 내용까지 확인 할 수 있다. 본 논문에서는 패킷분석방식을 사용하여 파일 전송 시 인증패킷으로 파일의 허가여부를 파악하여 정당한 파일인지 확인 후 전송되는 시나리오를 사용하고 있다[1].

4.2 인증패킷분석방식

인증패킷이란 문서의 전송허가 여부를 알 수 있는 고유의 정보를 지니고 있는 패킷을 말하며, 본 연구에서는 문서 전송에 앞서 인증패킷을 삽입하는 과정을 거치게 되며, 문서에 인증패킷을 삽입하는 과정에서는 마킹방식을 사용하게 된다.

마킹방식이란 각각의 문서에 대하여 저장장치 전송 허가여부를 파악할 수 있도록 문서 자체에 인증이 가능한 패킷을 삽입하여 패킷분석 시 확인이 가능하도록 하는 방식이다. 인증패킷의 내용으로는 각 문서들에 해쉬함수를 사용하여 얻어낸 해쉬값이며, 각각의 문서의 헤더부분에 삽입하는 방식으로 사용하게 된다[1] (그림 1 참조).

4.3 매체제어방식

PC에 저장된 파일이나 도면 등의 자료가 외부로 유출되는 것을 방지하기 위하여 파일에 접근 가능한 인가자일 경우에도 관리자의 허가 없이 파일에 대한 저장 및 복사를 할 수 없도록 제어가 필요하다. 저장장치의 제어를 위하여 저장장치를 디바이스와 드라이브로 인식할 수 있어야 하며, 저장장치의 사용을 제어하기 위한 제어값 설정으로 파일의 전송을 제어할 수 있어야 한다. 본 논문에서는 연결되어있는 저장장치에 대하여 강제적으로 연결을 해제하여 파일의 전송을 제어한다. 저장장치에 전송이 허가된 파일 전송 시 일시적으로 전송하려는 저장장치에 대하여 매체제어를 해제시켜서 파일의 전송을 허가하게 된다. 이때 전송이 허가되지 않은 파일전송 시 저장장치에 대한 실시간 패킷분석으로 인증패킷의 유•무를 파악하여 저장장치를 제어하게 된다[2].

4.4 시스템 계수

- * : 참여 객체 (s:서버, c:클라이언트)
- K : 세션키
- KU* : *의 공개키
- KR* : *의 개인키
- uID : 사용자 사원번호
- Pwd : 사용자 비밀번호
- SN : 사용자 저장장치 Serial Number
- Request : 세션키 요청 메세지
- E*[ ] : *의 키로 암호화
- D*[ ] : *의 키로 복호화
- TS : 타임 스탬프
- Auth : 사용자 인증 허가 메시지
- DB : 저장장치 데이터베이스

4.5 서버 / 에이전트 간 키 동기화

본 프로그램에서는 서버와 에이전트간 공개키의 분배가 되어있다고 가정한 상태에서 진행하게 된다. 에이전트는 세션키 요청 메시지와 타임 스탬프를 생성하여 서버의 공개키로 암호화하여 서버에 전송하고 서버는 이를 복호화하여 확인 후 세션키를 생성하여 전송받은 세션키 요청 메시지, 타임 스탬프와 함께 에이전트의 공개키로 암호화하여 에이전트로 전송한다. 에이전트는 개인키로 복호화

[그림 1] 인증패킷 마킹방식

후 세션키를 확인하며, 확인된 세션키를 세션키로 암호화하여 서버에 전송한다[3].

step 1. 에이전트는 세션키 요청 메시지와 타임 스태프를 서버의 공개키로 암호화 하여 서버에 전송한다.

E_{KUs}[Request||TS]

step 2. 서버는 에이전트에서 전송받은 값을 서버의 개인키로 복호화하여 세션키 요청 메시지를 확인 후 세션키를 생성한다.

$D_{KRs}[E_{KUs}[Request||TS]] = Request$

step 3. 서버는 생성한 세션키 K와 전송받은 세션키 요청 메세지와 타임 스탬프를 에이전트의 공개키로 암호화하여 에이전트에 전송한다.

E_{KUA}[K||Request||TS]

step 4. 에이전트는 서버에서 전송받은 값을 에이전트의 개인키로 복호화하여 세션키를 확인하고, 전송받은 세션키를 세션키로 암호화하여 서버에 전송한다.

$D_{KRs}[E_{KUA}[K||Request||TS]] = K$

E_K[K]

4.6 사용자의 저장장치 등록 및 인증

사용자는 저장장치를 사용하기 위해서 에이전트를 통해 서버에 등록하게 된다. 사용자는 저장장치의 등록을 위하여 연결 후 자신의 사원번호와 패스워드를 입력하여 저장장치를 등록한다. 입력받은 사원번호와 패스워드, 저장장치의 Serial Number는 세션키로 암호화하여 서버에 전송되며, 서버는 세션키로 복호화하여 전송받은 정보를 데이터베이스에 입력하게 된다.

사용자 인증단계는 사용자가 사용할 저장장치를 에이전트 PC에 연결 후 사원번호와 패스워드를 통하여 로그인하며 로그인 된 정보를 세션키로 암호화하여 서버로 전송하게 된다, 서버는 세션키로 복호화 후 전송받은 정보를 데이터베이스와 비교 확인 후 인증정보를 발급한다. 발급한 인증정보를 세션키로 암호화하여 에이전트에 전송하게 되며, 에이전트는 복호화 후 인증정보 확인 시 저장장치를 사용할 수 있게 된다[3].

• 등록단계

step 1. 사용자는 에이전트에 저장장치 연결 후 저장장치 등록페이지를 통하여 사원번호와 패스워드를 통해 장치를 등록한다.

step 2. 에이전트는 입력받은 사원번호와 패스워드, 연결된 저장장치의 Serial Number를 세션키로 암호화하여 서버에 전송한다.

E_K[uID||Pwd||SN]

step 3. 서버는 전송받은 값을 세션키로 복호화하여 데이터베이스에 저장한다.

$D_K[E_K[uID||Pwd||SN]] = uID \,||\, Pwd \,||\, SN$

• 인증단계

step 1. 사용자는 에이전트에 저장장치 연결 후 로그인페이지를 통하여 사원번호와 패스워드를 통해 에이전트에 연결한다.

step 2. 에이전트는 입력받은 사원번호와 패스워드, 연결된 저장장치의 Serial Number를 세션키로 암호화하여 서버에 전송한다.

E_K[uID||Pwd||SN]

step 3. 서버는 전송받은 값을 세션키로 복호화하여 데이터베이스와 비교 후 일치할 경우 인증정보를 발급한다.

$DB = uID \,||\, Pwd \,||\, SN$

$D_K[E_K[uID||Pwd||SN]] = uID \,||\, Pwd \,||\, SN$

$uID \,||\, Pwd \,||\, SN \stackrel{?}{=} DB$

step 4. 서버는 발급한 인증정보를 세션키로 암호화하여 에이전트에 전송한다.

E_K[Auth]

step 5. 에이전트는 전송받은 값을 세션키로 복호화하여 인증정보를 확인 후 저장장치가 사용 가능하도록 한다.

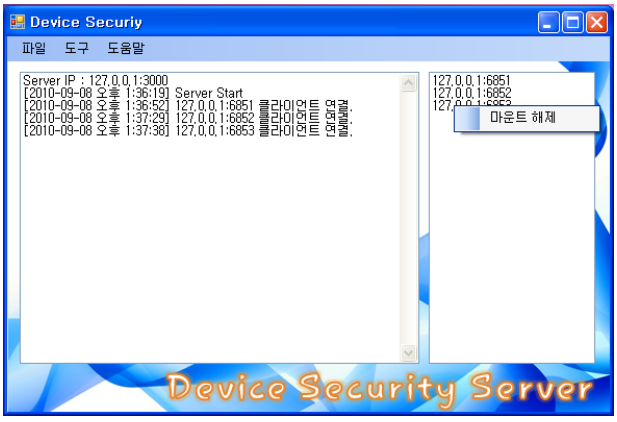
$D_K[E_K[Auth]] = Auth$

5.제안방식 구현

제안방식의 내용을 토대로 실시간 패킷분석을 통한 안전한 문서 유출 방지 시스템을 구현하였다.

5.1 서버 구현 내용

서버에서는 에이전트의 접속 및 파일전송에 대하여 확인할 수 있으며 필요시 강제로 에이전트에 대한 매체제어를 실행할 수 있다[4] (그림 2 참조).



[그림 2] 서버 실행화면

[그림 3] 에이전트 실행화면

5.2 에이전트 구현 내용

에이전트에서는 휴대용 저장장치의 매체제어와 저장장치 등록, 로그인을 통한 저장장치의 파일전송을 사용할 수 있으며, 파일전송 시 인증패킷을 실시간으로 확인하여 매체제어를 실행한다[4,5] (그림 3 참조).

6.제안방식 분석

본 연구의 제안방식은 다음과 같은 보안요구사항을 충족함으로써 다음과 같은 이점을 제공한다. 본 장에서는 2장에서 언급한 요구사항에 따라 분석한다.

6.1. 사용자 인증

사용자의 인증방식은 개인정보와 저장장치의 정보를 기반으로 ID & Password 방식을 사용하여 인증하는 방식을 사용한다.

6.2 기밀성

Server와 Agent 간의 공개키 암호화방식을 적용하여 세션키를 동기화하고 세션키를 통하여 대칭키 암호화 방식으로 데이터를 암호화하여 송·수신함으로 기밀성을 제공한다.

6.3 무결성

Server와 Agent 간의 공개키 암호화방식을 적용하여 세션키를 동기화하고 세션키를 통하여 대칭키 암호화 방식으로 데이터를 암호화하여 송·수신함으로 무결성을 제공한다.

인증패킷 삽입의 경우 문서에 해쉬 알고리즘을 사용하여 문서의 해쉬값을 얻어낸 후 Agent의 공개키로 암호화하여 문서의 헤더부분에 삽입하고 전송시 세션키를 통하여 문서를 암호화하여 전송함으로써 무결성을 제공한다.

7.결론 및 향후 연구 방향

본 논문은 실시간 저장장치 패킷분석을 이용한 문서유출 방지 시스템으로 문서의 등급 및 보안설정만을 제공하는 기존 문서관리 시스템에 비해 강력한 문서보안을 기대할 수 있다. 저장장치의 패킷분석으로 문서의 이동현황을 관리자가 별도의 입력 없이 확인 할 수 있다는 장점을 통해 효율적인 문서관리가 가능하다. 기존 문서관리 시스템과 달리 초기 등록된 휴대용 저장장치의 인증만으로도 별도의 복잡한 인증절차 없이 시스템을 사용 가능하게 함으로써 사용자의 불편을 최소화 하였다.

위의 특성들로 인하여 본 논문의 제안방식을 사용할 경우 휴대용 저장장치로 유출되는 사건사고의 피해가 감소할 것이다. 또한 문서관리 시스템의 발전으로 사용자에게 보다 강력하고 안전한 보안기술을 제공할 수 있으며, 문서관리에 대한 높은 효율성을 제공할 수 있을 것으로 기대된다.

향후 보안 USB와 문서관리 시스템에 응용할 수 있는 방향과 본 논문에서 구현한 프로그램에 추가로 발전시킬 수 있는 방향을 생각하여 구현부분에서도 발전할 수 있는 연구가 필요할 것으로 사료된다.

[참고문헌]

[1] 한국정보통신기술협회 회장, “개인휴대단말 중요정보 유출 방지 운용 모델 및 요구사항”, 한국정보통신기술협회, 2008. 12. 19

[2] 최주호, 류성열, “파일유출 방지를 위한 저장장치 제어 기법에 대한 연구”, 정보·보안 논문지 제 6권 제 2호, 2006. 6

[3] 최용락, 소우영, 이재광, 이임영, “컴퓨터 통신보안 3rd Edition”, 도서출판 그린, 2005. 8. 20

[4] Chris Cant. "윈도우즈 드라이버 모델“, 에이콘출판, 2002. 7. 5

[5] Jan Axelson, "USB 완전정복“, 에이콘출판, 2005. 12. 15