커버로스와 PDF를 적용한 프린터 보안 솔루션의 설계 및 구현

조병희, 김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[choasdl, kimsh, imylee]@sch.ac.kr

Design and implementation of printer security solution apply kerberos and PDF

Byeong-Hee Cho, Su-Hyun Kim, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

기업의 기술이 점점 고도화가 진행되면서 문서유출사건에 대한 기업의 피해가 매년마다 증가하고 있다. 특히 내부직원에 의한 유출사건이 크게 증가함으로써 기업은 내부의 보안수준을 올리고 있다. 이에 기업 내 출력물 보안을 위하여 프린터 보안 솔루션을 도입하지만 강한 보안성으로 인하여 인쇄가 많은 기업이나 부서에서는 잦은 사용자인증에 불편함을 느낄 수 있다. 따라서 본 논문에서는 기존의 출력물 보안 서비스에서 사용자인증의 간소화와 PDF를 통한 권한문서관리 방식을 통하여 보다 향상된 출력물 보안 솔루션을 설계하고 구현하였다.

1. 서론

산업기밀보호센터의 해외 기밀 유출 적발 통계에 따르면 05년부터 매년 기밀 유출 사건이 늘어나고 있다[1]. 이러한 통계들을 바탕으로 기업의 내부유출 방지의 중요성이 증대되고 있다.

일본 네트워크 시큐리티 협회에서 조사한 통계를 참고하면 기업 내부유출에 대한 매체별 유출 비중 중 인터넷이나 USB를 이용하여 문서를 유출보다 출력물을 통한 종이의 유출 비중이 73%를 차지하고 있다[2]. 이러한 문서유출을 방지하기 위하여 일반적인 기업의 보안정책을 살펴보면 외부 해킹에 대한 보안정책은 준비되어 있으나 점차 내부사용자에 의한 유출건수가 증가함에 따라 문서보안에 대한 중요성이 회사 내부 보안으로 초점이 맞춰지고 있다[3].

본위 내용을 통하여 회사의 기밀문서가 대부분 출력물 형태로 유출되고 있음을 알 수 있다. 인터넷이나 USB를 통한 유출방식은 기업 내의 보안 솔루션으로 대부분 감지할 수 있고, 출력물에 대한 보안은 프린터 보안 솔루션을 이용하여 출력물 로그를 생성하여 문서가 유출되었을 때 빠른 사후대처가 가능하게 하고 있다.

기존 프린터 보안 솔루션은 사용자인증을 위하여 인쇄 시마다 사용자의 사번이나 ID를 이용하여 사용자 인증절차를 거친 후 프린터 인쇄를 진행하도록 설계되어 있다. 그러나 회사 내 출력물이 많은 부서의 경우 인쇄를 할 때마다 로그인 절차를 매번 거쳐야 인쇄할 수 있다. 또한 기밀문서 유출시 사후에 적절한 조치를 취하는데 적절한 정보의 부재로 인하여 대응의 어려움이 있다. 때문에 출력을 이용하는 사용자로서는 문서인쇄에 큰 불편을 초래한다.

본 논문에서는 기존의 출력물 보안 서비스와 비교하여 티켓을 이용한 사용자인증의 간소화와 권한에 따른 문서관리를 제공하고 유사시를 대비하여 출력파일을 PDF로 변환하여 로그를 생성하는 출력물 보안 솔루션을 설계 및 구현하였다.

본 논문의 구성은 2장에서 커버러스(Kerberos)인증 메커니즘을 기술하고 3장에서는 프린터 보안 솔루션의 보안 요구사항을 기술한다. 4장에서는 이를 만족하는 제안방식에 대하여 기술하고, 5장에서는 제안방식의 구현에 대하여 기술하며, 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 기존 프린터 보안 솔루션에 대하여 알아보고, 본 논문의 프린터 보안 솔루션 프로그램의 티켓인증에 사용하는 커버로스 인증기술에 대하여 알아본다.

2.1 기존 프린터 보안 솔루션 동향

프린터 보안 솔루션은 기업 내의 프린터작업에 대한 모니터링 및 인쇄물 유출을 방지하기 위한 기능을 제공하고 있다. 그리고 인쇄물 유출을 막기 위하여 프린터 보안 솔루션 내에서 워터마크 및 출력정보 저장기능을 제공함으로써 내부사용자들에게 인쇄물을 이용한 문서유출을 할

수 없도록 하고 있다.

2.2 커버러스(Kerberos) 인증 메커니즘

커버로스 인증 메커니즘은 여러 가지 요소로 구성된 복합시스템으로 인증 서버와 TGS(Ticket Granting Server), 응용서버, 클라이언트로 구성되어 있다. 클라이언트는 응용서버에 접속하기 위해 인증 서버로부터 인증을 얻는다. 클라이언트는 인증 서버로부터 인증을 얻기 위해 패스워드를 사용하여 인증 서버에 자신을 인증 한다. 인증 서버는 인증된 클라이언트에게 티켓발급 서버로부터 티켓을 발행 받는 것을 허락한다, 티켓 발급 서버는 인증된 클라이언트에게 티켓을 발급 하고, 클라이언트는 이 티켓을 사용하여 응용 서버에 접속하게 된다. 티켓의 구성정보는 서버와 클라이언트 이름, 타임스탬프(TimeStamp), 유효시간, 세션키를 포함한다. 인증자는 클라이언트에 의해 생성되고 생성된 인증자는 사용을 1회로 제한하고 있으며 인증정보는 클라이언트의 사용자 이름과 네트워크 주소, 현재의 시간을 포함하고 있다[4].

3. 보안 요구사항

3.1 보안 요구사항

본 연구는 기밀성, 무결성, 사용자 인증에 대하여 다음과 같은 보안 요구사항을 가진다.

- 기밀성: 사용자의 정보를 조회하여 인증티켓을 생성한 후 사용자에게 전송할 때 제 3자가 인증티켓을 획득하지 못하도록 기밀성이 보장되어야 한다.
- 무결성: 서비스서버에서 생성한 인증티켓의 내용과 클라이언트에 전송한 인증티켓의 내용이 일치해야 한다. 따라서 서비스서버에서 인증티켓을 생성한 후 클라이언트에 전송하는 과정에서의 인증티켓의 내용에 대한 위·변조 및 삭제 등과 같이 인증티켓의 변경이 없어야 한다.
- 사용자 인증: 서비스서버에서 관리하는 사용자 데이터베이스의 정보를 이용하여 사용자의 권한에 맞는 인증티켓을 생성하는 것이므로 티켓을 이용한 사용자인증을 진행할 때 티켓을 복호화 하여 사용자의 신원과 권한을 확인할 수 있어야 한다.

4. 제안방식

본 논문에서 제안하는 방식은 사용자인증을 인증티켓을 이용하여 인증하는 방식이다. 즉, 인증 서버와 티켓발급 서버를 통하여 발급 받은 티켓을 통하여 응용 서버와 통신을 하기 때문에 티켓 발급만 된다면 응용프로그램 간의 불필요한 인증 절차를 수행하지 않아 강력한 사용자인증을 제공함과 동시에 사용자 인증과정의 과정을 줄일 수 있도록 설계하였다. 또한, 사후 기밀문서 유출시 로그기록 저장 시 인쇄 문서를 PDF형식으로 포맷을 바꾸어 서비스 서버에 저장을 한다. 이를 통하여 호환성과 파일의 무결성, 보안성과 관리의 편의성을 제공하고 이를 바탕으로 빠른 대처가 가능하다. 이 장에서는 제안방식의 시나리오, 사용자 인증티켓 발급과정, 인쇄 및 사용자인증 과정, 로그생성 및 저장 과정으로 이루어져 있다

4.1 시나리오

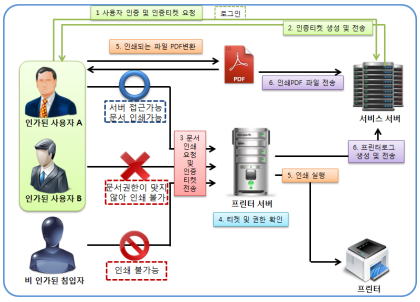
본 연구에서 제안하는 시나리오는 인증티켓을 발급받은 인가자와 인증티켓을 발급받지 않은 비인가자 두 가지의 경우로 나누어서 진행한다. 사용자는 인증티켓을 발급하고 발급받은 인증티켓을 이용하여 프린터 인쇄 시에 사용자 인증 및 권한문서확인 과정을 거쳐서 인쇄 작업을 할 수 있도록 한다(그림 1).

Step 1. 사용자는 서비스서버에 자신의 인증정보를 전송하고 인증티켓을 발급받을 수 있도록 요청한다.
Step 2. 서비스서버는 전송받은 인증정보를 데이터베이스에서 조회하여 사용자의 권한에 맞는 인증티켓을 생성한 후 사용자에게 전송한다.
Step 3. 서비스서버에서 인증티켓을 발급받은 사용자는 프린터서버에 문서인쇄를 요청하며, 자신의 인증티켓과 인쇄문서의 해쉬코드를 프린터서버에 전송한다.
Step 4. 프린터서버는 인증티켓을 확인하여 사용자의 정보와 권한을 확인한 후 문서권한을 조회하여 사용자가 인쇄할 수 있는 문서인지 확인을 한다.
Step 5. 문서 인쇄가 가능하다면 스풀링 데이터를 프린터에 전송하여 인쇄를 실행한다. 또한, 사용자가 출력 문서를 PDF 형식으로 바꾸어 Log전송에 준비 한다.
Step 6. 프린터에서 정상적으로 인쇄를 진행한 후 프린터서버에서 프린터로그를 생성하여 서비스서버에 전송한다.

4.2 시스템 계수

본 프로토콜에 사용 되는 시스템 계수는 다음과 같다.

- * : 참여 객체(s : 서비스서버, p : 프린터서버
  c : 클라이언트 서버)
- AD* : *의 네트워크 주소
- Rgt : 사용자 권한
- H[Docu] : 인쇄문서의 해쉬코드값
- K* : 세션키
- Request : 티켓 요청 메시지
- Time, TS1 : 타임 스탬프



(그림 1) 시나리오

- Lifetime : 유효시간
- Log : 프린터로그
- Nonce : 임시비표
- POK : 인쇄 완료 메시지
- file : 변환된 PDF 파일
- Ticket : E_{KUp}[ID||ADc||Rgt||TS1||Lifetime]

4.2 인증티켓 발급과정

사용자는 인쇄를 진행하기 전에 자신을 인증할 수 있는 인증티켓을 서비스서버에 요청하여 발급받아야 한다. 인증티켓의 발급 순서는 다음과 같다(그림 2).

Step 1. 클라이언트는 티켓발급메시지와 자신의 아이디, 패스워드, 클라이언트 IP 주소와 현재 시간(타임스탬프)을 서비스서버와의 세션키를 이용하여 암호화하여 서비스서버에 전송한다($E_{Kc,s}$[Request||ID||PW||ADc||Time]).

Step 2. 서버는 클라이언트에서 받은 암호문을 세션키로 복호화 하여 클라이언트의 정보로 Ticket을 생성한다. Ticket의 내용은 사용자 ID, IP 주소, 사용자권한, 타임스탬프, 티켓유효시간을 프린트서버의 공개키로 암호화하여 생성한다(E_{KUp}[ID||ADc||Rgt||TS1||Lifetime]).

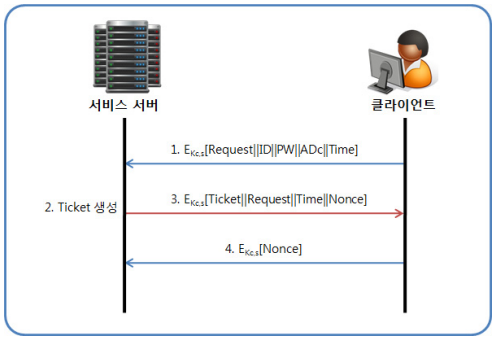
Step 3. 서버는 티켓을 생성한 후에 티켓과 티켓발급메시지, 타임스탬프, 임시비표를 클라이언트와의 세션키로 암호화하여 클라이언트에 전송한다 ($E_{Kc,s}$[Ticket||Request||Time||Nonce]).

Step 4. 클라이언트는 서버에서 전송받은 암호문을 세션키로 복호화 하여 티켓을 획득, 티켓확인 후 서비스서버에 임시비표를 세션키로 암호화하여 재전송함으로써 티켓전송이 완료됨을 확인한다($E_{Kc,s}$[Nonce]).

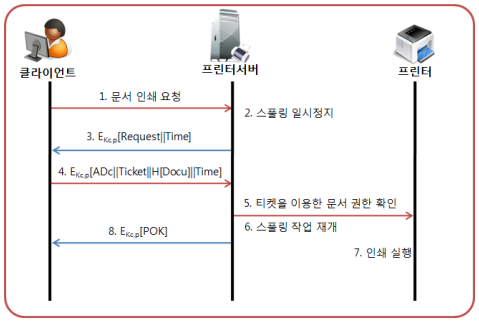
4.3 인쇄 및 사용자 인증과정

사용자는 인증티켓 발급과정을 통하여 인증티켓을 발급받게 되면 프린터서버와의 인쇄과정을 진행한다. 인쇄 및 사용자 인증과정의 순서는 다음과 같다(그림 3).

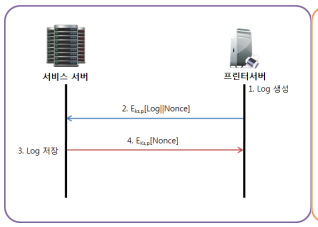
Step 1. 클라이언트는 프린터에 문서인쇄요청 전송한다.



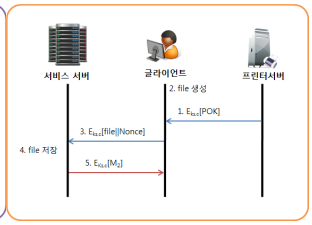
(그림 2) 인증티켓 발급과정



(그림 3) 인쇄 및 사용자 인증 과정



(그림 4) 로그생성 및 전송과정



(그림 5) 파일생성 및 전송과정

Step 2. 프린터서버에 스풀링 정보가 도착하게 되면 서버는 스풀링데이터를 일시정지 한다.

Step 3. 프린터서버는 클라이언트에 티켓요청메시지와 타임스탬프를 클라이언트와의 세션키로 암호화하여 전송한다($E_{Kc,p}$[Request||Time]).

Step 4. 사용자는 서비스서버에서 발급받은 티켓과 인쇄한 문서의 문서 해쉬 코드, 타임스탬프를 세션키로 암호화하여 프린터서버에 전송한다($E_{Kc,p}$[ADc||Ticket||H[Docu]||Time]).

Step 5. 클라이언트에서 암호문을 받은 서버는 세션키로 복호화 하여 티켓을 획득, 자신의 개인키로 복호화 하여 클라이언트인증과 사용자인증을 진행하고, 문서 해쉬 코드를 프린트서버의 해쉬 테이블과 대조하여 사용자의 권한으로 문서인쇄가 가능한지 확인한다.

Step 6. 프린트서버에서 모든 인증이 완료되면 정지되어 있던 스풀링작업을 재개한다.

Step 7. 프린터에서 문서를 정상적으로 인쇄한다.

Step 8. 프린터 서버에서 클라이언트 서버로 인쇄 완료 메시지를 보낸다($E_{Kc,p}$[POK]).

4.4 로그생성 및 전송과정

사용자는 인쇄요청을 하여 정상적으로 인증이 완료되어 프린터인쇄가 정상적으로 이루어지면 프린터서버는 정상적인 인쇄과정에 대한 프린터로그를 생성하고 서비스서버에 전송하여 프린터로그를 관리한다. 로그생성 및 전송과정의 순서는 다음과 같다(그림 4).

Step 1. 프린터서버는 스풀링정보와 인쇄할 문서의 내용을 바탕으로 프린터로그를 생성한다.

Step 2. 프린트서버에서 문서 인쇄완료 메시지가 도착하면 서비스서버에 프린터로그와 임시비표를 세션키로 암호화하여 전송한다.

Step 3. 서비스서버는 클라이언트에게서 받은 메시지를 복호화 하여 얻은 프린터로그를 데이터베이스에 저장한다.
Step 4. 서비스서버는 로그를 정상적으로 받았다는 것을 인증하기 위해 세션키로 임시비표를 암호화하여 재전송한다.

4.5 파일생성 및 전송과정

사용자는 인쇄요청을 하여 정상적으로 인증이 완료되어 프린터인쇄가 정상적으로 이루어지면 프린터서버는 정상적인 인쇄과정에 대한 프린터로그를 생성하고 서비스서버에 전송하여 프린터로그를 관리한다. 로그생성 및 전송과정의 순서는 다음과 같다(그림 5).

Step 1. 클라이언트는 인쇄할 문서를 바탕으로 이를 PDF 파일로 변환한다.
Step 2. 프린트서버에서 문서 인쇄완료 메시지가 도착하면 클라이언트에서 서비스 서버로 보낼 파일을 생성한다.
Step 3. 서비스서버는 클라이언트에게서 전송하는 파일을 정상적으로 저장한다.
Step 4. 서비스서버는 파일을 정상적으로 받았다는 메시지를 세션키로 암호화하여 클라이언트에게 전송한다.

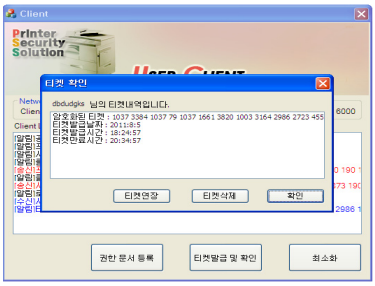
5. 제안방식 구현

본 연구는 Windos XP환경에서 Visual Studio 2010을 통하여 C++언어로 프로그래밍 하였다.

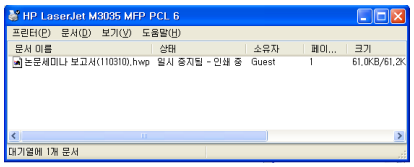
5.1 클라이언트 구현

클라이언트는 사용자의 인증티켓을 발급받으며 인증티켓의 유효시간 연장 및 티켓삭제를 할 수 있도록 구현하였다(그림 6).

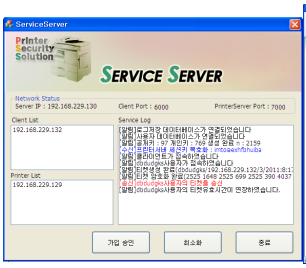
5.2 프린터서버 구현



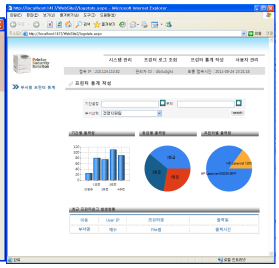
(그림 6) 클라이언트 티켓관리 기능



(그림 7) 스풀링 데이터 일시정지



(그림 8) 서비스서버 폼 구성



(그림 9) 웹페이지 통계 출력

프린터서버는 클라이언트에서 전송받은 인쇄 작업에 대한 사용자인증과정을 가지며 프린터서버에 연결된 프린터의 제어를 담당한다. 그리고 문서의 권한관리를 위하여 문서의 해쉬 테이블을 데이터베이스에 저장하여 프린터서버에서 관리한다(그림 7).

5.3 서비스서버 구현

서비스서버는 사용자 인증티켓을 생성하여 전송하는 기능을 제공한다. 서비스서버 폼에는 클라이언트와 프린터서버의 접속정보 및 서비스서버 로그를 출력하며, 서비스서버 내에서 사용자관리, 프린터로그 관리 데이터베이스를 관리한다(그림 8).

5.4 웹 페이지 구현

웹 페이지는 서비스서버에서 구동되며 서비스서버에서 관리하는 데이터베이스를 관리할 수 있는 기능이 있다. 서비스서버에 저장된 로그를 출력할 수 있으며, 로그 데이터를 이용하여 통계자료를 생성해서 출력할 수 있다. 그리고 서비스서버 내 사용자데이터베이스를 조회하여 사용자관리를 할 수 있다(그림 9).

6. 결론

본 연구는 기존 프린터 보안 솔루션에서의 불편한 점이었던 잦은 사용자 인증절차를 사용자 인증티켓을 이용하여 인증 절차를 간소화하여 프린터 인쇄의 불편함을 줄일 수 있다. 그리고 보안이 필요한 문서들의 출력물 보안강화로 출력물로 인한 국내 기술과 고객들의 개인정보의 외부유출을 방지할 수 있다. 또한, 유사시 PDF의 로그 기록을 통하여 빠른 대응이 가능하다. 따라서 제안방식을 통하여 사용자에게는 편리한 인증을 제공하고 기업에는 강력한 보안을 지원하는 프린터 보안 솔루션을 제공할 수 있을 것으로 기대한다.

참고문헌

[1] 산업기밀보호센터 “해외 기밀유출 적발 통계” 2012
[2] 일본 네트워크 시큐리티 협회, “매체별 유출 비중” 2010.05
[3] 보안뉴스, “기업의 정보보안관리 관련 기사” 2010.11
[4] William Stallings “컴퓨터 보안과 암호” 2011.03