분산 통신망 환경에서 부인방지 서비스를 제공하는 안전한 FTP 설계

최용환°, 박종운, 윤혁중, 이원호, 김동규

아주대학교 컴퓨터공학과

A Design of Secure FTP Supporting Non-repudidation Service in Distributed Network Environment

Yong-Hwan Choi, Jong-Woon Park, Hyuk-Joong Yoon, Won-Ho Lee, Dong-Kyoo Kim

Department of Computer Engineering, Ajou University

요 약

본 고에서는 분산 통신망 환경에서 여러 지역에 분산되어 있는 이기종의 각종 시스템들에게 효율적으로 정보보호 서비스를 제공하기 위해 수행중인 프로젝트의 일부분으로서, 송신자가 송신자의 이득을 위해, 수신자가 수신자의 이득을 위해 메시지를 보낸 적이 없다고 부인하는 것을 방지하는 발신처 부인방지와 수신처 부인방지 서비스의 제공과 통신망에서 오류에 의한 전송 실패와 수신자의 파일의 수신 사실 부인을 구분해 주는 전송 부인방지 서비스를 제공해 주는 FTP를 설계하였다. GSS-API를 사용하여 소스 수준에서 호환성을 갖도록 안전성 서비스들에 대해 일관된 인터페이스를 제공하도록 하였고, 응용 클라이언트와 응용 서버간의 안전한 문맥을 확립하기 위해 세션키를 사용하여 효율적인 키 사용으로 공개키 시스템에서의 오버헤드를 축소하였다. 논문서 설계된 안전한 FTP는 전자상거래 등의 여러 응용에서 활용될 수 있을 것이다.

1. 서 론

급속한 정보화 추세에 따른 컴퓨터의 대량 보급과 전산망의 확대는 정보 이용의 편리성과 효율성을 극대화 시키고 있으며 국가 산업 경쟁력의 근간이 되고 있다. 이러한 정보화 추세는 정보의 신속한 제공, 다양한 정보의 접근 등 여러 측면에서 긍정적인 효과를 가져왔지만 시스템 장애, 컴퓨터 범죄, 컴퓨터 바이러스, 프라이버시 침해 등 역기능적인 부작용 또한 심각하게 대두되고 있다.

현재의 정보보호 서비스 시스템은 지엽적인 정보보호 문제 해결용 상용 제품들이 주류를 이루고 있어서 이들 제품들은 단순한 인증이나 접근통제 서비스만이 적용되고 있는 실정에 있다.

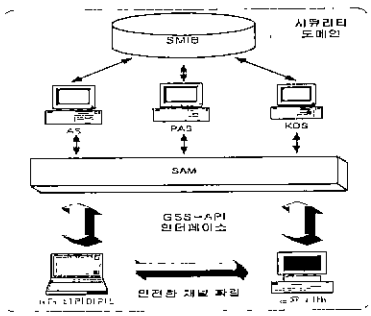
국책개발과제 "분산 통신망 환경에서 통합 정보보호 서비스 소프트웨어 기술 개발"은 통합적인 정보보호 서비스 제공의 요구사항을 해결하기 위한 것으로 인증, 기밀성, 무결성, 접근통제, 부인방지 서비스를 제공할 수 있도록 구현하였다[1].

본 논문에서는 통합 정보보호 서비스 시스템에서 부인방지 서비스 제공을 위한 요소 설계와 부인방지 서비스를 제공하는FTP 모델을 제안하였다. 본 논문의 구성은 2장에서는 통합 정보보호 시스템의 개요와 하부 메카니즘에 대해 소개하며, 3장에서 부인방지 서비스를 제공하는 안전한 FTP 모델을 제안하며, 마지막 4장에서 결론 및 향후 연구 방향에 대해 논의하도록 하겠다.

2. 통합정보보호 시스템 소개

2.1 전체 시스템 개요

통합 정보 보호 시스템은 시큐리티 도메인 서버, 응용 클라이언트, 응용 서버의 세 부분으로 나누어져 있다[그림 1].



[그림 1] 시큐리티 도메인 시스템

시큐리티 도메인 서버에는 인증 서버(Authentication Server), 권한속성 서버(Privilege Attribute Server), 키 분배 서버(Key Distribution Server)가 있고 각 시큐리티 도메인 서버내의 안전한 데이터를 저장하는 장소인 시큐리티 관리 정보 베이스(SMIB)가 있다.

각 서버들의 기능을 간단히 살펴보면, 인증 서버는 사용자에 대한 신분을 challenge-response 스킴을 사용하여 확인해 주고, 권한속성 서버는 사용자에 대한 권한 속성 즉 접근통제를 위해 권한속성 인증서(PAC : Privilege Attribute Certificate)와 키분배 서버에 접근할 수 있는 티켓을 발부해 준다. 키분배 서버의 역할은 양단간에

안전한 세션 확립을 위한 키 분배의 역할을 한다

응용 클라이언트가 특정한 응용 서비스를 요청하면 시큐리티 도메인 서버의 도움으로 인증이 이루어지고 권한속성과 안전한 세션을 위한 세션키를 분배 받게 된다. 응용 클라이언트는 응용 서버가 세션키를 확립하기 위한 정보를 보내주고 이에 따라 응용 서버가 세션키를 분배받은 후에는 응용 클라이언트와 응용 서버간 안전한 통신이 가능해 지는 것이다[1]

2.2 시스템의 특징

2.2.1 GSS-API

[그림 1]에서 보면 알 수 있듯이 사용자(응용 클라이언트나 응용 서버)는 GSS-API 를 호출함으로써 하부 메커니즘을 이용하게 된다. 사용자는 메커니즘의 작동에 관해서는 알 필요가 없고 GSS-API 가 일반적인 형태로 제공하는 서비스들의 인터페이스를 이용하여 정보 보호 서비스를 제공받는다[2].

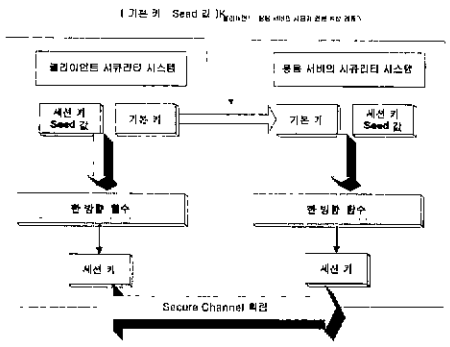
2.2.2 공개키 생성 메커니즘

사용자가 전자 서명 서비스를 요구할 경우 클라이언트 시스템에서는 사용자에 대한 공개키 쌍을 생성한다[6]. 그리고 사용자 공개키에 대한 인증서를 생성하여 인증서에 대한 공증을 받기 위해 키 분배 서버에게 인증서를 보낸다. 이 인증서를 수신한 키 분배 서버는 자신의 비밀키로 전자 서명하여 인증서에 대한 공증을 하고 클라이언트 시스템에게 되돌린다. 안전한 채널이 확립된 이후에 전송되는 데이터에 대해서는 각 사용자가 자신의 비밀키로 전자 서명하고 또한 응용 서버측에서 수신한 데이터는 사용자의 공개키로 검증한다.

본 시스템에서 구현된 전자 서명 서비스 프로토콜에서는 각 사용자에 대한 공개키 시스템에서 사용되는 키 길이를 축소하여 세션 동안에만 사용되어지기에 적합하도록 설계 되었다[1].

2.2.3 세션키 생성 메커니즘

안전한 통신을 하기 위한 채널 확립을 위해 양측의 정보 보호 서비스 문맥 관리기는 기본키와 세션키 패키지를 소유하게 된다.



[그림 2] 세션키 생성 구조

일단 키 정보를 공유하게 되면 세션키를 생성하는 요소들을 가지고 문맥 확립 동안에만 사용하는 무결성 세션키와 기밀성 세션키를 생성한다. 이러한 방법으로 생성한 결과 값을 키로 사용함으로 키 생성에 대한 안전성을 보장할 수 있게 되고 키를 생성한 시드 값의 유출을 방지할 수 있다.

3. 부인방지 서비스 제공 FTP 설계

3.1 설계의 목적

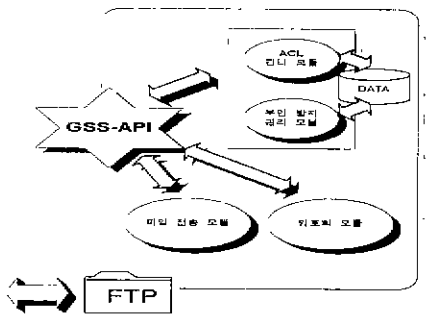
기존의 서비스되고 있는 FTP 들은 사용자의 ID 와 패스워드가 평문으로 전송되기 때문에 안전한 인증 메커니즘을 가질 수 없고, 또한 FTP 서버가 클라이언트의 호스트나 네트워크의 신뢰성을 확인할 수 없어서 침입자에 의해 파괴, 변조, 불법 유출 등이 발생할 수 있다. 이런 문제점은 전자상거래 등 여러 분야에서 FTP 를 활용하는데 장애요소가 되고 있다. 이에 인증, 접근통제, 무결성, 기밀성 서비스를 FTP 가 제공할 수 있도록 하는 연구들이 진행되고 있다

하지만 이들 서비스만으로는 허가된 내부 사용자에 의한 불법 행위 발생에 대해서는 보호를 해 줄 수가 없다. 즉, 메시지의 수신자가 메시지 수신사실 자체를 부인하거나, 수신된 메시지 내용을 변조하여 자신에게 이로운 변조된 메시지를 받았노라고 하는 행위나 메시지의 송신자가 메시지의 발신사실 자체를 부인하거나, 송신된 메시지를 변조하여 자신에게 이롭도록 수정한 후 자신이 보낸 메시지라고 주장하는 행위를 막지 못하는 것이다[3,8] 본 논문은 부인방지 서비스를 제공하는 가장 안전한 FTP 서비스를 제공하기 위한 것이며, 이를 통해 전자상거래 등의 응용에 활용할 수 있도록 하기 위한 것이다

3.2 설계의 특징

기존의 FTP 가 정보보호 서비스를 제공하지 못하므로, 서비스를 제공하기 위해 추가적인 모듈이 설계되어 첨가되었다. 이 모듈들은 기존 FTP 의 파일 전송 모듈과 롤베이스 접근통제를 제공하기 위한 ACL 관리 모듈, GSS-API 처리 모듈, 부인방지 정책 관리 모듈들이다

설계된 FTP 의 모듈의 구조는 [그림 3]과 같다. 시큐리티 도메인 시스템이 구축으로 설계된 FTP 는 다음과 같은 특징을 갖는다.



[그림 3] FTP 의구조

- 사용자가 시큐리티 도메인의 인증서버에 의해 인증되어 있기 때문에 응용에서의 개별적인 인증과정이 필요 없으므로 FTP 의 로그인시에 사용자 인증이 필요 없다
- 사용자는 권한속성 인증서의 롤(role)정보에 의해 접근권한을 갖으므로 FTP 는 롤베이스 접근통제를 사용한다.
- 세션키 사용에 의해 안전한 채널이 확립되었으므로 FTP 클라이언트와 서버간의 기밀성이 보장된다
- 분쟁 발생시에 해결을 위해 사용되는 부인방지 증명서는 사용자가 직접 수정하기나 위조할 수 없도록 시큐리티 도메인 서버에 의해 SMIB 에 저장되고 관리되므로 부인방지 증명서의 무결성과 기밀성이 보장된다

3.3 FTP 서비스의 운영 정책

FTP 서버는 관리자에 의해 3 가지 운영 정책으로 부인방지 서비스를 제공한다.

- 정책 1 : FTP 클라이언트와 세션키를 사용하여 기밀성 서비스만을 제공한다
- 정책 2 : FTP 클라이언트의 요청 메시지에 대한 발신처 부인방지 증명서를 요구하고, 전송하는 파일과 함께 수신처 부인방지 증명서를 전송하여 클라이언트의 요청에 대해 부인방지 서비스를 제공해 준다
- 정책 3 : 클라이언트의 파일 수신 사실을 부인방지하기 위해 전송 부인방지 증명서를 요구하는 것으로 클라이언트는 전송 부인방지 증명서를 서버에 제출하지 않으면 파일을 암호화한 세션키를 얻기위한 시드 값을 얻지 못하게 되어 수신한 파일에 대한 복호화를 할 수 없게 된다

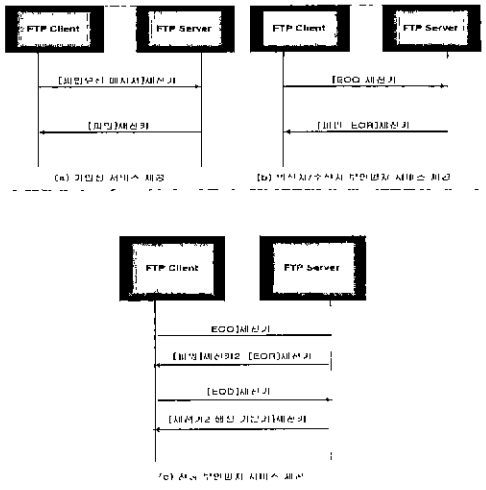
3.4 부인방지 증명서 종류

부인방지 증명서는 다음과 같은 3 가지 증명서가 사용된다

- 발신처 부인방지 증명서(EOO : Evidence of Origin)
  클라이언트가 요청한 메시지에 대해 클라이언트의 비밀키로 전자서명을 한 증명서로 FTP 서버가 분쟁 발생에 대비해 SMIB 에 저장한다
- 수신처 부인방지 증명서(EOR: Evidence of Receipt)
  FTP 서버가 클라이언트가 전송한 메시지의 수신 사실을 부인하는 것을 방지하기 위한 것으로 서버의 비밀키로 전자서명을 한 증명서로 클라이언트에 의해 SMIB 에 저장된다
- 전송 부인방지 증명서(EOD: Evidence of Delivery)
  클라이언트가 요청한 파일에 대해 FTP 가 파일을 전송하면 클라이언트는 파일을 수신했음을 서버에게 통지하는 증명서로 클라이언트가 파일을 수신받고도 이 사실을 부인하는 것을 방지한다 클라이언트는 전송 부인방지 증명서를 서버에게 전송하지 않으면 서버에게서 파일을 암호화한 세션키를 얻기 위한 기본키 값을 얻지 못하므로 수신한 파일을 복호화할 수 없게 된다

이들 증명서에는 부인방지 증명서 타입, 송신자의 식별자, 수신자의 식별자, 증명서 생성자의 식별자, 요청한 메시지 의 다이제스트, 증명서가 생성된 때를 식별할 수 있는 신뢰할 수 있는 타임 스탬프 등의 정보가 들어간다[7].

3.5 프로토콜 흐름도



[그림 4] 정책별 프로토콜 흐름도

EOO = [클라이언트 ID, 서버 ID, H(FTP 서비스 요청 메시지), 타임스탬프] 클라이언트비밀키
EOR = [클라이언트 ID, 서버 ID, H(EOO),타임스탬프] 서버비밀키
EOD = [FTP 로그정보, 타임스탬프] 클라이언트비밀키

부인방지 서비스를 위해 정책별로 프로토콜이 확장되었다 정책 2 가 적용되는 경우에는 클라이언트는 발신처 부인방지 증명서를 전송하고, FTP 서버는 수신처 부인방지 증명서와 파일을 전송해 준다 정책 3 이 적용되는 경우 FTP 서버는 파일을 제 2 의 세션키로 암호화해서 전송해주며, 클라이언트는 전송 부인방지 증명서를 FTP 서버에 전송해 주어서 FTP 서버에게서 제 2 의 세션키를 생성하기 위한 기본키를 수신받아야 파일을 복호화하여 사용할 수 있다 이 프로토콜들은 사용자가 직접 전자서명을 하고, 증명서를 다시 전송하는 것이 아니라 시큐리티 도메인 내에 인증서버에 한 번 인증을 받으면 시큐리티 도메인의 모든 시스템에 같은 정보가 유효하기 때문에 다시 로그인을 할 필요 없이 FTP 의 내부 모듈서 정보보호 서비스를 모두 처리해 주는 것이다 응용에서 GSS-API 를 이용해 사용자에게 투명한 하부 메커니즘을 작동하기 때문에 편리함을 제공하고 있다

4. 결론 및 향후 연구

본 논문에서는 분산 통신망 환경에서 송수신자간의 부인방지 서비스와 파일 전송에 대한 전송 부인방지 서비스가 제공되는 FTP 서비스를 제안하였다 세션키의 사용으로 공개키 시스템에서의 오버헤드를 최소화한 효율적인 암호화 시스템과 GSS-API 를 이용하여 시큐리티 도메인 내에서 응용에 독립적으로 부인방지 서비스가 제공될 수 있도록 설계되었다 관리자가 보안 수준에 따라 정책 운영 레벨을 선택하여 부인방지 서비스를 제공 할 수 있도록 하였다 부인방지 서비스가 제공되면 신뢰할 수 있는 통신망을 제공할 수 있게 될 것이고 지불 처리 프로토콜과의 확장을 하면 전자상거래 등의 응용에서 활용할 수 있을 것이다

향후 연구 방향은 구현된 시큐리티 도메인의 시큐리티 서버들과 안전한 FTP 와의 연동을 구축할 것이며, 응용 개발시에 가장 중요한 것이 편리성과 신속성, 안정성이므로 계속적인 테스트를 통해 요구사항을 해결할 것이다. 또한, GSS-API 의 표준에서는 부인방지 서비스를 지원하지 않기 때문에 약간의 변형을 하여 사용하였는데, 표준화 동향 등을 조사하여 확장된 GSS-API 표준에 맞도록 수정을 할 것이다.

[참고 문헌]

[1] 김동규, 최용희 외, 분산통신망 환경 통합정보보호 서비스 소프트웨어 기술, 2 차년도 연구개발보고서 1998
[2] J. Linn, GSS-API Version 2, RFC 2078, 1997
[3] ISO/IEC 13888-1, "Information Technology - Security Techniques - Nonrepudiation - Part 1 General Model", ISO/IEC JTC1 SC27, 1997.
[4] ISO/IEC 13888-2, "Information Technology - Security Techniques - Nonrepudiation - Part 2 Using Symmetric Encipherment Algorithms', ISO/IEC JTC1 SC27, 1998
[5] ISO/IEC 13888-3, "Information Technology - Security Techniques - Nonrepudiation - Part 3 Using Asymmetric Encipherment Algorithms", ISO/IEC JTC1 SC27, 1997
[6] J Nechvatal, "Public-Key Cryptography', NIST, 1991
[7] J. Zhou, D Gollmann, "A Fair Nonrepudiation Protocol" Proceedings of 1996 IEEE Symposiu Security and Privacy, 1996
[8] J Zhou D Gollmann, 'Observations on Nonrepudiation" Proceedings of Asiacrypt'96, 1996