RC4 스트림 암호방식을 이용한 데이터 파일의 보호

이경원 김정호
한밭대학교 컴퓨터공학과 통신서비스연구실
kwlee@hanbat.ac.kr jhkim@hanbat.ac.kr

요약

90년대를 전후하여 개인용 컴퓨터 보급이 일반화되면서 기업체 또는 공공기관 등의 전산 정보체계도 중앙 Host 중심에서 PC 중심의 전산체계로 정착되어가고 있는 추세이다.

그러나 이러한 정보 처리 시스템의 중심이 되는 PC는 누구나 쉽게 조작할 수 있다는 용이성에 의해 외부인의 무단 자료 유출 가능성은 항상 내재하고 있으며 자료 보관을 목적으로 하는 보조기억매체에 의한 자료 유출 가능성은 더욱 가중되고 있다.

PC에서의 보안을 위해 대형 시스템에서와 마찬가지로 종합적이고 체계적인 대책이 필요하다. 그러나 PC의 경우 그 특성상 전문 오퍼레이터의 고용, 별도의 안전한 장소 확보등 대형 시스템과 같은 수준의 보안체계 유지는 곤란하다. 그러므로 PC가 공유하는 환경에서 이에 적절한 체계적인 보안 대책이 다음과 같이 요구된다.

첫째가 환경적, 행정적 보안으로써 PC 노출환경에 따른 시스템의 고장 등을 고려한 "사무실내의 금연"과 같은 규율 적인 대책과 보안의식, 고취 및 시스템의 사용절차를 규정하는 등의 보안 절차를 말하며, 둘째로 물리적인 보안으로써 외부적인 보호대책을 위한 인원통제, 출입문의 견고한 잠금 장치 등을 들 수 있으며, 마지막으로 기술적인 보안 대책으로써 시스템 내부로의 접근을 통제하기 위한 Lock기능이나 인증기능, 그리고 불법적인 자료접근이나 우연한 노출로부터 자료의 비밀성을 유지하기 위한 자료의 암호화 방법 등이 있다.

본 연구에서는 데이터 파일의 최종 보호수단은 데이터 자체를 암호화하여 보관하는 것이라는 점에 착안하여 PC 데이터 파일의 암호시스템을 설계, 구현하여 주요 데이터의 손실 또는 외부 유출을 최소화하는 방안을 제시하는데 그 목적이 있다.

데이터 보호를 위한 암호시스템에는 하드웨어적 장비를 이용하는 시스템과 소프트웨어적 프로그램을 이용하는 시스템으로 구분할 수 있는데 하드웨어적인 방법은 암복호화시 소요되는 시간을 최소화할 수 있고 강도 높은 보안성을 유지시켜 줄 수 있으나 장비를 갖추는데 비용이 많이 소요되고 장비 사용의 융통성이 부족하다는 단점을 갖고 있다.

이와 반대로 소프트웨어적인 프로그램을 작성하여 사용할 경우에는 암복호화 시간이 많이 소요되고 프로그램 자체의 보호 대책이 강구되어야 하지만 값싸게 활용될 수 있고 컴퓨터 시스템의 어느 곳에서나 융통성 있게 사용될 수 있다는 장점을 갖추고 있다.

본 연구에서는 계속 확대 보급되고 있는 PC와 보조기억매체에 수록되는 데이터의 보호를 위한 암호시스템을 연구대상으로 선정하여 지금까지 공개되어 일반화된 암호화 기법들을 고

찰하고 이를 토대로 적합한 소프트웨어적인 암호시스템을 설계, 구현하며 그 결과를 분석하여 시스템의 효율성을 평가해 보고자 한다. 구현된 암호시스템은 사용자가 암호화 시스템에 신경 쓸 필요 없이 원하는 데이터를 암복호화 되도록 하는 암호화 방식으로, 암호화 알고리즘은 비밀키 암호방식 중 word 단위의 연산을 위주로 하는 S/W 구현용 스트림 암호중 대표적인 RC4를 사용하였으며, 데이터에 대한 무결성을 확인하는 방법으로는 해쉬 함수의 대표적인 MD5를 적용하여 설계하였으며, 프로그램은 Microsoft사의 Visual C++로 구현하였다.

본 암호시스템은 데이터파일의 최종 보호수단은 데이터자체를 암호화하여 보관하는 것이라는 점에 착안하여 내장된 데이터파일을 관리하는데 중점을 두었다. 따라서 시스템의 암호화 알고리즘은 앞에서 살펴본 알고리즘 중에서 데이터파일을 암호화/복호화 하므로 비밀키 암호방식을 이용하였으며, 파일의 기본연산이 용이하도록 설계하여야 하기 때문에 블록암호화 방식을 배제하고 스트림 암호방식을 적용하였다. 따라서 본 논문에서는 암호화 알고리즘은 비밀키 암호방식 중 word 단위의 연산을 위주로 하는 S/W 구현용 스트림 암호중 대표적인 RC4를 사용하였으며 데이터에 대한 무결성을 확인하는 방법으로는 해쉬 함수의 대표적인 MD5를 적용하였다.