비밀키 분할적용 정보보안 프로토콜

임 근
서울보건대학 전산정보처리과
lk04@shjc.ac.kr

Information-Security Protocol Using Secret-Key Splitting

Lim Keun
Dept. of Computer Information Process, Seoul Health College

요 약

본 논문에서는 암호화에 사용되는 키를 보호하기 위해서 비밀분할 프로토콜에 기반한 유일한 식별자인 사용자의 시스템 속성과 정보 소유자가 제공하는 임의의 값을 이용하여 키를 생성하는 방법을 제안하였다. 이것은 해독키를 전달할 필요가 없으며 복사된 정보를 비권한 사용자 시스템에서 재생할 수 없다는 의미이다. 또한 전달되는 메시지마다 암호키가 다르기 때문에 해독키가 발견되더라도 다른 시스템에서 적용이 불가능하므로 정보보안을 가능하게 한다.

1. 서 론

개방형 네트워크의 급속한 발전과 정보 인프라의 구축을 통해 수 없이 많은 정보의 교류가 진행되고 있으며, 정보의 안전성과 신뢰성을 보장하기 위한 수단으로서 암호가 적용되고 있다. 인터넷을 통한 정보 전달시 보호하고자 하는 기존의 방법들은 대부분 정보를 암호화된 형태로 전달하고 해독키를 권한이 있는 특정 사용자에게만 비밀리에 전달하는 방법을 사용하고 있다. 이러한 방식의 경우 비권한 사용자에게 노출될 수 있는 가능성이 있다. 따라서 암호키가 노출되더라도 정보를 사용할 수 없도록 하는 방안이 필요하다[1,2]. 본 논문에서는 일반적으로 사용되고 있는 방법 중에서 암호화 정보전달 방법에서 해독키 분실 및 노출로 인한 문제점을 방지할 수 있는 비밀분할 프로토콜 이용방법을 적용해 보았다. 이를 통해서 정보보안을 가능하게 할 수 있는 방법을 모색하는 것이 본 논문의 목적이며, 본 논문의 구성은 2장에서 보안 요구 사항 및 암호기술을 비교하고 3장에서 비밀분할 프로토콜을 사용한 보안 방법을 설명하고 4장에서 결론 및 향후 과제를 제시한다.

2. 정보보안 및 암호화 기술

2.1 정보보안

웹 상에서의 보안 요구사항은 클라이언트 인증, 웹 서버 인증, 웹 서버에 있는 문서 정보에 대한 접근제어, 서버와 클라이언트 사이에 일어나는 트랜젝션 데이터의 인증, 무결성과 기밀성 등에 대한 요구사항들로 요약할 수 있다. 이러한 요구 사항들의 발생요인은 네트워크의 특성상 도청자 또는 비권한 사용자의 공격이 가능하며, 이들을 통해 평문 또는 암호화 키를 발견하려는 시도 및 과정이 빈번히 발생하기 때문이다[3]. 이러한 시도에 대하여 방어하려는 수단으로 암호 기술이 발전하고 있다. 디지털 정보의 권한을 보호하는 기술은 불법적인 사용을 사전에 예방하는 방법과 불법적인 사용을 검출해 내는 사후처리 방법으로 구분할 수 있다.

2.2 암호화 기술

암호화기술은 사용되는 키의 종류에 따라 암호화 키와 복호화 키가 같은 비밀키 암호알고리즘과 암호화 키와 복호화 키가 다른 공개키 암호알고리즘으로 구분되며, 비밀키 암호알고리즘은 변환하는 방법에 따라 블록 암호알고리즘과 스트림 암호 알고리즘으로 구분된다. 정보보안을 위한 암호화는 정보의 기밀성을 지킬 수는 있지만 정보 내용에 대한 보증을 해줄 수 없다는 문제점이 있으며, 이 같은 내용에 관한 보증은 인증기능과 전자서명 기법으로 해결 가능할 것으로 판단된다. 또한 정보사회가 고도화될수록 통신정보의 불법적인 도청과 함께, 원거리 접근의 경우 발생되는 개인 식별 문제, 컴퓨터 정보의 무단 삭제 및 변조 등의 무결성 문제가 심각한 문제로 대두되고 있다. 이런 문제를 해결하는 암호기술이 정보보호 프로토콜(Cryptographic protocol)기술이다. 대표적인 정보보호 프로토콜로는 전산망에서의 상대방의 신분을 확인하는 개인식별 및 인증기술, 현재의 도장이나 서명을 정보사회에 적합하게 변화시킨 전자서명기술 등이 있으며 현재 많은 관심과 시급한 개발이 요구되는 전자결재 및 전자화폐도 정보보호 프로토콜기술의 응용분야이다.

3. 정보보안 프로토콜

본 논문에서는 디지털정보를 보호하는 가장 보편적인 방법인 정보를 암호화하여 전달하는 방법을 개선하고 나아가 안전한 디지털 정보 소유자의 권한을 보호할 수 있는 방법을 제시하고자 한다. 암호기술을 통한 정보보호

에는 암호 설계, 암호 분석, 암호구현 등으로 분류 할 수 있다. 본 논문에서는 암호 설계의 관점에서 다루고 있으며 이것의 세부방식으로 비밀키 방식, 공개키 방식 및 키 관리 방식으로 구분할 수 있다[4]. 비밀키 방식의 경우 블록 알고리즘, 스트림 알고리즘을 적용하는 것이 일반적이며, 공개키 방식의 경우 인수분해, 이산대수에 기반한 방식을 주로 사용하고 있다. 본 논문에서는 파일 형태로 해독키가 제공되는 문제를 해결하기 위해서 사용자에게 키를 전달하지 않고 사용자가 이미 가지고 있는 정보로부터 해독키를 만들어내는 방법을 사용하였다. 사용자마다 다른 암호키를 사용하기 위해 사용자가 가지고 있는 하드웨어의 속성을 정보로 사용한다. [3,5]

3.1 비밀분할 프로토콜

공개키의 최대의 문제점으로 하나의 암호키가 알려지면 모든 정보가 노출될 수 있으므로 이러한 위험을 줄이기 위해 키를 분산, 저장하는 비밀분할 프로토콜을 사용한다. 비밀분할 프로토콜은 퍼즐과 같이 조각으로는 의미가 없고 조각이 조합을 이루었을 경우에 의미가 있는 것을 의미한다. 정보를 한 사람에게 모두 공개할 경우 비밀 유지가 어렵다고 가정한다. 이러한 정보를 분리하여 보관하고 이것이 모두 모아졌을 때 의미 있는 정보가 된다는 것이 비밀분할 프로토콜이다. 본 논문에서는 사용자와 정보소유자간에 비밀분할 프로토콜을 적용한다. 사용자는 사용자 시스템사양을 킷값으로 가지며, 소유자는 임의의 킷값을 생성하여 제공한다. 사용자와 소유자의 킷값을 조합하여 암호키를 만들어내서 이후에 사용자가 암호키를 해독하여 사용한다. 이 경우 암호키가 사용자에게 노출되더라도 사용자 시스템 사양이 변수로 사용되므로 비권한 사용자의 단말기에서는 해독이 불가능하다[6,7].

3.2 암호키 설계

사용자로부터 직접 추출하는 값만으로 암호키를 생성할 경우의 문제점은 하나의 암호키가 노출되면 모든 정보가 노출될 수 있기 때문에 여기에 해독키 값을 구할 수 있는 식별키 값을 부여한다[8,9]. 사용자 시스템 속성값은 컴퓨터마다 가지는 유일한 값으로 포맷 등과 같은 과정을 거쳐도 새로운 값으로 교체하거나 재등록 과정을 거쳐서 속성값으로 사용할 수 있다. 정보 소유자는 임의의 킷값을 생성하여 암호키 구성에 이용하며, 임의의 킷값은 데이터베이스에 저장하여 권한사용자 여부를 파악한다. 비밀분할 프로토콜에 기반한 보안방법은 위에서 제시한 암호와 설계 방법에 의하여 사용자시스템의 사양을 전달받고자 하는 정보 소유자에게 알려주고, 정보소유자는 입력받은 사용자의 속성값 과 소유자가 제공하는 임의 값을 이용하여 암호키를 생성하여 해독시에 이용한다[10].

0 암호키 생성

Ek = Sv C ψ(n)

Sv = mh (m : mac add, h : harddisk no)

0 해독키 생성 : Sk = Ek(ψ(n)) C Sv

- 사용자 시스템 속성으로 m 와 h를 선정하여 합성수 Sv =mh 를 정의한다.

(m : mac 주소, h : hard disk number)

- n을 공개하고 ψ(n)과 서로소인 임의의 정수 e를 선택, 공개키로 한다.

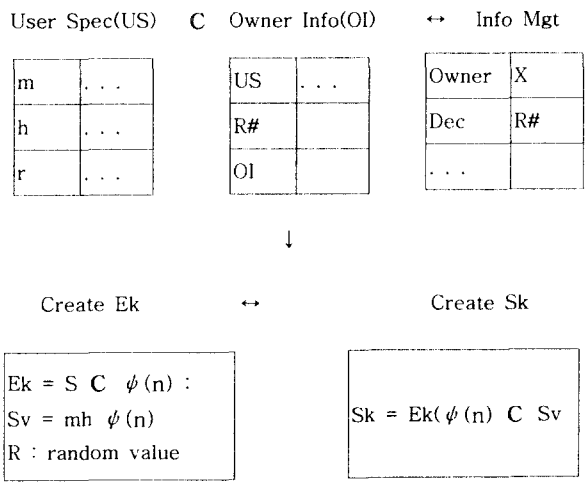
(n 이 두 소수의 곱 일 때 ψ(n)=(m-R)(h-R))

- R : 정보소유자가 제공하는 임의의 값

- ed ≡ 1 (mod ψ(n))이 되는 d를 구해 비밀키로 정한다.

3.3 적용방법

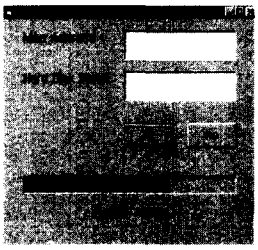
사용자와 정보 소유자간에는 서로 비밀분할 프로토콜에 의하여 자신만의 킷값을 가지고 있다[2,8]. 사용자의 경우는 시스템 사양을 유일하게 가지고 있으며, 소유자는 유일한 암호키를 생성할 수 있도록 해당 사용자마다 상이한 임의의 값 R을 생성하여 해독키와 함께 사용자에게 제공한다. 이때 소유자는 사용자정보를 DB에 기록한다. 미리 전달받은 해독키에서는 사용자 시스템 속성을 직접 읽어들이고 해당 값과 해독키에 담겨져 있는 임의 값을 조합하여 해독키를 만들어 낸다. 해독키에서는 정보가 사용되는 사이에 시스템 속성을 읽어 권한 사용자인지를 체크한다. 따라서 암호키가 사용자에게 알려지더라도 시스템 속성이 암호키의 변수로 사용되므로 비권한 장치에서는 정보의 해독이 불가능하게 된다[11]. 이전의 키 전달 방식은 해독키를 비밀스럽게 전달하므로서 해독키가 노출되면 비권한 사용자의 사용을 제한할 수 없다. 이것을 방지하기 위해서, 본 논문에서는 비밀분할 프로토콜을 적용하여 모든 메시지 마다 암호키를 다르게 하여 키가 발견될 위험을 최소화하였다[12].



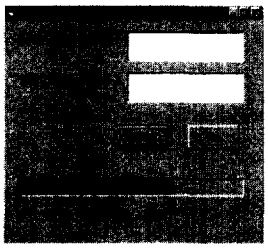
[그림 1] 시스템 속성 값과 암호화 과정

3.4 적용 예

디지털 정보 관리를 위한 동작은 다음과 같다. 그림 2 로그인 과정에서 등록절차를 수행한다. 이 과정에서 사용자의 시스템 사양을 입력하고 지불수단과 같은 정보를 소유자에게 전달한다.

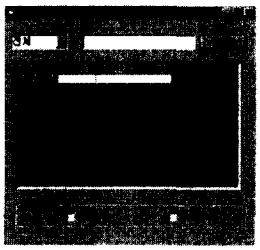


[그림 2] 초기화



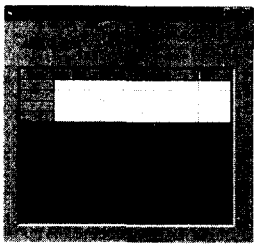
[그림 3] 정보선택

[그림 4] 선택 정보전송



[그림 5] 정보해독

그림 3에서 사용자가 원하는 각종 자료를 선택하여 소유자로부터 전송 받는다. 이때 소유자는 사용자에게 임의 값을 부여하여 암호키를 생성하고, 그림 4에서는 전송받은 정보에 대한 해독을 위한 과정으로 사용자 단말기 정보와 정보 소유자의 임의 값의 조합에 의해 해독이 진행된다. 이때 일치된 정보에서만 해독이 가능하다. 그림 5는 사용자의 정보 및 소유자가 제공한 임의 값과 더불어



[그림 6] 사용자정보 DB

사용자 정보 DB에 보관한다. 이를 통해서 이후에 발생될 수 있는 각종 분실 문제 등을 해결하도록 한다.

4. 결 론

암호키에 사용된 키를 사용자에게 알리지 않고 전달할 수 있는 방법과 정보를 사용하는 중에 정당한 사용자 여부를 확인하는 방법을 제안하였다. 암호키를 사용자의 유일한 정보인 하드웨어 속성과 정보 소유자가 제공하는 임의 값을 이용하여 만들고 이 값을 비밀분할 프로토콜을 사용하여 분리 저장한다. 본 논문에서 제안한 방법은 해독키를 별도로 제공할 필요가 없다는 것과 해독키가 노출되더라도 불법 복사된 정보를 다른 사용자 시스템에서 재생할 수 없다. 또 사용자나 전달되는 메시지마다 암호키가 모두 달라서 해독키가 발견되더라도 하나의 정보에 국한되기 때문에 위험성을 줄일 수 있어서 정보에 대한 권한을 보호할 수 있다. 추후 과제로는 실제로 교환되는 정보의 내용 보안에 관한 메시지 인증과 전자서명 방법 등을 주제로 다루어야 한다. 즉, A로부터 정보를 받기 원하는 B가 실제로 자료를 받았지만 중간과정에서 내용의 변경과 같은 사실을 확인할 수는 없다. 이러한 문제를 해결하기 위한 방법으로 메시지 인증기능과 전자서명 기법이 요구된다.s

참고문헌

[1] 데이터베이스 보안 기술, 정보처리학회지, Vol. 4, No. 2, pp33-43, 1997.

[2] 두소영, 공은배, "하드웨어에 종속된 암호키 비밀 분할을 이용한 정보권한 관리 시스템", 정보과학회 논문지, Vol.27, No.3 pp345-351, 2000.

[3] 이철원, 김홍근, "정보보증: 컴퓨터 보안의 새로운 파라다임 ", 정보과학학회지, Vol 18, No. 1, 2000.

[4] The joint Staff, Information Assurance : Legal, Regulatory, Policy and Organizational Considerations, 3rd Ed., Sep. 1997.

[5] Simson Garfinkel & Gene Spafford, "Practical UNIX & Intenet Security", 2nd Ed, O'Reilly & Associates, Inc. 1996.

[6] H. Debar, M. Dacier, and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Research Report RZ3030, IBM Research, June 1998.

[7] Nasir Memon and Ping Wah Wong, " Protecting Digital Media Content" Communications of the ACM, Vol.41, No.7, pp.35-43, 1998.

[8] 정보통신부, 정보시스템 침해사고 방지기술 개발에 관한 연구, Jan., 1999.

[9] Bishop, M., S. Cheung and C. Wee, the trreat from the Net, IEEE Spectrum, August, pp.56-63, 1997.

[10] Didio, L., Federal agencies fail security test, Computer World, May, 1998.

[11] Lawson, S., Web security to get simpler, InfoWorld, pp.1-24, July, 1997.

[12] Fraser, J. N., Fraser and F. McDonald, The strategic challenge of electronic commerce : Insight from industry, Management , International Journal, Vol.5, No.1, pp.7-14, 2000,