제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

전자지불 system 보안을 위한 인증 system 의 구현

장유진*, 최용식*, 신승호*
*인천대학교 컴퓨터공학과
e-mail: ktiger@incheon.ac.kr , mars@incheon.ac.kr , shin0354@incheon.ac.kr

Authentication System Implementation for Electronic Payment System Security

Yujin Jahng, Yong-Sik Choi, Seung-Ho Shin
Dept of Computer Science & Engineering, University of Incheon

요약

There are many security problems in the electronic payment system because it is built into the open network. Security problems include both system penetrations from outside and unauthorized access by the inside. Nevertheless, the integrity of messages can be guaranteed through a transfer message with the SEED and HASH encryption algorithm. This paper demonstrates how electronic payment system messages and the information they contain can be made safeguarded using the SEED and HASH encryption algorithm, even when there may be some information loss.

1. 서론

정보통신 분야는 컴퓨터와 통신 기술의 결합으로 환경이 급격히 변화하면서 전 세계적으로 Internet 의 용도가 지금까지의 학술 및 연구를 대상으로 한 정보 공유 목적에서 Internet 을 Marketing 의 대상으로 보고 이를 상업적으로 이용하고 있다. 즉, Internet Banking, Online Shopping mall 등 각종 물건을 판매하고, 대금을 지불하는 형태(E-Commerce)로 이루어지고 있다. 대금을 지불하기 위해서는 신용카드 번호, 신용카드 비밀번호, 신용카드 만료일, 카드개인 신상등, 지불에 필요한 정보를 주고 받는다. 전자 지불(Electronic Payment)은 전자상거래에서 구매한 물건의 대금을 전자화폐로 결제하는 행위를 말하고, 전자지불시스템은 거래에 참여하는 고객, 판매자 등이 서비스와 상품에 대한 대가를 안전하고 효과적으로 주고받을 수 있는 정보전달 및 대금 지불 체계이다. 따라서 전자지불 시스템은 Internet 을 기반으로 하여 빠르게 발전하고 있다. Internet 이 시간과 공간의 구애를 받지 않는다는 장점을 이용하여 각종 거래가 활성화되며, 특히 Mobile 기기를 사용할 때는, 언제 어디서나 누구나 쉽게 접근할 수 있는 개방형 Network 의 특성에 따라 보안사고의 위험이 증가하고 있다. 이를 안전하게 수행하기 위하여 암호화로 지불 정보 및 구매 정보의 기밀성을 보장하고, 디지털 서명을 이용한 전송 Data 에 대한 무결성을 보장하며, 디지털 서명과 인증서를 이용한 여러 가지 제반 사항을 제공하여 거래 도중의 위험 요소로부터의 대비책이 필요하다. 비자카드사가 최근 AC Neilson 사에 의뢰한 조사에 따르면 한국의 전자상거래 이용자 4 명 중 1 명 이상이 신용카드 결제의 보안을 온라인 쇼핑이 최대 불안요인이 되고 있다. 전자지불 시스템을 위한 기술적인 도구들은 어느 정도 확립되어 있음에도 불구하고 여전히 보안상의 인증 및 정보보호 등에 관한 거래 장소가 쉽게 노출 되는 가상의 공간에서 이루어지며, Network 을 공유하는 제 3 자에게 거래 내용이 노출되며, 서버의 보안상의 취약점이나 내부 관련자에 의한 비밀 정보의 유출의 위험이 있다. 사용자가 직접 금융시스템으로부터 인증을 받을 수 없고 지불 시스템을 통하여 연결되기 때문에 지불 시스템의 내부 관련자에 의한 정보 유출 위험이 있다. 그렇기 때문에 아무리 사용자의 시스템과 금융시스템의 보안상의 결함이 없다고 하더라도 문제의 소지는 항상 존재한다.

본 연구에서는 HASH 와 SEED 암호화 Algorithm 을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하도록, 인증을 함으로써 서버의 해킹이나 내부 참여자

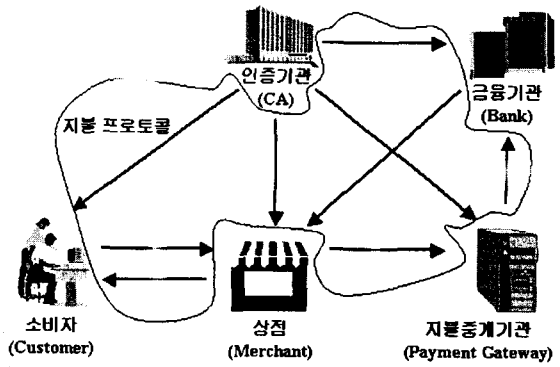
본 연구는 한국과학재단 지정 인천대학교 동북아전자물류연구센터의 지원에 의한 것입니다.

에 의한 지불정보의 유출이 있더라도 지불 정보를 안전하게 인증하는 방법을 제안하였다

2. 관련연구

2.1 전자 지불 시스템의 현황

전자 지불(electronic payment)이란 전자상거래에서 구매한 물건의 대금을 전자화폐로 결제하는 행위를 말하고, 전자지불시스템은 거래에 참여하는 고객, 판매자 등이 서비스와 상품에 대한 대가를 안전하고 효과적으로 주고받을 수 있는 정보전달 및 대금 지불 체계이다. 또한 전자지불시스템의 종류는 매우 다양하다고 할 수 있다. 소액 및 거액 전자지불시스템 등 거래 규모를 기준으로 구분할 수도 있으며, Internet 등을 통해 지급결제가 발생하는 Network 형과 Offline 에서 지급결제가 이루어지는 비 Network 형 등의 결제 형태에 따라서도 구분이 가능하다. 급속하게 발전하는 초고속 통신의 환경 하에서 Internet 사용자의 급속한 증가 추세와 관련된 서비스의 다양화는 과거 어떠한 산업의 새로운 출현에서의 경우와도 비교할 수 없을 정도로 빠르게 진전되고 있다. 즉, 사회 전반적으로 산재되어 있는 아날로그 정보들이 디지털정보로 전환되어 더욱 빠르게 유통되기 시작했을 뿐만 아니라 그 유통되는 물량도 많아지면서, 정보의 수요와 공급이 균형을 이루기 시작한 것이다. 따라서 전자 지불 시스템은 Internet 을 기반으로 하여 빠르게 발전하고 있다. 즉, Internet 이 시간과 공간에 구애를 받지 않는다는 장점을 이용하여 전자상거래가 활성화되고 있으나, 누구나 쉽게 접근할 수 있는 개방형 Network 의 특성에 따라 보안상의 문제가 큰 단점으로 대두되고 있다. 이를 안전하게 수행하기 위하여 암호화로 지불 정보 및 구매 정보의 기밀성을 보장하고, 디지털 서명을 이용한 전송 Data 에 대한 무결성을 보장하며, 디지털 서명과 인증서를 이용한 여러 가지 제반 사항을 제공해야 한다.



[그림 1] Mobile 기기를 이용한 전자지불 System 구성도

전자지불시스템은 전자상거래에 참여하는 개체간의 대금결제 서비스를 제공하는 시스템으로 전자상거래를 위한 자금의 흐름을 제어하고, 가상공간에서 이루어지는 전자상거래에 신뢰를 구축하는 시스템이다. 전자지불시스템은 그림 1 과 같이 사용자(Customer), 상점(Merchant), 금융기관(Bank)으로 구성되어 적절한 보안과 암호화가 유지되는 정보의 교환 및 고객의 신원을 확인할 수 있는 인증(authentication)의 기능을 필요로 하는 구조이다.

2.2 SEED

SEED 는 대칭키 암호 Algorithm 으로 블록 단위로 메시지를 처리하는 블록 암호 Algorithm 이다. 대칭키 블록 암호 Algorithm 은 비밀성을 제공하는 암호시스템의 중요 요소이다. n 비트 블록 암호화 Algorithm 이란 고정된 n 비트 평문을 같은 길이의 n 비트 암호문으로 바꾸는 함수를 말한다. 이러한 변형 과정에 암• 복호키를 적용하여 암호화와 복호화를 수행한다.

블록 암호 Algorithm 은 Feistel 구조로 설계된다. 블록 암호화 Algorithm 은 DES, FEAL, LOKI, MISTY, Blowfish, CAST, Twofish 등이 있다. Feistel 구조란 각각 t 비트인 블록으로 이루어진 2t 비트 평문 블록이 r 라운드($r \geq 1$)를 거쳐 암호문으로 변환되는 반복 구조를 말한다. 반복 구조란 평문 블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다. 보통 Feistel 구조는 3 라운드 이상이며, 짝수 라운드로 구성된다. 이러한 Feistel 구조는 ①라운드 함수에 관계없이 역 변환이 가능하며, ②두 번의 수행으로 블록간의 완전한 diffusion 이 이루어지며, ③Algorithm 의 수행속도가 빠르고, ④H/W 및 S/W 로 구현이 용이하고, ⑤아직 구조상의 문제점이 발견되고 있지 않다는 장점을 지니고 있다.

Data 처리단위는 8, 16, 32 비트 모두 가능하고 암• 복호화 방식은 블록 암호 방식이다.

2.3 HASH

Hash 함수는 원문의 무결성을 검증할 때 사용되며, 전자 서명에도 사용된다. Hash 함수는 단방향 성질 때문에 다이제스트된 메시지로부터 원문을 구해낼 수 없다. 암호에서의 Hash 함수와 일반적인 Hash 함수와의 차이점은 다음과 같다. 일반적으로 Hash 함수는 임의 길이의 평문 Data 를 정해진 길이의 Data 로 줄여주는 함수 이다. 하지만 암호에서 사용하는 Hash 함수는 이와 같은 성질이외에 다음의 성질을 추가적으로 요구한다. 약한 충동 회피성은 Hash 함수 h 에 대하여 특정 값 a 와 h(a)값이 주어졌을 때, h(b)=h(a)를 만족하는 a 와 서로 다른 b 를 찾기 어렵다. 강한 충동 회피성은 Hash 함수 h 에 대해서 특정 값 h(b)=h(a)를 만족하는 a, b 를 찾기 어렵다. 단 방향 성질은 h(a)값을 알 때, a 값을 알기 어렵다.

즉 원문 a 로부터 a 의 Hash 값인 h(a)는 쉽게 구할 수 있지만 Hash 값만 가지고는 원문을 알아내기 어렵다는 말이다.

Hash Algorithm 은 임의의 길이의 비트 열을 고정된 길이의 출력 값인 Hash 코드로 압축시키는 Algorithm 으로써 다음의 특성을 갖는다.

(1) 주어진 출력에 대하여 입력 값을 구하는 것이 계산 산으로 불가능하다.

(2) 주어진 입력에 대하여 같은 출력을 내는 또 다른 입력을 찾아내는 것이 계산상 불가능하다.

(3) 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능하다.

Hash Algorithm 은 크게 DES 와 같은 블록 암호 Algorithm 에 기초한 Hash Algorithm 과 전용 Hash Algorithm 으로 나눌 수 있다. 블록 암호 Algorithm 을 이용한 Hash Algorithm 은 이미 구현되어 사용되고 있는 블록 암호 Algorithm 을 사용할 수 있다는 장점이 있으나, 대부분의 블록 암호 Algorithm 의 경우 속도가 빠르지 않을 뿐더러 이를 기본함수로 이용한 경우 블록 암호 Algorithm 보다 훨씬 속도가 떨어지므로 현재는 대부분의 응용에서 전용 Hash Algorithm 이 주로 이용된다.

표준 Hash Algorithm 은 임의의 길이를 가지는 입력 메시지를 512 비트 블록 단위로 처리하여 160 비트의 출력을 낸다. 512 비트 단위 블록을 처리하는 압축함수는 모두 4 라운드, 80 단계로 구성되며, Hash 코드를 계산하는 연쇄변수는 5 개이다. 또한 각 라운드에 적용될 메시지 변수의 개수는 512 비트 입력블록으로부터 생성된 16 워드와 이로부터 추가로 생성되는 4 개의 워드를 포함하여 20 개가 된다.

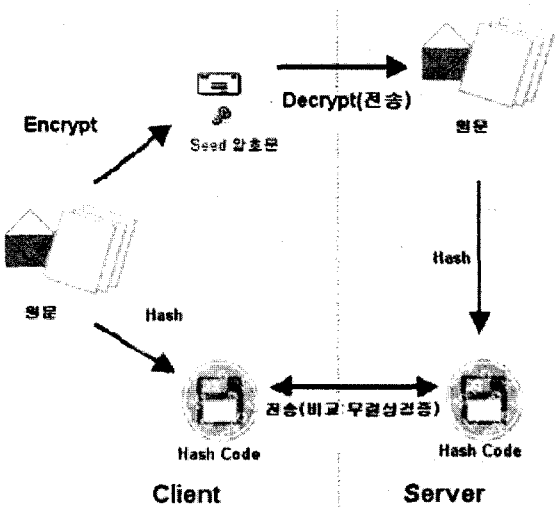
3. 종단간 보안을 제공하는 제안된 인증 시스템의 설계

전자 지불 시스템은 Internet 을 기반으로 하여 빠르게 발전하고 있다. Internet 이 시간과 공간의 구애를 받지 않는다는 장점을 이용하여 각종 거래가 활성화되고, 누구나 쉽게 접근할 수 있는 개방형 Network 의 특성에 따라 보안사고 위험 또한 증가하였다. 이를 안전하게 수행하기 위하여 기술적인 스펙으로 암호화를 통해 전송되는 지불 정보 및 구매 정보의 기밀성 보장, 디지털 서명을 이용한 전송 Data 에 대한 무결성 보장, 디지털 서명과 인증서를 이용한 여러 가지 제반 사항을 제공하여 거래 도중의 위험 요소로부터의 대비책이 필요하다.

또한 Network 를 공유하는 제 3 자에게 거래 내용이 노출되며, 서버의 보안상의 취약점이나 내부 관련자에 의한 비밀 정보의 유출의 위험이 있다. 이와 같은 구조적인 문제점은 사용자가 직접 금융시스템으로부터 인증을 받을 수 없고 지불 시스템을 통하여 연결되기 때문이다. 즉, 사용자의 시스템과 금융 시스템의 보안상의 결함이 없다고 할지라도 치명적인 약점이 될 수 있다. 이에 본 연구는 HASH Code 를 인증에 사용함으로 서 종단간의 보안을 제공하는 인증방안을 제안하려 한다.

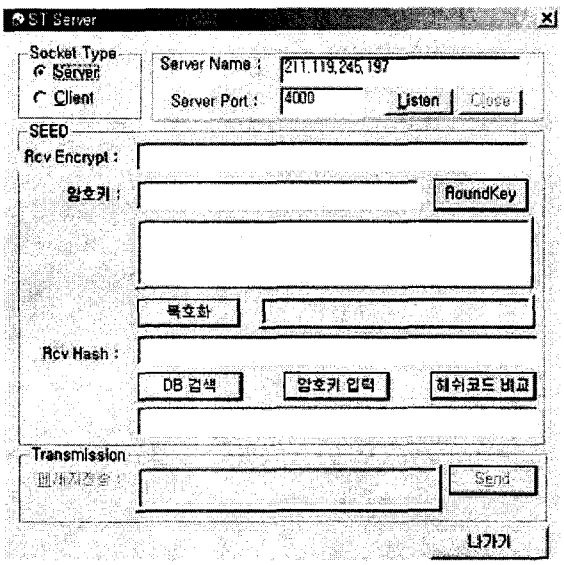
Server 측에서는 Client 측으로부터 받은 암호문을 다시 복호화 하였을 때 이 Data 가 제대로 복호화 되었는지 확인해 볼 수 없다. 왜냐하면 Server 측에서는 원문 Data 에 원래 어떤 Data 가 들어있는지 모르기 때문이다. 그렇다고 원문 Data 를 그대로 전송할 수 없기 때문이다. 따라서 Client 측에는 원문 Data 에 대한 추가적인 정보를 보내주어야 한다.

다이제스트된 메시지를 암호문메시지에 첨부하여 보내주면 Server 측에서는 우선 암호문을 복호화한 뒤 복호화된 메시지를 다시 메시지 다이제스트, 즉 HASH Code 를 생성하여 Server 가 직접 구한 메시지 다이제스트와 Client 가 보낸 메시지 다이제스트를 비교하여 두 값이 일치하는지 비교한다. 두 값이 일치하면 제대로 암호문이 전송되었다고 간주한다.



[그림 2] HASH Code 의 생성 과정

4. 제안된 인증 시스템의 구현

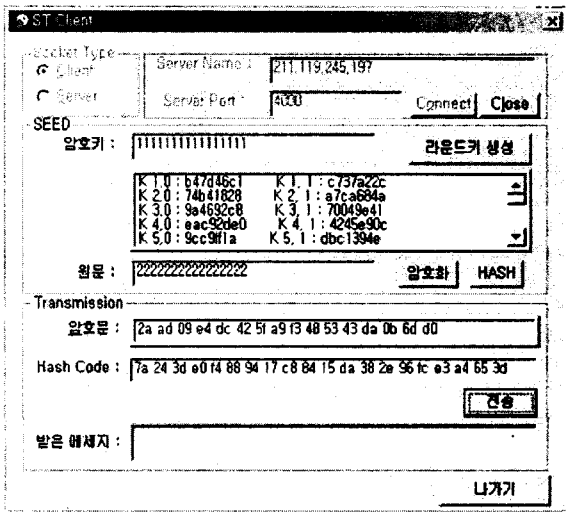


[그림 3] Server

SEED 암호화 Algorithm 을 적용한 메시지 전송 Module 은 HASH Code 를 통한 전송 메시지를 통하여 무결성을 보장한다. SEED 암호화를 적용하여 효율적이고, DC/LC 에 대하여 안전하다. 128 비트를 지원하므로 안전도를 충분히 제공한다.

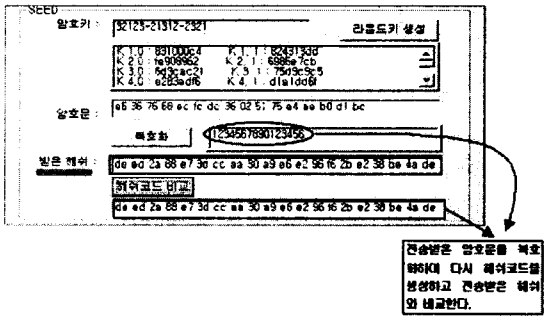
메시지를 전송 받을 Server 를 실행 시키고 Client 로부

터의 메시지 전송을 대하는 것은 [그림 3]과 같다.



[그림 4] Client

Client 에서 SEED 와 Hash 를 이용하여 암호문과 Hash 코드를 생성한 후 전송한다. 암호 키를 입력하고 입력된 암호 키를 통하여 라운드 키를 생성한다. 다음에 전송할 원문을 입력하여 암호문과 Hash 코드를 생성하여 서버측으로 전송하는 것은 [그림 4]과 같다.



[그림 5] HASH Code 비교

[그림 5]에서는 전송된 HASH Code 를 서버에 저장되어 있는 HASH Code 값과 비교하여 일치하면 인증이 올바르게 이루어졌다고 간주한다.

즉 원문의 내용을 모르더라도 HASH Code 값을 비교함으로써 인증 가능한 방법을 제안하였다. 이것은 서버의 보안상 취약점이나 내부 관련자에 의하여 비밀정보의 유출이 있더라도 안전하게 인증할 수 있다.

5. 결론

전자지불시스템의 구축은 많은 참여자가 필요하기 때문에 개발에는 많은 어려움이 있다. 많은 암호화 Algorithm 이 미국의 특허로 되어 있는 시점에서 국내 표준이고 KISA 에서 개발된 SEED 암호화 Algorithm 의 사용은 큰 의미를 가진다. SEED 는 128 비트 블록암호화 Algorithm 으로서 16 번의 암호화 과정을 반복한다. 그러므로 좀더 안전성을 기할 수 있다. 비자카드사가 최근 AC Neilson 사에 의뢰한 조사에 따르면 한국의 전자상거래 이용자 4 명 중 1 명 이상이 신용카드 결제의 보안이 온라인 쇼핑의 최대 불안요인이 되고 있다.

전자 지불 시스템을 위한 기술적 도구들이 많이 있음에도, 전자 지불 시스템이 활성화되지 못하는 주된 이유는 보안상의 인증 및 정보보호 등에 관한 거래 장소가 쉽게 노출될 수 있는 가상의 공간에서 이루어지며, Network 를 공유하는 제 3 자에게 거래에 관한 모든 내용이 노출됨으로써 보안이 완전히 해결되지 못한 것이 문제점으로 대두되고 있다. 이와 같이 지불결제 시스템의 불안정성은 전자상거래와 Internet 사업의 성장을 가로막는 요인으로 작용한다.

이에 본 연구에서는 서버의 보안상 취약점이나 내부 관련자에 의한 비밀 정보의 유출이 있다 하더라도 보다 안전하게 인증을 제공할 수 있는 인증 방안을 연구하였다. 그러나 암호화 기술이 발전함에 따라 그에 대응하는 위협도 같이 증가하고 있다. 따라서 이에 대응하는 기술적인 연구는 지속적으로 이루어져야 할 것이다.

참고문헌

[1] Joshua D. Guttman, "Security Protocol Design via Authentication Tests", Computer Security Foundations Workshop, April 11. 2002

[2] Amir Herzberg, "Payments and banking with mobile personal devices",

[3] B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design", *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121-144.

[4] Geraldine Gray, "Virtual Credit Card Processing System", Principle and Practice of Programming in Java 2002

[5] SET Secure Electronic Transaction – Setting the Stage for Safe Internet Shopping – an enticing concept. http://www.mastercardintl.com/netechnology/set/

[6] Overview of the SET Protocol, http://www.seas.upenn.edu/~tcom500/commerce/set.htm

[7] Bill McIntoshi, "Link Security A Tutorial", IEEE 802.11-00, March 2003

[8] SET Protocol Description, http://www.cl.cam.ac.uk/Research/Security/resources/SET/intro.html

[9] SET Secure Electronic Transaction protocol, http://simplythebest.net/info/set.html

[10] Simplified SET protocol, http://www.paytech.ru/eng/sset.asp

[11] 서장원, "전자상거래 보안을 위한 Y2K 암호시스템의 구현", The Journal of Korea Institute of CALS/EC Vol. 6, No. 1, April 2001

[12] 이혁, 이정규, "타원곡선 공개키 암호 Algorithm 을 이용한 전자지불 프로토콜", 통신정보보호학회논문지 제 10 권 제 1 호, 2000.3

[13] 한국정보보호진흥원, http://www.kisa.or.kr/