원타임 패스워드시스템을 적용한 지불시스템 모델

위장현*, 임인채*, 김한경*
*컴퓨터공학과, 창원대학교
e-mail : wijang@hanjung.co.kr

A study on Payment System Model Apply to One-Time Password System

Jang-hyeon Wi, Lin-Chae Lim, Han-kyung Kim*
*Dept. of Computer Science, Changwon National University

요 약

최근 정보통신기술을 활용한 전자상거래가 빠르게 발전하고 있다. 전자상거래는 인터넷이라는 공개된 가상공간에서 이루어지기 때문에 시스템 접근에 대한 강력한 인증과 상행위에 대한 정보의 보호가 필수적으로 요구된다. 따라서 본 논문에서는 관련 보안기술과 원타임 패스워드시스템, 그리고 지불시스템 로그인 단계에서 발생할 수 있는 문제점들을 검토하고, 이를 방지할 수 있는 원타임 패스워드시스템을 적용한 지불시스템의 모델을 제시하였다.

Ⅰ. 서 론

최근 정보통신 기술의 비약적인 발전에 힘입어 전자상거래가 빠르게 활성화 되고 있다. 전자상거래는 대부분 공개를 지향하는 인터넷에서 이루어지는 일련의 상행위로서 상거래 정보의 보호와 로그인 단계에서의 강력한 사용자 인증이 필수적으로 요구된다.

따라서 본 연구에서는 이러한 문제점 해결을 위해 적용 가능한 보안기술과 원타임 패스워드시스템(One-Time Password) 등의 관련 기술을 고찰한다. 그리고 웹 환경에서 발생하는 지불시스템 로그인 단계에서의 문제점들을 검토한 후, 이를 해결할 수 있는 방안으로 원타임 패스워드를 적용한 지불시스템 모델을 제시한다.

본 논문의 구성을 보면 2 장에서는 관련기술로서 지불시스템에서 적용되는 보안 기법과 원타임 패스워드시스템을, 3 장에서는 일반적으로 사용중인 지불시스템의 개념과 유형을 검토한다. 그리고 4 장에서는 지불시스템 로그인 단계에서 발생 가능한 보안문제를 검토한 후 원타임 패스워드시스템 적용 방안을 논하고, 마지막 5 장에서는 결론 및 향후 연구과제를 제시한다.

Ⅱ. 관련기술

전자상거래는 공개된 인터넷의 가상공간에서 이루어지기 때문에 거래의 전과정이 철저한 보안을 요구하므로 암호화는 필수적이다. 따라서 여기에서는 전자상거래에서 적용이 가능한 암호화 기술과 로그인 단계에서 강력한 인증을 수행할 수 있는 원타임 패스워드시스템에 대해 검토한다.

1. 보안기법

1) DES 암호화 방식

DES 암호화 방식은 대표적인 대칭적 알고리즘으로서 정보의 암호화와 해독에 64 Bits (56 Bits + 8 Bits 의 패리티)의 동일한 키를 사용한다. 정보를 교환하는 양측이 암호화에 사용된 키를 서로 상대방에게 교환하는 방식이다. 하지만 거래의 대상이 불특정 다수일 경우에 그만큼 키를 만들어야 하므로 현실적으로 매우 비효율적인 방법이라 할 수 있다.[5]

2) RSA 암호화 방식

RSA 알고리즘은 개인키와 공개키를 이용한 방법으로, 제안자 이름을 따서 RSA(Rivest, Shamir, Adoleman)라고 붙여졌다. 이 알고리즘은 개인키와 공개키를 이용하는데, 공개키로 암호화 된 문장은 공개키에 대응하는 개인키를 이용하여 해독할 수 있다. 또한 개인키로 암호화 할 경우에도 대응되는 공개키를 이용하면 원문을 재생할 수 있다.[6]

3) SEED 암호화 방식

SEED 암호화 방식은 국내의 전자상거래 및 정보보호를 목적으로 한국정보 보호센터에서 개발한 한국표준 암호 알고리즘으로서 블록단위로 메시지를 처리하는 대칭키 블록암호 알고리즘이다. SEED 는 8, 16, 32 비트의 데이터를 모두 처리하며 입출력문의 크기는 128 비트로서 라운드 동작과 동시에 암,복호화 키가 생성 된다.[7]

2. 원타임 패스워드시스템

원타임 패스워드 시스템은 인터넷을 포함한 네트웍 시스템에 접근하는데 있어 안전성을 보장하여준다. 보통의 경우 시스템에 로그인 하기위해서는 동일한 패스워드를 매번 사용하는 현재의 로그인 체계에서는 불법적인 방법으로 네트웍 도청을 통하여 계정과 패스워드를 쉽게 알아낼 수 있다. 그리고 이렇게 알아낸 패스워드는 부정사용이 언제든지 가능하다. 하지만 원타임 패스워드시스템은 시스템에 로그인 할 때마다 항상 다른 패스워드를 사용하게 함으로서 이러한 문제점을 해결할 수 있게 하여주며, 일단 한번 사용된 패스워드는 재사용이 불가능하므로 불법적인 방법으로 계정과 패스워드를 알아냈다 할지라도 시스템에 대한 접근을 허용하지 않는다.[4]

원타임 패스워드 시스템의 구현 방법으로는 다음과 같은 것이 있다.

- 동기화된 시간을 유지하여 Time-Stamp 를 사용
- 클라이언트와 서버가 가지고있는 임의의 패스워드 리스트 위치를 동기화하여 패스워드로 사용
- Sequence Generator 의 상태를 동기화하여 임시적인 Sequence Number 사용
- Challenge-Response Schemes 이용

Challenge-Response Schemes 을 이용한 인증절차는 먼저 사용자가 인증을 요구하면(로그인 시도), 서버쪽에서 임의의 Challenge 를 생성해서 사용자에게 전송한다. 사용자는 PIN(Personal Identification Number)과 Challenge 를 이용하여 서버에 전송할 원타임 패스워드를 생성하고, 서버에게 Response 메세지를 전송한다. 서버는 동일한 Challenge 와 등록된 사용자의 정보을 이용해 원타임 패스워드를 생성한 후 사용자가 전송한 Response 와 비교하여 사용자 인증을 해주는 방식이다.

IETF One Time Password Authentication (OTP) Working Group 에서는 원 타임 패스워드 인증 기법(One-time password Authentication Technologies)들에 대해서 여러 벤더들과의 상호 운용성을 개선하기 위해서 Standards-track RFC 1938 (A One-Time Password System)을 작성했으며, 현재 원 타임 패스워드 기법을 이용해 구현한 제품에는 Bellcore 의 S/KEY (TM) 시스템, the US Naval Research Laboratory (NRL)의 "One-time Passwords In Everything" (OPIE), logdaemon 등이 있다.[10][11]

Ⅲ. 지불 시스템

지불시스템은 구매자와 판매자 사이의 대금결제를 관장하는 시스템으로 전자상거래에서 자금의 흐름을 제어하는 중요한 시스템이다. 일반적으로 전자상거래에서의 전자지불 프로토콜은 SET 과 NON-SET 으로 분류할 수 있는데, 여기에서는 이들을 별도로 분류하지 않고 일반적인 현황과 유형을 검토한다.

1. 지불시스템 개요

인터넷을 이용한 전자 상거래는 단순한 상품 구입과 대금의 지불까지 인터넷으로 이루어지는 것을 의미한다. 실 거래에서 대금의 결재수단으로 가장 많이 사용되는 것은 현금, 수표, 신용카드 등이다. 현금이나 수표는 직접 주고 받아야 하기 때문에 인터넷과 같은 가상공간에서의 대금 결재는 신용카드나 전자화폐 등을 사용한다.

따라서 인터넷 상거래에서 대금을 지불하기 위해서는 신용카드 번호를 비롯한 여러 가지 개인의 정보들이 인터넷을 통해 전송되어야만 한다. 하지만 공개를 지향하는 인터넷의 특성상 이들 정보가 노출될 수 밖에 없어 부정적으로 이용될 수 있는 가능성을 내재하고 있다.

이에 따라, 전자상거래에서의 지불 시스템은 소비자와 상인, 그리고 중계자들이 상호 개입되어 거래를 진행할 때 적절한 수준의 보안이 유지되는 한편, 정보의 교환 및 고객의 신원을 확인할 수 있는 로그인 단계에서의 강력한 인증 기능 필요성이 날로 증대되고 있다.

2. 지불시스템 유형

전자상거래에서 가장 많이 사용되는 지불 수단은 전자화폐, 신용카드 등이 대표적이다. 전자상거래에서 사용되는 지불 방법은 그 형태나 거래 방식에 따라 다음과 같이 분류 할 수 있다.[5]

- 직접적인 상거래 방식에 기반한 분류
  - ✓ 전자자금 이체
  - ✓ 디지털 현금
  - ✓ 전자 화폐
- 자금 흐름에 따른 분류
  - ✓ 현금방식 지불
  - ✓ 수표방식 지불

- 거래 방식에 따른 분류
  - ✓ 직접 지불
  - ✓ 간접 지불
- 처리 방식에 따른 분류
  - ✓ Online 지불
  - ✓ Offline 지불
- 추적 가능 여부에 따른 분류
  - ✓ 추적 가능 지불
  - ✓ 추적 불가능 지불

위와 같이 인터넷을 기반으로 한 전자 상거래시스템은 다양한 지불 방식들을 활용할 수 있으며, 전송형 지불방식인 전자대금 이체, 가치 저장형 지불 방식인 디지털캐시, 지불지시형 지불 방식인 E-cash 등은 직접 적용이 가능하다.

이들 지불방식은 그 거래가 디지털화 된 정보로 이루어지므로 이들 자료의 보안은 매우 중요하다. 즉, 디지털화 된 정보는 불법적인 도용이나 복제가 비교적 간편하고 쉽게 이루어 질 수 있기 때문이다. 보안의 정도는 거래의 종류에 따라 다양한 형태의 요구가 발생할 수 있으나 보편적으로 전자상거래에서의 지불시스템은 무결성, 인증, 보안성, 가용성 및 신뢰성이 확보 되어져야 한다.

Ⅳ. 원타임 패스워드 적용 방안

인터넷의 개방성과 정보공유 및 교환의 용이성으로 인해 인터넷상에서의 해킹등의 사건은 날로 그 빈도수가 증가하고 있으며, 그 유형 또한 고도화 됨으로서 그로 인한 피해의 심각성은 하루가 다르게 증가하고 있다. 따라서 지불시스템 로그인 단계에서의 보안문제 유형을 검토하고 이들 문제점들을 해결할 수 있는 지불시스템 모델을 제안한다.

1. 지불시스템 로그인 단계에서 보안문제

일반적으로 지불시스템은 어떤 프로토콜을 구현한 것이고 이 시스템을 사용한다는 것은 가상의 공간에서 이루어지는 행위가 실제의 상거래와 동일하다는 것을 의미한다. 따라서 인터넷 상에서 이루어지는 전자상거래의 모든 정보는 반드시 보호되어야 한다. 하지만 현재의 인증시스템 구조에서는 암호화 기술을 이용 함으로서 정보의 보호는 어느 정도 되고있지만, 로그인 단계에서의 인증은 아직 많은 문제점들을 내포하고 있다.

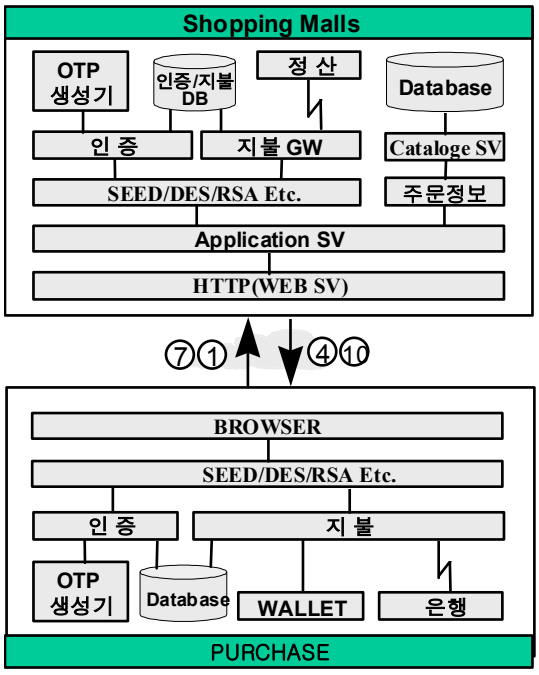
현재의 웹 환경에서 지불시스템 접근을 위한 로그인 단계에서의 문제점들은 다음과 같다.[9]

- 암호에 관한 공격
- 패킷 스니핑 공격
- 엑세스된 상태를 악용한 공격
- IP SPOOFING
- 순차적 번호 예측 공격
- 기술의 취약점을 악용한 공격

2. 원타임 패스워드 적용 방안

공개를 지향하는 인터넷의 가상 공간에서 이루어지는 모든 지불시스템, 특히 전자상거래에서의 로그인 단계는 강력한 사용자 인증이 필요하다. 특히 앞서 지적한 문제점과 같이 각종 불법적인 방법으로 사용자 계정과 암호를 도용하여 시스템에 접근을 시도할 때 근본적으로 접근(로그인)이 불가능하도록 하여야 한다.

따라서 지불시스템에서의 인증이 인터넷 환경에서 원활하게 이루어 지기위해서는, 앞에서 검토되었던 문제점, 특히 불법적인 도용을 예방하면서 사용자가 쉽게 시스템에 접근할 수 있도록 구현 되어야 한다. 이를 위하여 본 연구에서는 서비스를 원하는 사용자의 클라이언트와 서비스를 제공하는 서버의 로그인 단계에 있어 간편한 로그인 절차와 그리고 원타임 패스워드시스템 중 Challenge-Response Schemes 을 적용한 지불시스템의 모델을 제안한다.



[로그인 절차]

① [CL] Login 요청(인증 DB 의 계정, 식별번호)
② [SV] 수신/인증 DB 의 계정 확인(계정, 식별번호)
③ [SV] 동일하면 Challenge 생성, 아니면 종료
④ [SV] Challenge 송신/인증 DB 에 관련정보 저장
⑤ [CL] Challenge 수신
⑥ [CL] OTP 생성(Challenge, 사용자 패스워드 사용)
⑦ [CL] 계정, OTP 송신
⑧ [SV] OTP 생성 후 사용자 OTP 와 비교(계정,OTP)
⑨ [SV] 동일하면 인증/저장, 아니면 거부/종료
⑩ [SV] 인증 메시지 송신/세션 설정
⑪ [CL] 인증 메시지 수신

[그림 1] OTP 를 적용한 지불시스템 모델

위의 지불시스템 모델과 인증절차에서 볼 수 있듯이 서비스를 원하는 사용자는 원타임 패스워드를 생성할 수 있는 유일한 식별번호를 가진 생성기가 설치된 브라우저를 사용하여 서버에 접속 한다. 로그인을 할 때 자신의 계정은 다시 입력할 필요가 없으며, 이때 브라우저는 인증데이터베이스에 저장된 자신의 계정과 생성기의 식별번호를 가지고 서버에 접근한다. 로그인 정보를 수신한 서버는 인증 데이터베이스에 저장된 계정과 생성기의 식별번호를 확인하여 인가자인지를 판단한다. 이때 인가자일 경우 임의의 Challenge 메세지를 생성하고, 데이터베이스에 저장한 후 요청자에게 Challenge 를 송신한다. 요청자는 Challenge 와 계정 그리고 클라이언트에서 사용하는 암호를 이용하여 원타임 패스워드를 생성한 다음 계정과 패스워드를 가지고 다시 서버에 로그인을 요청한다. 이때 서버는 동일한 Challenge 와 사용자의 계정을 이용해 원타임 패스워드를 생성한 후 사용자가 전송한 계정과 패스워드를 비교하여 인증여부를 결정하므로 패스워드의 불법적인 사용을 확실하게 방지할 수 있다.

Shopping Mall 에서는 Application 서버 또는 관련 Demon 이 접수되는 클라이언트 정보를 받아 해당되는 G/W 로 거래내용을 중계 함으로서 제시된 모델에서 사용자 인증과 상거래를 원활하게 할 수 있다.

또한, 구매자는 처음 등록할 때에만 서버에 정보의 등록/변경을 요청하게 함으로서 일반적인 거래에서는 로그인 정보를 별도 입력하지 않아도 되기 때문에 매번 계정을 입력하는 불편함을 해결할 수 있다. 또한 클라이언트와 서버는 세션이 매번 새로 설정될 때마다 로그인 패스워드가 변경되므로 앞서 검토하였던, 가상공간에서의 불법적인 정보유출이나 해킹에 의한 피해를 사전에 예방할 수 있다. 그리고 암호화 부문에 있어서는 SEED 등을 포함한 우리의 환경에 적합한 알고리즘을 독립적으로 적용 함으로서 정보의 보안성을 보장하여 준다. 따라서 제시된 모델은 다양한 형태의 전자상거래 시스템 로그인 단계에서의 강력한 사용자 인증을 할 수 있음을 보여주고 있다.

V. 결 론

전자상거래는 실제의 상거래와 동일하기 때문에 시스템에 대한 절대적인 안전성이 필수적으로 요구된다. 하지만 모든 상거래 시스템은 공개된 인터넷에서 이루어지기 때문에 언제나 불법적으로 계정과 패스워드를 도용한 부정 거래를 할 수 있는 문제점을 다분히 내포하고 있다.

그래서 본 연구에서는 지불시스템의 로그인 단계에서 보다 철저한 인증절차를 거치게 함으로서 계정과 패스워드의 도용을 방지할 수 있도록 원타임 패스워드시스템을 적용한 지불시스템 모델을 제시하였다.

앞으로도 전자상거래 분야는 지속적으로 발전할 것이며, 이에 따라 지불시스템은 보다 안전한 지불을 위한 새로운 요구사항이 계속해서 요구되어 질 것이다. 따라서 다양한 형태의 지불시스템에서 보다 강력한 인증을 수행할 수 있는 지불시스템으로 발전시켜 나가야 할 것으로 생각된다.

앞으로, 제안된 모델의 구현과 현재 사용중인 전자상거래 지불시스템 그리고 국내의 금융환경을 모두 수용할 수 있는 SET/NON-SET 이 통합된 지불시스템 등의 적용에 관한 연구가 필요하다.

참 고 문 헌

[1] 송익진 외, 인터넷 전자상거래 지불시스템, 멀티미디어 연구소, 1998 년 3 월
[2] 이재일, 전자서명 인증관리센터의 인증업무 준칙, 정보보호센터, 1997 년 7 월
[3] 송상헌 외, 전자상거래를 위한 소액전자 지불시스템 구현
[4] 송상헌 외, 웹 보안을 위한 사용자 인증과 암호화 통신구현, http://esperosun.chungnam.ac.kr/~shsong/my_paper/jcci_paper
[5] 김기병, 김수홍, 전자상거래를 위한 지불방법, 정보처리학회지, VOL 6 NO. 1, 1999 년 1 월
[6] 임인채 외, 전자상거래를 위한 지불프로토콜의 통합 모델, 한국정보처리학회 추계 학술발표논문집 제 6 권 제 2 호, 1999
[7] 한국정보보호센터, 128Bit 블록 암호알고리즘(SEED) 개발 및 분석보고서, 정보통신부, 1998 년 12 월
[8] 최용락 외, 통신망 정보보호, 그린, 1997 년 2 월
[9] 박재현, 해킹의 최신 형태와 방지 테크닉, 현대전자 소프트웨어 연구소
[10]“A One-Time Password System “, rfc1938
[11]“S/KEY One-Time Password System”, rfc1780