

인터넷상에서 안전한 전자복권 시스템 개발에 관한 연구

공 현 정*, 강 서 일*, 이 임 영*, 문 기 영**
순천향대학교 정보기술공학부*
한국전자통신연구원**

A Study on Development Secure Electronic Lottery System

Hyeon-Jeong Gong*, Se-Il Kang*, Im-Yeong Lee*, Ki-Young Moon**
Division of Information Technology Engineering, SoonChunHyang University*
Electronic and Telecommunications Research Institute**

요약

최근 인터넷의 급속한 보급으로 인터넷을 이용한 전자상거래 분야에 관심이 높아지고 있다. 이에 많은 오프라인 서비스들이 온라인을 통하여 제공되고 있다. 이러한 다양한 서비스들 중 복권을 온라인상에서 운영함으로써 편리성 및 비용 절약 효과를 가지울 수 있다. 그러나 개인의 프라이버시 뿐만 아니라 구입한 복권에 관한 정보 등 보안에 대한 관심이 높아지고 있다. 또한 기존 서비스 상에서 복권의 중복 구매 및 복권의 저장문제 등 취약점이 제기되고 있으므로 사용자에게 안전한 서비스에 대한 신뢰성을 줄 수 없다. 따라서 본 논문에서는 개인의 프라이버시를 보호하고 전자복권 서비스를 제공할 때 불법적인 제3자로부터 보호하기 위해 사용자가 구입한 복권에 대하여 보안 서비스를 제공함으로써 안전성을 높일 수 있고 사용자에게 안전하고 신뢰성 있는 전자 복권 시스템을 제안한다.

1. 서 론

인터넷의 이용이 확산되면서 여러 분야의 서비스들이 온라인으로 제공되고 있다. 인터넷을 이용한 서비스의 제공은 시·공간적 제약을 벗어날 수 있는 장점을 제공한다. 이를 기반으로 하여 복권 서비스도 온라인 화하여 복권의 유지비용을 줄이며 사용자에게 편리성을 제공하고 있다.

그러나 인터넷과 같은 공개된 통신망을 이용한 상거래의 경우 그 특성상 시스템의 오류나 해커, 악의적인 제 3자 등의 외부 침입으로 인해 개인정보가 유출될 수 있다. 또한 복권의 데이터는 금액적인 가치가 매우 높기 때문에 보안 시스템이 요구된다.

따라서 본 논문에서는 기존의 전자복권 시스템과 비교하여 효율적이면서 안전한 전자복권 방식 및 시스템을 제안한다. 2장에서는 전자복권에 대해 살펴보고 3장에서는 전자복권의 요구사항 및 기존 복권서비스에 대해 분석한다. 4장에서는 안전한 복권 시스템을 제안한다. 5장에서는 제안방식과 기존방식을 3장에서 제시한 요구사항을 기반으로 분석한 뒤 6장에서 결론을 맺고자 한다.

2. 전자복권 시스템의 개요

복권의 정의는 국가 또는 공공기관이 번호를

기입하였거나 어떤 표시를 해 놓은 표를 팔아서 추첨 과정을 통해 당첨된 표에 대해서는 표의 값보다 훨씬 많은 배당금을 주는 번호표를 말한다. 일정한 발행자가 구매자로부터 금전이나 기타 재물을 받고 미리 표를 제공하되, 당선자만이 큰 배당을 받는다.

복권의 종류를 크게 다음과 같이 구분할 수 있다.

① 로또 복권 : 가장 기본적인 방식은 1부터 30~55 정도의 숫자에서 5~7개의 숫자 조합을 선택하는 방식이고 가장 많이 채택되고 있는 방식은 6/6/49로 1~49까지의 숫자 중에서 순서에 관계없이 6개의 숫자를 선택하는 것이다.

② 스크래치 복권 : 기존 오프라인 상에서의 스크래치 복권과 당첨자 결정방식은 동일하다.

③ 추첨 복권 : 기존 오프라인에서 판매하고 추첨을 통해 당첨자를 결정하던 것을 온라인에서는 실물을 전혀 인쇄하지 않고 인터넷상에서만 복권을 발행, 당첨자 결정, 당첨금을 지급하는 방식이다.

④ 키노 : 키노라는 이름은 카지노 게임 이름에서 원용한 것이다. 80개의 숫자 중에서 구매자가 10개의 수를 선택하면 20개의 숫자를 추첨하여 10개의 숫자가 20개의 숫자에 많이 포함되어 있을수록 높은 등수에 당첨되는 것이다.

⑤ 넘버스 : 가장 일반적인 형태는 0~9(10개) 숫자 중 중복을 허용하여 3개의 숫자를 선택하여 추첨결과 3개의 숫자와 숫자배열 순서가 일치하면 당첨되는 'Straight' 방식이다.

이러한 여러 종류의 복권은 온라인 서비스를 제공함으로써 다양한 콘텐츠와 함께 취미, 오락의 개념을 갖게 되었다.

3. 전자 복권 보안 요구 사항 및 기존 방식 분석

이 번장에서는 전자복권 보안 요구사항 및 기존 방식에 대해서 논의하고자 한다.

3.1 전자복권 시스템의 보안 요구사항

전자복권은 다음과 같은 보안요구사항이 필요하다.

① 발권 예측 방지

사용자는 복권 구매 이전에 복권의 내용, 또는 복권의 발권 주기를 예측할 수 없어야 한다.

② 기밀성

전자 상거래시 모든 거래에 대한 전송 내용은 타인에게 유출되지 않고 비밀이 보장되어야 한다.

③ 부인방지

사용자가 복권을 구입한 후 발권 자가 판매사실을 부인할 수 없어야하며 사용자가 구매 사실을 부인할 수 없어야 한다.

④ 공정성

복권 사업자는 복권을 발권, 추첨할시 사용자와 결탁하지 않고 공정하게 행하여야 한다.

⑤ 위조 및 복제 방지

구매자가 당첨된 복권을 복제하여 2중으로 당첨금을 수령할 수 없어야 하며 제 3자로부터의 위조 및 복제가 방지 되어야 한다.

3.2 기존방식

기존방식의 전자복권 시스템으로 다음과 같이 4가지를 분석한다.

① Xecure Lotto (소프트포럼)

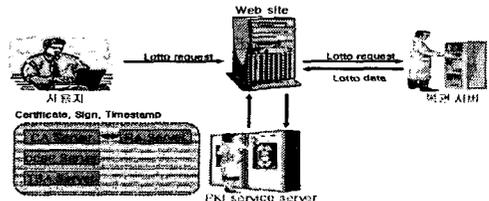


그림1. Xecure Lotto 전체 흐름도

Xecure Lotto는 현재 가장 상용화된 제품으로 PKI구조를 기반으로 하고 있다. 랜덤 제너레이터를 사용하여 복권의 발권뿐만 아니라 복권 숫자의 추첨의 주기를 예측하기 힘들다. 하지만 내부가 매우 복잡한 구조로 되어 있어 실행속도가 느리다.[1]

② Trust Lotto (시큐아이닷컴)

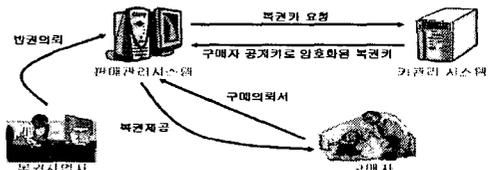


그림2. Trust Lotto 전체 흐름도

Trust Lotto의 방식은 구매자의 구매의뢰서에 있는 인증서를 확인을 한 뒤 구매자의 공개키를 사용하여 복권기와 암호화된 복권을 전달하게 된다.

이 방법은 구매자에게 복권을 안전하게 전달할 수는 있으나 복권 추첨의 공정성은 알 수 없다.[2]

③ 안전한 전자복권 시스템

㉠ 시스템 계수

- Rn : 20자리의 숫자로 구성된 해쉬전의 값

- EKR : 사업자의 비밀 키로 암호화수행
- ANS : 사용자가 작성한 4자리의 일련번호
- ID : 사용자가 초기에 사업자에게 등록해 놓은값

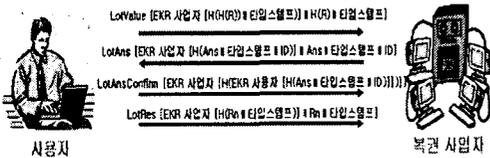


그림3. 안전한 전자복권 시스템 흐름도

안전한 전자복권 시스템에서는 해쉬되기 전의 값을 당첨번호로 사용하므로 복권 구매의 중복성이 문제된다. 또한 서버, 사용자, 사업자간의 결탁문제도 제기되고 있다.

④ 전자복권 시스템 구현

전자복권 시스템 구현에서는 ③의 안전한 전자복권 시스템의 취약점을 분석하여 이를 토대로 구현한 시스템이다. 서버, 사용자, 사업자간의 결탁을 막기 위하여 서버와 CA(인증기관)에서 복권 당첨번호를 1/2씩 생성하게 되어있다.

4. 제안방식

본 논문에서는 복권의 기본적 요구사항을 만족하면서 사용자가 편리하게 사용하는 데에 목적이 있다. 정보의 보호를 위하여 공개키와 해쉬함수를 사용하고, 복권 사업자의 부정을 방지하기 위하여 사용자는 자신만이 사용하는 개인 식별자를 가지고 있다.

4.1 시스템 계수

다음은 복권 시스템에서 안전하게 데이터를 저장하기 위한 시스템 계수를 설명한다.

- Epk_s : 사업자의 공개키
- id : 사용자의 아이디
- pwd : 사용자의 패스워드
- R : 사업자가 제공하는 랜덤 수
- $h()$: 일 방향 해수 함수 (위에와 양식차이)
- B : 사용자만의 식별자
- $C = h(R || h(pwd))$

- $K = h(C || h(N))$
- N : 사용자가 선택한 로또 번호
- T : 타임스탬프

4.2 프로토콜

제안 시스템의 프로토콜은 3단계로 나누어 볼 수 있다.

① 등록단계

- 사용자는 등록을 하기위해 사이트에 접속, 사업자의 공개키를 이용하여 id 와 pwd 를 안전하게 등록한다.

$$Epk_s [Id || pwd]$$

- 사이트 접속시, 로그인시 사업자는 사용자에게 랜덤으로 생성한 R 을 전송한다.
- 사용자 측에서는 받은 R 을 이용하여 C 를 생성한 뒤 로그인을 하기위하여 id 와 C 를 전송한다.

$$C = h(R || h(pwd))$$

$$[Id || C]$$

- 사업자 측에서는 R 값뿐만 아니라 pwd 값을 데이터베이스에 가지고 있으므로 C' 값을 연산할 수 있다. 사용자에게서 받은 C 값과 사업자가 계산하여 얻어진 C' 값을 비교하여 사용자를 인증한다.

$$C' = h(R || h(pwd))$$

$$C' \neq C$$

② 서비스 단계

- 인증을 받은 사용자에게 사업자는 복권 서비스를 제공하게 된다.
- 사용자는 자신이 원하는 복권 번호를 선택한다.
- 자신이 선택한 복권번호 N 과 타임스탬프, 인증을 받기위해 사용했던 C 값으로 계산한 K 값과 사용자의 개인 식별자가 들어간 $h(BK)$ 값을 사업자 측으로 전송한다.

그림4. 제안방식의 전체 흐름도

$$[N | T | K | h(BK)]$$

$$K = h(C | N)$$

- 사업자는 받은 N 과 C 값을 이용하여 K' 를 생성하여 사용자가 전송한 K 값과 같

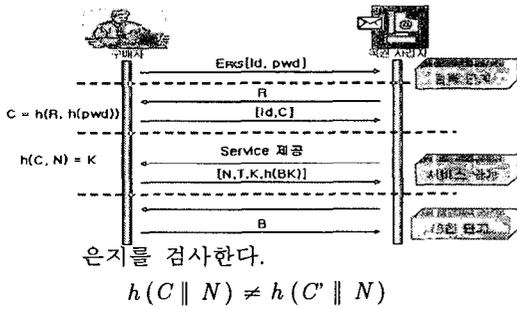


그림5. 제안방식의 복권



그림6. 암호화 되어 저장된 복권 데이터

③ 추첨 단계

④ 추후 추첨날짜가 되면 사업자는 추첨을 한 뒤 그 결과를 공개보드를 통하여 통보한다.

⑤ 개인적으로 당첨을 확인할 시 개인 식별자를 요구하여 개인 식별자와 사업자가 가지고 있는 K를 해쉬취한 값이 같으면 추첨여부를 알린다. 이를 통하여 구매자가 구매를 부인할 경우 증명할 수 있다.

$$h(BK) \neq h(BK)$$

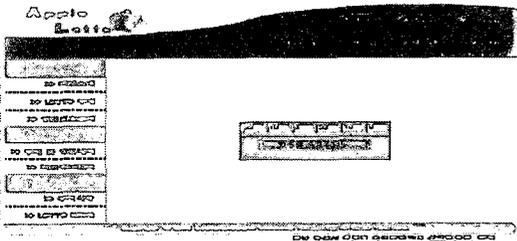


그림7. 복권 번호 추첨 단계

5. 제안방식 분석

본 논문에서는 기존방식에서 주로 사용했던 공개키 방식보다는 해쉬 함수를 사용하여 안전

하면서도 효율성을 높이도록 하였다. 또한 복권 시스템의 기본적인 요구사항을 만족시키도록 하였다.

① 유출 및 위변조

서버에서 제공되는 R값을 이용하여 해쉬를 취하고 여러 번의 결과 비교로 타인으로 인하여 내용이 유출되거나, 위조되는 문제를 해결하였다.

② 부인방지

사용자가 복권을 구매한 후 부인을 할 경우 개인식별자 입력을 요구하여 저장된 데이터 값을 비교함으로써 부인방지를 막았다.

③ 공정성

복권 사업자가 원하는 숫자가 아니라 랜덤제너레이터를 이용한 추첨으로 공정성을 유지하였다.

④ 복제, 위조

매번 접속시 R값이 변하므로 복권을 구매자가 복제, 위조할 수 없게 하였다. 또한 제 3자는 복권 사업자가 제공하는 R 값과 개인식별자 B값을 알 수 없으므로 복제, 위조가 어렵다.

6. 결론

본 논문에서는 기존의 전자복권 시스템에 대하여 보안 사항에 대해서 분석하고 이를 해쉬함수를 이용하여 효율성을 높인 전자 복권 시스템을 제안하였다. 구조에 의존하던 기존의 방식과 달리 해쉬함수를 이용하여 보안적 사항을 만족시키도록 하였다. 그러나 제안방식에서 사용되는 R(사업자가 제공하는 랜덤 수)와 B값(개인 식별자)는(은) 일종의 패스워드와 같으므로 그에 따른 보안적 취약점을 가지고 있다.

따라서 본 논문에서 제안되었던 방식을 기반으로 하여 위에서 지적한 취약점을 보완할 수 있는 연구를 수행할 예정이다.

[참고문헌]

[1] 소프트포럼㈜ "디지털 전자복권의 추첨 방법 및 그를 위한 시스템" 대한민국 특허청, 공개특허 정보, 특2002-0066053
 [2] <http://www.softforum.com> 소프트포럼㈜
 [3] <http://www.secui.com> 시큐아이닷컴
 [4] 정보과학회 추계학술대회, "안전한 전자 복권 시스템" 충남대학교, 1999년
 [5] 이덕규, 모병수, "전자복권 시스템 구현", 순천향대학교 학사논문, 2000년
 [6] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신보안", 도서출판 그린, 2001