스마트폰 게임 사용자의 효율적인 인증 방법

An Efficient Authentication Method of User using Smartphone Game

정 윤 수
목원대학교

Jeong Yoon-Su
Mokwon Univ.

요약

최근 스마트폰이 대중화 되면서 스마트폰을 사용하는 사용자의 계층이 다양화되고 있다. 그러나 스마트폰을 사용하는 사용자 계층 중 청소년이 다른 계층보다 스마트폰 게임에 쉽게 중독되어 다른 일상 생활이 힘든 상황이 발생하고 있다. 본 논문에서는 스마트폰 게임을 통해 일상 생활이 불가능한 청소년을 대상으로 게임 사용을 강제적으로 조절할 수 있는 인증 프로토콜을 제안한다. 제안 프로토콜은 사용자의 게임 시간과 접속 횟수 등의 정보를 이용하여 게임 사용을 자제하도록 함으로써 사용자의 게임 중독을 예방하는 것을 목표로 하고 있다. 또한, 청소년이 온라인 게임 상에 물품을 구입할 경우 청소년의 부모에게 게임 아이템 구입 확인 메시지를 전달하여 게임 사용을 제한한다.

Ⅰ. 서론

최근 이동통신망의 급속한 발전과 단말기 보급 확대로 인하여 스마트폰 사용이 확대되고 있다[1,2]. 그러나 최근 청소년들은 스마트폰내 게임을 무분별하게 사용하면서 게임 중독이 다른 매체에 비해 증가 추세에 있다.

그러나, 청소년은 스마트폰 게임을 부모의 간섭없이 손쉽게 사용할 수 있을 뿐만 아니라 게임 아이템도 쉽게 구매하여 게임을 즐길 수 있다. 게임 아이템 구매에 대한 지불능력이 없는 청소년이 게임 아이템을 무분별하게 구매하는 것은 부모입장에서 많은 부담을 느낄 수 있다[3].

이 논문에서는 스마트폰 게임을 통해 일상 생활이 불가능한 청소년을 대상으로 게임 사용을 인증서버가 강제적으로 청소년의 게임 사용을 제한하는 스마트폰 게임 사용자 인증 프로토콜을 제안한다. 제안 프로토콜은 사용자의 게임 시간과 접속 횟수 등의 정보를 이용하여 게임 사용을 자제하도록 함으로써 사용자의 게임 중독을 예방하는 것을 목표로 하고 있다. 또한, 제안 프로토콜은 청소년이 게임 아이템을 구매할 때마다 새로운 승인 코드를 새로 부여받아 청소년의 불법 게임 아이템 구매 충동을 사전에 예방할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 스마트폰의 정의에 대해서 분석한다. 3장에서는 게임 중독을 갖고 있는 청소년이 스마트폰 게임을 자제하기 위한 인증 프로토콜을 제시하고, 4장에서는 제안 프로토콜의 보안 평가를 수행한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련연구

스마트폰은 휴대폰과 개인휴대단말기의 장점을 결합한 것으로써, 휴대폰 기능에 일정관리, 팩스 송·수신 및 인터넷 접속 등의 데이터 통신기능을 통합시킨 차세대 휴대폰을 의미한다. 스마트폰은 기존 휴대폰과는 달리 수백여 종의 다양한 응용프로그램을 사용자가 원하는 대로 설치하고 추가 또는 삭제할 수 있는 특징이 있다. 스마트폰은 무선인터넷을 이용하여 인터넷에 직접 저속할 수 있을 뿐 아니라 여러 가지 브라우징 프로그램을 이용하여 다양한 방법으로 접속할 수 있는 점, 사용자가 원하는 애플리케이션을 직접 제작할 수 있는 점, 다양한 애플리케이션을 통하여 자신에게 알맞은 인터페이스를 구현할 수 있는 점, 운영체제를 가진 스마트폰 간에 애플리케이션을 공유할 수 있는 점 등 기존 휴대폰이 갖지 못하는 장점을 가지고 있다. 스마트폰은 2000년 중반 이후 RIM사의 블랙베리폰을 시작으로 개인휴대단말기(PDA · personal digital assistant)를 대체하였고, 터치스크린 기술과 결합하여 휴대폰과 경쟁할 수 있는 기기로 성장하여 현재는 애플의 iPhone, 삼성 갤럭시, LG 옵티머스, SKY 베가, 구글 넥서스원 등 많은 스마트폰이 대중화 되고 있다[4,5].

Ⅲ. 스마트폰 게임 사용자 인증 프로토콜

본 연구에서는 스마트폰 게임에 중독되어 있는 청소년이 강제적으로 게임에 접속하는 과정을 서버에서 중재하는 인증 프로토콜을 제안한다.

· 단계 1

이 단계는 청소년이 게임 서비스를 제공받기 전에 게임서버에 사용자 정보를 등록하는 단계로써, 청소년의 인식자 $KU_U(=ID_U)$와 패스워드 $KR_U(=KU_U \bullet g^{CW})$의 공개키와 개인키를 해쉬 함수 $H(\bullet)$에 적용하여 권한 정보 I_U를 생성한다. 등록된 권한 정보 I_U는 청소년이 게임에 접속할 때마다 청소년이 게임에 접속한 시간, 게임을 한 시간, 접속 시간대 등을 데이터베이스에 저장한다.

· 단계 2

게임서버는 청소년의 공개키 정보 KU_U와 인증서버 AS 가 생성한 비밀키 X_{AS}를 해쉬 함수 $H(\bullet)$에 적용한 후 사용자에게 전달받은 I_U와 exclusive-OR 하여 보안 정보 SI로 대체한다.

· 단계 3

청소년은 게임서버가 생성한 SI와 함께 사용자 인식자 ID_U를 해쉬 함수 $H(\bullet)$에 적용한 후 보안 인식자 $SID_U(=I_U \oplus ID_U)$를 생성한 후 게임서버에게 전달한다.

· 단계 4

게임 서비스를 제공받기 원하는 청소년은 게임서버에 등록한 후 인증 유·무를 통해 인식자 KU_U와 패스워드 KR_U를 입력한다. 인증이 성공적으로 이루어지면 청소년의 게임 사용 유·무를 게임 서버가 확인한 후 일회용 패스워드 OTP를 생성하여 청소년에게 전달한다.

· 단계 5

청소년은 일회용 패스워드 OTP를 보안 인식자 SID_U와 함께 게임서버의 공개키로 암호화하여 인증서버에게 전달한다.

· 단계 6

게임 서버는 청소년으로부터 전달된 정보 중 SID_U을 데이터베이스에 저장된 사용자 정보와 비교한다. 비교 결과가 일치하지 않으면 서비스는 종료되고 일치하면 전달된 사용자 정보를 이용하여 OTP' 를 생성한다. 서버는 생성된 OTP' 와 사용자가 전달한 OTP를 비교하여 사용자를 검증한다.

Ⅳ. 보안평가

제안 프로토콜은 스마트폰을 사용하는 청소년과 인증서버 사이에서 생성한 OTP를 이용하여 각 청소년이 서비스를 요청할 때마다 청소년이 소유하고 있는 시간동기화 값 T_U, 카운트 CT, PIN 정보를 이용하여 제 3자가 시도하는 악의적인 공격 중 replay 공격과 impersonation 공격을 예방한다. 제안 프로토콜에서는 스마트폰 환경에서 발생하기 쉬운 cloning 문제를 해결하기 위해 사용자의 인식자 $KU_U(=ID_U)$와 패스워드 $KR_U(=KU_U \bullet g^{CW})$를 해쉬 함수 $H(\bullet)$에 적용하여 권한 정보 I_U를 생성하여 예방하고 있다. 제안 프로토콜에서 생성한 보안 인식자 SID_U는 청소년마다 서로 다른 보안 인식자 SID_U를 사용하기 때문에 제 3자가 복제된 자신의 정보를 다른 스마트폰에 적용할 경우 정상적인 청소년으로 인식하지 못하도록 하고 있다. 제안 프로토콜은 cloning 문제이외에 제3자가 소유하고 있는 스마트카드를 이용하여 다른 스마트카드가 전송한 메시지를 다른 수신기에게 전달하도록 하는 방법으로써 McCormac Hack 문제를 예방하고 있다.

Ⅴ. 결론

본 연구는 스마트폰 게임에 중독된 청소년이 게임에 접속하는 것을 강제적으로 제한하는 프로토콜을 제안하였다. 제안된 프로토콜은 청소년의 게임 시간과 접속 횟수 등의 정보를 이용하여 게임 사용을 자제하도록 하였다. 또한, 청소년이 온라인 게임 상에 물품을 구입할 경우 청소년의 부모에게 게임 아이템 구입 확인 메시지를 전달하여 게임 사용을 제한한다. 향후 연구에서는 제안 메커니즘을 실제 스마트폰에 적용할 계획이다.

■ 참 고 문 헌 ■

[1] 정윤수, 김용태, "PIN 코드를 이용한 IPTV 게임 사용자의 개별 인증 프로토콜", 한국정보통신학회논문지, 제15권 제12호, pp. 2670-2678, 2011.

[2] S. Lee, N. Park,S. Kim, and J. Choi, "Cryptanalysis of secure key exchange protocol between STB and smart card in IPTV broadcasting", Proc. of the Advances in Information Security and Assurance (AISA), Vol 5576, LNCS, pp. 797-803, 2009.

[3] Y. S. Jeong, Y. S. Jung, Y. T. Kim, G. C. Park and S. H. Lee, "A Security Model Analysis Adopt to Authentication State Information in IPTV Environment", The Journal of Korea Information and Communication Society, Vol. 35, No. 3, pp 421-430, Mar. 2010.

[4] Y. S. Jeong, Y. T. Kim, G. C. Park and S. H. Lee, "User Authentication Mechanism for using a Secure IPTV Service in Mobile Device", The Journal of Korea Information and Communication Society, Vol. 34, No. 4, pp. 377-386, Apr. 2009.

[5] S. Lee, N. Park,S. Kim, and J. Choi, "Cryptanalysis of secure key exchange protocol between STB and smart card in IPTV broadcasting", Proc. of the Advances in Information Security and Assurance (AISA), Vol 5576, LNCS, pp. 797-803, 2009.