한국항행학회 논문지 제14권 제6호 2010년 12월

이중 서명을 이용한 온라인 게임 서버 간의 안전한 게임 캐릭터 이주 시스템 설계

Design of Secure Game Character Migration System Between Online Game Servers using Dual Signature

석진원*, 임웅택**

Jin-Weon Suk*, Ung-Taeg Lim**

요 약

네트워크 기술의 발전은 인터넷 상에서 온라인 게임 산업을 급성장하게 만들었다. 최근, 게임 플레이어들은 이종의 온라인 게임 서버에서 관리되는 게임 캐릭터에 대하여 자유로운 이주를 원하게 되었다. 기존 연구는 게임 플레이어의 요구를 수용한 게임 캐릭터 이주 모델을 제시하고 있다. 그러나 이종 게임 서버 간의 게임 캐릭터의 이주 절차에만 중점을 두었고, 온라인 거래에서 필수적으로 요구되는 안전성 문제가 간과되었다. 그러므로 거래 내용에 대한 안전성 확보 및 분쟁 발생 시 해결 대책 마련이 필요하다. 본 논문에서는 기존 연구(CMP) 를 기반으로 이종 게임 서버 간의 게임 캐릭터를 이주할 때 이중 서명 방법을 사용한 안전한 게임 캐릭터 이주 시스템(SCMP)을 제안하고, 안전성을 검증해 본다.

Abstract

The development of network technology has made rapid growth for online gaming industry on the Internet. Recently, game players have been wanting for a free migration on the game character for game player managed by online game servers of different types. Existing research on the acceptance of the game players demands have suggested migration model of the game character. However, the game Character Migration Process between the game server of different types migration is focused only, and safety issue that is necessary in an online transaction is overlooked. Therefore, ensure the safety of transactions information and when a dispute arises is necessary countermeasures. In this paper, Secure game Character Migration System (SCMP) using dual signature method when migrating game characters between the game servers of different types based on existing research is propose and looks to examine the safety.

Key words :Dual Signature, Online Game Servers, Game Servers, Character Migration

I. 서 론

네트워크 기술의 발전으로 인터넷 상에서 온라인 게임 산업이 급성장함에 따라 게임 아이템의 현금 거래에 대한 수요와 공급이 계속 증가하고 있다 [1]. 온

* 경희대학교 컴퓨터공학과(Dept. of Computer Engineering, Kyung-Hee University)
** 부천대학 전산정보처리과(Dept. of Computer Science, Bu-Cheon University)
· 제1저자 (First Author) : 석진원, 교신저자 : 임웅택
· 투고일자 : 2010년 10월 14일
· 심사(수정)일자 : 2010년 10월 15일 (수정일자 : 2010년 12월 23일)
· 게재일자 : 2010년 12월 30일

라인 게임 중에서 다중 접속 역할 수행 게임 (MMORPG, Massively MultiPlayer Online Role-Playing Game)에서 게임 플레이어는 게임 캐릭터가 자신을 대신하는 존재로 여기게 되어 게임 캐릭터 성장에 많은 시간과 노력을 기울이게 되었다. 그리고 게임 플레이어는 보다 빠른 게임 캐릭터의 성장을 위해 현금을 지불하는 게임 아이템 거래 시장의 이용에 대한 많은 유혹을 받고 있으나 현재의 게임 아이템 거래 시장은 온라인과 오프라인을 병행하는 시스템으로 운영되고 있어서 많은 분쟁의 소지를 안고 있다 [2].

현재까지 게임 아이템의 거래와 관련한 법적 규제 및 장치가 완전하게 마련되지 않은 상황이며, 기존의 관련 연구에서는 서로 다른 온라인 게임 서버에서 관리되는 게임 플레이어의 게임 캐릭터 능력치를 사이버 머니로 환산하여 게임 서버 간에 이전할 수 있는 게임 캐릭터 이주 모델을 제시하고 있다 [3],[4]. 이러한 이종의 게임 서버 간의 게임 캐릭터 이주 모델은 현금 거래가 없이 게임 플레이어 자신이 정당한 노력에 의해 형성된 능력치를 가진 자신의 게임 캐릭터를 다른 게임 서버로 이주하는 건전한 모델로써 그 의미가 크다고 할 수 있다. 그러나 제시된 게임 캐릭터 이주 모델은 게임 캐릭터 소유자와 원본 게임 캐릭터 관리 서버, 목적지 게임 캐릭터 관리 서버 간에 게임 캐릭터 이주 절차에만 중점을 두고 설계하였기 때문에 온라인 거래에서 요구되는 안전성, 즉 기밀성과 상대에 대한 인증, 거래 내용에 대한 무결성 입증 절차가 생략되어 있다. 특히 거래 당사자 간에 거래 내용에 대한 분쟁 발생 시 해결 대책이 마련되어 있지 못하다.

인터넷 환경에서 익명의 상대방 간에 비대면으로 이루어지는 대부분의 온라인 거래는 안전한 방식을 요구하고 있으며, 차후 분쟁이 발생하였을 때 상호 간에 신뢰할 수 있고 제 3자에 의한 분쟁 해결이 가능한 공개키 기반 (PKI, Public Key Infrastructure)의 전자서명 방식을 대부분 적용하고 있다. 특히 기존 연구 [3]에서와 같이 온라인 거래의 형태가 1대 1 거래가 아닌 중계자가 존재하는 1대 다 형태가 존재할 경우에는 더 복잡한 안전장치가 필요하다. 이러한 중계자가 있는 1대 다 거래 환경에서는 최초 요청자와 중계자, 최종 목적지까지 서로 신뢰할 수 있어야 하고, 경우에 따라서는 최초 요청자와 최종 목적지 간의 거래 내용이 중계자에게는 노출되어서는 안 되는 경우도 있다. 이러한 중계자가 있는 1대 다 환경에서의 안전하고 효율적인 거래 방식을 SET (Secure Electronic Transaction)에서 제공하고 있다.

SET은 인터넷에서 신용카드 트랜잭션을 안전하게 처리하기 위해 Visa와 MasterCard사가 공동으로 개발한 프로토콜이다 [5]. SET은 기본적으로 이중 서명 (Dual Signature) 기법을 사용하여 구매자, 판매자, 지불은행으로 이어지는 당사자들 간에 기밀성 및 데이터 무결성, 그리고 인증 기능을 제공한다. SET의 이중 서명에서 구매자는 구매정보와 지불정보에 대해 서명을 하고 지불정보에 대해서는 판매자가 해독할 수 없도록 암호화하여 판매자를 통해 지불은행으로 보냄으로서 판매자에 의해 구매자의 지불정보가 임의로 사용되는 것을 막을 수 있으며, 지불정보를 받은 운행은 이중 서명된 정보를 통해 구매자와 판매자를 함께 신뢰할 수 있다.

본 논문은 기존 연구에서 제안된 이종 게임 서버 간의 게임 캐릭터 이주를 위한 프로토콜 절차를 유지하면서 안전성을 확보하기 위해 전자서명 방식과 SET에서의 이중 서명 방식을 적용한 안전한 게임 캐릭터 이주 시스템을 제안한다.

본 논문의 구성은 2장에서 기존에 제안된 게임 캐릭터 이주를 위한 프로토콜 (CMP) 절차와 안전성 측면에서 문제점을 분석해보고, 3장에서는 일반적인 온라인 거래에서의 보안 요구사항과 이중 서명을 적용한 안전한 게임 캐릭터 이주 시스템 (SCMP)을 제안하며, 4장에서는 제안한 내용에 대한 안전성 분석을 통하여 검증해 본다. 마지막 5장에서는 연구 결과를 돌아보고 향후 연구 방향을 제시한다.

Ⅱ. 기존의 CMP (Character Migration Protocol) 시스템 분석

기존의 연구에서 제안되어진 CMP (Character Migration Protocol)는 어떤 게임 플레이어가 서로 다른 게임 서버에서 운영 중인 자신의 게임 캐릭터 간에 사이버 머니를 이전하는 과정에 대한 프로토콜이

다 [3]. CMP에서 게임 캐릭터의 이주 프로세스를 알아보고 이 과정에서 어떠한 안전성 문제가 발생할 수 있는지 파악한다.

2-1 게임 캐릭터 이주 절차

게임 캐릭터의 이주는 그림 1과 같이 게임 캐릭터 이주를 원하는 게임 플레이어 (GP, Game Player)에 의해 요청되어 원본 게임 캐릭터를 관리하는 게임 서버 (SS, Source Server)와 이주 목적지 서버 (DS, Destination Server) 간에 서버 이주 작업이 이루어지고, 이주 결과는 SS를 통해 GP에게 전달된다.

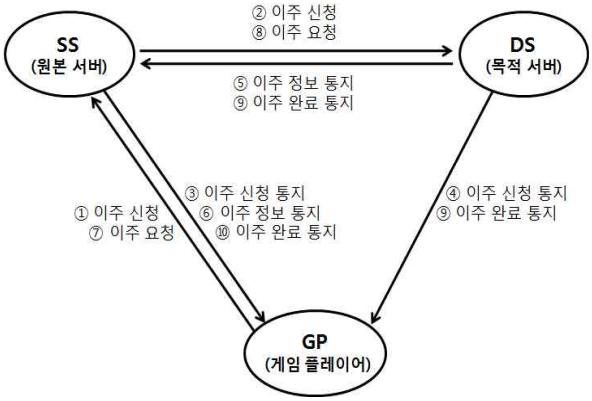

그림 1. 게임 캐릭터 이주 프로토콜 CMP
Fig. 1. Game Character Migration Protocol CMP

① 이주 신청 (GP→SS)

GP는 이주 원본 정보 (SS_info)와 이주 목적지 정보 (DS_info)를 원본 서버 (SS)에게 전달함으로써 이주 신청이 이루어진다. 이주 원본 정보는 이주 대상 게임 캐릭터가 있는 원본 서버명 (SS_name), 사용자 아이디 (SS_UID), 게임 캐릭터 아이디 (SS_CID), 환전 요구 금액 (GP_money)으로 구성되고, 이주 목적지 정보 (DS_info)는 이주 목적지 서버명 (DS_name), 사용자 아이디 (DS_UID), 게임 캐릭터 아이디 (DS_CID)로 이루어져 있다.

user_transfer_request = {SS_info, DS_info}
SS_info = {SS_name, SS_UID, SS_CID, GP_money}
DS_info = {DS_name, DS_UID, DS_CID}

② 이주 신청 (SS→DS)

GP로부터 이주 신청을 받은 SS는 이주 신청된 게임 캐릭터에 대한 원본 게임 캐릭터 정보 (SCI, Source Character Information)을 생성하여 목적지 게임 캐릭터 정보와 함께 DS에 전달함으로써 이주 신청을 마친다. SCI는 SS가 환산한 이주 신청 게임 캐릭터에 대한 환산 정보를 가지고 있다.

ss_transfer_request = {SS_info,DS_info,SS_SCI, SS_CK}
SS_SCI = {SS_CLR,SS_level, SS_HP, SS_MP, SS_SCI}
SS_CLR : 환산 생명치
SS_level : 현재 레벨 / 최대 레벨
SS_HP : 계산 결과 HP (Hit Point)
SS_MP : 계산 결과 MP (Mana Point)
SS_CK : 인증키

③ 이주 신청 통지 (SS→GP)

SS는 GP에게 이주 신청에 대한 처리 결과를 접수번호와 함께 통지한다.

ss_transfer_notification = {SS_AN_info}
SS_AN_info = {SS_AN, SS_RT}
SS_AN : SS가 발급하는 GP의 이주신청 접수번호
SS_RT : 처리 결과

④ 이주 신청 통지 (DS→GP)

DS는 GP에게 이주 신청에 대한 처리 결과를 접수번호와 함께 통지한다.

ds_transfer_notification = {DS_AN_info}
DS_AN_info = {DS_AN, DS_RT}
DS_AN : DS가 발급하는 GP 이주신청 접수번호
DS_RT : 처리 결과

⑤ 이주 정보 통지 (DS→SS)

DS는 SS로부터 전달받은 SCI를 참조하여 예상되는 게임 캐릭터 능력치 (PCI, Predicted Character Information)를 생성하여 이를 SS에게 이주가 가능 여부를 통지한다. 이 때 PCI는 DS에 의해 결정된 환산 정보와 인증키로 구성된다.

ds_transinfo_notification = {DS_AN_info, DS_PCI, DS_CK}
DS_PCI = {DS_money, DS_level, DS_HP, DS_MP}
DS_money : 환산된 금액, DS_level : 환산된 레벨
DS_HP : 환산된 HP, DS_MP : 환산된 MP
DS_CK : 인증키

⑥ 이주 정보 통지 (SS→GP)

SS는 DS로부터 전달받은 PCI 정보를 접수 번호, 처리 결과와 함께 GP에게 전달한다.

ss_transinfo_notification = {DS_AN_info, DS_PCI}

⑦ 이주 요청 (GP→SS)

GP가 전달받은 PCI 정보를 검토하여 게임 캐릭터 이전을 결정하면 SS에게 접수 번호를 전달하여 게임 캐릭터 이전 신청을 한다.

user_update_request = {SS_AN}

⑧ 이주 요청 (SS→DS)

GP로부터 이주 처리 요청을 받은 SS는 접수 번호로 DS에게 이주 처리 변경을 요청한다.

ss_update_request = {DS_AN}

⑨ 이주 완료 통지 (DS→SS, DS→GP)

정상적인 이주 처리를 한 DS는 접수 번호와 처리 결과를 SS와 GP에게 전달함으로써 이주 처리 완료 여부를 통지한다.

ds_changeinfo_notification = {DS_AN_info}
user_changeinfo_notification = {DS_AN_info}

⑩ 이주 완료 통지 (SS→GP)

DS로부터 이주 처리 통지를 받은 SS는 자신이 발급한 접수 번호와 처리 결과를 GP에게 통지한다.

ss_changeinfo_notification = {SS_AN_info}

2-2 CMP의 안전 문제점

① 정보 유출

온라인 방식의 특성으로 GP의 사용자 정보나 게임 캐릭터 정보가 유출 될 수 있고, 이주 신청 중에 접수 번호와 인증키까지 유출된다면 인증되지 않은 제 3자에 의해 악용될 수 있다. 또한 GP 입장에서는 DS와 관련된 게임 캐릭터 정보나 환산된 PCI 정보를 중계자인 SS에게 노출 시킬 필요가 없고, SS가 악의적으로 DS의 PCI 정보를 임의로 수정하여 중계할 수 있다.

② 상대 인증

SS와 DS는 각각 자신을 인증하기 위해 별도의 인증키를 발급하고 있다. 이러한 인증키는 서버 쪽에서 일방적으로 발행하는 인증키로써 분쟁이 발생하였을 때 신뢰할 수 있는 제 3자에 의한 증명이 곤란하게 된다. 또한 SS와 DS 서버 입장에서는 GP를 인증하는 장치가 마련되어 있지 않다.

③ 무결성

거래 당사자 간에는 전달한 정보가 원본과 일치하는지 확인할 수 있어야 한다. 특히 GP와 DS 간의 정보 전달이 SS에 의해 경유되므로 GP와 DS 간에는 무결성을 증명할 장치가 마련되어야 한다.

④ 이주 요청의 부인

이주 요청을 한 GP가 이주 완료 통지를 받고도 마음이 변하여 이주 요청한 사실을 부인할 수 있다.

Ⅲ. 이중 서명을 적용한 SCMP (Secure Character Migration Protocol) 시스템 제안

3-1 온라인 거래에서 보안 요구사항

다음은 앞에서 제시한 기존 게임 캐릭터의 이주 절차에 대한 보안 문제점을 중심으로 안전한 게임 캐릭터의 이주 절차를 위한 온라인 거래에서의 보안 요구사항을 보안 특성과 관련하여 제안한다.

① 기밀성 : GP와 SS, SS와 DS 간의 전송 내용은 비밀성이 보장되어야 한다. 또한 SS를 경유하는 GP나 DS의 정보가 중계자인 SS에게 노출되어서는 안된다.

② 인증 : GP는 거래 당사자인 SS와 DS를 인증할 수 있어야 한다. 또한 SS와 DS 간에도 상호인증이 되어야 한다.

③ 무결성 : 전송 자료가 원문과 일치한다는 점을

입증할 수 있어야 한다.

④ 부인 방지 : 이해 당사자 간에 이주 요청 또는 이주 처리 완료 통지 사실에 대한 부인이 발생할 경우 이를 해결할 수 있는 장치가 마련되어야 한다.

3-2 표기법

- GP : 이주 신청자, Game Player
- SS : 게임 캐릭터 보유한 원본 서버, Source Server
- DS : 게임 캐릭터 이주할 목적 서버, Destination Server
- SK_g, PK_g : GP의 개인키와 공개키
- K_g : GP의 세션키
- $(M)K_g$: M을 K_g로 암호화
- H( ) : 해쉬 함수

3-3 안전한 이주 절차

① 이주 신청 (GP→SS)

GP에서 SS로의 이주 신청 단계에서의 보안 요구사항은 GP가 자신을 SS와 DS에게 각각 인증시켜야 하고, DS에게만 전달되어야 하는 이주 목적지 정보(DS_info)를 SS에게는 숨겨야 하며, 전달되는 모든 정보는 기밀성을 유지하고 무결성을 증명할 수 있어야 한다.

en_user_transfer_request = {SS_info, $(DS\_info)K_g$, $(K_g)PK_d$, M_g, $H(M_g)SK_g\}PK_s$

M_g = {H(SS_info), H(DS_info)}

GP는 이중 서명 정보인 Mg를 생성하고 H(Mg)에 자신의 개인키인 SKg로 서명함으로써 자신을 SS와 DS에게 각각 인증시키고, 전송 정보에 대한 무결성을 확인할 수 있도록 한다. 그리고 DS에게만 필요한 이주 목적지 정보는 SS에게 노출시키지 않기 위해 자신이 생성한 세션키 Kg로 암호화 하고 Kg는 DS의 공개키 PKd로 암호화하여 기밀성을 유지한다. 끝으로 전체 전송 내용에 대한 기밀성을 위해 SS의 공개키 PKs로 암호화 한다.

en_user_transfer_request를 수신한 SS는 SS_info로 H(SS_info)를 구한다, 그리고 Mg의 H(SS_info) 부분과 대체하여 생성한 H(Mg)와 GP가 전송한 H(Mg)를 비교하여 무결성을 확인한다.

② 이주 신청 (SS→DS)

SS에서 DS로의 이주 신청 단계에서의 보안 요구사항은 SS가 자신을 DS에게 인증시켜야 하고, 환산한 원본 게임 캐릭터 정보 (SCI)에 대한 무결성을 보증하며, 전달되는 모든 정보는 기밀성을 유지하여야 한다.

en_ss_transfer_request = {SS_SCI, $H(SS\_SCI)SK_s$, $(DS\_info)K_g$, $(K_g)PK_d$, M_g, $H(M_g)SK_g\}PK_d$

SS는 자신이 생성한 SS_SCI로 구한 H(SS_SCI)에 자신의 개인키인 SKs로 서명함으로서 자신을 DS에게 인증시키고, 전송 정보에 대한 무결성을 보증할 수 있도록 한다. 나머지 GP로부터 전달받은 정보들은 그대로 나머지 정보와 함께 DS의 공개키로 암호화하여 기밀성을 유지한다.

SS로부터 en_ss_transfer_request를 수신한 DS는 DS_info를 구하여 H(DS_info)를 생성한 다음 Mg의 H(DS_info) 부분과 대체하여 생성한 H(Mg)와 GP가 전송한 H(Mg)를 비교하여 무결성을 확인한다.

제안된 단계에서는 기존 CMP의 이주 신청 단계(SS→DS)에서 인증을 위해 사용한 인증키 SS_CK를 전달 정보에서 제외시켰다. 그 이유는 제안된 단계에서 인증 기능이 포함되어 있기 때문이다.

③ 이주 신청 통지 (SS→GP)

이주 신청을 접수한 SS는 이주 신청 접수 번호를 자신의 개인키로 암호화 하여 GP에게 전송한다. 접수 번호는 SS의 개인키로 서명되어 있으므로, SS는 GP에게 이주 접수를 받은 사실을 부인할 수 없다. 또한, 접수 번호의 변조를 방지하기 위해 해쉬 함수를 이용하여 무결성을 보증한다. 전송 정보는 기밀성 유지를 위해 GP의 공개키로 암호화 한다.

en_ss_transfer_notification = {SS_AN_info, $H(SS\_AN\_info)SK_s\}PK_g$

④ 이주 신청 통지 (DS→GP)

이주 신청을 접수한 DS는 이주 신청 접수 번호를 생성한 다음 해쉬 함수와 자신의 개인키를 사용하여 무결성 보장과 부인방지 서명을 한다. 전송 정보는 기밀성 유지를 위해 GP의 공개키로 암호화 한다.

en_ds_transfer_notification =
{DS_AN_info, H(DS_AN_info)SK_d}PK_g

⑤ 이주 정보 통지 (DS→SS)

DS에서 SS로의 이주정보 통지 단계에서의 보안 요구사항은 DS가 자신을 SS와 GP에게 각각 인증시켜야 하고, GP에게만 전달되어야 하는 환산된 예상 게임 캐릭터 능력치인 PCI를 SS에게는 숨겨야 하며, 전달되는 모든 정보는 기밀성 유지하고 무결성을 증명할 수 있어야 한다.

en_ds_transinfo_notification = {DS_AN_info, H(DS_AN_info)SK_d, (DS_PCI)K_g, H(DS_PCI)SK_d}PK_s

DS는 GP에게만 공개할 PCI를 GP가 생성한 세션키 Kg로 암호화 하고, H(DS_PCI)를 자신의 개인키로 서명하여 GP에게 인증을 받을 수 있도록 한다. 또한 SS에게 자신을 인증하기 위해 H(DS_AN_info)에도 자신의 개인키로 서명한다.

en_ds_transinfo_notification를 수신한 SS는 DS_AN_info로 H(DS_AN_info)를 구하여 수신한 H(DS_AN_info)와 동일함을 확인함으로서 DS를 인증하고 무결성을 확인한다.

제안된 단계에서는 기존 CMP의 이주 신청 단계(DS→SS)에서 인증을 위해 사용한 인증키 DS_CK를 전달 정보에서 제외시켰다. 그 이유는 제안된 단계에서는 인증기능이 포함되어 있기 때문이다.

⑥ 이주 정보 통지 (SS→GP)

DS에서 SS를 경유하여 GP에게 전달되는 이주정보 통지 단계에서의 보안 요구사항은 GP가 SS와 DS를 모두 인증할 수 있어야 하고, GP에게만 전달되어야 하는 PCI는 여전히 기밀성을 유지하고 무결성을 증명할 수 있어야 한다.

en_ss_transinfo_notification = {SS_AN_info, H(SS_AN_info)SK_s, (DS_PCI)K_g, H(DS_PCI)SK_d}PK_g

SS는 GP에게 자신을 인증하기 위해 H(SS_AN_info)에 자신의 개인키로 서명하여 자신을 경유만하는 암호화된 DS_PCI 정보와 함께 GP의 공개키로 암호화한다.

en_ss_transinfo_notification를 수신한 GP는 SS_AN_info와 DS_PCI로 H(SS_AN_info)와 H(DS_PCI)를 구하여 SS와 DS에 대한 인증과 무결성을 확인한다.

⑦ 이주 요청 (GP→SS)

GP가 SS에게 이주 요청을 하는 단계에서의 보안 요구사항은 서명을 통한 자기 인증과 무결성 증명방법의 확보이다.

en_user_update_request =
{SS_AN, H(SS_AN)SK_g}PK_s

GP는 SS에게 자신을 인증하고 무결성 보증을 위해 SS가 발급한 접수번호로 H(SS_AN)를 구하여 여기에 자신의 개인키로 암호화 한다.

⑧ 이주 요청 (SS→DS)

SS가 DS에게 이주 요청을 하는 단계에서의 보안 요구사항은 서명을 통한 자기 인증과 무결성 증명방법의 확보이다.

en_ss_update_request =
{SS_AN, H(SS_AN)SK_s}PK_d

SS는 DS에게 자신을 인증하고 무결성 보증을 위해 DS가 발급한 접수번호로 H(DS_AN)를 구하여 여기에 자신의 개인키로 암호화 한다.

⑨ 이주 완료 통지 (DS→SS, DS→GP)

정상적인 이주 처리가 완료한 DS는 접수 번호에 서명하여 SS와 GP에게 전달한다.

en_ds_changeinfo_notification =
{DS_AN_info, H(DS_AN_info)SK_d}PK_s
en_user_changeinfo_notification =
{DS_AN_info, H(DS_AN_info)SK_d}PK_g

DS는 SS와 GP에게 각각 자신을 인증하고 무결성 보증을 위하여 자신이 발급한 접수 번호와 처리 결과로 H(DS_AN_info)를 구하여 여기에 자신의 개인키로 암호화 한다.

⑩ 이주 완료 통지 (SS→GP)

DS로부터 이주 처리 완료 통지를 받은 SS는 자신이 발급한 접수 번호에 서명을 하여 GP에게 통지한다.

$en\_ss\_changeinfo\_notification$ =
$\{SS\_AN\_info,\ H(SS\_AN\_info)SK_s\}PK_g$

SS는 GP에게 자신을 인증하고 무결성 보증을 위해 자신이 발급한 접수 번호와 처리 결과로 H(SS_AN_info)를 구하여 여기에 자신의 개인키로 암호화 한다.

Ⅳ. 제안 시스템 (SCMP)에 대한 안전성 분석

지금까지 기존 연구 [3],[4]에서 제안한 이종의 온라인 게임 서버 간의 게임 캐릭터 이주를 위하여 이주 절차와 보안측면에서의 문제점을 알아보았고, 이러한 문제점을 보완한 이중 서명 방법을 적용하여 안전한 게임 캐릭터 이주 시스템을 제안하였다. 이 장에서는 제안된 시스템이 3-1절에서 제시한 보안 요구사항들을 얼마나 만족하는지 검증해 본다.

① 기밀성

모든 단계에서 기밀성 확보를 위해 전송 데이터에 대해 수신자의 공개키로 암호화 하여 해당 개인키를 소유한 정당한 수신자만이 복호화가 가능하도록 하였다. 또한 GP와 SS 간에 SS를 경유하여 전달해야 하는 정보 중에 이주 목적지 정보 (GP→SS→DS)와 예상되는 게임 캐릭터 능력치 PCI 정보 (GP←SS←DS)에 대해서는 GP가 생성하여 안전하게 DS에게 전달한 세션키를 이용하여 암호화함으로써 단순 중계자인 SS로부터 보호되도록 하였다.

② 인증

모든 단계에서 수신자가 송신자를 인증할 수 있도록 전송하는 데이터 중 일부에 대해 해쉬 함수를 적용한 다음 전송자의 개인키로 암호화 하여 서명한 정보를 부가하여 보내도록 하였다. 이렇게 함으로써 수신자는 자신이 구한 해쉬 함수 결과와 수신한 내용을 비교하여 무결성을 확인함과 동시에 송신자 개인키로 서명한 결과에 대한 무결성을 입증함으로써 송신자를 정당한 상대로 인증할 수 있다. 특히 최초 이주 신청 단계에서는 신청 당사자인 GP가 이중 서명 방식을 이용하여 서명함으로써 한 번의 서명으로 SS와 DS에게 동시에 인증을 할 수 있게 하였다.

③ 무결성

모든 단계에서 무결성 입증이 필요한 정보에 대해서는 해당 메시지와 메시지에 대해 해쉬 함수를 적용시킨 코드를 함께 전달하여 수신자가 무결성을 증명할 수 있도록 하였다. 이 때 해쉬 함수를 적용시킨 코드는 불법적인 변조로부터 보호하기 위하여 송신자의 개인키로 암호화 하였다. 특히 GP에서 SS를 경유하여 SS와 DS에게 각각 별도의 게임 캐릭터 이주 정보를 전달해야 하는 상황에서 이중 서명 방식을 사용함으로써 무결성 입증 방법을 보다 간소화 할 수 있었다.

④ 부인 방지

제안된 절차는 공개키 기반 (PKI, Public Key Infrastructure) 전자 서명 방식을 적용함으로써 거래 당사자 간에 분쟁이 발생할 경우에 거래 당사자의 신원과 공개키를 보유하고 있는 신뢰할 만한 기관에 의해 분쟁이 해결될 수 있다.

예를 들면, 이주 요청을 한 GP가 이주 완료 통지를 받고도 마음이 변하여 이주 요청한 사실을 부인할 경우, SS나 DS는 GP의 개인키로 서명된 이주 요청 정보를 근거로 분쟁을 해결할 수 있다.

Ⅴ. 결 론

본 논문은 기존에 제안된 게임 캐릭터 이주를 위한 프로토콜 (CMP)을 기반으로 공개키 기반의 전자

서명 방식을 적용한 실제 온라인 환경에서 안전하고 효과적으로 당사자들 간의 분쟁 해결을 할 수 있는 안전한 게임 캐릭터 이주 시스템 (SCMP)을 제안하였다. 그리고 제안된 SCMP에 앞에서 제시한 보안요구사항을 적용한 안전성 분석을 통하여 이종 게임 서버 간에 게임 캐릭터를 이주시킬 때 안전하게 게임 플레이어의 캐릭터 정보를 이주시킬 수 있음을 증명하였다.

금번 연구에서 제안한 SCMP 시스템은 온라인 게임 서버에 직접 적용하여 문제점을 찾아보고 지속적으로 개선할 필요가 있다. 그리고 향후에는 이종의 온라인 게임 서버 간의 정보 공유에 대한 보안 아키텍처 정립 및 상호운용성 보장 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] 한국콘텐츠진흥원, "(대한민국)게임백서", 2009.

[2] 정윤경, 기준백, 천정희, "온라인 게임 아이템의 안전한 전자 거래 시스템", *정보보호학회 논문지, 제13권, 제3호,* 2003.

[3] 김주연, 강준규, "게임 캐릭터 이주를 위한 프로토콜 설계", *부천대학 논문집, 제30집,* pp. 81-87, 2009.

[4] 김주연, 강준규, "온라인 게임 간의 게임 캐릭터 이주 모델에 관한 연구", *한국정보처리학회 논문지, 제3권, 제3호,* pp. 217-222, 2008.

[5] Visa & MasterCard Co, "Secure Electronic Transaction(SET) Specification Book 2: Programmer's Guide", *SET version 1.0, May 31,* 1997.

석 진 원 (昔鎭元)

1990년 2월 : 금오공과대학교 전자공학과(컴퓨터공학전공, 공학사)
1996년12월 : 국방대학원 전자계산학과 (국방과학석사)
2004년 2월 : 경희대학교 일반대학원 컴퓨터공학과(박사수료)
현재 : (주)비전앤바이오테크 이사
관심분야 : 온라인 게임, 네트워크 보안, RFID/USN

임 웅 택 (林雄澤)

1985년 2월 : 금오공과대학교 전자공학과(컴퓨터공학전공, 공학사)
1992년 1월 : 국방대학원 전자계산학과 (국방과학석사)
2005년 2월 : 숭실대학교 일반대학원 컴퓨터공학과(공학박사)
1997년 3월~현재 : 부천대학 전산정보처리과 부교수
관심분야 : 암호 알고리즘, 네트워크 보안