International Journal of Innovative Computing, Information and Control
Volume **5**, Number **12(A)**, December **2009**

 ISSN 1349-4198
pp. 4715–4723

A SECURE EVENT UPDATE PROTOCOL FOR PEER-TO-PEER MASSIVELY MULTIPLAYER ONLINE GAMES AGAINST MASQUERADE ATTACKS

Chun-Ta Li[1,*], Chia-Hui Wei[2] and Yeo-Hao Chin[2]

[1]Department of Information Management
Tainan University of Technology
529 Jhong Jheng Road, Yongkang, Tainan, 710, Taiwan
*Corresponding author: th0040@mail.tut.edu.tw

[2]Department of Computer Science
National Tsing Hua University
101, Section 2, Kuang Fu Road, Hsinchu, 300, Taiwan
{ chwei; yhchin }@cs.nthu.edu.tw

Received June 2008; revised October 2008

Abstract. *In recent years, several massively multiplayer online games (MMOGs) for peer-to-peer (P2P) networks have been proposed. In 2008, Chan, Hu, and Jiang* [3] *proposed a hihyly efficient, secure event signature protocol (EASES) for P2P-based MMOGs. The security of EASES is based on one-time signature keys and hash-chain keys. However, in this paper, we demonstrate that the cheat-prevention EASES protocol, introduced by Chan et al. is vulnerable to a passive attack. As a result, an attacker, Known as an Eve, can masquerade as a legal player to deceive other players and lead them to believe Eve's illegitimate actions. A simple improvement is suggested to eliminate this vulnerability.*

Keywords: Attack, Hash-chain, One-time signature, Peer-to-peer, Security

1. **Introduction.** Massively Multiplayer Online Games (MMOGs) are computer games that enable thousands of international players to simultaneously interact in a game world. These games have rapidly gained popularity in recent years. The market researcher for IDC [7] reported that the revenue from China's online gaming market reached $298 million in 2004. This was a 48 percent increase from the previous year. Revenue is expected to quadruple by 2009, due to widespread accessibility to the Internet within the region. The rapid growth in online gaming has created challenges in the geographical distribution of massive players, amount of data, as well as, the heterogeneity of devices and wireless platforms. Many studies [5, 20, 23, 25] pointed out that client/server systems do not cope well with salability, thereby limiting the potential number of player interactions. They are also not sufficiently robust, and can be subject to bottleneck due to their centralized infrastructure and bandwidth. Peer-to-peer (P2P) [9, 10, 22, 24, 26] MMOGs have many advantages over traditional server/client systems. P2P overlay approach is able to provide network connectivity and basic network services in a self-organizing manner. It provides a scalable, flexible and robust technology. P2P generally used for file sharing resources, such as movies or musics, on the Internet. These applications and MMOGs communicate on the Internet raise the security issues of authentication and authorization for the use of resources.