Design and Implementation of a Secure Online Lottery System

Pramote Kuacharoen

Department of Computer Science, Graduate School of Applied Statistics
National Institute of Development Administration
118 Serithai Rd. Bangkapi, Bangkok 10240 Thailand
pramote@as.nida.ac.th

Abstract. Government has the authority to operate lottery schemes. Since the operation of the lottery system is controlled by the government, there are issues with public trust. The people may speculate that the lottery is rigged. This issue becomes critical with an online lottery system since the unprotected data can be easy manipulated. If all combinations which have been sold are known before the drawing, the government may draw winning numbers which pay the least. Moreover, winning tickets may be added after the drawing. As a result, corruption may be inevitable. The government should operate lottery schemes with integrity which include transparency and accountability.

This paper presents the design and the implementation of a secure online lottery system. The proposed system can provide accuracy, privacy, transparency, and verifiability. Using the proposed system, the government can operate lottery schemes with integrity.

Keywords: Online lottery system, secure online lottery system, information security

1 Introduction

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. The requirements of information security have undergone changes in the last several decades. When data was not accessible remotely, the security of information that was valuable was provided primarily by physical and administrative means. However, with the use of networks and communications facilities for carrying data between computers, different measures are needed to protect data. The importance of information security to the economic and national security interests has been recognized. The Federal Information Security Management Act (FISMA) defines three levels of potential impact; namely, low, moderate, and high, on organizations and individuals should there be a breach of security [2]. For a system that has a high level of the potential impact, a breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Therefore, such a system demands a high level of security requirements. Examples of