SAWT: A New System for Secure and Anonymous Web Transactions over the Internet

Changjie Wang, Fangguo Zhang and Yumin Wang
P.O.Box 119, National Key Lab. on ISN, Xidian University, Xi’an 710071, P.R.China
Email: cjwang@ee.cityu.edu.hk , ymwang@xidian.edu.cn

This paper proposes a new kind of Secure Anonymous Web Transaction (SAWT) system for anonymous browsing and communication on the Web with high security. In the proposed system, normal users can surf or shop online anonymously while malicious accesses to a Web server can be traced and discovered. The latter property has not been achieved in other existing systems, which can bring greater fairness for both users and Web servers.

Keywords: Anonymity, Proxy Server, Group Signature, and Elliptic Curve

1. INTRODUCTION

With the development of computer science and the popularisation of the Internet, both private communication and commercial transactions on the World-Wide-Web are becoming important and has attracted much research interest. Many of the security concerns for existing systems focus on eavesdropping to prevent outsiders from listening in on electronic conversations. Encryption of communication to and from web servers can effectively hide the content of a conversation from eavesdroppers, and has been integrated into many systems. However, the hiding of the identities of users is often not considered. Thus, eavesdroppers can still learn information such as the IP addresses of users and server computers, the length of the data being exchanged and the time and frequency of these exchanges. Encryption also does little to protect the privacy of the user from the server. It is easy for a Web server to record the contents of each access by checking the log file, which contains much information about its visitors. The server can also record other information such as the user’s IP address, Internet domain name, workplace, approximate location and the type of computing platform being used. With additional effort, this information can be combined with other data to invade user’s privacy. This is analogous to being asked to register private information when roaming in shops or parks in the real world.

Some proposals have been suggested for hiding the identities of users in an electronic transaction, such as blind signature scheme (Chaum, 1983), and steganographic techniques (Neil, Zoran and Sushil, 2000). Most of those proposals are suitable for offline electronic transactions, where multiple iterations are commonly needed, and are short of anonymity control mechanism, which limits their usage in online Web transaction applications. There are also some existing systems to protect user’s anonymity on the Internet, such as Onion Routing (Reed, Syverson and Goldschlag, 1998), Anonymizer (Anonymizer, 2002), LPWA (Gabber, Gibbons, Marias, and Mayer, 1998).