Research on Mobile Agent Security

Wataru Hasegawa (510080)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 8, 2007

Keywords: Mobile Agent, Security, Oblivious Transfer, Encrypted Circuits, Secure Function Evaluation.

Mobile Agents are autonomous programs capable of migrating from hosts to hosts during their execution. The features of autonomy and mobility provide mobile agents enormous potential for application in distributed computation. Typical areas include an auction, a travel agent system and so on. Mobile Agent technology has drawn attention as a fundamental technology in next generation computing and has been studied extensively. The advantages of mobile agents are reducing communication lag between users and hosts by autonomy and parallelizing computations by creating multiple agents. However, realization of mobile agent is facing two serious problems. First, an attack on hosts by malicious agents such as computer virus, malware and so on. Second, an attack on mobile agents by malicious hosts such as tampering and eavesdropping agents' secret during their execution.

Although the former can be solved by the confirmed countermeasures, for example, anti-virus software and JAVA security technology, the latter is difficult to be solved since programs must be eventually decrypted into plaintexts form at the time of program execution. So the ways of executing an encrypted program without decrypting it have been studied so far. One of the solutions is the method using secure function evaluation proposed by C. Cachin et al.. However, this method is vulnerable to malicious hosts which can operate encrypted circuits, encrypted circuit inputs and outputs at the their convenience. Then, Algesheimer et al. applied Trusted Third Party between agents and hosts, and they proposed the method where agents' circuit inputs are encrypted by Trusted Third Party's public key. Oblivious Transfer as a communication protocol is used to send encrypted circuit inputs from Trusted Third Party to hosts. But it is inefficient to apply simply 1-out-of-2 oblivious transfer since we have to repeat 1-out-of-2 oblivious transfer for each encrypted circuit inputs. So, Mori et al. improved k-out-of-n oblivious transfer for mobile agents and substituted it for 1-out-of-2 oblivious transfer. They succeeded in reducing the communication cost and the computational complexity.

By the way, oblivious transfer has three requirements for the security. One is correctness. Correctness means that an oblivious transfer is correct if the receiver obtains the secrets of his choices when the sender with the secrets and the receiver with the choices follows the step of the protocol. Second is the receiver's privacy. The receiver's privacy,

indistinguishability, means that the information of the receiver are hidden to the sender. In fact, any two different sets of choices, the transcripts received by the sender are indistinguishable. If the received messages of the sender are identically distributed, the choices of the receiver are unconditionally secure. Third is the sender's privacy. The sender's privacy has the definitions for two types of hosts. The first type is indistingusihability for the host which has honest-but-curious (semi-honest) behavior. semi-honest means that hosts follow the protocol but always try to obtain agent's messages. Indistinguishability means that the sender's massages except chosen by the receiver are hidden to the receiver. In fact, for any choice set, the unchosen messages should be indistinguishable from the random ones. Second types is comparing with the Ideal model for the host which has malicious behavior. Malicious behavior means that hosts do not follow the protocol and always try to obtain agent's messages. In the Ideal model, the sender sends all secrets and the receiver send his choices to the trusted third party. The trusted third party then sends the chosen secrets to the receiver. This is the most secure way to implement the oblivious transfer scheme. The receiver can not obtain extra information from the sender in the Ideal model. We say that the sender's privacy is achieved if, for any receiver in the real oblivious transfer scheme, there is another polynomial-time-bounded probabilistic Turing machine, called simulator, in the Ideal model such that the outputs of the receiver and the simulator are indistinguishable.

Cachin's scheme has correctness, the receiver's privacy and the sender's privacy based on Computational Diffie-Hellman (CDH) Assumption. But it is not efficient because it used 1-out-of-2 oblivious transfer in that scheme. Mori's scheme has correctness and the sender's privacy based on Chosen-Target Computational Diffie-Hellman (CT-CDH) Problem. However, the queries of the receiver are divided into two sets consists of the bits 1 or 0 in that scheme. So, if the queries have all 0s or all 1s and either bits have a selection bias, Mori's scheme does not have the receiver's privacy on specific condition.

In this paper, we suggest oblivious transfer without dividing the queries of the receiver into two sets in order to ensure The receiver's privacy on that condition. And we define a new problem and an assumption, named New Target Computational Diffie-Hellman (NT-CDH), to prove the Sender's privacy. Consequently, our schemes have correctness, the receiver's privacy, the sender's privacy and good efficiency too. In fact, we propose efficient and secure communication schemes between agents and hosts. However, our scheme1 might be only secure for hosts which have honest-but-curious (semi-honest) behavior . If hosts are malicious in behavior, they might be able to obtain the both messages of Trusted Third Party by sending particular queries to Trusted Third Party. So, our scheme1 might not have the sender's privacy in that case. We propose our scheme2 with the sender's privacy even if hosts are of malicious behavior. But our scheme1 and 2 need the communication three times between Trusted Third Party and hosts.

As a result, we conqure the problem of the security for attackers who eavesdrop the communication between hosts. Furthermore, we compare the efficiency of our schemes about the communication cost and the computational complexity. Consequently, our schemes are more efficient than Cachin's scheme and same efficient as Mori's scheme.