Design and Implementation of Trusted Chatting Room Using Software TPM

Chinyere Grace Kennedy and DongSub Cho
Dept. of Computer Science and Engineering, Ewha Womans University

Abstract
Chatting room has become widely using technology and it is vulnerable to the internet attackers. We proposed a chatting system using a Purebasic programming language to communicate across networks system. Chatting room text is a form of instant messaging between two or group of people. A Communication experiment was designed and implemented to confirm the validity of the developed chatting system on a trusted platform.

1. Introduction
Chatting room is an internet based platform where users can hold conversations using text, audio or video. In [7] a chatting system or conversation is a pure real time event, unlike sending and receiving messages that can take hours or even days in email messaging system. Figure 1 below shows the diagram of a chatting set up, where server starts to run and match client according to order of connection [9]. Each client waits to send their information to the server if the other client is not ready to connect. However, to protect the chatting system from the internet attack, then trusted platform module was introduced.

Trusted platform module (TPM) is a special micro-controller of purpose that is attached on a motherboard of a system [3]. Trusted platform module has the capability of securing identity of any network because it has a key storage. It is a very strong cryptographic primitive, with RSA, SHA-1; random numbers (no symmetric crypto). The performance is as low to avoid export restriction. Its operational validation is assured: with a standard client interface function [5] [3]. TPM is a specialized chip that can be installed on the motherboard of a personal computer for the purpose of hardware authentication. The TPM authenticates the computer in question rather than the user.

The background information on the TPM that follows is taken primarily from the TPM Design Specification [3] and the TPM Protection Profile [6]. All references to the TPM and its capabilities will be with respect to the TPM version 1.2 specification unless otherwise noted. Figure 2 below shows the architecture of the trusted platform module.
2. Related Works

Wu et al [1] work is a novel approach for sentence level emotion detection which is based on the semantic labels and attributes of entities of a sentence. Jiang et al proposed the concept of AIO (Area of Interest), their idea improves the way players communicate with one another and provides a more realistic virtual environment, and player can also easily chat by voice [2]. Li et al [8] in their paper "Enhanced Architecture of TPM" added a new special information I/O interface, through connecting with various parallel or serial trusted devices outside. This new special information I/O interface replaced the function of the physical-presence and implementation of preconfiguration, backup, and the restoration of information within TPM. They considered the shortcoming of the TPM such as owner's unawareness, backup keys and restores keys being captured by the Trojan horse or virus program, and lack of physical presence.

3. Architecture of Our of Idea

![Diagram](image)

Figure 3. Architecture of secure chat system.

Figure 3 above shows the architecture of the secure chatting system. The key web server management is extensively flexible model for empowering customization of the system. It is one of the powerful tools for diagnostic and troubleshooting, it enhances security and reduces attack surface through customization. It also improves and delegates administration tools. Device ID collects information from client, which is checked and verified. Private Key is used by the client to decrypt message received which was encrypted. The PC server provides the service while PC client uses the service provided. In above figure 3 shows the connections 1 to 4 and A to D.

4. Experimental Result

The Purebasic programming environment is used for this chatting interface, Purebasic Development Kit 4.51 was installed, and trusted platform module version 1.2 specifications were also installed in each computer system. Figure 4 showed the starting page the server page of the chatting system. The chatting interface of the client page is shown in figure 5. The server must be selected first because it is server side that needs to be running, before the client within the chatting room. Two dialog boxes are displayed in a window as in figures 4, and 5 respectively. The Server page, after the host is selected then inert name, then click on connect. As the system is connection is shown successful, it displays the IP address of the system, which the guest can use to connect to the host page. Here the work of the TPM is then to secure the message between the host and the guest. TPM will not allow any intruder to penetrate in any of the side, since it is successful installed in each of system. The protection is sure and can be trusted. Trusted platform helps internet chat user to be protected from third party, a worm, virus or other malware on PC that connect to the network by encrypting the message from server and the client decrypt it.
5. Conclusion

This paper designs a secure chatting room with Purebasic Platform applications. The approach proposed is based on common actions between the Client and Server of a PC.

The method runs both Purebasic and TPM on the same PC and use TPM to authenticate the information shares within the chatting room. With this approach third party cannot penetrate into the chat room without officially invited.

In the future study it is expected that chatting server algorithm to implemented in a deep level.

Reference


