要 旨

ユーザによる直接入力を利用した携帯端末向け鍵交換方式の研究

小 松　佐 典

代表的な鍵交換方式として Diffie-Hellman 鍵交換方式や, 公開鍵暗号方式を用いた鍵交換方式がある. 標準的なこれらの方式は中間者攻撃に対して脆弱であった. そこで, これらの方式と公開鍵基盤による認証を組み合わせることで, 中間者攻撃に対する安全性を向上した方式が研究され, 現在, 広く利用されている. しかし, それらの方式は公開鍵基盤による認証を利用する際に, 2 つの問題が発生する. 公開鍵証明書の発行や管理のためのコストが発生するという問題と, 公開鍵証明書の検証に認証局への接続環境が要求されるという問題である.

本論文では, 特に携帯端末向けに鍵交換とユーザによる直接入力を組み合わせた方式を提案した. 提案方式では公開鍵基盤の代わりにユーザによる直接入力が認証の役割を果たす. 既存方式との比較評価によって, 提案方式の有効性を検証し, 応用例を述べた.

キーワード　中間者攻撃, 鍵交換方式, Diffie-Hellman, 認証

Abstract

Key Exchange method for portable terminal with direct input by user

Sasuke KOMATSU

Diffie-Hellman key exchange and the key exchange method with public key cryptosystem is a typical key exchange method. These standerd methods were vulnerable to Man-in-the-middle Attacks. Then, new methods improved sacurity against Man-in-the-middle Attacks by combining authentication with PKI is studied, and used generically now. however, two problems occur when those methods use the authentication by PKI. one is the cost which to issue and to manage public key certificate, and another is a problem that is necessary to be able to connect to certificate authority to verify public key certificate.

In this paper, we propose the method that combine key exchange and direct input by user especially for PDA. Direct input function in authentication in place of PKI. As a result, we examined the effectiveness of the proposed method by the comparison with existing methods, and mentioned application examples.

Man-in-the-middle Attacks, key exchange, Diffie-Hellman, authentication