要 旨

SASプロトコルにおける同期問題

上岡 隆

情報通信分野の発展に伴い，インタネットやモバイルコミュニケーション環境において，通信相手の資格認証が必要不可欠なものとなっている．本研究室では，セキュリティが十分でないネットワーク上でユーザ等の資格認証を行う際，被認証者側および認証者側共に，実行する計算量が極めて少なく，被認証者側にも認証者側にも簡易で小さいプログラムサイズで実現可能，さらに，通信路上での盗聴に強い安全な認証方式，SASパスワード認証方法を提案している．本方式は現在，携帯電話における個人認証用に実装されているが，この実用システムにおいて用いられている同期管理方式には，第三者の改ざんにより認証が不能になる問題がある．

本論文では，SASプロトコルにおける既存の同期管理方式における問題点を指摘し，ほとんど追加コストを必要とせずにこの問題を解決する方法を提案・評価する．

キーワード　SAS認証方式，ワンタイムパスワード，同期管理，盗聴，サービス不能攻撃

Abstract

A synchronous problem in SAS protocol

Takashi KAMIOKA

As information communication technology advances, it has become of extreme importance to authenticate the user and the other party communicated with, in Internet and mobile communication. Our laboratory have proposed the SAS (Simple And Secure) password authentication method for networks that are not sufficiently secure. This features a low processing load on both the authenticated and authenticating sides, with only a small, simple program required at both sides. In addition, it provides strong protection against tapping on the communication path. There is a problem to which authentication becomes impossible by a third person's alteration in the synchronous management system used in this practical use system.

In this paper, I will shown the problem in the existing synchronous management system in an SAS protocol, and propose and evaluate the method of solving this problem, without hardly needing additional cost.

key words SAS Authenticaton protocol, one-time passward, Synchronous management, tapping, Denial of Service Attack