平成 19 年度

フロンティアプロジェクト

学士学位論文

フォワードセキュア RFID プロトコル

Forward Secure RFID Protocol

1080391　　野倉 宏和

指導教員　　清水　明宏

2007 年 3 月 16 日

高知工科大学 フロンティア工学コース

要 旨

フォワードセキュア RFID プロトコル

野倉 宏和

近年，RFID(Radio Frequency IDentification) システムは，バーコードに代わる商品管理システムとしてだけでなく，Felica など，様々な分野への利用が可能な技術として注目されている．RFID システムは，無線通信を用いており第三者による通信内容の盗聴が可能である．また，リーダを用いることで誰でもタグの内容を読み取ることができ，そのため特定の RFID タグの情報を追跡することによる RFID タグの所有者の追跡といった，プライバシ問題が懸念されている．プライバシ問題を解決するためにはプライバシ要件を満たす必要があるとされており，これまで通信毎に通信内容を変化させるワンタイムパスワード認証方式を用いた通信プロトコルによる解決方法が提案されている．しかし，これらの通信プロトコルには，サーバ情報を盗取された際にサーバ上の情報に対応するタグの過去に送信した情報が算出されてしまうという問題がある．

本論文では，プライバシ要件を満たした上で，サーバ，タグの情報を盗取された場合でも過去にそのタグが送信した情報と結びつかない通信プロトコルを提案する．

キーワード　RFID プライバシ問題 ワンタイムパスワード認証方式 サーバ タグ

Abstract

Forward Secure RFID Protocol

Hirokazu NOGURA

Recently, RFID System are expected to be a basic technology on various field not only for Identification, for example Felica. Anyone can intercept messages because RFID systems are using a radio communication. Additionaly anyone can read data in tags easily by using RFID tag reader, so attacker can trace the owner by tracing the RFID tag that he has. That problems called a privasy problems. To solve the privasy problems, it is said that it must be satisfied with privasy requirements. So it is proposed some solution by using a one time password authentication method. Because one time password authentication method change authentication data on communication at each communication. But if you use these solution, anyone can get a past informations on communication by getting a information on server. So I will suggest a information protocol that solved the privasy problems and problems in situation that stealed a information on server in this research.

key words RFID, privasy problem,server,tag,one time password authentication method