論 文 内 容 の 要 旨

博士論文題目

Studies on Authentication and Authorization Mechanism
for Inter-device Communication on Wide Area Network Environment
(広域ネットワーク環境における機器間通信の認証と認可機構に関する研究)

氏　名

平 野　学

This dissertation first introduces the new paradigm for inter-device communication and its characteristics. A new attempt for inter-device communication paradigm causes some security problems that need to be solved. This dissertation shows requirements analysis for security mechanism on the inter-device communication paradigm. This dissertation first presents an extension method of the standard network layer's security mechanism, especially the IPsec protocol and the IKE protocol, for user-level applications. This attempt shows the feasibility study of the network layer's security mechanism on the inter-device communication paradigm. Next, this dissertation presents a novel inter-device authentication and authorization mechanism guaranteeing explicit ownership. The multiple ownerships model is the main concept of the proposal. The proposed model emphasizes the importance of the distinguishing and binding of the device's identity and the ownership explicitly. The dissertation shows the design and implementation of novel smart card software and middleware system based on IPsec and IKE. This dissertation presents demonstration experiments for a TV device and a security camera to show the usability of the proposed inter-device authentication and authorization mechanism. The entire system works as a security proxy for the target appliance. This dissertation shows some discussions about life cycle management for devices, hardware dependent problem, group management methods for devices, prospective future applications and bridging architecture among heterogeneous systems. Finally, the dissertation summarizes main contributions and future work.

氏　名	平野　学

（論文審査結果の要旨）

本博士論文では機器間通信における機器同士の認証と認可を扱う為のセキュリティ・フレームワークを提案している。本博士論文では将来のユビキタス・コンピューティング環境において、1人のユーザが多数の機器を所有し、機器同士が連携して動作するような機器間通信パラダイムの必要性が高まっていくことを述べ、その技術的特徴とセキュリティ上生じる新たな課題を整理している。更に、産業界でどのような機器間通信システムが求められているかを調査分析し、実産業アプリケーションと提案システムに乖離が生じないように要求分析を実施している。具体的には、高度道路交通システム、ビルディングオートメーション及びホームネットワークについて機器間通信パラダイムにおいて生じ得るセキュリティ上の問題点を指摘し、以下の要件を満たすセキュリティ機能が必要となることを示している：（1）分散環境での機器の認証・認可、（2）ユーザ中心の機器管理、（3）機器IDと所有権の分離・関連付け、（4）ID保護機構、（5）実装・アプリケーションから独立した設計。本博士論文では以上の要件を満たす機器間の認証と認可を実現するための新しいセキュリティ機能を、ICチップで動作するID管理ソフトウェア、IPsecとIKEを利用した通信ミドルウェア、IC チップ管理ツールとして設計・実装している。提案システムは、機器ID（公開鍵証明書）、所有権（公開鍵証明書に関連付けられた属性証明書）及びアクセス制御リストをIC チップに格納し、認証処理をIC チップ上のソフトウェアで実行するものである。最終的に開発したシステムは実際の家電機器（通信機能を持たないテレビ、IP 通信機能を持つセキュリティカメラ）に適用する実証実験を行っており、提案システムの有用性の高さを示している。本博士論文では開発したシステムに対する性能評価を実施し、性能面での改善案を提示している。また、機器間通信システムのセキュリティ機能に関する関連研究についても十分議論されており、本研究課題の貢献が明確に示されている。更に、実際の組み込み機器に適用した場合の問題点、機器IDと所有権のライフサイクル、機器の効率的なグループ管理手法、異種システム同士のブリッジといった提案システムの今後の課題についても議論しており、提案システムの検証についても十分に行われているといえる。以上により、本博士論文は研究内容について新規性並びに有効性があることが認められ、博士（工学）の学位を授与するにあたって十分な内容であると認められる。