2007年度第Ⅰ期 未踏ソフトウェア創造事業
機器指向の認証トークンを用いた従来型家電のネット化装置の開発

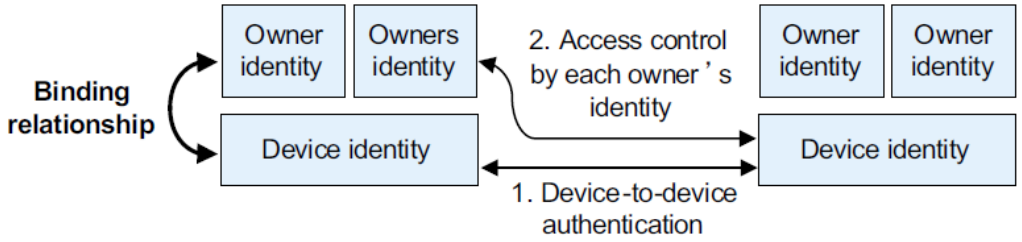
開発者： 平野　学

開発の背景

将来のネットワークには様々な機器が接続され、相互に作用しながら新しいサービスを提供していくと考えられる。このような新しい機器同士が連携するシステムにおいて、従来のクライアントサーバ型アーキテクチャに基づく、ユーザ対サービスの認証、認可の機構をそのまま適用することは難しい。そこで、本プロジェクトでは「機器間通信」のための新しいセキュリティモデルを提案し、認証認可のシステムを開発した。提案システムは従来型家電を簡単に拡張して安全にネットワーク通信が行えることを意図している。

実現した機能

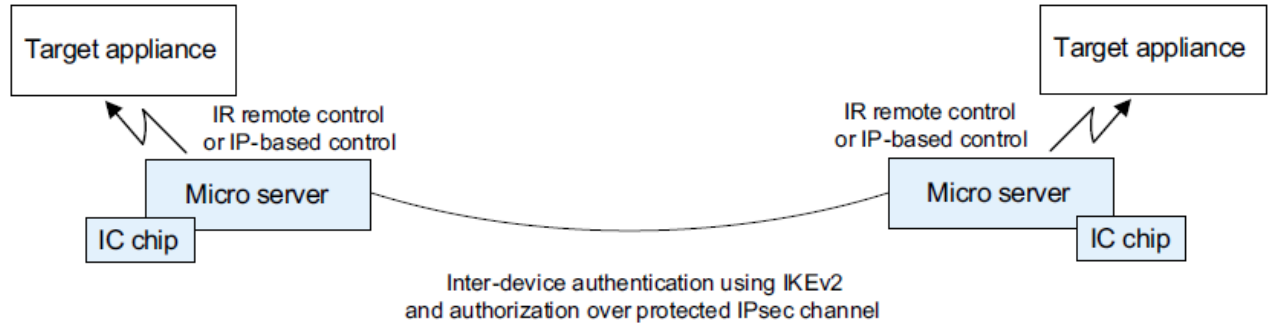
「機器指向の認証トークン」は開発者が従来から提案している機器のIDを格納し認証するソフトウェアを実装したICチップである。このICチップには機器の所有権を格納できる機能も持つ。これにより、機器IDによる相互認証と所有権に基づくアクセス制御を実現することができる。本プロジェクトでは「機器指向の認証トークン」とそれを用いた認証と暗号化通信を行うミドルウェアをマイクロサーバ上に実装し、実際に家電機器の制御を行うためのセキュリティシステムを開発した。



基本コンセプトである「複数所有者モデル」
ひとつの機器に対して、複数の所有者が権限を格納することができる。

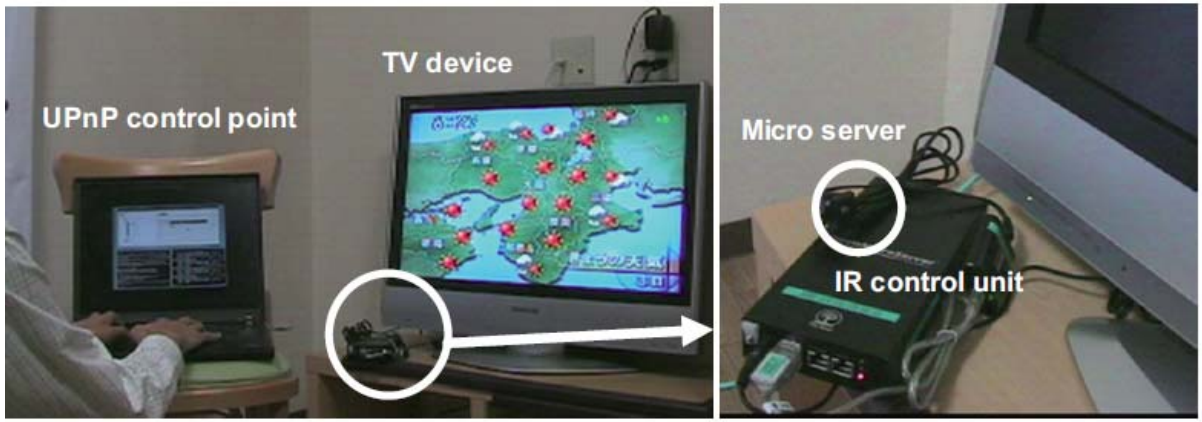
開発したシステムの概要

マイクロサーバと独自開発したソフトウェアを実装したICチップを組み合わせた「セキュリティプロキシ」システム



デモシステム

機器間の認証と暗号化通信は IKEv2 プログラムとICチップの連携によって実現する。家電制御機能は、UPnPサービスとして実装し、ICチップのアクセス制御リストおよび所有権によって認可判定する。実際の機器制御は、(1)IRユニットによるリモコン制御(2)IP対応機器はアプリケーションプロキシ、として実装した。実装は TV(従来型家電) と セキュリティカメラ(IP機器)の両方について行った。開発したシステムによってリモコン制御できる家電機器は、提案する認証認可フレームワークに基づき安全に遠隔制御できるようになる。



従来型家電の安全なネット化

TVを対象としてマイクロサーバで安全に遠隔制御している様子。手前のデモ端末にもマイクロサーバと同じソフトウェアとICチップが動作しており、機器間での安全な連携が可能であることを実証した。

市場効果

ここ数年のトレンドとしてウェブサービスなどを用いたサービス連携が実現されつつある。これらの技術は TCP/IP や HTTP といった通信基盤に XML ベースの機器制御やサービスディスカバリ、イベント通知などの機能をアプリケーション層に実装したシステムであることが多い。本提案で示したミドルウェアはネットワーク層で実現するものであり、上位のアプリケーション層プロトコルに全く依存しない。よって、IPを用いた通信を用いるアーキテクチャに汎用的に適用できる利点がある。本提案の特徴は単なるセキュリティプロキシアプライアンスを開発しただけではなく、認証と認可に「機器ID」と「所有権」を利用する点にある。本提案ではこれらの機能を実現するためにICチップとPKI(公開化基盤)ベースのアプリケーションを実装している。

本提案が活用できる可能性があるのは家電機器フレームワークへの適用、オフィス機器への適用、信頼性やコスト削減によって工場装置やビル管理などでの活用も考えられる。代表的な家電機器フレームワークのひとつであるUPnPへの適用が容易であることは本プロジェクトの実装で示した。今後の課題としてシステムの小型化、低コスト化、高信頼性化が挙げられる。

Short paper:
Manabu Hirano, Takeshi Okuda, and Suguru Yamaguchi. Towards Securing Inter-device Communication: Applying Inter-device Authentication and Authorization Framework to Home Appliances. In *Proceedings of 23rd Annual Computer Security Applications Conference (ACSAC), Works in Progress Session, Miami, FL*, Dec 2007.