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
～　安全な機器間通信のフレームワーク　～

1. 背景

今後のユビキタス社会では、一人のユーザが所有する多数のハードウェア機器をインターネットに接続し、ユーザは必要に応じてそれらを組み合わせ、特定の目的を達成するための機器として再構成して操作する、といった利用形態が具体化していくと考えられる。このような真のユビキタス社会を実現するには、ハードウェアが本当に安全で確認された環境を提供しているかを検証する為の、いわゆる、ネットワーク環境におけるハードウェアの認証基盤技術が必要になると考えられる。

2. 目的

提案者はこれまでの開発で機器指向の認証・アクセス制御を実現する IC チップソフトウェア（機器指向の認証トークン）の開発を進めている。これは、機器のIDを安全に格納し、セキュリティ処理を安全で信頼された IC チップ上の CPU とメモリで実行する IC チップ用のソフトウェアである。本提案ではこの機器指向のセキュリティ機能を持つ IC チップを応用して、従来型の家電にアドオンして「簡単」「安全」にネットワーク化する為の Linux マイクロサーバのソフトウェアシステムを開発する。本提案により従来型の家電機器の安全なネット対応を推進する。

具体的には、機器間の相互認証は IC チップと連携するインターネット鍵交換プログラムで実現する。機器間の暗号化通信は IPsec VPN で実現する。マイクロサーバには UPnP サービスを実装するものとし、ユーザはウェブブラウザ経由で機器に操作命令を送信できるようにする。機器を操作する際には、IC チップに格納された属性証明書とアクセス制御リストを用いて権限に基づく機器のアクセス制御を実現する。最終的に開発したシステムを用いて、従来型家電の安全な遠隔制御ができることを実証実験によって確認するものとする。

3. 開発の内容

本提案では機器指向の認証トークンを応用し、以下に示す各セキュリティ機能を有する従来型家電機器の為のネット化装置を開発した。

（ア） IC チップを接続したマイクロサーバとユーザ操作端末、並びに2台のマイクロサーバ間の相互認証の機能

IC チップの認証機能とインターネット鍵交換プロトコルを連携させて機器間の相互認証を実現する機能。

（イ） マイクロサーバ向けの家電制御用ユーザインターフェース機能

ウェブブラウザを用いて家電機器を操作する為のユーザインターフェース機能を UPnP サービスアプリケーションとしてマイクロサーバに実装する。

（ウ） （イ）を IC チップのアクセス制御機能と連携させる機能

（イ）に IC チップのアクセス制御機能と連携する機能を追加実装する。

（エ） マイクロサーバの UPnP サービスを実際の家電機器と連携させる機能

デモンストレーション用に従来型の家電機器を UPnP サービスから制御できるようにする機能。本プロジェクトでは従来型家電としてテレビを対象として実装を行った。また、IP 対応機器としてセキュリティカメラを対象とした実装も実施した。

本プロジェクトは図 1 に示すような機器同士の通信におけるセキュリティシステムを開発することを目的としている。図 1 は各機器がそれぞれが所属するネットワークからピアツーピアで相互接続している様子を示している。本プロジェクトで仮定している機器間通信システムはこのように複数の機器が連携してサービスを提供するものである。つまり、各機器はクライアントサーバの両方の機能を持つことになり、結果としてピアツーピアネットワークを形成する。本プロジェクトで開発するシステムもピアツーピアで動作する機器に適用できる設計になっている。つまり、機器はある時はクライアントに、ある時はサーバにもなることができる。なお、本プロジェクトでは上位で動作する連携サービスを特定せず、汎用的なセキュリティシステムとなることを目指している。

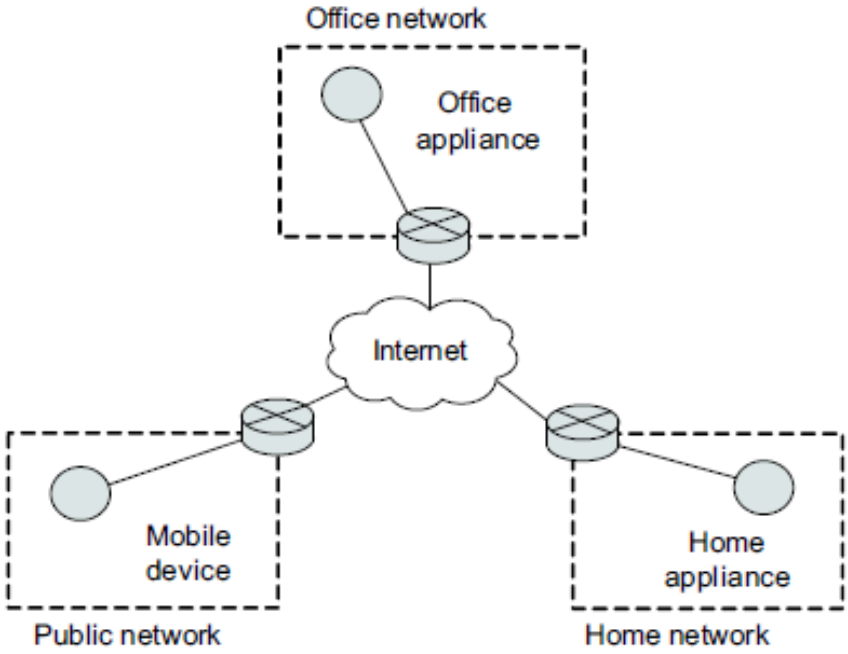

図 1 機器間通信モデル

本プロジェクトで想定している機器とユーザの関係モデルを図 2 に示す。ユーザは対象機器に対して「所有権」(Ownership)を獲得する。続いて、機器同士での認証とアクセス制御が実行される。ここで重要なことは、最初の段階において、ユーザが機器に自分の権限を委譲(delegate)していることである。これによって、機器自身はユーザの「所有権」に基づいて相手の機器にリクエストを送り、相手の機器もその所有権の情報に基づいてアクセス制御を実行することが可能となる。図 3 に単一所有権しかサポートしない従来型のセキュリティモデル(Single Ownership Model)と、複数の所有権情報をサポートする提案モデル(Multiple Ownerships Model)の違いを示す。図 3 の(A)では、ある機器に対して一人のユーザだけが所有権獲得オペレーションによって所有権を設定することができる。しかしながら、このモデルでは機器IDと所有権は 1 対1対応であるため、複数の所有権を登録することができない。また、機器と所有権の関連付けも保証されることはない。対して、図 3 の(B)では機器に対して複数の所有権を設定し、機器IDと所有権を明確に分離、関連付けることが可能である。本プロジェクトでは(B)に示す複数所有者をサポートする新しいセキュリティモデルを利用したシステムを開発する。

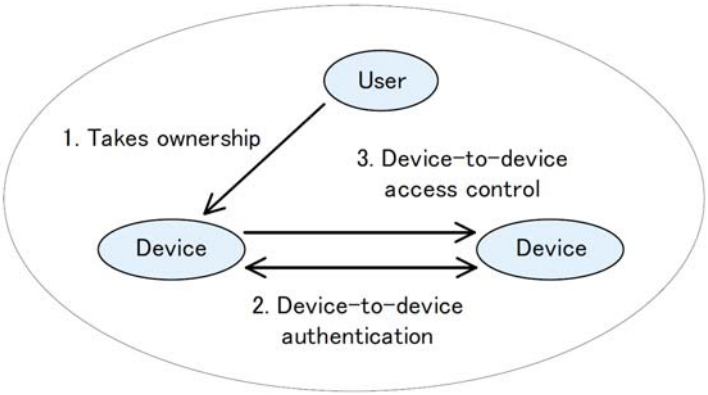

図 2 ユーザと機器との関係モデル

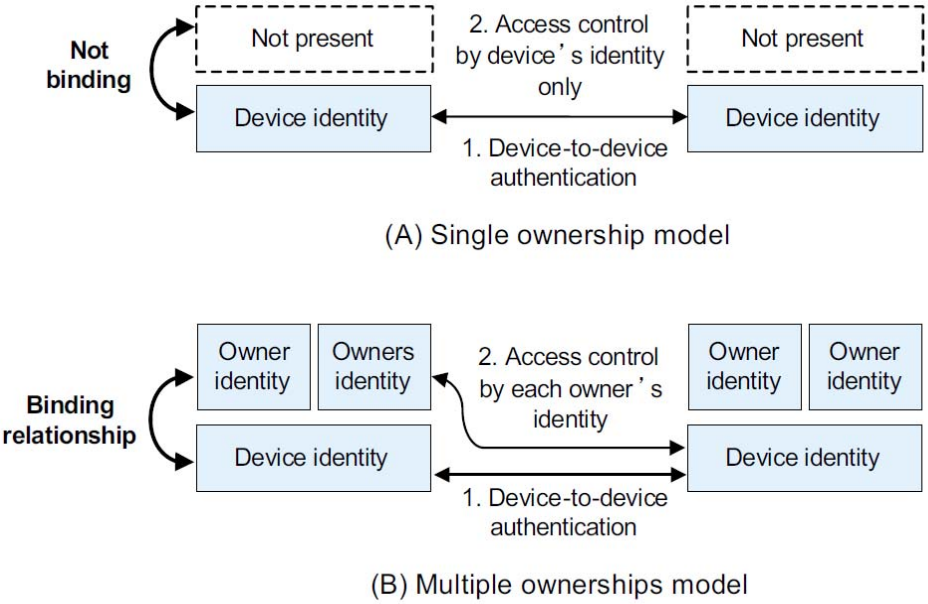

図 3 単一所有権モデルと複数所有権モデルの違い

提案するセキュリティモデルを実現するのに、開発者はこれまでに機器IDと所有権の情報をICチップに安全に格納できるシステムを開発してきている。プロジェクトでは開発者が以前に開発してきている機器指向の認証トークンを用いるものとする。機器指向の認証トークンは機器IDと所有権を分離して扱うことのできる、機器間通信を安全にするためのICチップである。提案システムを実現するには IC チップに独自の機能を実装する必要があったため、本提案システムで利用している IC チップのソフトウェア開発には、Sun Microsystems 社が提供する Java Card API を利用している。

開発したシステムは、機器認証とアクセス制御のための IC チップソフトウェア、認証ミドルウェア、管理ツールから構成され、ネット家電化装置は IC チップを接続したマイクロサーバシステムによって実現した。本プロジェクトで開発したシステムの構成を図 4 に示す。

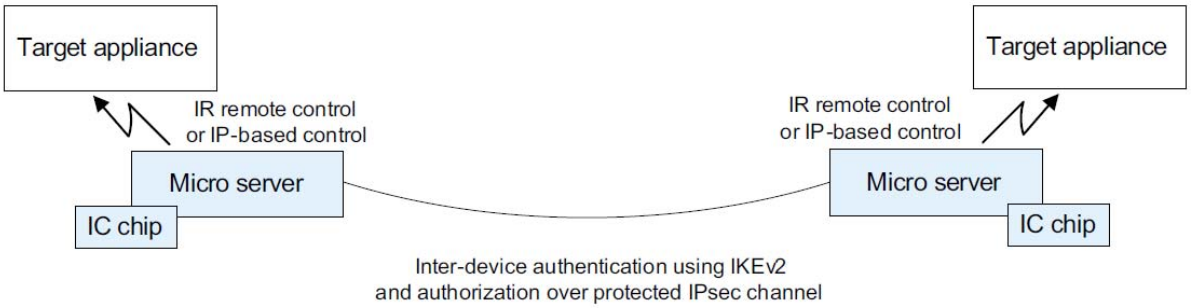

図 4 家電ネット化装置の構成

表 1 ハードウェア仕様

マイクロサーバ	Plathome's Open Micro Server (AMD Alchemy au1550 400MHz)
赤外線リモコンキット	BUFFALO's PC-OP-RS1
ICチップ	Gemalto Cyber° ex Access e-gate 32k
ICチップリーダ	Gemalto e-gate token connector

表 2 ソフトウェア仕様

OS	Debian GNU/Linux 2.6.18
IPv6/IPsec スタック	USAGI
IPsec ポリシ管理プログラム	setkey (ipsec-tools 0.6.6)
UPnP SDK	Intel's portable SDK for UPnP Devices 1.6.0
IKEv2 プログラム	racoon2-20070720a
IR 制御ソフトウェア	usbserial.ko ftdi sio.ko (カーネルモジュール)
PC/SC ライブラリ	PCSC-Lite 1.3.2
CCID ライブラリ	ifd-egate-0.05

マイクロサーバでは IKEv2 プログラムと提案する IC チップが連携して機器認証を実行する。相互認証に成功したマイクロサーバ間は IPsec VPN によって暗号化され通信が保護されるようになる。また、実際の機器の制御の為に、マイクロサーバに UPnP サービスを実装し、UPnP サービスプログラムから IC チップのアクセス制御機能を呼び出せるように改造した。実装に用いたハードウェア構成を表 1 に、ソフトウェア構成を表 2 に示す。

最終的に開発したマイクロサーバのシステムは、ネット接続機能を持たないテレビ(従来型の家電機器)に適用し、IC チップの機能を用いた認証とアクセス制御が利用できることを示した。図 5 に開発システムを用いて TV をネットワーク経由で操作している様子を示す。

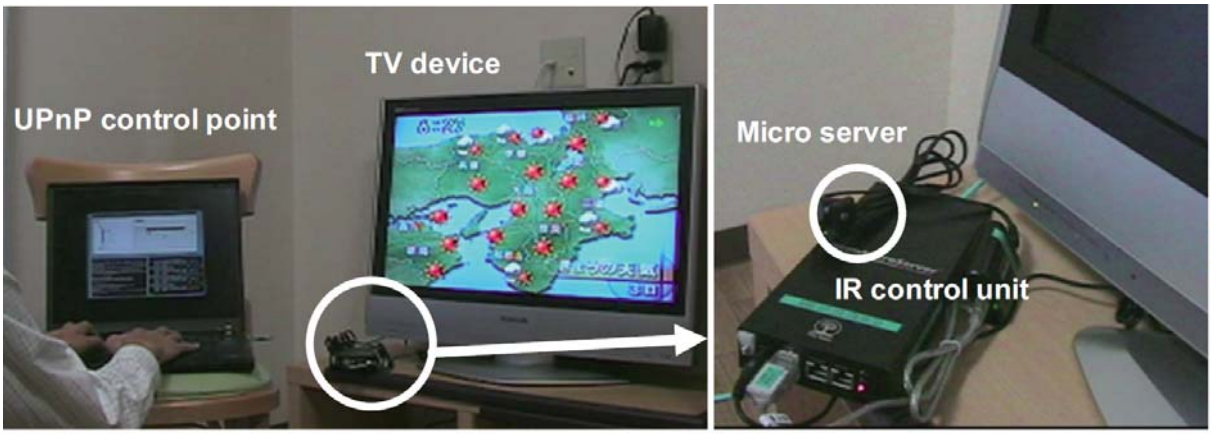

図 5 デモターミナルと TV 間での制御の様子

4. 従来の技術(または機能)との相違

提案したシステムは機器の認証とアクセス制御の為のセキュリティ機能を持つ独自の IC チップソフトウェアを用いている。IC チップを用いた機器認証の関連研究に eTRON があるが、提案システムではユーザの所有権と機器 ID を分離して扱えるようにした特徴がある。その他、耐タンパ性を有する装置に ID を保存する技術に TPM があるが、やはり機器 ID と所有権を分離して扱うことはできない。

5. 期待される効果

開発した IC チップとマイクロサーバのシステムを更に小型化して信頼性を確保することで、様々な機器に搭載できるようになると考えられる。例えば、自動車の情報系ネットワークと外部システムとの相互認証・アクセス制御、ビルオートメーションにおけるコントローラと管理システムとの相互認証・アクセス制御などが挙げられる。

6. 普及(または活用)の見通し

提案システムはオープンソースで開発している為、仕様を一般公開して開発を進めることで広く普及させることができると考えている。

7. 開発者名 (所属)

平野 学 (豊田工業高等専門学校 情報工学科 助手)

学術発表

"Towards Securing Inter-device Communication: Applying Inter-device Authentication and Authorization Framework to Home Appliances", 23rd Annual Computer Security Applications Conference, Works in Progress Session, Miami, FL, Dec. 2007.