情報家電ネットワークに対するKerberosの適用

鎌田 健一† 坂根 昌一‡ 岡部 宣夫‡ 江崎 浩†

†東京大学大学院 情報理工学系研究科 ‡横河電機株式会社

1 はじめに

インターネット技術の普及により、家電などのPC以外のさまざまなディジタル機器がネットワークにつながる機能を持ちはじめている。本論文では、このようなPCとは異なる性質を持つ機器が家庭に導入された場合に生じる、セキュリティー面での課題について議論する。また、その解決策としてKerberos/KINKを用いたアーキテクチャを提案する。

本論文の構成は以下のとおりである。2章でPC以外のディジタル機器がホームネットワークに導入される際のセキュリティー上の問題点を述べ、この問題を解決する際の要求事項を整理する。3章でKerberosを用いたアクセスコントロールについて、4章でKINKを用いた際のアドレス解決についての提案を行なう。最後に5章で本論文のまとめについて述べる。

2 情報家電ネットワークにおけるセキュリティーアーキテクチャ

2.1 背景と課題

家庭に存在するさまざまなディジタル機器が互いにつながり協調動作するという状況が実現しようとしている。また、ネットワークの普及、ブロードバンド化により、家庭の外から家庭内の機器を監視・制御したり、さまざまなデータをやりとりしたりといった要求が出てくる。このように家庭とインターネットとの境界を越えて自由に通信しようとすると、機器同士は対等に通信を確立できる必要があり、その結果、各機器にグローバルなアドレスの割り当てが不可欠になる。しかし、IPv4の32ビットアドレス空間では、全世界の人に対して一つずつアドレスを割り当てることさえできないので、アドレス空間の大きさが不十分であることは明らかである。現在、IPv4のアドレス空間の制約を解消するための技術としてNAT [1]が使われている。しかし、これは機器同士の直接的な通信を制限してしまうので、グローバルなアドレスの替わりにはならない。このため、広いアドレス空間を持ったIPv6が重要な基盤技術となる。

インターネットから家庭内の機器へのアクセス、あるいは、家庭内からインターネットへのアクセスを考えた場合、ファイアウォールのような、ネットワークトポロジーに依存したセキュリティーやアクセス制御は適用できない。すなわち、各ディジタル機器の間でend-to-endにセキュリティーを確保する手段が必要があり、また、ネットワークトポロジーに依存しないアクセス制御の方法が必要である。

2.2 システム要求条件

2.2.1 end-to-endでの通信の安全性(レイヤ3での実現の必要性)

現在セキュリティープロトコルとして代表的なものをあげると、SSL/TLS [2, 3]やIPsec [4]がある。SSL/TLSはアプリケーション層とトランスポート層(TCP)の間で動作するように設計されている。そのため、RSTフラグの立ったパケットを送って接続を切るDoS (Denial of Service)やIPパケットのヘッダを書き換えるなどの、トランスポート層以下の層への攻撃に対処できないという弱点を持つ。また、ホームネットワークで需要の高いと思われる、UDPを用いたストリーミング通信などには対応できない。一方、IPsecはネットワーク層で実現するプロトコルであり、IP上で動作するすべてのプロトコルを保護することができる。そのため、ホームネットワークにおいてend-to-endのセキュリティーを実現する際にはIPsecがふさわしいと考えられる。

IPsecを利用するためには、通信する機器同士が秘密鍵を共有する必要がある。IETF IPSECワーキンググループ[5]では、秘密鍵を共有するプロトコルとして、Diffie-Hellman (DH)鍵交換アルゴリズム[6]を使ったIKE [7]という方式が標準化された。しかし、IKEは本論文で想定している機器には適していない。なぜなら、これらの機器は、コスト、消費電力、物理的サイズなどの制約により、CPUの性能が一般的なPCのそれよりもはるかに劣っており、妥当な時間でIKEを処理できないからである。

一方、IETF KINKワーキンググループ[8]では、Kerberized Internet Negotiation of Keys (KINK) [9]と呼ばれる鍵管理の方式について検討している。KINKでは機

Applying Kerberos to the Communication Environment for Information Appliances

†Ken'ichi KAMADA, Graduate School of Information Science and Technology, The University of Tokyo.

‡Shoichi SAKANE, Yokogawa Electric Corporation.

‡Nobuo OKABE, Yokogawa Electric Corporation.

†Hiroshi Esaki, Graduate School of Information Science and Technology, The University of Tokyo.

器の認証に Kerberos を利用し、個々の鍵交換に関しては対称鍵暗号方式のみを用いるため、妥当な安全性を確保しつつ、IKE に比べて低い計算コストを実現していると期待できる。しかし、KINK では認証に Kerberos [10] を用いるため、IPsec SA の交換時に相手のアドレスだけではなく principal 名を知る必要がある。

2.2.2 アドレス解決

IPv6 のプラグ&プレイ機能 [11] は、機器がネットワークにつながった時に、IP アドレスを自動的に生成する機能である。これによって面倒なアドレスの設定を省略することができる。さらに、携帯する機器を考えると、これらの機器は使う人の位置によって取得するアドレスが変わる。これらのことは、通信を開始しようとした時、相手機器が使っている IP アドレスを動的に解決しなければならないことを意味する。

また、ホームネットワークにおいてはローカルな名前空間も必要になる。ローカルな名前空間では、自分が別のネットワークにいたとしても自分の TV は「自分の TV」としてアクセスできる、ということが必要であるが、それだけではなく、他人からはどのような名前が存在するか見えないようにし、また、アドレス解決もできないように設定できるといった機能が必要な場合もある。現在、ローカルな名前に対するアドレス解決には、DNS のように広く普及したプロトコルが存在しない。また、人によって使いたい手法も異なる。そこで、ローカルな名前の解決には、プロトコルをさまざまな選択肢から選ぶことのできる仕組みが必要である。

2.2.3 アクセス制御

セキュリティーやプライバシーの観点から、アクセスされた機器は相手の機器を正しく認識し、適切なアクセス制御を行なう必要がある。例として、ビデオテープレコーダー (VTR) とそのコントローラを考える。この VTR は、家族の持っているコントローラからは制御できる必要があるが、他人の持っているコントローラから制御できてはならない。また、家族以外の人物でも、ゲストとして家に訪れた場合は、限定された期間だけ VTR を制御できるよう設定できる必要がある。

3 Kerberos を用いたアクセスコントロール

本章では、機器単位の粒度のアクセス制御方式を提案する。より詳細な粒度のアクセス制御 (どのユーザが、どのようなアプリケーションを用いて、どのデータにアクセスするのかに関する制御) については、アプリケーション層で扱う必要がある。このような詳細な粒度のアクセス制御は、本論文の範囲外であり、将来の研究課題である。

Kerberos は、認証する対象に関する情報を中央サーバで一元管理している。このため、巨大な組織などを管理する場合には、スケーラビリティの問題が指摘されている。しかし、ホームネットワークにおける機器の数は小さいので、十分に一元管理が可能であると考えられる。さらに、家庭では、親などの一部の人物だけが、その家のセキュリティの責任を担っているので、情報を一元管理するという Kerberos のモデルに合致していると言えよう。

本論文で提案するアクセスコントロールは、以下の方法で実現する。

- Kerberos により相互に認証できた機器同士のみが通信を行える。
- 家族を構成する人物は、それぞれ自分の realm を持っている。
- ある人物がアクセスしたい機器は、かならずその人の realm に属さねばならない。つまり、realm 内で一意な principal 名と秘密鍵を登録せねばならない。
- Key Distribution Center (KDC) は、同一 realm 内においてのみチケットを発行する。(inter-realm 認証を行なわない)

これにより、その人物が所有するコントローラは、適切な principal 名を用いた場合にのみ、相手の機器と相互認証を行うことができ、適切なアクセス制御を行うことが可能となる。

例として A と B からなる家族を考える (図 1)。A は TV コントローラ CON-a、B は TV コントローラ CON-b を持っている。TV は、A と B からアクセス可能であるが、VTR は、A のみがアクセス可能であるとする。この場合、A の realm として REALM-a、B の realm として REALM-b を定義する。各機器については、CON-a、TV、VCR を REALM-a に所属させ、CON-b と TV を REALM-b に所属させる。CON-b が VTR にアクセスしようとしても、VTR は REALM-b に属していないのでアクセスすることが出来ない。

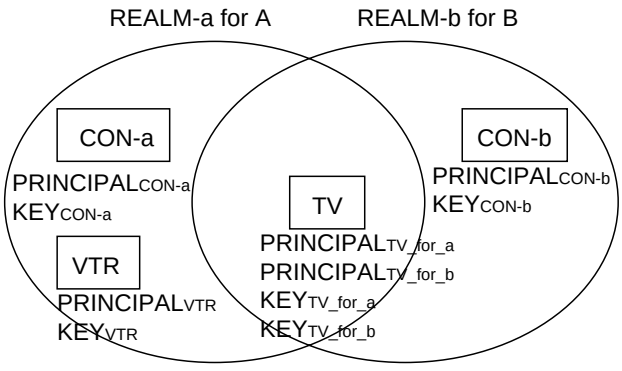

図 1: 家族/機器と realm/principal の対応

次に、ゲスト G の持つコントローラ CON-g に、一定の間だけ TV へアクセスすることを許す場合を考える。この場合、あらかじめ、ゲストのための realm として REALM-g を定義し、REALM-g における TV の principal 名と秘密鍵を TV へインストールしておく。ゲスト G が訪れた時には、CON-g のための principal 名と秘密鍵を CON-g へ割り当てる。これにより、CON-g は、REALM-g のチケットの有効期限の間だけ、TV へアクセスすることが可能となる。以上を図 2 にまとめる。

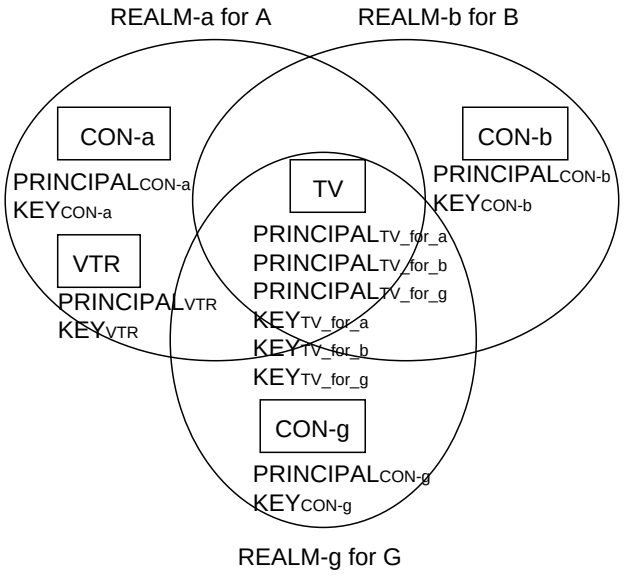

図 2: ゲストのための realm

4 KINK を用いた際の名前/アドレスの対応

IPsec を利用する際、使うたびに機器のアドレスが変わる可能性があるという前提の元では、決まったアドレスを Security Policy Database (SPD) に書いておくのは不可能である。

これは、SPD に名前を書けるようにするだけで解決できる問題ではない。現在広く用いられている socket インターフェイスでは、アプリケーションは名前からアドレスを解決した後、実際に通信を確立する際にはアドレスのみを用いる。このためアプリケーションに何らかの改造を施さない限り、名前の情報を用いることはできない。

送信側は、アプリケーションが相手の名前からアドレスを引く際に、名前ベースのポリシーデータベースを見て、IPsec が必要な場合はそれをアドレスに変換して SPD に登録するといった手法が必要になる。

KINK によって IPsec SA を交換する際には、以下の情報が必要となる。

自分の principal 名 自分の Ticket-Granting Ticket (TGT) や、Service Ticket を取得するために必要。

相手の principal 名 Service Ticket を取得するために必要。

自分/相手のアドレス 実際に IPsec SA を交換するために必要。

そのため、KINK による鍵交換プログラムをどこから起動するかは、重要な問題となる。IP パケットを送信しようとした瞬間にカーネルが起動するという仕組みでは、アドレス情報しか分からず、principal 名が分からないので、KINK による鍵交換ができない。

応答側の KINK 鍵交換プログラムにおいては、始動側が送ってきた Service Ticket に principal 情報が含まれているので、この問題はない。

以上をまとめると、以下の 2 点について解決する必要がある。

1. 名前のポリシーからアドレスのポリシーへ変換して SPD に登録するのはどこで行なうか。
2. KINK をどこで起動するか。

まず 1 に関しては、アプリケーションが用いる名前とアドレスの対応が分かるのは、アプリケーションが resolve したときであるが、このときが適切であろう。resolver などのシステム側が SPD への登録処理を行なうことで、既存のアプリケーションに対する改造の必要がなくなる。

次に 2 であるが、これには大きく分けて 2 つのアプローチが考えられる。IP パケットが送信される時にカーネルから起動する方法と、アプリケーションが resolve した時点で起動する方法である。

まず、カーネルから起動する方法であるが、IP パケットが送信される時点では、IP アドレス情報は利用できるが、相手の名前 (principal 名) は分からない。そこでアドレスから principal 名を逆に求める必要があるが、1 つのノードが複数の principal 名を持つ場合など、一意に決まらない可能性がある。アプリケーションがソケットオプションを用いて、カーネルに principal 名の情報を与えることは可能かもしれないが、これは既存のアプリケーションの改造が必要となり、非常にコストが高い。

次に resolve した時点で起動する方法について考察する。この方法ではまず resolver を改造する手法が考えられる。この手法ではアプリケーションの改造は必要ないが、static link されたアプリケーションをリンクし直す手間がかかる。また、さまざまな resolver を改造するコストがかかり、それらの改造が resolver 本体のコードに統合されるかどうかという問題も残る。そこで、各ノードにローカルな DNS relay のようなものを用意するという手法が考えられる。この手法の場合はアプリケーショ

ンや resolver の改造を行なう必要がないので、普及させるコストが低いと予想される。

1、2 から、以下の方法が最善であると考えられる。各ノードに DNS relay を用意し、resolver からの要求を受ける。DNS relay は与えられた名前を解決すると同時に、名前ベースのポリシーをアドレスに変更して SPD に登録する。その後、解決したアドレスをアプリケーションに返す。図 3 に提案するシステムの概要を示す。

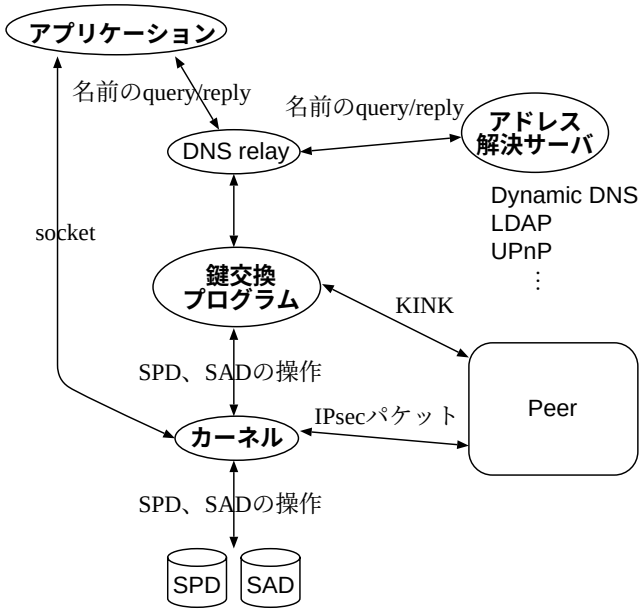

図 3: システムの構成

5 まとめ

ホームネットワーク (情報家電ネットワーク) という環境では、多様なディジタル機器がネットワークトポロジの制約を受けず、直接通信できなければならない。本論文では、そのような環境において生じるセキュリティー、アドレス解決、アクセス制御の問題について議論・考察を行ない、システム提案を行なった。具体的には、Kerberos/KINK を用いたシステムの概要設計を行なった。今後、システムの詳細化、実装と、実証的検証評価を行なう予定である。

参考文献

[1] P. Srisuresh, K. Egevang, “Traditional IP Network Address Translator (Traditional NAT)”, RFC 3022, 2001.

[2] A. Frier, P. Karlton, and P. Kocher, “The SSL 3.0 Protocol”, draft-freier-ssl-version3-02.txt, 1996.

[3] T. Dierks, C. Allen, “The TLS Protocol Version 1.0”, RFC 2246, 1999.

[4] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, 1998.

[5] IETF IP Security Protocol WG (ipsec), `http://www.ietf.org/html.charters/ipsec-charter.html`

[6] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993.

[7] D. Harkins, D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, 1998.

[8] IETF Kerberized Internet Negotiation of Keys WG (kink), `http://www.ietf.org/html.charters/kink-charter.html`

[9] M. Thomas, J. Vilhuber, “Kerberized Internet Negotiation of Keys (KINK)”, draft-ietf-kink-kink-04.txt, 2002.

[10] J. Kohl, C. Neuman, “The Kerberos Network Authentication Service (V5)”, RFC 1510, 1993.

[11] S. Thomson, T. Narten, “IPv6 Stateless Address Autoconfiguration”, RFC 2462, 1998.