M-72 携帯電話網を利用した分散コンピューティングセキュリティに関する一考察

A Note for Distributed Computing Security Based on Cellular Phone Network

富岡 淳樹† 津田 雅之† 倉掛 正治†
Atsuki Tomioka Masayuki Tsuda Shoji Kurakake

1 はじめに

近年、PDA，携帯電話を始めとした小型端末での分散コンピューティングが現実的なものとなってきた[1][2]。分散コンピューティングに限らず、高度なサービスを提供する場合にはそのサービスで用いられるアプリケーションの認証、認可が必須の要件となる。しかし、現行の公開鍵暗号系インフラストラクチャを前提とした認証システムは比較的多くの計算量を必要とし、条件によっては端末側の負担となる場合がある。本稿では「信頼できるサーバ、信頼できるネットワークが存在する」という前提条件の下で、小型端末向けアプリケーション認証の枠組みを提示し、その利点や欠点、適用範囲などについて議論する。

2 既存のアプリケーション認証方式

アプリケーション認証の枠組みで広く認知されているのが Java である。ここでは Java を中心に、既存のアプリケーション認証フレームワークについて簡単に述べてみたい。

2.1 Java2 Platform Security

Java2 Security ではコード署名によるアプリケーション認証方式が規定されている[2]。クライアントはダウンロードしてきた Java アプリケーション（あるいは Java アプレット。以下同様）の署名をローカルの鍵ストアを用いて検証し、署名者を認識する。署名者とダウンロード元 URL の組に対してあらかじめクライアント側で規定されているパーミッションの集合が当該アプリケーションに対して適用される。

この認証方式は自由度が高い一方、アプリケーション署名者の公開鍵証明書を事前に署名者ごとにインストールしておく必要がある。また、署名者とパーミッションの対応付けをクライアント側で行わなければならず、Java およびセキュリティに関する高度な知識を要求される。

2.2 3GPP MExE

3GPP MExE では、あらかじめ Operator, Manufacturer, Third Party, Untrusted というセキュリティドメイン（Security Domain）が規定されており、それぞれに異なるアクセス権限が割り当てられている[3]。アプリケーションはアプリケーション製作者の秘密鍵で署名され、アプリケーション製作者の公開鍵証明書とともにクライアントにダウンロードされる。アプリケーション製作者の公開鍵は各セキュリティドメインのルート公開鍵で検証され、当該アプリケーションは検証に成功したセキュリティドメインに属することになる。

あらかじめドメイン（およびドメインに付与されるアクセス権限）を規定することによって Java2 に比べてシンプルな構造になっているが、アプリケーション製作者ごとに公開鍵を保持しなければならないのは Java2 と同様である。また、セキュリティドメインをルート公開鍵ごとに規定するという枠組みになっているため、運用が大掛かりにならざるを得ないという問題点がある。

2.3 DoJa , BREW

NTT ドコモが提供する携帯電話内に組み込まれた Java 実行環境では、いわゆる Sandbox モデルと呼ばれる厳格なセキュリティポリシーが適用されているため、アプリケーション認証のための枠組みは特に用意されていない。ダウンロードされたどのようなアプリケーションに対しても等しくパーミッションが割り当てられ、限定されたアクセス権限しか持つことができないようになっている[4]。

Qualcom 社が提供する BREW 上で実行されるアプリケーションには「ディベロッパ署名」「公証署名」「実行許可署名」の 3 種類の署名が必要になる。アプリケーション製作者は事前に Qualcomm によってアプリケーションの検証を受けなければならない[5]。

2.4 既存のアプリケーション認証方式の問題点

以上をまとめると、小型携帯端末でのアプリケーション認証の課題は以下の通りである：

- クライアント側の鍵管理の問題
  アプリケーション認証として一般的な署名検証をする場合にアプリケーション開発者ごとの公開鍵をクライアントローカルに保持しなければならない。メモリ容量に十分な余裕の無い小型端末では負担となり得る。また、公開鍵証明書の revocation も考慮しなければならない。
- 低スペック端末での証明書および署名検証
  小型端末は搭載メモリサイズなどの制限から PC などに比べ署名検証などに時間を要する。暗号系演算の専用プロセッサを搭載するという方法もあるが、端末コストとのトレードオフになる。
- セキュリティポリシ運用の柔軟性
  既存の認証・認可モデルは厳格なものが多いため柔軟性に欠き、実運用においてサービス普及を阻害する要因となる可能性がある。

† （株）NTT ドコモ マルチメディア研究所，
Multimedia Laboratories, NTT DoCoMo, Inc.

3 携帯電話網を利用したアプリケーション認証

前節で挙げた問題を部分的に解消するために今回提案するのは、「携帯電話網内でのアプリケーション認証」という限定条件を導入することで、認証のための機構／プロセスを単純化しようというものである。PC のようなプラットフォームと異なり、携帯電話網は現在のところ外界と隔絶されたセキュアなネットワークとインターネットがゲートウェイで接続されているという非常にシンプルな構造になっている。この特性を生かし、従来クライアントが担っていたアプリケーション認証機能をセキュアなネットワーク内の認証用サーバに委譲することを考える。

3.1 前提条件

以下の条件を仮定する：

1. 携帯電話網は信頼できる通信路である
2. 携帯電話網内のサーバは信頼できる
3. 携帯電話網と外界のネットワークを結ぶゲートウェイは信頼できる
4. 外界のネットワークは信頼できない
5. 外界のネットワークに存在するホストは信頼できない

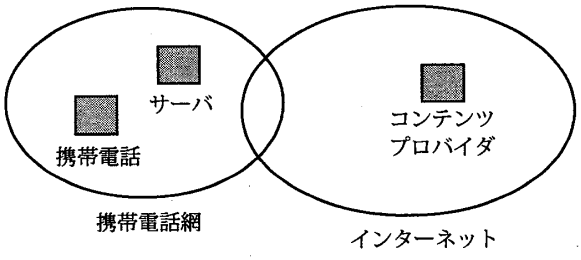

図1 想定するネットワーク構成

3.2 提案方式

インターネットに存在する CP が携帯電話向けにアプリケーションを提供するという状況を考える。CP は秘密鍵と、PKCS#10 などを用いて CA から取得した公開鍵証明書の鍵ペアを持ち、公開鍵証明書を検証できるルート CA 証明書および CP の公開鍵証明書が携帯電話網内のサーバの中に保持されているものとする。また、アプリケーションは事前にキャリアに登録をされているものとし、アプリケーションには事前にアクセス権限情報がアサインされているものとする。また、ADF(Application Descriptor File)内にはコンテンツプロバイダが作成したアプリケーションに対する署名を含んでいるものとする。加えて、アプリケーションダウンロードの方法は基本的に DoJa のそれに従うものとする。

① クライアントがコンテンツプロバイダに ADF を要求する
② クライアントは ADF を解釈する
③ クライアントはアプリケーションのダウンロードを要求する
④ クライアントはアプリケーションをダウンロードし、認証サーバに ADF 内の署名およびアプリケーションを送信する
⑤ 認証サーバは署名検証を行なう
⑥ 認証サーバは検証結果および当該アプリケーションにアサインされているアクセス権限情報を送り返す

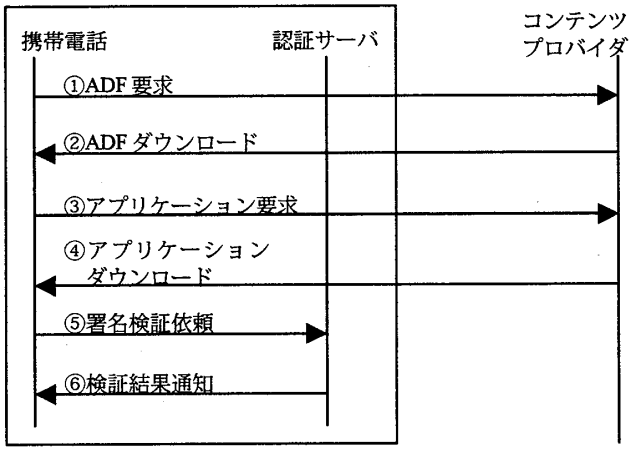

図2 認証シーケンス

5 議論

これはクライアントのアプリケーション認証機能をサーバに単純に委譲した最もシンプルなモデルである。この場合、クライアント側は認証部分をサーバに委譲することで公開鍵検証、署名検証に伴う計算負荷を全てサーバ側に負担させることができる。また、CP の公開鍵証明書は認証サーバ側で保持しているため revocation や expiration の管理も認証サーバ側で一括して行うことができる。

一方、認証サーバに対してアプリケーションおよび ADF 内の情報を送信する必要があり、ネットワーク資源を消費する形になる。この問題はアプリケーションをクライアントにダウンロードする段階において認証サーバを経由させ、認証サーバによる認証を経た上でクライアントにダウンロードさせることである程度軽減可能である。

4 まとめ

携帯電話網という特性を生かしたアプリケーション認証の一手法を提案し、信頼できるネットワーク／サーバが存在するという条件下においてアプリケーション認証機能を委譲できることを示した。携帯電話の性能の向上速度をみれば端末でのアプリケーション認証が計算量的に大きな問題とならなくなるのは時間の問題ではあるが、携帯電話よりさらに小型軽量な端末におけるアプリケーション認証の手法としては依然有効であると考える。

参考文献

[1] BLUEGRID, http://www.ntts.co.jp/java/bluegrid/index.html
[2] iHORB, http://mascot.mis.ous.ac.jp/horb-ous/ihorb/
[3] Li Gong, "Inside Java2 Platform Security", Addison Wesley, 1999
[4] 3GPP Technical Specification 23.057 V3.4.0(2001-03)
[5] i アプリコンテンツ開発ガイド for 504i, NTT ドコモ
[6] "The Road to Profit is Paved with Data Revenue", QUALCOMM Internet Services White Paper, 2002