マルチメディア通信と分散処理　106－8
コンピュータセキュリティ　16－8
（２００２．２．１４）

楕円曲線暗号を利用したSPKIによるネットワーク機器用認証システムの設計

北川 福太郎　西山 裕之　溝口 文雄
東京理科大学　理工学研究科

現在、企業のオフィス環境ではネットワークの権限管理にその多くはPKIが用いられている。しかし、PKIによる権限管理はユーザーの権限が常に固定されているために、柔軟な権限の委譲ということが困難である。そこで本論文ではSPKIを利用した機器の権限管理システムを提案し、設計する。

Design of Authentication System for Network Appliances Using Simple Public Key Infrastructure with Elliptic Curve Cryptography

Fukutarou KITAGAWA　Hiroyuki NISHIYAMA　Fumio MIZOGUCHI
Faculty of Science and Technology , Science University Of Tokyo

Authority of commonly used Access Control in PKI is generically fixed , so it is difficult to delegate authority to others flexibly . In this paper , We propose and design authentication system for network appliances using Simple Public Key Infrastructure.

1.はじめに

近年、情報家電や携帯情報端末（PDA)、SmartCard などの登場により、企業のオフィス環境内においてコンピューターだけに限らない機器のネットワーク化が急速に進みつつある。また、そういった企業などのオフィス環境には様々な種類の人間－正社員、派遣社員、契約社員・・・－やその階層構造－平社員、係長、課長、部長・・・－が存在する。それらの人々のネットワーク上の機器の不正利用を防止するため、機器を利用する際に個人認証を行い、適切な利用権限を与えることは重要である。企業内におけるこれらの個人認証の問題を解決するために、従来はRSA 暗号を用いた Public Key Infrastructure(PKI)と呼ばれるものが多く

用いられてきた。しかしながら RSA 暗号を用いた PKI には、

・柔軟ではない権限管理

・RSA 暗号の実行速度の問題

などのいくつかの欠点がある。

「柔軟でない権限管理」とは、PKI では認証局（CA）からその人の権限情報を含んだ証明書を発行してもらうので一時的に自分の持ってない権限を必要とする事態が発生したときに柔軟に対応できないことを指している。例えば、ある人間が上司から自分が権限を持たない機器を利用した仕事を頼まれたとき、PKI ではその都度 CA に問い合わせて新しい権限証明書を発行してもらう必要がある。

「RSA 暗号の実行速度の問題」とは RSA 暗号が実行にマシンパワーを必要とすることである。昨今のデスクトップ PC や Workstation などでは問題無く実行できるが、携帯情報端末などでは難しい。したがって、今後様々な性能の機器が混在するようになると考えられる企業のオフィス環境に RSA 暗号を適用するのは困難である。

本研究ではそれらの問題の解決として、楕円曲線暗号が利用可能な Simple Public Key Infrastructure(SPKI)を用いたネットワーク機器の認証システムを提案・設計する。SPKI は IETF SPKI Working Group[1]によって仕様が定められており、MIT で SDSI[2]という名称で実装されている。また、楕円曲線暗号[3]は離散対数問題に基づいた公開鍵暗号で RSA 暗号より高速に動作するという利点がある。

2.関連研究

関連研究としては東京理科大学の“SPKI(Simple Public Key Infrastructure)によるプライバシー重視の権限管理の提案と Java を用いた実装”[4]と“X.509 証明書を用いた安全な情報機器制御”[5]がある。“SPKI(Simple Public Key Infrastructure)によるプライバシー重視の権限管理の提案と Java を用いた実装”では SPKI の権限証明書の匿名性を利用して、Web 上での匿名サービスを行うシステムを提案している。また“X.509 証明書を用いた安全な情報機器制御”は X.509-PKI を用いた情報機器の権限管理システムを構築し、X.509 証明書 Version3 の拡張領域をロールに関する情報の記載場所として利用している。ユーザーが機器を利用するときは一旦 Authority Server に証明書を渡し、一定期間有効なチケットを発行してもらう。そのチケットを Authentication Server に提示し、サービスを受ける。このシステムの問題点は CA に証明書を発行してもらう時点でその人の権限が固定されてしまうことである。従って、緊急に何らかの権限が必要になったときに柔軟に対処することができない。

3.楕円曲線暗号

楕円曲線暗号は 1985 年に Koblitz と Miller によってほぼ同時に考案された公開鍵暗号方式の一種で、楕円曲線の性質を応用した暗号であり、その安全性は楕円曲線上の離散対数問題に依存している。現在、ECELGmal や ECDSA、ECDiffer-Hellman、ECRSA といったさまざまな楕円曲線暗号が研究、提案されている。

4.セキュリティ API

本研究では Menezes-Vanstone 楕円曲線暗号と楕円曲線 DSA 暗号を実装したセキュリティ API[6][7]を Java 言語で作成した。セキ

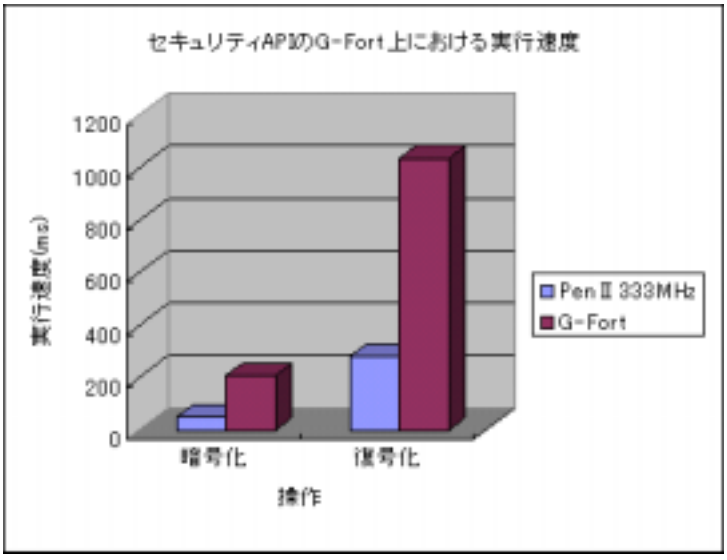

図１．セキュリティ API の G-Fort 上での実行速度

ュリティ API は imc.cipher、imc.security の２つのパッケージから構成される。

・imc.cipher パッケージ

imc.cipher パッケージは主にバイト列を楕円曲線暗号で暗号化したり、復号化したりする機能を提供する。

・imc.security パッケージ

imc.security パッケージはデジタル証明書（SPKI 証明書）とバイト列に対する署名・認証機能を提供する。

5.PocketPC 用セキュリティ API

本研究でサービスを受けるクライアントとして利用する PocketPC(G-Fort)のために、PocketPC 用セキュリティ API を新たに実装した。

5.1 PersonalJava1.0

PocketPC 上の Java 言語の実行環境は PersonalJava1.0 である。PersonalJava1.0 は JDK1.1.X のサブセットという位置付けで、JDK1.1.X の大部分のパッケージが利用可能である。しかしながら java.security パッケージのいくつかは実装されてないために利用できない。

5.2 セキュリティ API の改良

そこでセキュリティ API を一部改良し、PersonalJava 上でも動作可能な API を作成した。セキュリティ API の PersonalJava 上での実行時に問題となるのは主に、ECPublicKey クラスの IAIK-JCE の PublicKeyInfo クラスの extends と ECPrivateKey クラスの PrivateKey クラスの implement である。そこでこれらのクラスの extends と implement をやめ、鍵の利用時にクラスを変換するように API の変更を行った。

5.3 実験－PocketPC 上での実行速度の評価

目的：PocketPC 用セキュリティ API の実行速度を G-Fort 上で測定・評価する。

方法：G-Fort 上で ECC160 ビットのキー長で 10 文字のデータを 20 回暗号化，復号化

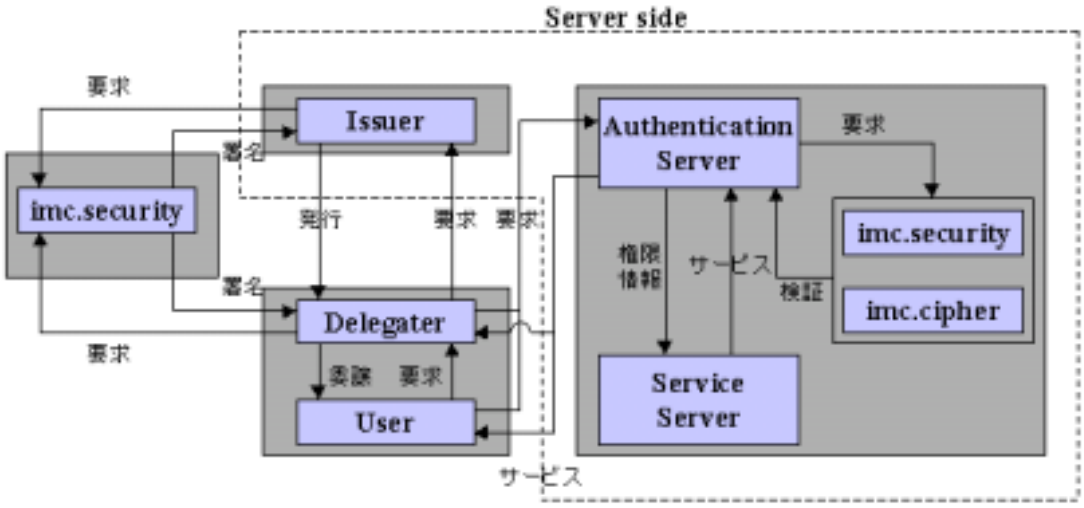

図２．SPKI クラス構成図

してその平均時間を計測する。
利用したツール：VR4122 150MHz, メモリ 32MB の G-Fort, PocketPC 用セキュリティ API
この測定結果を図１に示した。

6.SPKI の実装

6.1 SPKI とは

SPKI(Simple Public Key Infrastructure)はネットワーク上で公開鍵暗号を用いた安全なインフラストラクチャーと主体の権限管理機能を提供するための枠組みであり、現在、IETF によってドラフトが定められている。機器の利用者に利用権限を与えるためには権限証明書とよばれる証明書を発行する必要がある。一般的な PKI の X.509 証明書がその表現形式で ASN.1 フォーマットを用いているのに対して、SPKI の証明書では S-expression という人間が判読可能な ASCII テキストベースの表現形式を用いる。

6.2 SPKI 権限証明書の形式

権限証明書の形式は以下の通りである。

[*Ip*,*Sp*,*D*,*A*,*V*,*DS*]

Ip:Issuer.権限証明書の発行者の公開鍵
Sp:Subject.サービスを要求するユーザーの公開鍵
D:Delgation.*Sp* が権限を委譲することが可能かどうかを示す bool 値
A:Authority.機器の利用権限情報
V:Validity.証明書の有効期限
DS:Digital Signature.署名データ

6.3 SPKI 権限証明書の発行

権限証明書を発行するためには発行者に依頼する必要がある。ユーザー*A*が発行者に権限証明書 *Cert_A* を依頼し、権限を行使する場合の手順は以下の通りである。
(1)ユーザー*A* は発行者に自分の本人情報と公開鍵を提出する。
(2)発行者は *A* の公開鍵と *A* に許される利用権限に、発行者の公開鍵、証明書の有効期限、権限の委譲が可能かどうかを示す bool 値を付加し、最後に署名して権限証明書 *Cert_A*

を作成する。
(3) *A* はサービス要求時に *Cert_A* を提出し、*Cert_A* の検証を経た後に、*Cert_A* の権限情報の範囲内でサービスを受ける。

6.4 権限の委譲

ユーザー*A*が委譲者としてユーザー*B* に権限証明書 *Cert_ B* を発行し、*B* がその権限を行使する場合の手順は以下の通りである。
(1) ユーザー*B* はユーザー*A* に自分の本人情報と公開鍵を提出する。
(2) *A* は *B* の公開鍵と本人情報から *A* の秘密鍵で署名された権限証明書 *Cert_B* を作成する。
(3) *A* は *B* に *Cert_A*、*Cert_B* を渡す。
(4) *B* はサービス要求時に *Cert_A*、*Cert_B* を提出し、*Cert_A*、*Cert_B* の検証を経た後に、*Cert_B* の権限情報の範囲内でサービスを受ける。

6.5 SPKI の実装

ネットワーク機器の認証システム用の SPKI の実装は Java 言語で行った。SPKI API 内のパッケージとパッケージ毎の機能を以下に示す。
(1)SPKI Cert:SPKI による証明書生成、権限管理などを行うクラス郡である。署名、検証はセキュリティ API で行う。
・ Issue:権限証明書の発行クラス郡
・Verify:権限証明書の検証クラス郡
・Delegate:権限委譲用の権限証明書発行クラス郡
(2)Service Server:Authentication Server からの要求に応じてサービスを提供するクラスのフレームワーク。
(3)S-expression:証明書と S-expression フォーマット間の変換をクラスである。
これらのクラスのシステム構成を図 2 に示した。

7.認証システムの構築

現在、企業のオフィス環境には様々な人間や様々な種類の機器が存在する。将来的にそういった機器がネットワークで接続されたとき、不正利用を防止し、利用者に適切な機器の利用権限を与えるための認証システムが必要になる。

7.1 設計方針

システムの設計方針は以下の通りである。
・セッション層上での実装による透過的な相互認証
・クロスプラットフォームでも実行可能
・クライアントは PDA 上で実行

7.2 認証システムの構成

本システムは次の５つのコンポーネントから構成され、全てのコンポーネントが Java で実装されている。全体の構成を図 3 に示した。
・Issuer
・Authentication Server
・Delegater
・User
・機器

7.3 システムの性能評価

G-Fort から認証システムを経由して 10 回 PC の On/Off を実行した場合のセッション

表１．各セッションの平均実行時間

	G-Fort(s)	Authentication Server(s)	合計 (s)
SSL	1.96	2.53	4.49
サービス	0.20	0.10	0.30
合計	2.16	2.63	4.79

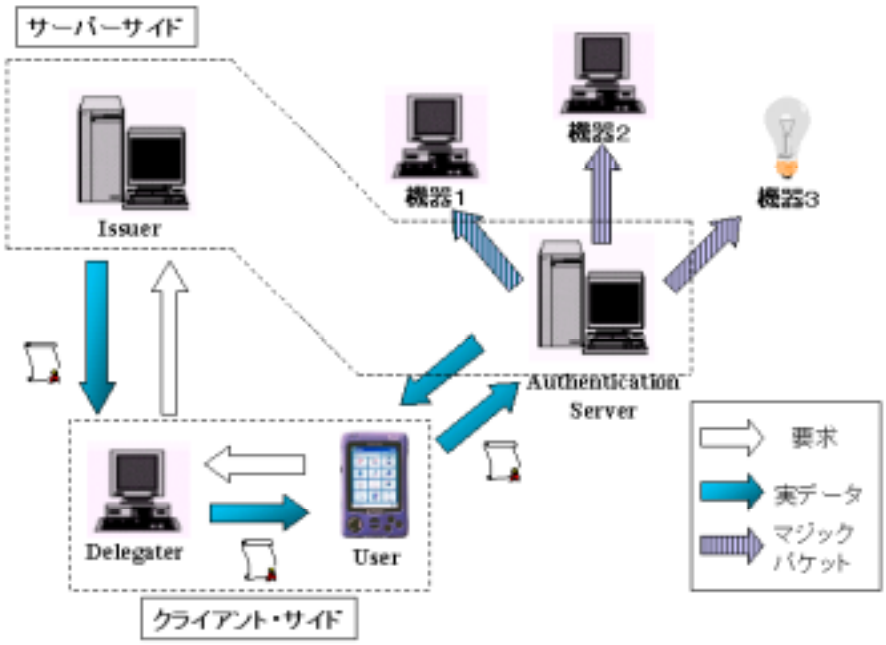

図３．認証システムの構成

の平均時間を表 1 に示した。表 1 より、通信時間を加えた場合の実際の実行時間は 5〜6 秒程度になることがわかる。

8.まとめ

本研究では権限の委譲可能な、楕円曲線暗号で署名された SPKI 証明書によるネットワーク機器用認証システムを設計し、Java 言語でそれを実装した。また、PocketPC を搭載した G-Fort から相互認証を行い、PDA でネットワーク用機器を安全に利用できることを示した。

9.参考文献

[1]Simple Public Key Infrastructure (spki) Charter,http://www.ietf.org/html.charters/spki-charter.html

[2]CIS:SDSI(A Simple Distributed Security Infrastructure), http://theory.lcs.mit.edu/~cis/sdsi.html

[3]N.Koblitz.Elliptic curve cryptosystems, Mathematics of Computation,vol.48, pp.203-209,(1987)

[4]梅澤健太郎,齋藤孝道,奥乃博. SPKI(Simple Public Key Infrastructure)によるプライバシー重視の権限管理の提案と Java を用いた実装,情報処理学会第 60 回全国大会,2000 年 3 月

[5]冨岡和陽,文武,溝口文雄.X.509 証明書を用いた安全な情報機器制御,情報処理学会第 59 回全国大会,1999 年 9 月

[6]北川福太郎,文武,溝口文雄.楕円曲線暗号を利用した情報家電用認証システムの構築,SCIS200,2000 年 1 月

[7]北川福太郎,文武,溝口文雄, 楕円曲線暗号を利用した情報家電用認証システムの構築,CSS2000,2000 年 10 月