1ZA-08

暗号化・署名機能の追加による RMX のセキュリティ向上

小坂祐介† 遠山元道††
慶應義塾大学理工学部情報工学科† ††

1 はじめに

RMX[1]とはデータベースを利用したメール転送エージェントである。メールはセキュリティ上の問題として、なりすましや改竄、そして盗聴といった問題を抱えていて、一般的なメールにおいては暗号化や署名など、それらの問題への解決策があるが、RMX やその他のメーリングリストはそういった問題への解決策がない。そこで、著者らは RMX にその他のメーリングリストにも応用できる形の暗号化・署名機能の追加を提案する。ただし、今回提案している RMX における暗号化・署名機能は、RMX への拡張プラグインとしての提案であり、本来 RMX の概念として存在しないユーザー登録(ユーザーの鍵情報の登録)が必要になる事を前提とする。

2 RMX

Rule-based e-Mail eXchangee(RMX)は遠山研究室で提案している電子メールの配信形式である。RMX ではメールアドレスを下記のように記述することによって、複数の送信先を指定する。RMX ではアドレスの記述方式は標準形式と自然形式の 2 種類があり、これはそのうち標準形式の記述形式である。

< RMX のメールの配信先指定(標準形式)>:=
<配送ルール名>{<パラメータ>}@<サブドメイン>.<ドメイン>

RMX はこのように、配送範囲を記述するサブドメイン以前の部分と、ドメイン以降が”.”によって組み合わされている。配送範囲記述部は一つ以上のパラメータの組み合わせで構成され、標準形式の場合は”{}”の左側にルール名、内側にパラメータが記述される。サブドメインは設定ファイルの名前に相当する。RMX はこのような配送ルールとそのパラメータに基づきデータベース問い合わせを行い、実際の配送先アドレスを取得する。最終的に、そうして得られたメールアドレスに対して配送が行われる。(図 1)

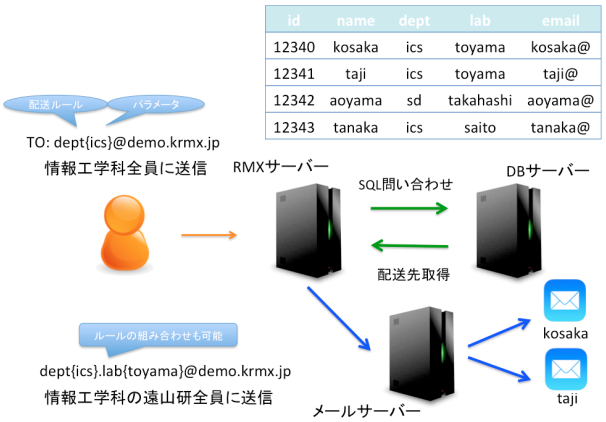

図 1 RMX におけるメール配信の流れ

3 公開鍵暗号と暗号化・署名

公開鍵暗号[3]とは、対になる 2 つの鍵を使って、データの暗号化・復号化を行う方式で、電子メールの世界においてはこれらの技術を用いて、暗号化や署名といった機能が広く利用されている。対になる鍵のうち、1 つは公開鍵、他方は秘密鍵と呼ばれる。メールにおける暗号化は、送信相手以外にメールの中身がわからないようにする仕組みである。一方、メールにおける署名は、きちんとした送信者からメッセージが着たか否かがわかり、そのメッセージが改竄されていない事が確認できる仕組みである。また暗号化機能を利用するには、送信者は送信相手の公開鍵を予め持っている必要があり、署名機能を利用するには、送信者は送信相手に予め自分の公開鍵を渡している必要がある。本実装では、暗号ソフトウェアとして、PGP を用いている。

4 RMX における暗号化と署名

RMX やその他のメーリングリストのように送信者が 1 通のメールを送り、それらが複数人に転送されるような場合、送るメールが 1 通なのに対し、送信相手は複数存在してしまう。すると、従来のようには暗号化や署名が行えない。そこで、著者らは図 2 のような機構を提案する。こ

Improved security of RMX by additional encryption and signature function
† Yusuke Kosaka
†† Motomichi Toyama

の機構は送信者と RMX サーバー、RMX サーバーと受信者の間で暗号化・復号化、署名・検証というプロセスを 2 回行うというもので、送信者と受信者が 1 対 1 の時に使う自分の鍵ペア(以後 A とする)の他に RMX サーバーが各ユーザーとの間で作る鍵ペア(以後 B とする)を 1 つ作ることで、実現可能である。この章では、この機構の利用の仕方と機構の詳細について、説明する。

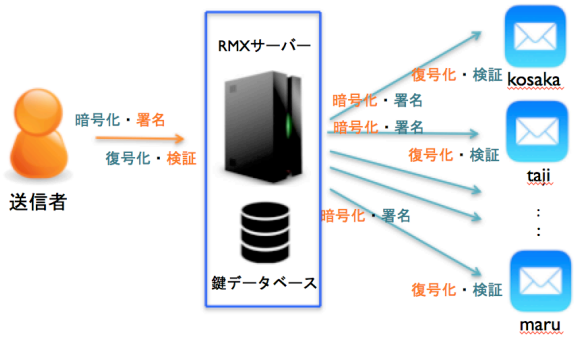

図 2 提案する機構(橙が A, 緑が B)

4-1 鍵の登録

この機構では RMX サーバーを介して、暗号化・復号化、署名・検証というプロセスを 2 回行うので、送信者と受信者が 1 対 1 の場合とは違い、相手の公開鍵の代わりに前で説明した RMX の鍵ペアの公開鍵を受け取っておく必要があり、またそれに対応する秘密鍵を RMX サーバーに登録している。また相手に自分の公開鍵を渡す代わりに RMX サーバーに自分の公開鍵を渡しておく必要がある。本実装では RMX のプラグイン機能[2]を用いて、これらの鍵の登録を行うようにした。具体的には以下のようなコマンドを使う。

(1)鍵ペア A の公開鍵の登録
#PGPMAIL.keygen.[USER_NAME]#@<subdomain>.<domain>
※[USER_NAME]は鍵の ID に使う
(2)鍵ペア B の生成・登録と公開鍵の返信
#PGPMAIL.regpub#@<subdomain>.<domain>

4-2 提案機構

この機構では暗号化と復号化が 2 回行われる。1 度目の暗号化では、鍵ペア B を用いて、送信者は暗号化して RMX サーバーにメールを送り、それを受け取った RMX 側では鍵ペア B を用いて復号化する。2 度目の暗号化では、それを各ユーザーの鍵ペア A で暗号化し、各ユーザーへメールを転送する。一方、この機構では署名・検証も 2 回行われる。1 度目の署名では、鍵ペア A を用いて、送信者は署名を行い、RMX サーバーへメールを送り、それを受け取った RMX 側では鍵ペア A を用いて検証が行われる。2 度目の署名では、鍵ペア B を用いて、署名をして、各ユーザーへメールを転送する。このような暗号化・署名を利用する際も鍵の登録と同様に拡張プラグイン機能を用いて、メールを送る必要がある。

#PGPMAIL.send#[target]

[target]には RMX 形式のアドレスを記述する。

4-3 Thunderbird 等における利用法

多くのメーラーがあるが、ここでは Thunderbird を例に挙げる。Thunderbird で PGP を用いた暗号化・署名を簡単に行う為には、Enigmail という拡張プラグインを用いる。本機構を用いずに暗号化・署名を利用する時と比べて、暗号化の際に選択する鍵が個々の送信相手の鍵でなく、鍵ペア B の公開鍵であるだけでそれ以外は何も特別な事はせずに利用できる。

5 評価

N 人に対して、本機構を用いて、暗号化・署名を行い、送信する場合と、本機構を用いずに N 人に対して 1 通 1 通送る場合の送信に掛かる時間や、本機構の利用に必要な鍵登録と本機構を利用しない場合に送信相手に鍵を渡しておく手間、そして管理する鍵の数の比較を行う予定である。

6 おわりに

本研究では、メールのセキュリティに対する解決案として、RMX における暗号化・署名の機構の提案および実装を行った。今後はこの実装に対する評価を行い、その結果を用いて、更なる改善を行っていきたいと考えている。

参考文献

[1] Kim Hanki, Sang-Gyu Shin, Motomichi Toyama. “A Rule-Based Mailing System for an Organization”, International Workshop on Information Processing over Evolving Networks, June 2006
[2] 松本 洋平, 北 和人, 遠山 元道. “RMX における拡張プラグイン機構の導入及び各種プラグインの開発”, DEIM2014
[3] Williams, Henry. "A modification of the RSA public-key encryption procedure (Corresp.)." Information Theory, IEEE Transactions on 26.6 (1980): 726-729.