1S-03　不正アクセス発信源追跡システムの通信データ防御に関する鍵管理方式の検討*

永吉　孝行
東日本電信電話株式会社　研究開発センタ
渡部　陽子、田中　美穂
東日本電信電話株式会社　法人営業本部マルチメディア推進部

1. はじめに

本稿では、不正アクセス発信源追跡システム(以下、追跡システム)の研究開発の一環として、前年度行った追跡システムの通信データ防御方式検討を踏まえ[1]、通信データの原本性保証及びデータの隠蔽を効率的に実現する鍵管理方式について検討する。

前年度は、通信データ防御の観点からAMN間で行われる追跡マネージャ～追跡マネージャ間の通信とAMN内で行われる追跡マネージャ～不正アクセスセンサ(以下、センサ)・トレーサ間の通信それぞれに対して、公開鍵暗号と共通鍵暗号の両暗号化技術が通信データの原本性保証及びデータの隠蔽技術として適用可能かどうか検討を行った。その結果、両暗号化技術ともそれぞれ課題を抱えつつも適用可能との判断を行った。

本稿では、暗号を利用する際の鍵の生成・配送・更新と言った鍵管理方式の検討を行うが共通鍵暗号を利用する場合は、Diffie-Hellman 鍵配送方式を用いることで鍵の生成・配送・更新の問題がクリアされる為、ここでは詳細について述べない。以下では、公開鍵暗号を利用する場合についての検討を行う。

2. 基本方式

追跡システムの通信へ暗号化を適用する際、考慮すべき追跡システムの特徴は以下の4つが挙げられる。

①追跡データは数十～数百 byte と小さい。
②AMN はインターネット上に散在している。
③センサ、トレーサは自 AMN の追跡マネージャのみと通信する。
④追跡マネージャ～センサ間では、センサからのみコネクションを確立できる。

一般的に公開鍵は共通鍵と比較して暗号化処理時間が長い為、通信データを公開鍵で暗号化するのは好ましくないが、追跡システムの特徴①より公開鍵で直接暗号化する方式を採用する。また通信データは、電子署名を用いて送信元認証と改ざん防止を行う。

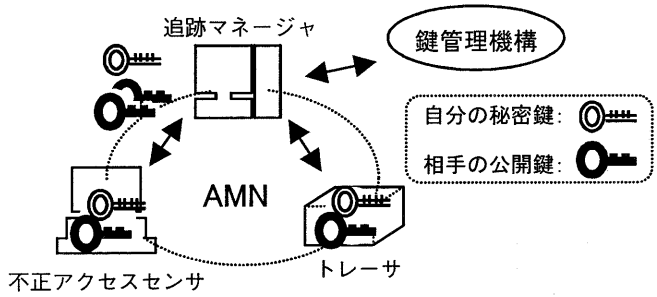

図1: 構成要素の保持する情報

特徴②より、追跡マネージャ間では、新たに鍵管理機構を追加する。鍵管理機構では追跡マネージャ公開鍵の管理を行い、AMN 間の通信発生時に追跡マネージャの要求に応じて公開鍵の配布を行う。AMN 内では特徴③より、あらかじめ通信者間で相手の公開鍵を共有しておくことで暗号通信を行う(図1参照)。

新たな構成要素を追跡システムへ登録する際には、追跡システムにより正当性を保証された公開鍵のペアを配布する。また追跡システム構成要素が使用している鍵は解読される危険性を伴っている為、ある周期をもって更新する。

3. 鍵管理方式

3－1. 課題

(1)鍵生成:生成場所によっては配送に伴う危険性が生じるため、秘密鍵の配送を必要としない場所で生成することが好ましい。また生成時の負荷やリスクも勘案しなければならない。

(2)鍵配送: 暗号化・認証用として取得した公開鍵の正当性を継承できる鍵配送の仕組みを用いて追跡システム構成要素間の信頼関係を維持する必要がある。

(3)鍵の世代管理: 鍵の更新処理や、管理する鍵の世

* A discussion of a key management about protections of communication data for unauthorized access tracing system: Takayuki Nagayoshi,Yoko Watanabe and Miho Tanaka, NTT East Corp.

代が多くなることにより、追跡システムに本来の目的外で大きな負荷がかからないようにしなければならない。

3－2. 検討内容

(1) 鍵生成

後述(2)に示す配送方法により追跡システムの信頼関係を維持できる為、新しい鍵の生成はそれを使用する構成要素上で行う。これにより漏えいによる追跡システム構成要素へのなりすましの危険性を回避することができる。

(2) 鍵配送

新たな公開鍵の送信には、それまで使用していた鍵のペアを利用し電子署名を付けて配送を行う。これにより認証され、新しい鍵として使用することができる。

(3) 鍵の世代管理

AMN 内において、追跡システムの特徴④より、鍵更新のトリガーをセンサ・トレーサの鍵生成時とする。同時に追跡マネージャの公開鍵も更新することで追跡マネージャの公開鍵更新処理を分散できる。

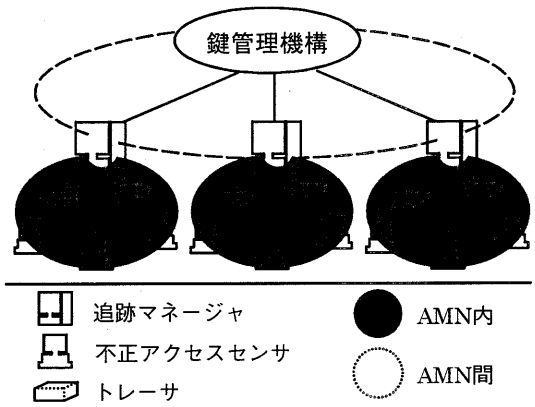

図2: 追跡システム構成

AMN 間の構成要素も鍵管理機構を頂点としたツリー構造と見ることができるので(図2参照)鍵更新のトリガーは追跡マネージャとし、同時に鍵管理機構の公開鍵も更新する。

鍵の世代管理を極力少なくする為、鍵生成周期を

鍵管理機構 ≧ 追跡マネージャ ≧ センサ・トレーサ

と設定する。これにより鍵管理機構～追跡マネージャ間で鍵管理機構の公開鍵の有効期限中に追跡マネージャの公開鍵の生成周期が一度は訪れ、鍵管理機構の最新の公開鍵を取得することができる。従って鍵管理機構は2世代の鍵を管理すればよい。追跡マネージャ～センサ・トレーサ間でも同様の仕組みを利用することでシステム全体では、鍵管理機構・追跡マネージャは2世代、センサ・トレーサは1世代の鍵を管理する(図3参照)。

これにより不正アクセス追跡の際には、鍵の世代を気にすることなく、各デバイスが現在保持している鍵を使用して通信を行うことが可能である。

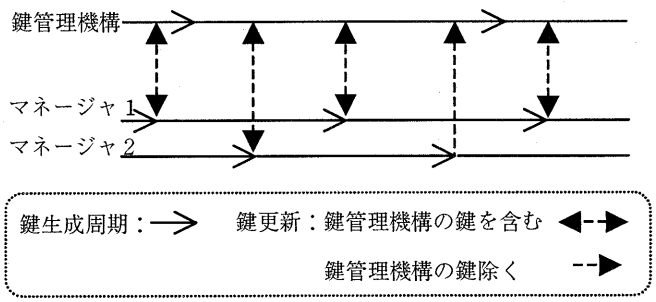

図3: 鍵管理機構～追跡マネージャ間の鍵更新

3－3. 考察

鍵生成を各構成要素上で行うことにより、鍵生成の負荷分散はなされているが、鍵生成が頻繁に起こりデバイス本来の機能に悪影響を及ぼすことのないよう対処しなければならない。

また AMN 内においてセンサ・トレーサからの鍵更新要求が追跡マネージャに一度に集中することのないよう、センサ・トレーサの鍵生成周期を設定する必要がある。

AMN 間でも同様の点に注意し、追跡マネージャの鍵生成周期を設定する必要がある。

4. 今後の課題

今後は、更に実環境へ追跡システムを展開することを考慮し、不正アクセス追跡時にインターネット上のトラヒック状態が追跡システムの性能に与える影響や、暗号通信の認証失敗時の処理、暗号化・認証用の鍵が漏えい・解読された場合の対策等も勘案した上で、公開鍵暗号と共通鍵暗号の適用性評価を行っていく予定である。

謝辞

本研究は、通信・放送機構(TAO)の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われているものである。

参考文献

[1]建部他:"不正アクセス発信源追跡システムの不正利用防止アーキテクチャの検討",情処 60 全大, 6Q-08,March 2000.