多段構成ネットワークにおける鍵配送方式の一検討

保母　雅敏（名城大学理工学部）†
渡邊　晃（名城大学理工学部）‡

1. はじめに

イントラネット内で安全な通信を行うための技術として、閉域通信グループを構築する研究が行われている。この研究の一方式として、一定の条件で作られた通信グループと共通鍵を一対一に対応させる方式が提案されている。この方式では、暗号装置(EE)が通信経路上に 3 台以上存在するような多段構成ネットワークにおいても柔軟なシステムを構築することが可能である。しかし、共通鍵は管理装置(MS)から各 EE に配送するため、MS から対象の EE に配送する際に、第三の暗号装置(中間 EE)を通過しなければならない場合があり、この部分において確実な認証が行えないという課題があった。

本研究では、中間 EE で確実に認証を行いながら鍵配送が実現できる方式を検討したので報告する。

2. 既存技術とその問題点

対象となるシステム(図 1)では、EES(ソフトウェア型 EE)、EEN(ネットワーク型 EE)、EEA(アダプタ型 EE)が存在する。EES は主にクライアント端末に内蔵、EEN は配下のネットワークを保護、EEA は直下の端末を保護する目的で設置される。これらの EE は企業内の部署同士などといった一定の条件に基づきグループ化され、同じグループに属している端末とは、グループに割り当てられた共通のグループ鍵を用いて暗号通信を行うことが出来る。また、このグループ鍵を用いて暗号通信に先立って DPRP(Dynamic Process Resolution Protocol)と呼ばれる事前認証を行う。これにより通信対象との間で使われるグループ鍵を決定し、中間 EE での転送の可否も同時に決定する。このときに生成される動作テーブルを参照しなければ、パケットは中間 EE を通過することは出来ない。

MS からのグループ鍵の配送では、EE を確実に認証し、対応するグループ鍵を配送する。また、セキュリティを確保するため、MS は定期的にグループ鍵の更新を行い、各 EE に配送する。グループ鍵の更新周期は 24 時間程度を想定しているため、通常は常に電源が投入されていると想定される EEN/EEA のみに定期配送をし、EES は電源投入時にグループ鍵を配送する。

既存の鍵配送方式[1]では、秘密情報として MS と各 EE との間で RSA といった非対称暗号鍵を用い、この非対称暗号鍵と鍵配送毎に作成される乱数を用いて鍵配送を行う。しかし既存方式では中間 EE の認証を考慮していないため、鍵配送パケットは無条件で通過させているという課題があった。

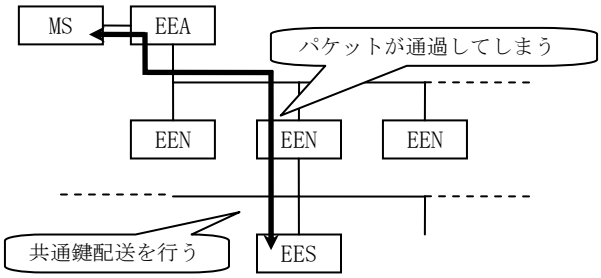

図 1　多段構成ネットワークと従来方式の問題点
Fig.1　Vertical Networks and Problem of Conventional Key Distribution Method

3. 提案方式

この問題を解決するため、鍵配送パケットを受信した中間 EE は確実な認証を行い、その結果によりパケットの通過を決定できる方式を提案する。そのため、MS と EE 間に表 1 に示すような情報を初期情報として保存させる。

従来各 EE には、ユーザ ID(IDx)、秘密鍵(Prx) 、MS の公開鍵(PuS)を初期情報として与えていたが、これに加え、EE の公開鍵を MS の秘密鍵(PrS)で暗号化した Eprs[Pux]を新たな初期情報として追加する。

また、MS には従来通り各 EE のユーザ ID(IDx)、公開鍵(Pux)、MS 自身の秘密鍵(PrS)を所持する。

EES/EEN/EEA	EE のユーザ ID(IDx) EE の秘密鍵(Prx) MS の公開鍵(PuS) ※暗号化データ(Eprs[Pux])
MS	MS の秘密鍵(PrS) 各 EE のユーザ ID(IDx) 各 EE の公開鍵(Pux)　(x=1,2,3…)

※追加した初期情報

表 1　各端末が所持している情報
Table.1　Information which each entity has

中間 EE は、終端 EE から MS、MS から終端 EE への両方向のパケットを認証する必要がある。

終端 EE からのパケットの転送判定を行うために、EE の公開鍵を MS の秘密鍵で暗号化したデータ(Eprs[Pux])をパケットに付加して送信する。このデータは MS の公開鍵で復号できるため、どの EE でも Pux を取得することが可能である。この Pux を用いることで、中間 EE においてもディジタル署名の検証を行う事が可能となる。データの正当性が認められた場合は、MS が作成したユーザが生成したパケットであると判断し、パケットを転送する。

MS からのパケットの転送判定は、初期情報として与えられた PuS を用いて MS からのパケットのディジタル署名を検証することによって行う。これにより、データの正当性が認められた場合は、MS が生成したパケットであると判断し、パケットを転送する。

Proposal of a Key Distribution Method for Vertical Networks
†Masatoshi Hobo, ‡Akira Watanabe
Faculty of Science and Technology, Meijo University, Japan

提案方式における鍵配送のシーケンスを図 2 に示す。

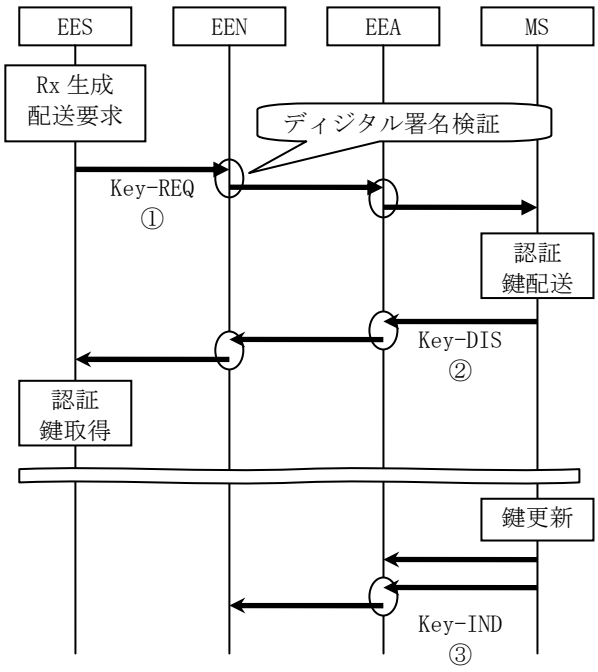

図 2　提案する鍵配送方式
Fig.2　Proposal of Key Distribution Method

①終端 EE→MS ：鍵配送要求(Key-REQ)
終端 EE が MS に鍵配送の要求を行うためのパケットである。鍵配送要求に先立ち、鍵配送に用いる乱数 Rx を生成する。この Rx に加え、③で述べる鍵更新通知によって鍵配送が行われる場合は、取得の対象となるグループを記述したＤを MS の公開鍵 Pux で暗号化した Epus[Rx|D]と、ユーザ ID である IDx を追加する。そして、ディジタル署名 Eprx[H(Epus[Rx|D]|IDx)]を付加し、Eprs[Pux]を付加したものを鍵配送要求のパケットとして送信する。

Epus[Rx/D]/IDx/Eprx[H(Epus[Rx/D]/IDx)]/Eprs[Pux]

このパケットを受信した中間 EE は、Eprs[Pux]を復号し、送信元端末の公開鍵 Pux を得る。この Pux を用いてディジタル署名 Eprx[H(Epus[Rx]|IDx)]を検証する。これによりデータの正当性が認められた場合、パケットは MS が認証した秘密鍵をもつ端末が作成したものであるとし、中間 EE はパケットを転送する。
MS がこのパケットを受信した時、中間 EE と同様にディジタル署名の検証を行う。その後 Epus[Rx|D]を復号し、IDx を元にユーザが所属しているグループを決定し、対応するグループ鍵を選択する。

②MS→終端 EE ：鍵配送(Key-DIS)
MS での認証によって決定されたグループ鍵を配送するためのパケットである。終端 EE が所属するグループと、それに対応するグループ鍵を情報Ｄとし、①で取得した Rx とともに Rx で暗号化したデータ Erx[Rx|D]と、ディジタル署名 Eprs[H(Erx[Rx|D])]を終端 EE に送信する。

Erx[Rx/D]/Eprs[H(Erx[Rx/D])]

このパケットを受信した中間 EE は、予め所持している MS の公開鍵 PuS を用いてディジタル署名を検証する。データの正当性が認められた場合、中間 EE はパケットを転送する。
終端 EE がこのパケットを受信した時、Erx[Rx|D]を復号し、自身が作成した Rx と比較して一致していた場合は、Ｄを取得する。

③MS→終端 EE ：鍵更新指示(Key-IND)
グループ鍵が更新されたことを EE に通知し、グループ鍵の更新を指示するためのパケットである。鍵更新指示ではグループ鍵が更新されたグループに属する EE に対して送信される。このパケットは②と同様のパケットを作成し送信するが、このときのＤの内容は更新されたグループの情報のみとなる。中間 EE での認証も②と同様にして行う。
終端 EE がこのパケットを受信した時、Erx[Rx|D]を復号し、自身が作成した Rx と比較して一致していた場合は、Ｄを取得する。その後更新されたグループ鍵を取得するため、Ｄを用いて①の鍵配送要求パケットを生成する。

これにより、終端 EE と MS との間に中間 EE が存在していても、無条件にパケットを通過させることなく認証によってパケットを通過と判断することが可能となる。

4.　おわりに

鍵配送を行う上で、通信経路上に中間 EE が存在する場合においても、パケットを確実に認証して通過させる方式を提案した。今後は提案方式を実装し、機能評価を行っていく予定である。また、既存方式に比べ一つのパケットあたりの処理が増加しているため、処理要求が増加した際の端末に掛かる負荷についても検討していく。

参考文献

[1]　渡邊、岡崎、朴、井手口、笹瀬“イントラネット閉域通信グループの構築に適した安全な鍵配送方式とその運用管理方式”電気学会論文誌 C　Vol.121-C, No.9 Sep.2001
[2]　渡邊、井手口、笹瀬“イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案”電子情報処理学会論文誌 Vol.J84-D-I No.3 Mar.2001
[3]　渡邊、厚井、井手口、横山、妹尾“暗号技術を用いたセキュア通信グループの構築方式とその実現”情報処理学会論文誌 Vol.38 No.4 Apr.1997
[4]　http://www-is.meijo-u.ac.jp/~watanabe/ “研究内容”内