GSCIP を構成する DPRP の仕組みの検討

鈴木　秀和　　渡邊　晃

名城大学理工学部

1　はじめに

近年増加傾向にあるイントラネット内部の犯罪に対するセキュリティ対策が重要視されている．既存技術の1つとしてIPsecが考えられるが，頻繁にシステム構成が変わるような環境では設定情報の変更が必要であるため，イントラネット内ではほとんど利用されていない．

そこでイントラネット内のセキュリティと運用管理負荷軽減を両立したシステムを実現するFPN（Flexible Private Network）環境[1]の構築を目指している．この環境では各端末にグループ鍵GKを持たせた暗号装置EE（Encryption Element）を用意し，同一の鍵を保持するEEの集合を閉域通信グループCCGI（Closed Communication Group for Intranet）として構成する．CCGI内の端末間の通信はこのGKで暗号化され，異なるCCGI内の端末がアクセスすることや，通信を盗聴することが不可能となっている．ここで端末は通信相手が同一のCCGIに帰属しているかを確認する必要があり，そのネゴシエーションを行うのがDPRP（Dynamic Process Resolution Protocol）である．DPRPは通信に先立ち行われ，認証と動作処理情報テーブルPIT（Process Information Table）を動的に生成する．このDPRPによってネットワーク構成の変更や端末の移動があっても，初期通信をトリガーとしてDPRPが実行され，システムに位置透過性があり柔軟な通信グループを構築できる．本システムを実現するために現在，GSCIP（Grouped Secure Communication for IP；ジースキップ）というネットワークセキュリティアーキテクチャを検討している．

本研究ではその一機能として，通信経路の認証および設定情報の動的作成を実現するDPRPについて報告する．

2　既存DPRPの仕組みと課題

CCGIを構成するEEには，クライアント端末にソフトウェアをインストールして実現するソフトウェア型暗号装置EES，セキュリティゲートウェイのようにセキュリティドメインを形成し配下の端末を保護するネットワーク型暗号装置EENがある．またEEには同一のCCGIに帰属する端末との通信だけが可能な閉域モードと，全ての端末と通信が可能な開放モードの2種類の動作モードが設定される．企業ネットワークでは部署や役職ごとにアクセスポリシーが異なるため，図1のようなCCGI構成が考えられる．ここでEES2はCCGI1に帰属し，閉域モードのEENによって守られているエリアに存在しているサーバとする．

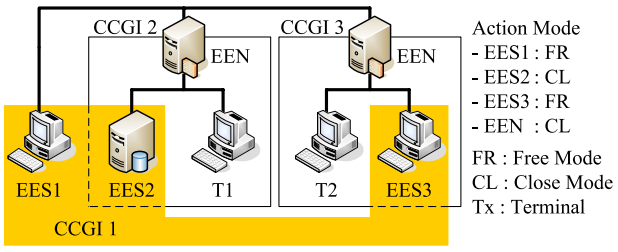

図 1　ネットワーク構成とCCGI構成
Fig. 1　Network model and CCGI model

EES1-EES2間の通信を考えた場合，通信経路上に3台以上のEEが存在する多段構成になっている．閉域モードであるEENは両終端EEが共通に持つGK1を保持していないため，本来ならば通信が許可されないはずである．しかし[2]において提案されている既存のDPRPでは図2のように両終端EE間での鍵の一致のみを確認するため，中間EEであるEENは動作モードに関係なく無条件に中継させていた．これでは閉域モードの概念が反映されておらず，PITを作成する制御パケットを無条件で透過させることにより，EEに不正なテーブルを作成される懸念がある．また無条件で透過させるとDOS攻撃の対象となり，不要なDPRPの発生も考えられる．

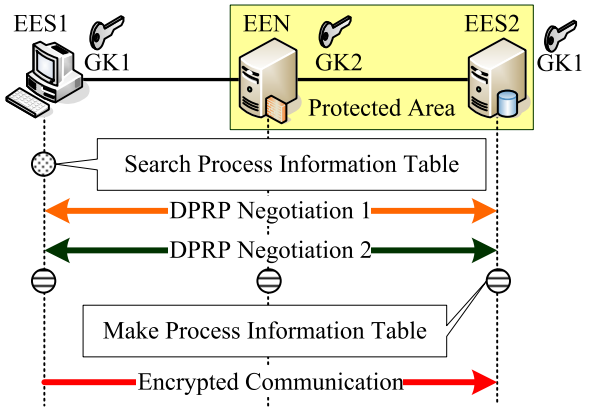

図 2　既存DPRPシーケンス
Fig. 2　Existing DPRP sequences

3　改良したDPRPの機能概要

このような問題を解決するために，先にアクセスを開始する始点EEに通信経路上に存在する全てのEEと同じ鍵を持たせることにした．これにより両終端EE間で行っていた認証処理を通信経路上に存在する全てのEEで行うことに変更して，確実にPITが生成されるようにした．それに伴いDPRPシーケンスを見直して通信経路の認証とPITの自動作成を行うために，ACG（Authenticate Communication Groups），DPI（Define Process Information），MCI（Make CCGI Information）の3種類の制御パケットを定義した．

これらの制御パケットにより図4のようなネゴシエーションを行う．鍵の持たせ方を変更したため，予めEES1には鍵管理装置から新たにGK2を配送しておかなければならない．図4を基にして3種類の制御パケットの機能概要を以下に説明する．

ACGは認証処理とEEの情報を通知する役割を担い，ICMP ECHOパケットを利用する．通信経路を認証するために必要な情報は，グループ番号，鍵バージョン，GMAC（Group Message Authentication Code）等をパッケージ化したものであり，これをACGにのせて送信する．GMACとは各EEで発生させる128bit乱数RNとそのHMAC-MD5値128bitをグループ鍵GKで暗号化した計256bitのものを示す（図3）．HMAC-MD5は反復暗号ハッシュ関数MD5を秘密共有鍵と組み合わせて使用したもので，第三者によるメッセージの改竄の検出と送信元の認証を行うための技術であり，IPsecでも利用される．ここで使用される秘密共有鍵はEEが保持しているGKである．

“Researches on DPRP mechanism which make GSCIP architecture”
Hidekazu SUZUKI and Akira WATANABE
Faculty of Science and Technology, MEIJO University, Japan

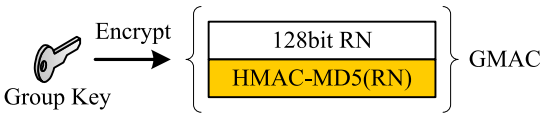

図 3　GMAC生成方法
Fig. 3　Method of making GMAC

ACGを受信したEEは自分が保持するGKでGMACを復号した後，取得した乱数RNのHMAC-MD5値を算出して，GMACに含まれていた値と比較する．一致した場合は認証成功としてACGを中継し，一致しなかった場合は認証失敗としてACGを破棄した後，MCIにより破棄テーブルを生成する．ACGを送信または中継するとEEはMCIパケット待ち状態に移る．この動作を終点EEまで繰り返すことで通信経路をGMACによって片方向認証することが可能となる．

また各EEはACGを中継する際，PITの作成に関わる自らの情報をACGに追加する．情報の内容は自端末の始点/中間/終点EEといった位置情報，閉域/開放の動作モード，GMACを認証することができた鍵情報である．終点EEがこの情報を受け取って動作処理情報を決定する．

DPIは終点EEで決定した動作処理情報を始点EEへ通知するために送信され，ICMP ECHO REPLYパケットを利用する．動作処理情報は両終点EE間で決定したグループ鍵で暗号化される．DPIはエンド-エンドの認証を行えばよく，中間EEではACGによって認証されていればDPIを透過中継する．

MCIはPITの作成を担い，UDPパケットを利用する．ACGと同じ情報を搭載しており，さらに決定した動作処理情報が追加されている．MCIを受信したEEはACGと同じ方法でMCIに含まれるGMACを認証した後，取得した動作処理情報からPITの作成を行う．違う状態や認証されなかった場合は不正なMCIパケットと判断して破棄する．

始点EEであるEES1が通信開始時にPITを検索して情報が見つからなかった場合に，通信パケットを一時待避させてからDPRPネゴシエーションを開始する．始点EEがMCIを送信したらネゴシエーションは完了したと見なして，待避していた通信パケットをPITに従って処理および送信する．

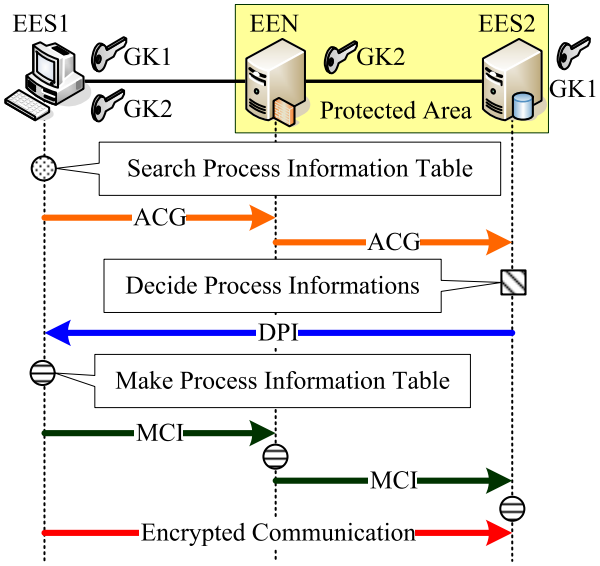

図 4　改良した DPRP シーケンス
Fig. 4　Improved DPRP sequences

4　評価

始点 EE の鍵の持たせ方を変更して通信経路の認証という概念を導入したことにより，DPRP の仕組みを改良した．この結果，確実に PIT を生成することが可能になった．また各 EE で認証することから不正なパケットを早期段階で発見し破棄することが可能になり，既存の DPRP と比べてセキュリティの向上が図られた．

EES1 は通信経路を認証するために必要な鍵を保持したため，図 4 における右方向の通信が許可されるようになった．しかし EES2 は通信経路を認証するために必要な鍵を完全に保持していないため，CCGI2 に帰属しない EES2 から始まる左方向の通信アクセスは拒否される．

5　実装

DPRP はアプリケーションに依存することなく全ての IP 通信を対象としているため IP 層に実装される．開発･実装環境は IP 層の詳細な処理フローに関する情報が多い FreeBSD で行っている．図 5 のように BSD カーネル内における IP 層を改造して組み込む．受信したパケットや送信するパケットをデータリンク層に近い場所で抜き取って処理を行う．現段階ではカーネルに組み込む前に，ソケットを利用したサーバ･クライアントアプリケーションとして DPRP のテスト開発を行っている．

PIT はパケット受信時に毎回検索するため高速性が求められ，また GSCIP に実装される DPRP 以外のモジュールなども参照することになる．そのためカーネルの介在なしにプロセス間でデータの受け渡しが可能で，最も高速な IPC（Interprocess Communication）である共有メモリ上にハッシュテーブルとして構築する．ハッシュのキーとなるのは送信元/宛先 IP アドレスである．また DPRP を開始するときに待避させておくパケットも共有メモリに記憶する．

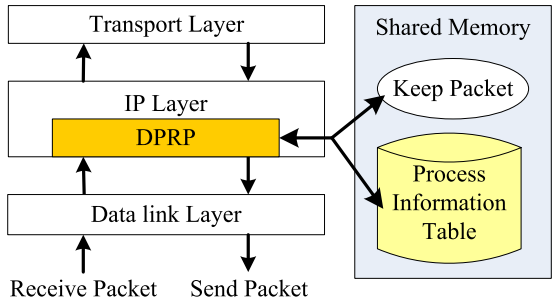

図 5　DPRP の実装と動作概要
Fig. 5　Implementation and summary behavior of DPRP

6　むすび

FPN 環境を構築するためのアーキテクチャ GSCIP を構成する DPRP の仕組みについて検討した．今後は DPRP の開発を進めカーネルに組み込み認証処理と PIT 作成の動作確認をすると共に，類似技術である IPsec の IKE との定量的比較を行う予定である．BSD での開発･動作確認ができた後は Linux への移植も考えている．

参考文献

[1]　http://www-is.meijo-u.ac.jp/~watanabe/ “研究内容”内
[2]　渡邊 晃, 井手口 哲夫, 笹瀬 巌, “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”, 電子情報通信学会論文誌, VOL.J84-D-I No.3, March 2001
[3]　馬場 達也　著, “マスタリング IPsec”, O’REILLY JAPAN, 2002