BGP FlowSpec を用いた DNS リフレクション攻撃対策

1180345　武嶋　千明　【 セキュリティシステム研究室 】

1　はじめに

近年，ネットワーク上に存在する多数のコンピュータを踏み台にし，特定のホストのサービスをダウンさせる DNS リフレクション攻撃が多く発生している．この攻撃は，DNS(Domain Name Server) サーバの特性を悪用したもので，攻撃元の特定が困難という特徴がある．攻撃への対策として，BGP ルータには FlowSpec という機能が搭載されている．この機能は，物理的に接続されていない BGP ルータに対してフィルタリングルールを伝搬させることができるというものである．しかし，FlowSpec はメッセージの改ざんや偽装をチェックする手段を持っていないという問題がある．

本稿では，DNS リフレクション攻撃への攻撃対策として BGP FlowSpec をさらに普及させるため，FlowSpec 機能の課題を解決することを目的とした手法を提案する．

2　研究内容

BGP(Border Gateway Protocol) は，組織間を接続するための経路制御プロトコルである．BGP ルータは ISP(Internet Service Provider) 等に設置され，BGP ルータ同士が経路情報を交換することで隣接していないネットワークにパケットの転送ができる．BGP ルータの FlowSpec 機能は，遠隔ルータへのフィルタリングルールの伝搬が可能であり，攻撃の発生源に近い場所で攻撃パケットへの対処が可能となる [1]．しかし，ルール伝搬の際に経路情報を偽装されても気づくことができないという問題がある．

3　提案手法

本稿では，FlowSpec 機能によるフィルタリングルール伝搬の際に ROA(Route Origin Authorization) による認証を行うことで，伝搬されてきたルールの経路情報が本当に正しいものか否かを判断し，偽装された経路情報の伝搬を防ぐ手法を提案する．図 1 は提案手法の概略図である．

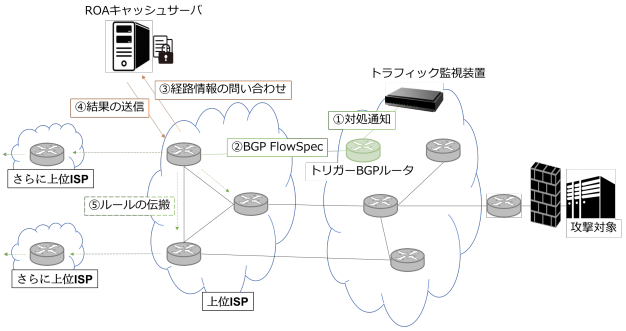

図 1　提案手法の概略図

1. 攻撃の検知
   ネットワークを流れるトラフィックを監視している監視装置が，あらかじめ設定されている閾値を基にトラフィックが正常なものか異常なものかを判断する．攻撃を検知した場合，トリガー BGP ルータに対処要請を通知する．

2. FlowSpec によるフィルタリングルールの伝搬
   対処要請を受けたトリガー BGP ルータは被害を受けているホストの IP アドレスに対するパケットを破棄，ないしは転送等の対処を行うよう上位 ISP の BGP ルータに対して FlowSpec 通知を送信する．

3. 伝搬された経路情報の検証
   FlowSpec 通知を受け取った BGP ルータは，ROA サーバへ接続し通知された IP アドレスと AS 番号の組み合わせが有効な経路であるかを検証する．検証の結果が真であれば，要請通りフィルタリングを有効にし，隣接する BGP ルータに対して同様のフィルタリングルールを伝搬させる．結果が偽の場合，改ざんされた経路情報である可能性があるため，メッセージを破棄する．

4　評価

提案手法を用いた場合と用いない場合を想定し評価を行った．

提案手法では ROA による認証を行っているため，ルール伝搬の途中でメッセージを改ざんされる恐れはないが，経路情報の信憑性を ROA サーバに問い合わせる時間が必要なため，対策をしない場合と比較してフィルタリングが有効になるまでに時間が掛かる可能性がある．しかし，問い合わせにはそれほど時間を要しないと思われるため，遅延は許容範囲内になると思われる．

5　まとめ

本稿では，DNS リフレクション攻撃への対策として BGP ルータの FlowSpec 機能を挙げ，この機能の課題を解決する手法を提案した．

今後の展望としては，システムを実装して実験を行い，提案手法に期待通りの優位性があるかを評価したい．

参考文献

[1] 中島智広,”DDoS 対策の戦略と戦術”, NRI セキュアテクノロジーズ株式会社,2016.