G-14

Linux カーネルモジュールを利用した 透過型汎用防御システムの構築と提案

橋中 義典† 川橋 裕‡
Yoshinori Hashinaka Yutaka Kawahashi

1 はじめに

近年インターネットの広域な普及にともない，ネットワークの多様化が進み，多くの企業や機関が提供するサービスも同様に多様化している．一方で，サーバが提供しているサービスの正常な運用を阻害するDoS(Denial of Service)攻撃やDDoS(Destributed Denial of Service)攻撃が大きな脅威の1つとなっている．

和歌山大学の既存研究に，B-DRIP[1][2][3]というDoS攻撃やDDoS攻撃に対しての透過型防御システムと代理応答サーバがある．攻撃を防御するだけでなく，代理応答サーバを用いた警告コンテンツを攻撃者に表示することができる．しかし，B-DRIPの構築にはカーネルソースコードの変更を要する．また攻撃の検知方法が単位時間あたりのパケット数のみであるため，多様化する攻撃に対応できず，誤検知時の調整が困難である．本研究ではこれらの問題を解決し，多様化する攻撃に柔軟に対応でき，調整が容易で，保守性が高いシステムの構築を目標とする．

2 既存研究

B-DRIPはWebサーバに対し単位時間あたりに閾値を越えた異常な数のアクセスがあった場合，その送信元IPアドレスを攻撃者と判定する．そして攻撃者とみなしたIPアドレスからのアクセスのルーティングをB-DRIPで変更し，代理応答サーバに転送する．代理応答サーバはステートレスな代理応答をおこなうことができ，Webサーバへの攻撃を代理で受け取るだけでなく，攻撃者に対して警告コンテンツを表示する．またB-DRIPはブリッジ構成となっているため，ネットワークの構造やサーバの構成を変更することなく導入ができる．

3 研究目的

既存研究の問題点として，システム構築の際にOSのカーネルソースコードの変更を要することが挙げられる．B-DRIPは代理応答をおこなう際，ipfwを用いて送信先MACアドレスを書き換えることで代理応答サーバへと転送している．だがシステムがブリッジ構成の場合，ipfwは送信先MACアドレスの書き換えをおこなうことができない．そこで既存研究では，FreeBSDのカーネルソースコードを書き換え，ipfwの動作を変更し書き換え動作に対応させている．しかしカーネルは日々アップデートされ続け変更が行われており，ipfwの動作を変更するための書き換えは容易でない．またサポート切れのままの運用はセキュリティ面でも非常に危険であり，保守性に欠ける．またB-DRIPの攻撃判定はWebサーバに対する単位時間あたりのパケット数でのみ判定している．パケット数が閾値を越えた異常な数のアクセスのみが攻撃とは限らず，false positive(誤検知)があった際も閾値を変更し調整することしかできない．帯域制御を利用したDoS攻撃に対する防御方法[4]も考案されているが，既存研究の問題点と同様に，帯域を圧迫するDoS攻撃にしか対処できない．そこで本研究では，Linuxのカーネルモジュールを利用してB-DRIPの問題点を解決し機能を拡張した新たなシステムを構築する．

4 提案手法・システム

提案システムでは現在動作しているB-DRIPを，LinuxのモジュールであるnetfilterとNetwork Namespaceを用いて実装する．これら2つのモジュールを組み合わせることにより豊富なルールを組み合わせた柔軟な攻撃検知，代理応答が可能となる．またB-DRIPとは異なり，カーネルソースコードの変更や代理応答サーバを別途構築する必要がないことが利点である．図1に提案システムの概要を示す．提案システムは，攻撃検知部，攻撃処理部，攻撃防御部の3か所に分かれる．

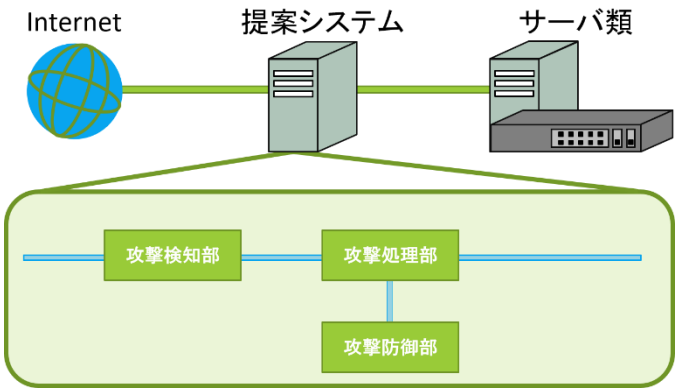

図1：提案システム

† 和歌山大学大学院
‡ 和歌山大学 学術情報センター

攻撃検知部では，iptablesの拡張マッチングルールを利用した攻撃検知をおこなう．攻撃と判定されたパケットに対しては，ヘッダ内のTOS(Type of Service)フィールドに対し操作を加え，攻撃処理部へと転送する．

攻撃処理部ではパケットのヘッダ内のTOS値を検査し，攻撃と判定された通信に対し，送信先MACアドレスを書き換えることで内部ネットワークへの攻撃を防ぎつつ，攻撃防御部へと転送する．

攻撃防御部では，80番ポートに対する攻撃には代理応答を行い，その他の攻撃に対しては受け取るが全てを破棄することで防御する．

提案システムの上記3か所の動作は，設定ファイル内のルールを変更することで自由に動作を変更させることが可能であることも特徴である．

5 実験・評価

提案システムは多様化する攻撃への防御を目的とし，構築している．そこで攻撃手法の中からSYN Flood攻撃，HTTP GET Flood攻撃，Slow HTTP DoS攻撃の3手法を用いて実験用のローカルネットワークのWebサーバを攻撃し，提案システムで防御実験をおこなった．

実験では，全ての攻撃手法において，提案システムでの汎用的な防御ができた．図2にHTTP GET Flood攻撃での攻撃パケット数と内部Webサーバまで到達したパケット数を示す．また代理応答とルーティングによる防御手法を用いたことで，提案システムへの負荷も少なくすることができた．しかし，SYN Flood 攻撃に対する防御実験では，提案システムは秒間40000パケットを超える攻撃を受けるとCPUの負荷が上がってしまった．理由として，提案システムがセッションごとに攻撃判定していることがあげられる．攻撃時に受け取る各SYNパケットに対し，提案システムは新規セッションとしてコネクション情報を保存する．SYN Flood攻撃による秒間攻撃パケット数が増えれば増えるほど，この処理が増加し，CPUへの負荷が増大してしまうと考えられる．SYNパケットを連続で受信し続けた場合は破棄するなど別のルールを追加して対応する必要がある．

6 今後の課題

提案システムはローカルネットワーク上で運用実験と防御実験を行った．しかし，ローカルネットワーク上と実環境で流れる通信量は大きく異なるため，提案システムへの負荷も異なると考えられる．実環境，または実環境と同様の通信量で動作の検証が必要であると考える．

また先述した通り提案システムは，Linuxのカーネルモジュールを用いて構築されている．カーネルのパケットフィルタリングモジュールには豊富なマッチングルールがあり，それらを組み合わせることで，様々な攻撃に対する汎用的な防御をおこなえることが利点である．しかし現在の提案システムでは，これらのルールを自分で作成し，組み合わせて運用しなければならない．利便性をさらに高めるため，防御ルールを簡単に設定するためのシステムが必要であると考えられる．

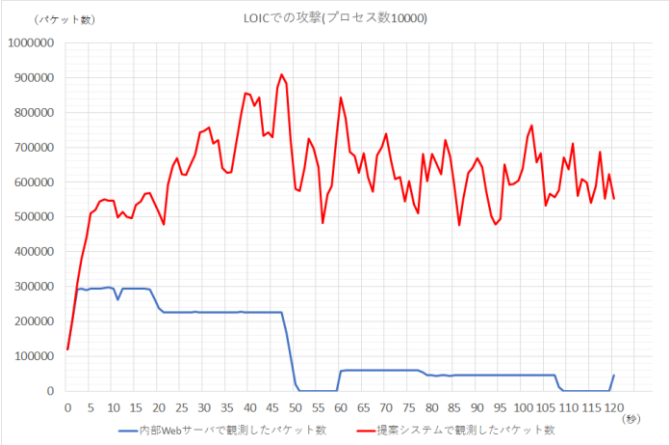

図2：HTTP GET Flood攻撃での攻撃パケット数と内部Webサーバまで到達したパケット数

参考文献

[1] 金森励起，元木伸宏，川橋裕，塚田晃司，“ソースアドレスルーティングによるトラフィック管理システム”電子情報通信学会技術研究報告， IN， 情報ネットワーク 108(342)， 25-30， 2008-12-04

[2] 澤　和晃，“トラフィック監視によるホスト・サービス単位の境界型ネットワーク防御システムの構築”
2010年度 和歌山大学 卒業論文

[3] 羽場　賢，”DoS攻撃に対する透過型防御システムの構築とステートレスなTCP代理応答の評価”
2011年度 和歌山大学 卒業論文

[4] 武藤 展敬，佐藤 直，“帯域制御を利用した能動的DoS攻撃対策 ”
2008年度　情報処理学会研究報告コンピュータセキュリティ（CSEC）