DDoS 攻撃模擬ツールの試作

2012SE104 川上　健人　2012SE134 黒田　涼介
指導教員：後藤　邦夫

1　はじめに

近年 IT 技術の発展により世界中で PC やスマートフォンなどの通信機器が広く普及している．誰でも簡単にインターネットを利用することができるため，コミュニケーションもインターネットで図っていることもある．誰でも使うことができる一方で，PC やスマートフォンのセキュリティや PC に対する知識が乏しい人がサイバー犯罪に巻き込まれることが増えてきた．様々なサイバー犯罪がある中で有効な対策が難しいとされる DDoS(Distributed Denial of Service) について研究する．DDoS 攻撃は攻撃元が複数あり，多くの場合 bot を使用したり，踏み台を使用するため攻撃元が特定できない．そのため有効な対策が無く脅威である．対策が 3 つ存在するが，軽減するだけであり，どれも有効な対策ではない．

本研究では IPv4，IPv6 において UDP Flood，ICMP Flood，TCP SYN Flood，TCP Connection Flood 攻撃を選んで実行できるよう C++ でひとつにまとめる．また，まとめたプログラムを GUI で実行可能にすることを目標とする．2014 年度大平，山下の卒業研究「IPv6 のための異常トラフィック生成プログラムの試作と評価」[3] ではこのプログラムの完成，さらに IPv6 に関係する異常トラフィックを用いた脅威を再現・試作するという課題が残っていた．先輩の研究に引き続き動作一般的なソケットでは無く raw ソケットを使い，事実上無制約なパケットを生成する．それを実際に送信することで負荷を与えて，通信を妨害する．しかし，raw ソケットプログラミングにより自由度が向上する半面，普段意識することのないプロトコルの詳細まで設定しなければならない．そのため，raw ソケットプログラミングに慣れていない人にとっては実装が容易ではない．本研究では，その難しい raw ソケットを用いて攻撃プログラムを作成する．

DDoS 攻撃の対策を研究，テストをするためには模擬攻撃が必要である．外部に被害や迷惑をかけないために閉じたネットワークで実験しなければならないため，確認・模擬実験には，ネットワークエミュレータの CORE(CommonOpen Research Emulator)[2] を使用する．CORE を使用するにあたり実験環境には Linux10.04 を用いる．GUI を作成するために wxglade[1] を用いる．wxglade を使用するにあたり Linux14.04 を用いる．

なお，川上は主に GUI の作成，黒田は主にネットワーク構成を担当する．攻撃プログラムは二人で作成した．

2　DDoS 攻撃の概要

現在の DDoS 攻撃の種類や対策について説明する．

2.1　IP Spoofing

通常，ホストやネットワーク同士の接続において，ホストは特定の IP アドレスに制限をかけて接続先をフィルタリングする．しかし，IP Spoofing 攻撃とは攻撃元が IP ヘッダ部の SrcIP アドレスを攻撃対象のアドレス空間のものに偽装することで，攻撃対象へのアクセス制限を突破する攻撃手法であるこの攻撃は攻撃対象のシステムログに嘘の Src アドレスが残るため攻撃元を特定することが非常に困難である．本研究ではランダムな嘘の Src アドレスを作成し，IPSpoofing による DDoS 攻撃手法を提案することで，セキュリティリスクの明確化と低減化を図る．

2.2　DDoS 攻撃の種類

DDoS 攻撃には大きく分けて 2 種類の攻撃がある [4]．一つ目は大きなパケットを大量に送るなどして，サーバまでの接続回線容量を埋め尽くすネットワークの回線の帯域を狙う攻撃である．

もう一つは攻撃対象のサーバを過負荷に陥れるサーバーを狙う攻撃である．本研究では，UDP Flood，ICMP Flood，TCP SYN Flood，TCP Connection Flood を試作する．以下で実現が最も困難である TCP Connection Flood について説明する．

2.2.1　TCP Connection Flood 攻撃

TCP SYN Food 攻撃では確立しない中途半端な TCP 接続を発生させるが，この攻撃ではコネクションを確立する．コネクションを確立させた後は何もしない．コネクション大量にを確立させつづけことでメモリを占領する．TCP Connect Flood 攻撃の際に困難であるのは，どのような方法によって偽装のホストから盗聴して対象から送信された SYN，ACK を手に入れるかである．攻撃の流れを図 1 に示す．

1. 嘘の Src アドレスを使って対象に SYN パケットを送信する
2. 対象はそれを受けて SYN と ACK を嘘の Src アドレスに送信する
3. 攻撃元は偽装に使用したホストから SYN と ACK を盗聴する
4. 嘘の Src アドレスから ACK を返させる

3　システムの概要

作成する攻撃プログラムの利用想定，実験するネットワーク構成を説明する．

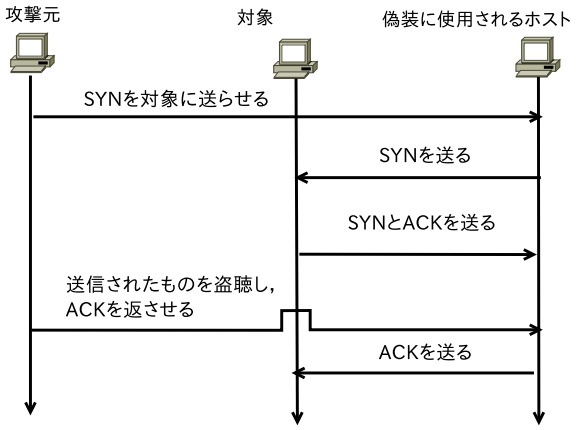

図 1　攻撃の流れ

3.1　攻撃プログラムの使用想定

本研究では IPv4，IPv6 それぞれにおいて UDP Flood，ICMP Flood，TCP SYN Flood，TCP Connection Flood 攻撃を選択して攻撃できるものを作成する．攻撃のパラメータは IP のバージョン，攻撃に使用するプロトコル，攻撃の間隔，Src，DstIP の範囲，Src，Dst ポートの範囲を設定できるようする．

3.2　攻撃プログラムの処理の流れ

はじめに選択された IP のバージョンの raw socket を作る．次に設定された Src，Dst アドレス範囲からサブネットマスクを作成する．そのサブネットマスクを元にホスト部をランダムに変化させ，アドレスを作成する．設定された Src，Dst ポートの範囲からランダムにポートを作成する．その後攻撃の間隔を設定し，最後にそれらを格納し，チェックサム計算をした後，ペイロードを送信する．指定範囲の攻撃間隔で繰り返しをする．大まかなプログラムの流れは上記の通りで，それぞれ関数に分けてプログラムを書く．各関数の細かい処理の流れは後の節で述べる．

3.3　ネットワーク構築

攻撃プログラムは外部接続があると危険であるためネットワークエミュレータの CORE 上で動作させる．攻撃プログラムを動かすホストを Attacker，直接攻撃対象を Target，間接攻撃を受けるネットワーク，ホストを Victim と定義する．本研究の実験に用いるネットワーク構成図を図 2 に示す．

攻撃側のホストで嘘の Src アドレスを使って対象にパケットを送信する．対象側のホストでパケットをキャプチャする．

3.4　メインプログラムと GUI

C++ でまとめた攻撃プログラムを実行するために，メインプログラムを作成する．以下にメインプログラムのソースコードを示す．

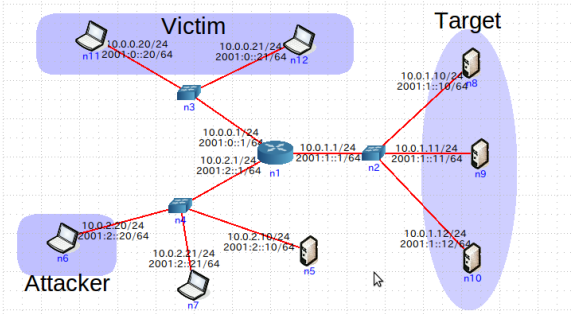

図 2　ネットワーク構成

メインプログラムのソースコード

```
obj = new DDoSTester(
          DDoSTester::IPv4, DDoSTester::UDP,
          DDoSTester::NONE, DDoSTester::UNIFORM
          );
         ......................
  obj->setSrcIPRange("192.168.0.0/16");
  obj->setDstIPRange("10.0.0.1/32");
  obj->setSrcPortRange(60000,61000);
  obj->setDstPortRange(80,80);
  obj->setInterval(1.0); // second
while(true){
    uint8_t payload[1500];
    int len = 0;
    int ret = obj->sendPayload(payload, len);
    cerr << ret << " bytes sent " << endl;
    usleep(obj->getInterval());
```

まず，Version，Protocol などを入力する．次に，各パラメータを代入する．その後ペイロードを送信する．

本研究では，メインプログラムの代わりに GUI で値を設定する．GUI を作成するために wxglade を用いる．wxglade とは python で書かれたオープンソースのツールで wxWidgets を使用して GUI を作成できる．wxglade は GUI を作成すると python の他に C++ のコードが出力できる．作成した GUI を図 3 に示す．

図 3　wxglade で作成した GUI

4　システムの実現

実験環境を作る CORE，C++ で統合した模擬攻撃プログラムの説明をする．

4.1 クラスの設計

本研究ではクラスを 4 個に分けてプログラムを構成する．commoncpp2 をインストールしスレッドを用いる．スレッドはパケットを送信するスレッドと SYN+ACK を検出するスレッドの 2 種類である．二つは wxglade によって出力される MyApp，MyFrame．MyApp は GUI を起動するためのクラスで，MyFrame は GUI で入力した値を受けとるものである．三個目は DDoSTester で，これは raw ソケットを生成，嘘のランダムアドレス作成など攻撃に必要なパラメータを設定，ペイロードを送信するクラスである．最後のクラスは MainThread で，これは MyFrame が受け取った値を DDoSTester に投げる GUI と攻撃プログラムの架け橋になるクラスである．

4.2 DDoSTester.cpp

本研究のメインとなる攻撃プログラムである．細かい処理毎に関数に分けて作成し，それらをまとめたクラス．

4.2.1 raw ソケットの生成

raw ソケットとは通常のソケットとは異なりヘッダ情報を含んだデータを送受信できる．しかし，raw ソケットを扱うためには普段意識することのないプロトコルの詳細まで設定しなければならない．そのため，raw ソケットプログラミングに慣れていない人にとっては実装が容易ではない．

raw ソケットの生成

```
if (ver == IPv4){
    raw4sock = socket(AF_INET,
               SOCK_RAW, IPPROTO_RAW);}
else if (ver == IPv6)
    raw6sock = socket(AF_INET6,
               SOCK_RAW, IPPROTO_RAW);

  pfsock = socket(AF_PACKET,
           SOCK_RAW, htons(ETH_P_ALL));
```

4.2.2 嘘の Src アドレス作成

IP Spoofing 攻撃では Src アドレスを偽装する必要があるため嘘の Src アドレスを生成するプログラムが必要である．嘘のアドレスをランダムで 100 個用意する．指定したアドレス範囲でランダムにアドレスを生成するために，まず IP アドレスとプリフィックス長からサブネットマスクを作成する．ソースコードは以下の通りである．

IPv4 のサブネットマスク作成のコード

```
size_t found = addressRange.find("/");
  if (found == string::npos) {
   cerr << "/ not found in addressRange" << endl;
   return false;
  }
string netAddrStr = addressRange.substr(0,found);
string prefixStr  = addressRange.substr(found+1);

  if (ver == IPv4){
inet_pton(AF_INET, netAddrStr.c_str(), &saddr);
//  アドレスを文字列からアドレス構造体に変換し saddr
にコピーする
smask.s_addr = htonl(0xffffffff <<
           (32-atoi(prefixStr.c_str())));
//  32 ビットからプリフィックス分だけ 1 を左にシフト
させる
```

サブネットを作成した後にランダムでアドレスを作成する．

IPv6 ランダム Src アドレス作成のソースコード

```
  struct in6_addr randomAddr;

  for (int j=0; j < 4; j++){
//アドレスを 32 ビットずつに 4 回分けて生成する
   randomAddr.s6_addr32[j]
      = (addr.s6_addr32[j] & mask.s6_addr32[j])
        //この部分でネットワーク部を固定
      | ((u_int32_t) (2147483648*drand48())
      &  ~mask.s6_addr32[j]);
      //この部分でホスト部をランダムに作成
   }
   return randomAddr;
  }
```

4.2.3 パケットを送信

上記で作成してきたランダムアドレスを sendbuf を用いてペイロード送信する．送信には raw socket を用いる．IP ヘッダなどに適切なパラメータを埋める．fill4checksum() と fill6checksum() でチェックサムを確認し，sendto 関数を使用し送信する．使用ソケット，メッセージ，メッセージのサイズ，フラグ，接続先のアドレス，そのアドレスのサイズの情報を格納している．

4.2.4 ACK を返すクラス

TCP Connection をするために run() クラスを作成する．run() は SYN+ACK を受信し，受信した SYN+ACK を確認し，ACK を返す部分になる．SYN+ACK を確認するために while 文と if 文を用いて，IP やプロトコルを判別する．SYN+ACK 受信にはデータリンク層 socket を使用する．まず，IPv4，IPv6 であるかを確認する．どちらかであれば，次に TCP であるかを確認する．TCP であれば，次に TCP flags を確認する．すべての確認が成功すれば，ACK を送信する．IPv4，IPv6 ヘッダ，TCP ヘッダに適切なパラメータを代入し，ACK を生成する．生成し

た ACK を sendto() を用いて送信する．

5 実験

実験の手順，実験の結果について示す．

5.1 実験手順

実験の手順は以下の通りである．

1. CORE 内でネットワークを構築する
2. Attacker から Target に攻撃プログラムを実行する．
3. 実験結果のキャプチャには tcpdump コマンドを使用し，観測する

IPv4 アドレスで実験する場合は SrcIP のアドレス範囲は 192.168.0.0/16，DstIP のアドレス範囲は 10.0.0.1/32，Src ポートの範囲は最大 61000，最小は 60000，Dst ポートの範囲は最大最小共に 5001，攻撃間隔は 1.0 秒に設定する．また IPv6 アドレスで実験する場合は SrcIP のアドレス範囲は 2001:ff::/120，DstIP のアドレス範囲は 2001:1::10/128 に設定する．TCP 攻撃の場合，ターゲットで IPv4 は iperf -s，IPv6 は iperf -s -V を起動して実験をする．

5.2 実験結果

IPv4 の UDP Flood 攻撃の実験結果を以下に記述する．

IPv4 UDP Flood Attacker

```
tcpdump -l
00:10:23.739915 IP 192.168.0.115.60863
> 10.0.1.8.www: UDP, length 100
00:10:25.186052 IP 192.168.0.74.60058
> 10.0.1.10.www: UDP, length 100
00:10:25.262018 IP 10.0.2.1
> 192.168.0.12: ICMP host 10.0.1.9
  unreachable, length 136
.....................................
```

IPv4 と IPv6 の TCP Connection Flood 攻撃の実験結果を以下に記述する．

IPv4 TCP Connection Flood Attacker

```
tcpdump -l
13:00:29.712828 IP 192.168.130.5.60166
> 10.0.1.10.5001: Flags [S], seq 3707035660,
win 60000, length 0
13:00:29.712996 IP 10.0.1.10.5001
> 192.168.130.5.60166: Flags [S.],
seq 442129107, ack 3707035661,
win 14600, options [mss 1460], length 0
13:00:29.713566 IP 192.168.130.5.60166
> 10.0.1.10.5001: Flags [.], ack 1, win 60000,
length 0
.....................................
```

IPv6 TCP Connection Flood Attacker

```
tcpdump -l
13:00:29.712828 IP 192.168.130.5.60166
> 10.0.1.10.5001: Flags [S], seq 3707035660,
win 60000, length 0
13:00:29.712996 IP 10.0.1.10.5001
> 192.168.130.5.60166: Flags [S.],
seq 442129107, ack 3707035661,
win 14600, options [mss 1460], length 0
13:00:29.713566 IP 192.168.130.5.60166
> 10.0.1.10.5001: Flags [.], ack 1, win 60000,
length 0
.....................................
```

IPv6 TCP Connection Flood Target

```
netstat -at
tcp6       0      0 2001:1::10\%3076119:5001
2001:ff::16\%1:60707     ESTABLISHED
```

以上より IPv4，IPv6 の TCP Connection Flood 攻撃は成功していることが分かる．

6 おわりに

本研究で，実験した結果を表 1 にまとめた．また攻撃の

表 1 実験結果

	IPv4	IPv6
UDP	○	○
ICMP	○	○
TCP SYN	○	○
TCP CONN	○	○

パラメータを設定し，攻撃を開始できるよう一つのクラスにまとめることができた．wxglade で GUI を作成し，送信開始の処理もできるようになった．TCP Connection に必要な run() プログラムは完成した．

参考文献

[1] Marcello Semboli and Alberto Griggio and Carsten Grohmann: wxGlade manual (accessed Jan. 2016). http://wxglade.sourceforge.net/manual/.

[2] U.S. Naval Research Laboratory Networks and Communication Systems Branch: Common Open Research Emulator (accessed Dec. 2015). http://www.nrl.navy.mil/itd/ncs/products/core.

[3] 大平峻也，山下瑞樹：IPv6 のための異常トラフィック生成プログラムの試作と評価，南山大学システム創成工学科 2014 年度卒業論文 (2015).

[4] 田村奈央：ぜい弱性に揺らぐインターネット (accessed Jan. 2016). http://itpro.nikkeibp.co.jp/article/COLUMN/20090225/325453/.