断片ダークネットのためのパケット観測用ブリッジの提案

今間　俊介[†]　福田　健介[‡]　廣津　登志夫[*]　菅原　俊治[†]

[†]早稲田大学理工学部　[‡]国立情報学研究所　[*]豊橋技術科学大学

概 要

インターネット上のさまざまなサービスに対し、 DoS アタック、ウイルス、侵入などの妨害処理があり、社会的に問題になっている。これに対し侵入検知システムによる発見やハニーポット、ダークネット等による攻撃検知システムが提案されている。我々はこの中でダークネットによる攻撃あるいは攻撃のための事前調査パケットの検出に着目している。しかし、これまでのダークネット観測は、たとえば、/12 などの広大な未使用 IP アドレス空間を観測することが主であったが、このような広い空間を用意することは難しい。一方で、各組織に割り当てられた IP アドレスは、100%使われている訳ではなく、いわゆる虫食い状態で使われていると考えられる。そこで本研究では、ブリッジとしてルータの直前に設置し、ネットワークの内で稼働（あるいは応答）する IP アドレスを自動抽出しながら、未使用アドレス宛へのパケットを収集する観測用ブリッジを開発した。このブリッジは、観測対象ネットワーク内の未使用アドレスのみを抽出し、そのアドレス宛のパケットのみを収集するため、従来の Darknet 観測モニタでは不可能であった、観測ネットワーク内に生存ホストを含めることができるようになる。本稿では、このブリッジのパケット収集評価を行った。結果、使用アドレスの通信の有無にかかわらず、未使用アドレスへのトラフィックが 95.7Mbps の場合まで収集可能なことがわかった。

1　序論

1.1　背景

近年、インターネットの利用者数はますます増加し、接続されている PC の数も急速に増加している。このようなインターネットの急速な普及により、利用者はインターネットを利用し、ネットバンキング、ネットショッピングなど距離や時間を意識しないサービスの利用が可能になっている。しかしその一方で、機密情報や個人情報の流出、サービス提供サイトへの DDoS 攻撃、ネットワーク全体を蔓延するようなウィルス、ワームの感染など、利用者を脅かす脅威が発生しているのも事実である。これら脅威の影響は、インターネットを介すデータ量が増加するほど大きくなり、人間生活のネットワークに対する依存度が高くなっている現在、社会的な問題となっている。

例えば、例外的に感染力の強かった Nimda ワームの場合、ピーク時で 1 日に 50 億回の感染試行を行い、脆弱な全ホストにわずか数分で感染した [10]。Slammer ワームの場合も同様に、脆弱なホストの大多数（75,000 強）に 30 分足らずで感染した [9]。このような感染力の強いワームの場合、ホストだけでなくその間を介するルータ、スイッチなどのネットワーク機器にも多大な負荷をかけ、その機器に接続されている脆弱でないホストにまで問題を引き起こすような影響を及ぼした。また、これらの脅威は、パターンファイルやパッチが公開されていない脆弱性を悪用する、zero-day の可能性も秘めており、このような脅威の場合には、特に素早く対応しなければならない。

このような問題を対処するため、現在のインターネット上に、後述するインターネット攻撃検知手法を用いた防衛基盤を構築することが不可欠である。

1.2　インターネット攻撃検知

各種の侵入検知システム、攻撃検知システムが提案されている。これらインターネットに対する攻撃の検知手法の種類は、大きくアクティブ手法とパッシブ手法の 2 種類に分類される。

アクティブ手法には、Honeypot がある。特徴として、実際に攻撃を受けると、攻撃を受けたホスト、ソフトウェアの挙動を模倣し、攻撃を仕掛けてきたウィルスやワームの詳細な情報を得ることができる。

Honeypot を使用した例として、BackOfficer Friendly(BOF)[12]、Spector[13]、Honeyd[14]、Honeynet[7] などが挙げられる [15]。これらの手法では、挙動を模倣しなければいけないので、ホストに負荷がかかることを考えると、この手法ではそこまで広い範囲のネットワークを監視することができない。また、backscatter による二次被害として、関係ないホストに攻撃トラフィックが転送されてしまう可能性もある。

パッシブ手法では、アクティブ手法とは異なり、ファイアウォールにより遮断されたパケットのログ、または実際にはホストが存在しない IP アドレス宛ての（本来ありえない）パケットを収集、解析を行うことにより攻撃の情報を得る。そのため、観測ホストに負荷がかからず、二次被害も起こらない。

前者の例として、JPCERT/CC によるインターネット定点観測システム ISDAS[1]、警察庁によるインターネット定点観測システム [2]、インターネット早期広域攻撃警戒システム [3] が挙げられる。これらのシステムは、各種ログを用いて結果を出力しているため、運用の負荷は小さ

Proposal of the bridge for monitoring packets to fragmented unused network

Syunsuke KOMMA[†], Kensuke FUKUDA[‡], Toshio Hirotsu[*], Toshiharu SUGAWARA[†]

[†]Waseda University, Faculty of Science and Engineering

[‡]National Institute of Informatics

[*]Toyohashi University of Technology

いが、正常/異常の判断、どのような攻撃か、などのトラフィックの詳細な情報を取得することは困難である。

一方、後者の例として、Network Telescope[4]、Darknet[8]、Blackhole[10]、Internet Motion Sensor (IMS)[6] が挙げられる。特に、我々はこの中で運用負荷の小さい Darknet による攻撃パケットの検出に着目している [5]。

1.3 目的

従来の Darknet 観測は、図 1 に示すように、広大な未使用 IP アドレス空間を用意し、観測することが主であったが、一般的にこのような広い空間を用意することは難しい。その上、観測対象のアドレス空間には、生存ホストを含めることができず、観測目的だけに貴重なアドレス空間を無駄にすることになる。また、観測機を設置するために、上位ルータなどの既設ネットワーク機器設定の変更が必要である。これにより、設定ミスによるネットワーク不通など、既設ネットワークに影響を及ぼしかねない。

一方、観測ネットワークの規模については、比較的小規模 (/27) なダークネットアドレス空間の観測結果が、10,000 アドレス先まで確率的に正の相関があることが報告されている [16]。これは、断片的な観測でも、それらを統合することにより、広い空間での事象を推測できる可能性を示している。

そこで本研究では、100%利用されてはいない、いわゆる虫食い状態（第 2.2 節参照）で使用されている各組織に割り当てられた IP アドレス空間を使用し、ブリッジとしてルータの直後に設置するだけで、ネットワーク内で稼働していない IP アドレスを自動抽出しながら、未使用アドレス（ダークアドレス）宛へのパケットを収集する観測用ブリッジの開発を目的とする。このブリッジは、生存マシンにおける通信には一切影響してはいけない。

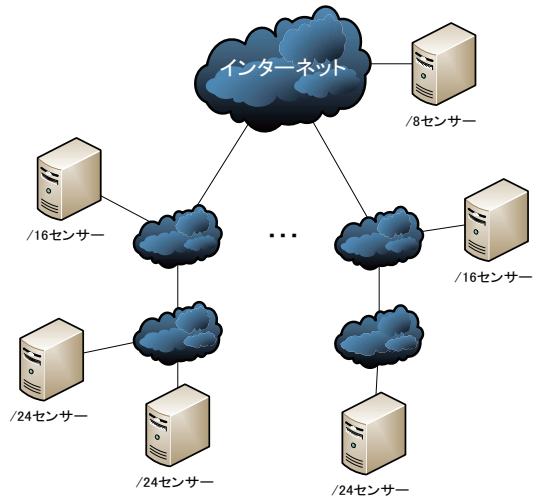

図 1: 従来の Darknet システム構成図

2 提案システム

2.1 システム構成

システムの基本的な機能は、通常のブリッジ機能に加えて、受信したパケットをフィルタして、未使用アドレス宛パケットを DB に収集する。DB には 1 パケットを 1 レコードとしてデータを書き込み、テーブルには以下のようなフィールドを用意する。

- ID（プライマリキー）
  収集パケットの通し番号が入る。
- 日付（インデックス）
- 時刻マイクロ秒
- プロトコルの種類
  tcp、udp、icmp などが入る。
- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号
  プロトコルの種類が tcp、udp の場合のみ、ポート番号が入る。
- TCP フラグ
  プロトコルの種類が tcp の場合のみ入る。
- ICMP メッセージタイプ
- ICMP 応答コード
  プロトコルの種類が icmp の場合のみ入る。
- ペイロードデータ (128 バイト)
  ヘッダのみの場合は、データが入らない。

将来的に、受信したパケットを即時に解析できるように、取得したパケットデータから必要データのみ DB に書き込み、日付にインデックスを付ける。

システム構成図は、図 2 に示す。図では、太線はパケットの流れ、実線は未使用アドレスデータ読み書き、点線は未使用アドレス宛パケットデータをそれぞれ示している。フィルタする際に、宛先アドレスを見て、未使用アドレス検出 (Unused Address Detection、以下 UAD と記述) 機能を使用してホストの生存確認をして、生存していない場合のみ DB にパケットデータを保存する。この UAD 機能は、ルータの内部において、ブリッジと同一サブネットに設置された未使用アドレスの検出を行う。

2.2 想定利用構成

このブリッジを使用したパケット収集を行う場合のネットワーク構成の例を図 3 に示す。

ブリッジが担当するネットワークには、生存するホスト、生存しないホストが混在可能であり、生存するホストへのパケット、生存するホストからのパケットに対しては、ブリッジは関与しない。生存しないホストへのパケットに関しては、ブリッジが生存確認を行った後、DB にパケットデータを保存する。

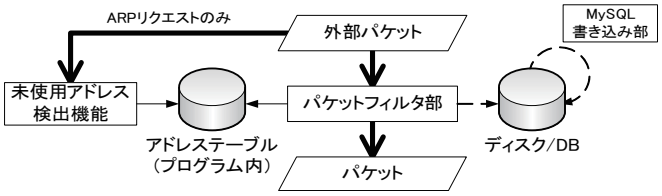

図 2: システム構成図

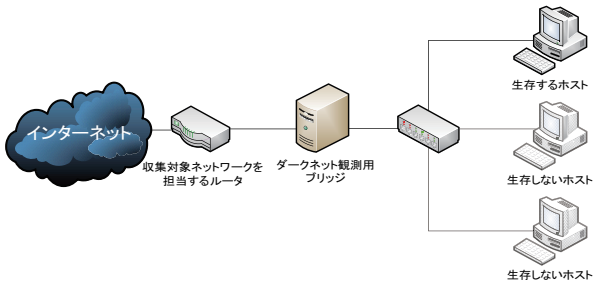

図 3: 想定利用構成図

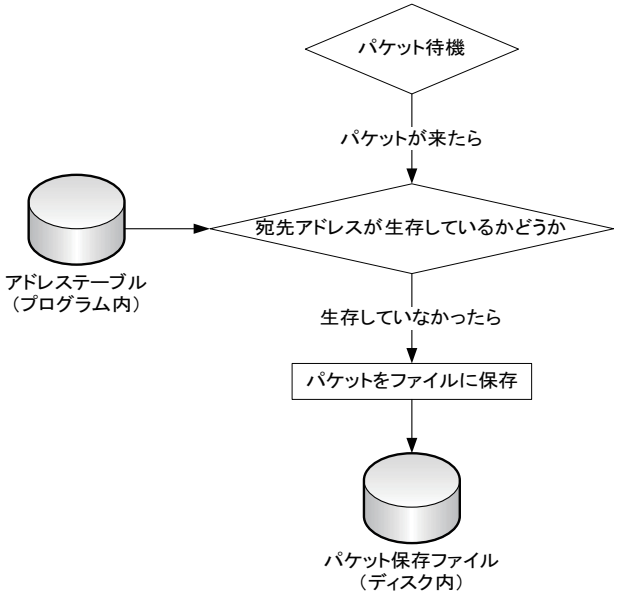

図 4: 動作概略図（パケットフィルタ部）

3 実装

3.1 DB 書き込み部/パケットフィルタ部

前述のブリッジを、Linux 上に構築した。パケット収集プログラムは、perl を使用した。パケット収集モジュールには libpcap を、単純に perl でラップした perl モジュールである Net::Pcap を使用した。パケットフィルタ部の動作概略図を図 4 に、DB 書き込み部の動作概略図を図 5 に、示す。

libpcap には受信パケットをバッファリングする機能が搭載されており、ある程度のパケット数まではパケットデータをメモリ上のバッファに保持する。しかし、1 パケットの処理時間が長いとバッファが溢れてしまい、バッファに蓄えられない受信パケットに関しては、libpcap が破棄する。この機能を本研究ではドロップ機能と呼ぶ。データベースへのデータ書き込み動作は、処理時間が相対的に長いので、このドロップ機能によるパケット破棄を防ぐため、受信パケットを直接ファイルに保存するスレッド（パケットフィルタ部）と、ファイルから保存したパケットデータを読み出すスレッド（DB 書き込み部）と、複数のスレッドに分離した。

3.2 未使用アドレス検出部（UAD 機能）

UAD 機能は、上記 2 スレッドと独立に動作し、パケット収集もパケットフィルタ部とは独立して行う。今回、UAD 機能には、ARP(Address Resolution Protocol) を用いた。上位ルータが、ブリッジの観測対象ネットワーク内の未使用アドレス向けの ARP リクエストを発行すると、ブリッジではそれを検知する。収集プログラム内のアドレステーブルに生存情報がない場合は、ブリッジでもそのホストの生存チェックを行い、返答がない場合、観測機自身の MAC アドレスを載せた ARP 返答をルータに送信し、上位ルータから該当パケットを収集する。

この機能を使用すると、ARP パケットを使用するという性格上、ルータの内部に設置し、同一セグメントの未使用アドレスの検出しか行えない。従って、今回の手法は、ルータの内部に設置した場合の検出しか行うことができない。最近の PC では、DDoS などのパケットを防止するため、ICMP をフィルタリングしている可能性が高いため、ping は使用しない。動作概略図を、図 6 に示す。

ハードウェア

CPU	Core 2 Duo E6300
メモリ	1GB
NIC	Broadcom NetXtreme BCM5754
	Realtek RTL-8169
HDD	Seagate ST3250820AS(7200rpm, SATA3Gbps)

表 1: ブリッジ用実験マシンの概要（ハードウェア）

4 実験と評価結果

4.1 実験環境/計測手法

ダークアドレス宛てパケット検出・収集、及び UAD 機能を実装したことによる効率の評価を行った。計測には iperf で、帯域幅を自由に設定することができる UDP を使用し、パケット収集状況を評価する。iperf は、クライアント/サーバ型のソフトであるため、ブリッジ以外に計測用マシンを 2 台用意した。今回使用する実験環境図は図 7 に、ブリッジの概要については表 1、表 2 に示す。このクライアント、サーバは使用/未使用アドレス混在の/24 のネットワークに設置した。今回の計測では、計測クライアントを上位ルータに見立てて行う。

なお、ブリッジのみの機能を当該マシンに実装したところ、最大で 95.7Mbps のスループットを得られた。

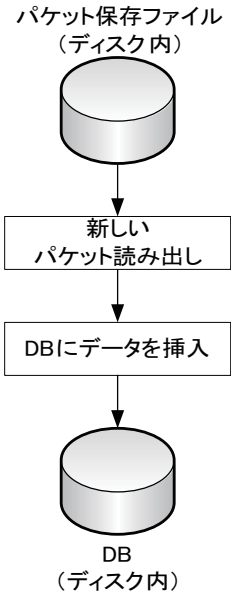

図 5: 動作概略図（DB 書き込み部）

ソフトウェア

OS	CentOS Linux 5
kernel	2.6.18-8
libpcap	0.9.4-8
mysql	5.0.22-2
perl	5.8.8-10

表 2: ブリッジ用実験マシンの概要（ソフトウェア）

4.2 評価結果

4.2.1 UAD 機能なしの場合

この実験では、ブリッジを間に挟み UAD 未使用で、1 分間計測を、以下の 3 通りについて 10 回ずつ行った。帯域幅は iperf のオプションで指定している。

(1) 収集対象パケットしか流さない場合
帯域幅 10~90Mbps が 10Mbps 刻み、90~100Mbps が 1Mbps 刻み

(2) 収集対象外パケットを 10Mbps 流す場合
帯域幅 10~80Mbps が 10Mbps 刻み、80~90Mbps が 1Mbps 刻み

(3) 収集対象外パケットを 50Mbps 流す場合
帯域幅 10~40Mbps が 10Mbps 刻み、40~50Mbps が 1Mbps 刻み

今回の実験では、間に挟まれているスイッチの制限上、対象パケット、対象外パケットのスループットの合計は、スイッチの上限値である 100Mbps になる。なお、対象外パケットとは、使用アドレス宛てのパケットを意味し、UAD 未使用状態では、ダークアドレスが予め与えられた場合、もしくは既に UAD による未使用アドレス検出が完了している状態に相当する。

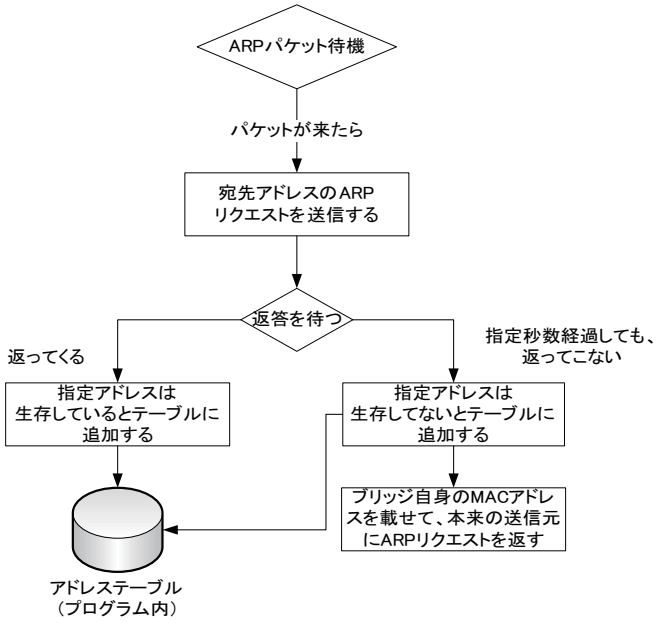

図 6: 動作概略図（未使用アドレス検出部）

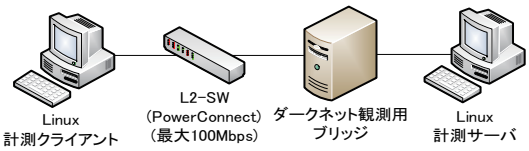

図 7: 計測環境図

UAD 未使用時の測定に関しては、スイッチでのパケットロスによる影響も調べるため、ダークアドレスを予め与えておく。そして、実際に宛先ホストで受信されたパケット数と、ブリッジで収集されたパケット数を比較した。(3) の場合のグラフを、図 8 に示す。収集パケット数は、対象受信パケット数とほぼ一致し、パケットドロップはほとんど発生しなかった。対象外受信パケット数が 46Mbps から激減しているのは、対象パケットと対象外パケットの合計スループットが、スイッチの転送限界スループットである 95.7Mbps を超えたためであると考えられる。

また、(1)、(2) の場合も、パケットドロップはほとんど発生しなかった。

4.2.2 UAD 機能ありの場合

今度は、UAD 機能を使用して、第 4.2.1 節と同様の計測を行った。観測機の UAD 機能設定では、上位ルータが出した ARP リクエストの宛先に対して、観測機自身からも ARP リクエストを出し、1 秒間待って返答がない場合自身の MAC アドレスを載せて返答を返す。宛先ホストの MAC アドレスが ARP キャッシュに入っていない場合、観測機からの ARP 返答が来るまで、上位ルータはパケットを送出できず、その間パケットは収集できないので、ブリッジでは最初の 1 秒分を除いたパケットが収集される。[†1]

[†1]ただし、実環境では、ARP 返答があるまでルータはパケットを送出しないので、実際には収集する必要はない。

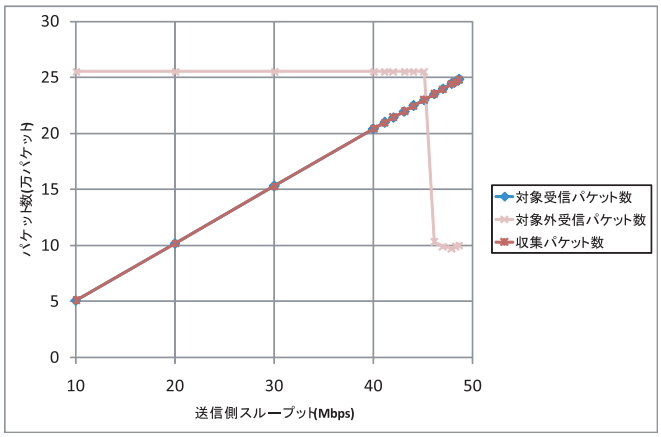

図 8: UAD 未使用時 (対象外 50Mbps の場合)

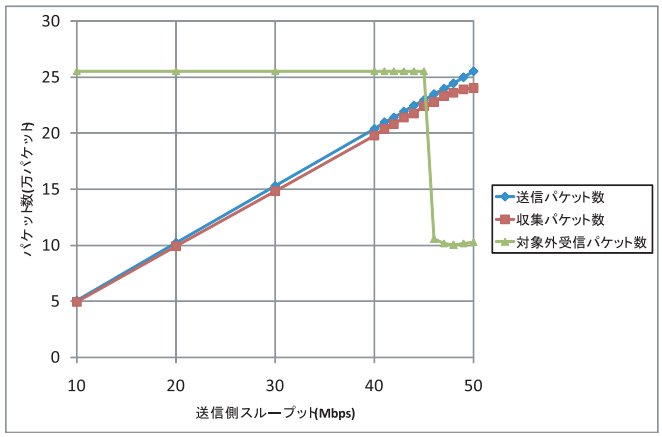

図 9: UAD 使用時 (対象外 50Mbps の場合)

UAD 使用時の計測に関しては、想定環境同様に、ダークアドレスに生存しないホストを指定するので受信パケット数は測定できない。代わりに、クライアントからの送信パケット数と、ブリッジでの収集パケット数を比較している。(3) の場合のグラフを、図 9 に示す。結果は、UAD 機能による未使用アドレス検出の 1 秒間分のパケットを除き、それ以後のパケットに関してはほぼ収集できていることが確認できた（図 9 グラフにおける差は、ほぼ 1 秒間のパケットに相当する)。送信側スループットが 46Mbps から送信パケット数と収集パケット数の差が徐々に大きくなっているのは、UAD 未使用時の測定同様、スイッチによるパケットロスであると考えられる。

4.3 実環境データとの比較

実験で得られたデータが、どの程度の規模のネットワーク範囲まで対応できるかを調査するため、実稼働環境で収集された Darknet パケット量と比較してみた。比較データとして、/18、/23、独立した 1 アドレス（16897 ホスト）に対するパケットを観測している、ある観測ネットワーク内に設置された Darknet モニタで、収集量が特に多かった 2007/01/09 と 2007/08/27 分のデータを使用した。15 分毎に平均毎秒パケット数をグラフ化したものを図 10、11 に示す。それぞれパケット量の最高値は、83.51 パケット/秒、131.01 パケット/秒、帯域の最高値は、94.2kbps、73.8kbps であった。この比較データでは、ネットワーク内に生存マシンがないため、このネットワーク内で受信されるすべてのパケットがブリッジの収集対象パケットとなるが、前述の実験結果では、生存マシンの通信（対象外パケット）の有無にかかわらず転送速度で 95.7Mbps、転送パケットレートで約 48 万パケット/秒まではドロップ機能が動作せずに、未使用アドレス宛の全パケットデータが DB に書き込むことができる。よって、同様のネットワーク範囲の場合で、ネットワーク内に生存マシンがいる場合でも十分実用に耐えうる。

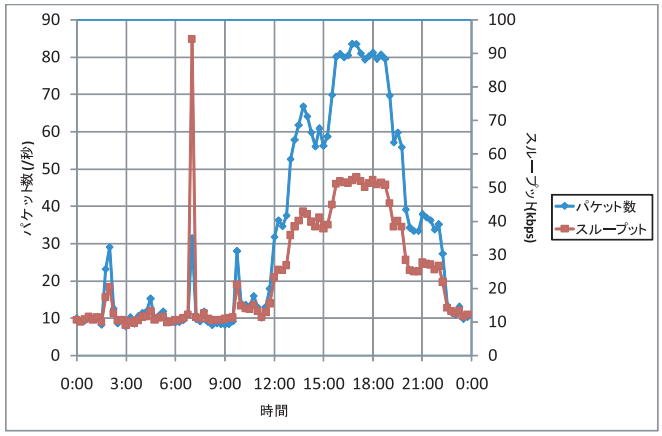

図 10: ある観測ネットワークにおける 15 分毎の平均毎秒パケット数/スループット (2007/01/09 分)

5 問題点

現行の実装における問題として、ブリッジが流した ARP 返答が送信側のキャッシュに入ってしまった場合、次のキャッシュ更新までそのアドレスで起動したマシンにアクセスできない、という点が挙げられる。これに対する対策として、そのアドレスが本当に使用されていないアドレスかどうかを、ARP だけではなく DNS で逆引きしてホスト名が登録されていないかどうか調べる、または、観測対象ネットワーク内の ARP テーブルをブリッジ内で統合管理し、ProxyARP によるパケットの中継を行う、などの対策手法が考えられる。

6 結論

本研究では、未使用アドレス宛てパケット収集を行う観測ブリッジについて、収集プログラムを用い、収集スループット、送受信マシンでの通信への影響の評価を行った。

現在のインターネット攻撃検知手法の中で、我々は Darknet に注目していたが、従来の Darknet センサーでは、観測には広大な未使用 IP アドレス空間が必要、そのアドレス空間上のアドレスを使用することができない、などの欠

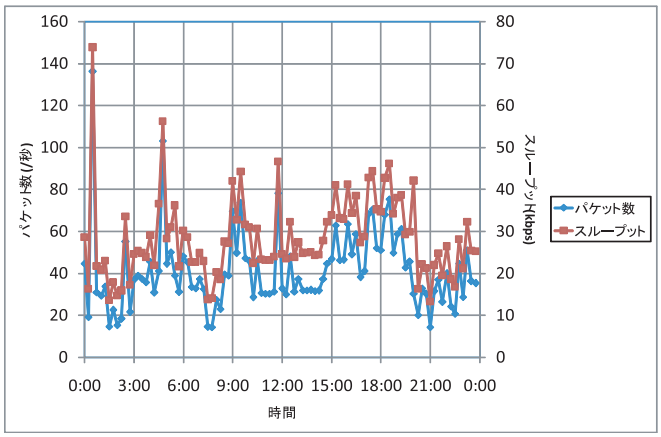

図 11: ある観測ネットワークにおける 15 分毎の平均毎秒パケット数/スループット (2007/08/27 分)

点が存在した。そこで、本研究では各組織に割り当てられた IP アドレス空間を使用し、ネットワーク内で未使用の IP アドレスを自動抽出しながら、未使用アドレス（ダークアドレス）宛へのパケットのみを収集する観測用ブリッジを開発することを目標とした。

このブリッジ上で動作するプログラムでは、攻撃を即座に検知、対処できるようにデータベースにパケットのデータを挿入することを前提としたため、パケットフィルタ部、DB 書き込み部、未使用アドレス検出部 (UAD) を分けて、マルチスレッドを使用して作成した。

ブリッジの計測実験では、実ネットワーク上で、収集対象外パケットを流さない場合、10Mbps 流す場合、50Mbps 流す場合、という条件で行った。全ての場合において、収集対象パケット（生存しないホスト宛のパケット）における受信側スループットが、スイッチのほぼ上限である 95.7Mbps までブリッジで完全に収集できることがわかった。

今後の課題としては、プログラムの C 言語への移植による速度向上、Gigabit Ethernet 上でのスループット評価がある。また、ルータの上流側に本ブリッジを配置することを想定した実装も挙げられる。

謝辞

本研究は科学研究費補助金特定領域「情報爆発時代に向けた新しい IT 基盤技術の研究」の支援を受けている。

参考文献

[1] JPCERT/CC: インターネット定点観測システム (ISDAS: Internet Scan Data Acquisition System). http://www.jpcert.or.jp/isdas/.

[2] 警察庁セキュリティポータルサイト @police–インターネット定点観測. http://www.cyberpolice.go.jp/detect/observation.html.

[3] Ishiguro, M., Suzuki, H., Murase, I. and Ohno, H. “Internet Threat Detection System Using Bayesian Estimation,” The 16 the FIRST Annual Conference on Information Security Incident 2004, 2004.

[4] D. Moore, C. Shannon, G. Voelker, and S. Savage. “Network telescopes: Technical Report,” CS2004-0795, UC San Diego, July 2004.

[5] 廣津, 福田, 栗原, 明石, 菅原, “断片アドレス を用いた分散協調インターネット監視に関する一考察,” SWoPP 2007, 情報処理学会 OS 研究会, Vol. 2007, No. 83, pp.39–45, 2007.

[6] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. “The Internet Motion Sensor: A distributed blackhole monitoring system,” NDSS’05, 2005.

[7] The Honeynet Project & Research Alliance: Know your Enemy: Honeynets, 2003. http://www.honeynet.org/papers/honeynet/.

[8] E. Cooke, M. Bailey, F. Jahanian, and R. Mortier, “The Dark Oracle: Perspective-Aware Unused and Unreachable Address Discovery,” NSDI’06, pp.101–114, 2006.

[9] Lad, Zhao, Zhang, Massey, and Zhang. “Analysis of BGP update surge during slammer worm attack,” In International Workshop on Distributed Computing: Mobile and Wireless Computing, LNCS, volume 5, 2003.

[10] D. Song, R. Malan, and R. Stone. “A snapshot of global Internet worm activity,” FIRST Conference on Computer Security Incident Handling and Response, June 2002.

[11] NLANR/DAST : Iperf - The TCP/UDP Bandwidth Measurement Tool. http://dast.nlanr.net/Projects/Iperf/.

[12] M. Ranum. “BackOfficer Friendly (BOF).” http://www.nfr.net/products/.

[13] Spector. http://www.spector.com/

[14] N. Provos. “Honeyd: A Virtual Honeypot Daemon,” Proceedings of the 10th DFN-CERT Workshop, 2003.

[15] F. Zhang, S. Zhou, Z. Qin, J. Liu, “Honeypot: a supplemented active defense system for network security,” Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT’2003. Proceedings of the Fourth International Conference on, pp.231–235, 27–29 Aug. 2003.

[16] 福田健介, 廣津登志夫, 明石修, 栗原聡, 菅原俊治, ”異常パケットトレースのアドレス局所性に関する解析,” 情報処理学会全国大会, 4K-5, 筑波大学, March, 2008.