L-027

UTM では検出困難な DDoS 攻撃を統計的手法を用いて検出する研究における DDoS 攻撃環境の開発

宇井哲也 † 湯原大二郎 ‡ 成瀬慎 § 鈴木彦文 ¶

Tetsuya Ui Daijirou Yuhara Shin Naruse Hikofumi Suzuki

1. 研究背景

近年インターネットの普及に伴い, インターネット上の犯罪は増加の傾向にある. 巧妙で多様化するサイバー攻撃で最も多い手口の一つが, サービス不能攻撃 (以下,DoS 攻撃) である.DoS 攻撃は, ネットワークシステムその他のリソースへの正規のユーザーからのサービスを妨害したり, 完全に利用不能に陥らせるようなタイプの攻撃である [1].DoS 攻撃のうち踏み台にした多数のマシンに攻撃用のプログラムをインスートルし, それをリモート操作して, 一度に複数のサイトから標的のマシンに大量のデータを送信することで, 標的のマシンあるいはネットワークをダウンさせる攻撃を分散型サービス不能攻撃 (以下,DDoS 攻撃) という [1].

攻撃の影響はウェブサイトを利用するユーザの不便から重大な損失にいたるまで多岐にわたる. 小規模な攻撃は世界中で日常的に行われている. また大規模な攻撃は, 抗議団体による活動としての攻撃がある [2].DoS 攻撃の効果的な検出が可能となればこれらの被害を大幅に軽減できる.

2. 目的と概要

本研究は統合脅威管理装置 (以下,UTM) が出力する通信ログデータを統計処理して正常な通信と DoS 攻撃の通信を分類し,DoS 攻撃を検出することを目的とする. 研究で使用したログデータは実際に信州大学で動作している UTM に到達した全ての通信のログデータである.

通常, セキュリティ装置として UTM を利用する場合, 様々な通信の制御に対して多くの機能を提供しているが，多くの場合，閾値やシグネチャパターン等に基づいた制御である．この制御方法は，シグネチャーパターンの開発や高帯域・高速通信においてはボトルネックになることが非常に多い．また，近年では，DoS のような攻撃であっても，前述のような制御を行う機器をすり抜けるような手法が主流となりつつある.

そこで, 通信ログデータの解析には自己組織化マップ (以下,SOM) や K 平均法を利用しデータをクラスタリングさせ DoS 攻撃の検出を試みる. そのためには正常時の通信ログデータと攻撃を受けた通信ログデータの比較が必要となる. 本研究では通信ログデータを攻撃を受けた通信ログデータに近いものにするため仮想的な攻撃をしかけた.

†信州大学大学院総合理工学研究科
‡信州大学大学院理工学系研究科
§株式会社タイテック
¶信州大学総合情報センター

3. 理論

3.1. 攻撃の手法

DoS 攻撃には大量の大量のパケットを送信する Flood 攻撃タイプと, セキュリティホールを衝く脆弱性を狙った攻撃のタイプに分けることができる. 本研究では DNS サーバに対して UDPflood 攻撃を仕掛けた.UDPflood 攻撃はコネクションレス型の UDP の特徴を利用するもので, いきなり非常に大きなサイズの UDP パケットを大量に送りつける攻撃である. 逆に極端に短いパケット 長のデータを大量に送りつけることにより, ネットワークデバイスに負荷を掛けることができる [3]. また UDP はコネクションレス型なので送信元の IP の偽装が容易である.

3.2. 環境

信州大学は総合大学であり図 1 からもわかるように５つのキャンパスが長野県内の様々な場所に点在しており各キャンパスの通信が工学部に集まり総合情報センターからインターネットへと出ている. ネットワーク利用者の規模は学生, 教職員を含め 14369 人である [1]. これは小さな市町村の規模と同じである．そのため工学部では大量かつ多様な通信ログデータを採取することができる. ゆえに, 実験環境としては理想的である.

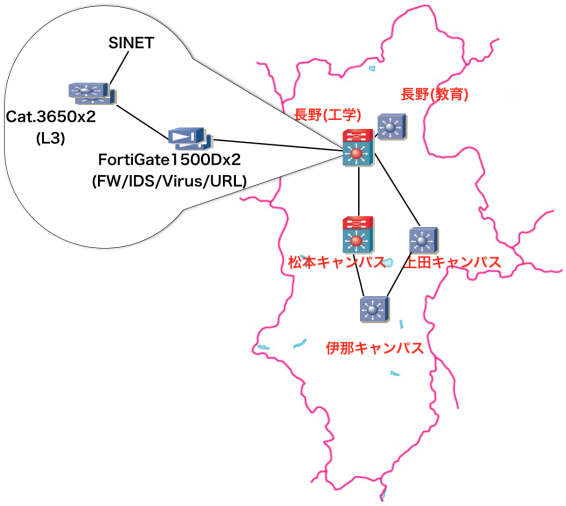


図 1: 信州大学のネットワークの形態

攻撃環境を構築する前にローカルな環境で DNS サーバの設定と攻撃が正常に行われるかの確認をした.DNS サーバの設定では意図しない外部との通信が行われていないか, また DNS サーバとしての機能が正常であるかの確認をした. 図 2 は信州大学総合情報センターに設

[1]信州大学 : 広報・刊行物 大学概要 2015

置した攻撃環境のイメージ図である.

図 2 からわかるように外部のネットワークから信州大学内部に設置した DNS サーバに UDPflood 攻撃を仕掛けた. 攻撃側の PC は信州大学ネットワークの内部に設置しても攻撃は可能であったが, 通常の攻撃は外部から行われるものと想定し攻撃の再現性を高くするため外部に設置した. 外部のネットワークからルータを通り,SINET のルータを経由し右の信州大学のネットワークへ入る. 信州大学のネットワークのルータを通り UTM を通過しサーバへとパケットが送られる. 解析にはこの時 UTM で記録された通信ログデータを利用する.

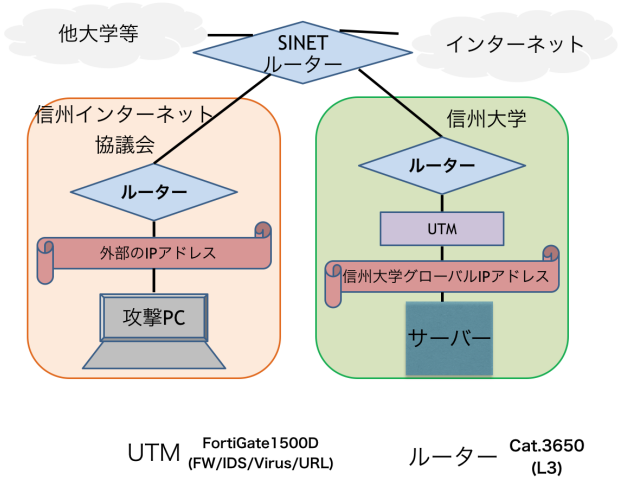


図 2: 信州大学総合情報センターに設置した攻撃環境のイメージ

また単一 IP アドレスからの攻撃であると UTM の機能で直ぐに攻撃が判別できてしまうため検証としては好ましくない. しかし,DDoS 攻撃に十分と言えるほどの大量の PC を用意することは難しい. そこで図 3 に示すパケット構造 [4] の送信元 IP アドレスを偽装するプログラムにすることで一台の PC で模擬的な DDoS 攻撃を再現した.

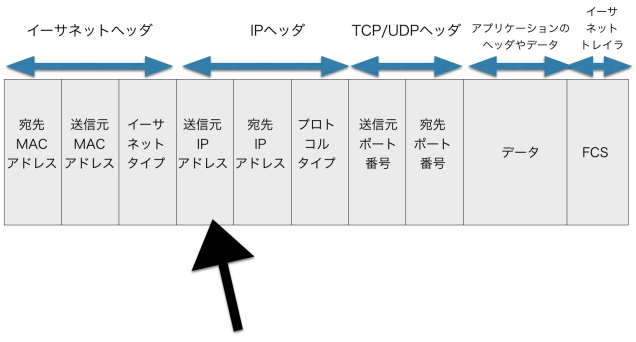


図 3: UDP パケット構造

4. 実験

4.1. 攻撃内容

IP アドレスの詐称はランダムなものを無数に設定することができるが今回は攻撃を検出する実験の際にどれが攻撃の通信かをわかるようにするために表 1 に示す 4 つにしぼり,IP アドレスを詐称し攻撃を行った. 実際に攻撃した日時と回数は表 2 に示す. 表 3 の UTM の性能 [5] にもある通り, ファイアウォールの同時セッション数は 12,000,000 である. しかし同時に 5,000,000 パケットの通信を発生させたところ UTM が停止してしまった. そこで攻撃で送るパケット数は,UTM が停止しないように設定した.
128.64.32.16,168.86.66.91,77.111.222.99,10.2.77.140

表 1: 設定した 4 つの詐称 IP

128.64.32.16
168.86.66.91
77.111.222.99
10.2.77.140

表 2: 試験攻撃を行った日時と回数

日付	時間	攻撃回数
2016/01/25	10:48:14	10,000
2016/01/26	00:11:59	20,000
2016/01/26	17:37:27	20,000
2016/01/26	18:34:47	4,000
2016/01/27	15:39:50	50,000
2016/01/28	02:26:45	100,000
2016/01/28	02:52:42	100,000
2016/01/28	03:11:45	65,000
2016/01/28	10:45:16	115,000
2016/01/28	15:03:58	115,000
2016/01/28	18:21:42	115,000
2016/01/29	21:25:20	110,000
2016/01/29	02:34:40	115,000
2016/01/29	23:18:29	115,000

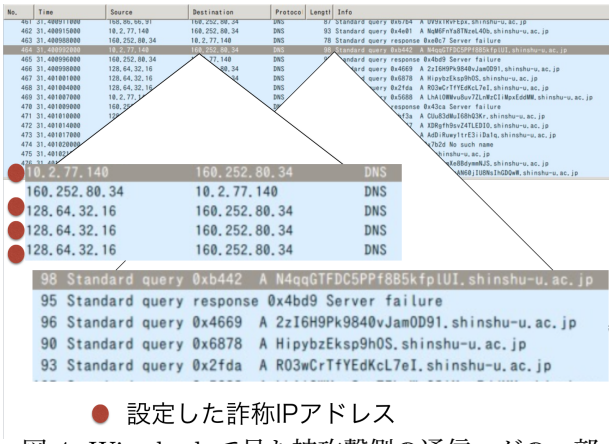
表 3: UTM(FortiGate-1500D) の性能

ファイヤーウォールスループット (1518/512/64 バイト UDP パケット)	80 / 80 / 55 Gbps
ファイヤーウォールスループット (1518/512/86 バイト UDP パケット)	80 / 80 / 55 Gbps
ファイアウォール同時セッション	12,000,000
ファイアウォール新規セッション/ 秒	300,000
ファイアウォール ポリシー	100,000

4.2. 結果

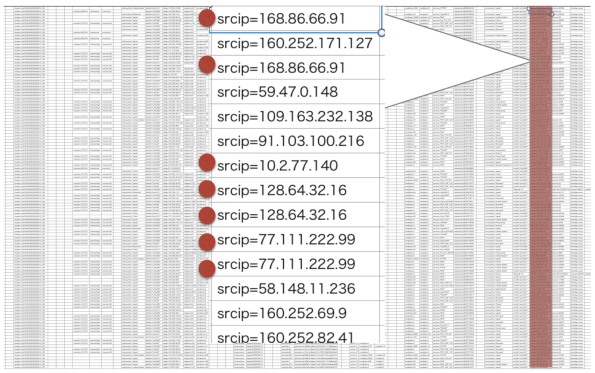
図 4 は,Wireshark で見た被攻撃側の通信ログである, 設定した攻撃 IP アドレスからの通信が記録されている

ことがわかる. 図 5 は UTM の通信ログの一部である. こちらも設定した攻撃 IP アドレスが記録されている.



● 設定した詐称IPアドレス

図 4: Wireshark で見た被攻撃側の通信ログの一部



● 設定した詐称IPアドレス

図 5: UTM に記録されたの通信ログの一部

また, 攻撃試験の最初の段階で大量のパケットを送ってしまった時 UTM が不安定になり機能が停止した. 攻撃としては成功と言える. 今回の実験で DNS サーバに攻撃を仕掛ける環境が構築された.

今回の研究とは直接関係は無いが,UTM が停止したことによって冗長構成になっているはずの UTM の切り替えがうまく機能していないという問題点がみつかった.

5. 評価と考察

攻撃としては UTM を停止させることができたので成功と言える. 模擬的な DDoS 攻撃を再現したが実際の攻撃に比べて同時に送られるパケットが少ないため, 複数の PC を利用した場合の DDoS 攻撃とは UTM の動作結果が異なる可能性がある. そのため, 実際の攻撃と今回の実験を比較をする必要がある. また攻撃の内容に関して今回は DNS サーバに対する UDP Flood 攻撃のみでの実験であったが, 他の攻撃環境の構築も考えている.

例えば [6] では http を用いた通信について,http session の通信タイミングを利用して攻撃の判定をしようとしている. この攻撃を再現するような環境を構築し, 比較研究できる環境を構築していくことで, データマイニングなどを用いた攻撃手法検出の研究をより広く実施できるようにしたいと考えている.

参考文献

[1] 久米原栄:TCP/IP セキュリティシステムアタックを防御するネットワークの構築と管理, ソフトバン ク パブリッシング, 2000

[2] 警察庁:Slow http DoS attack に対する注意喚起について; https://www.npa.go.jp/cyberpolice/detect/pdf/20151216.pdf,2015

[3] 警察庁技術対策課:DoS/DDoS 対策について; https://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf, 2003

[4] 荒井 透, 苅田 幸雄, 竹下 隆史:マスタリング TCP/IP 入門編 第 5 版; オーム社,2012

[5] Fortinet:FortiGate-1500D;http://www.fortinet.co.jp/doc/FGT1500DDS.pdf(最終確認日 2016 年 6 月 25 日)

[6] 林祐平, 西山聡史, 阪井勝彦, 鈴木昭徳, 工藤伊知郎:パケット連続到着時間を尺度とした攻撃検知法; 電子情報通信学会総合大会講演論文集 2016 年通 信 (2), 27, 2016-03-01

謝辞

本論文を作成するにあたって使用された UTM(統合脅威管理, Unified Threat Management) 装置による通信ログは, 信州大学情報総合センターの協力を得て取得致しました.