Computer Security Symposium 2018
22 - 25 October 2018

ユーザの行動履歴を考慮したDDoS攻撃加担対策手法の検討

高岡 奈央[1]　小林 孝史[2]

概要：DDoS（Distributed Denial of Service）攻撃の規模が年々増大している．近年では IoT 機器の増加やボットネットを形成するマルウェアの流行により，DDoS 攻撃に加担する機器が増加している．そこで我々は，DDoS 攻撃に加担している機器における正規ユーザの行動履歴を参照することにより，DDoS 攻撃に加担していると思われる不正な通信を検知する手法を提案する．ユーザの行動履歴として，マウスクリックやキー操作などのユーザの機器操作ログと，プロセスの起動ログ，機器から他の機器へ向けた通信のログを用いる．これらを分析することで，ユーザが意図した通信であるかどうかを判別し，意図しない通信である場合は不正な通信とみなす．実験では，機器の正常利用・悪意のあるプログラムによる利用時のシナリオを用意し，それぞれの場合による不正な通信の検知や，正常な通信の誤検知について検証を行なった．

キーワード：ネットワークセキュリティ，DDoS 攻撃への加担，通信検知，ユーザの行動履歴

DDoS attack participation countermeasure method considering user's behavior history

Nao Takaoka[1]　Takashi Kobayashi[2]

Abstract: The scale of DDoS attacks is increasing. In recent years, the number of devices participating in DDoS attacks are increasing due to the increase in IoT devices and the spread of malware forming botnets. Therefore, we propose a method to detect unauthorized communication which seems to be participating in DDoS attack by referring to the authorized user's behavior history of the device. As the user's behavior history, a device operation log such as mouse click and key operation, a process start log, and a log of communication from the device to another device are used. By analyzing these, it is judged whether communication intended by the user, and if not, it is regarded as unauthorized communication. In the experiment, we created two device usage scenario that normal and malicious, and verified unauthorized communication detection and false detection of normal communication in each case.

Keywords: Network security, Participating DDoS attack, Communication detection, User's behavior history

1. はじめに

DoS 攻撃とは，標的のサービスに多量の負荷をかけたり，脆弱性を利用したりしてサービス提供を不能な状態にする攻撃の総称である．近年流行している DDoS 攻撃は分散型であるため，攻撃元は複数存在する．Akamai の調査 [1] では，2017 年には携帯電話や IoT 機器などの新しい機器が膨大なボットネットを構成し，過去最大規模の DDoS 攻撃を引き起こしたことや，2018 年 2 月には 2017 年での膨大なボットネットによる攻撃の規模を上回る memcached リフレクター攻撃による 1Tbps の攻撃が観測されたことに触れられている．また，DDoS 攻撃の平均規模も調査現在では 1.3Gbps と以前に比べて拡大したことが報告されている．現在での DDoS 攻撃の主な攻撃元はボットネットを形成するマルウェアに感染した機器となっており，IoT の流

1 関西大学大学院
Kansai University Graduate School
2 関西大学
Kansai University

© 2018 Information Processing Society of Japan

行を伴ってボットネットを形成するマルウェアに感染した機器は年々増え続けている．DDoS 攻撃の対策として一般的に攻撃を受けているサービス側でトラフィック制御を行うことや，CDN の導入等が行われるが，根本的な DDoS 攻撃の減少には繋がらない．そこで我々は，ユーザの機器操作のログを用いて DDoS 攻撃に加担している機器内で悪性の通信を検知することで，DDoS 攻撃のトラフィック量を減少させることを目的とした研究を行う．

2. 関連研究

2.1 ユーザの振る舞いの特徴を用いてアプリケーションレイヤの DDoS 攻撃を検知する研究

Bravo らの研究 [2] では，ユーザのインタラクティブな機器操作イベントを参照することで，アプリケーションレイヤを対象とした DDoS 攻撃を検知する．Web を利用するユーザの振る舞いとしてマウス移動，マウスクリック，マウスハイライト，マウスでのドラッグアンドドロップ，マウスホイールのスクロール，キー押下を記録し，これらの動作がアクティブ状態でなかった場合は攻撃とみなす．攻撃とみなした場合は CAPTCHA による検証プロセスを作動させ，CAPTCHA の検証テストをユーザが解決できれば検証プロセスが停止するようになっている．提案手法の検証のために，一般的に用いられる DoS 攻撃ツール 3 種が攻撃ツールとして使用された．実験の結果，提案手法によってこれらの攻撃ツールの使用を 100 %検知することができ，また攻撃ツールの作動から攻撃を検知するまでの時間は平均 60 秒であり，その間に 4,000〜5,300 リクエストが攻撃の生成に使用された．

また，Xie らの研究 [3] では，アプリケーションレイヤの DDoS 攻撃の検知に着目し，拡張隠れセミマルコフモデルに基づいた Web ブラウジングの動作の特徴を取得する新規モデルが提案された．ここではユーザの正常性の判断基準として，モデルに適合するユーザの HTTP リクエストシーケンスのエントロピーが採用された．アプリケーションレイヤの DDoS 攻撃についてオンラインで検知する．

本研究では，アプリケーションレイヤの DDoS 攻撃だけでなく，その他のレイヤを対象とした Flood 型の DDoS 攻撃についても検知することを目標とする．

2.2 DDoS 攻撃の観測・分析についての研究

鉄らの研究 [4] では，IoT マルウェア検体をサンドボックス内で実行し，DDoS 攻撃の観測と分析が行われている．短期観測として 5 分間，長期観測として 240 時間の観測が行われており，短期観測を行なった 4,093 検体のうち 99.4 %にあたる 4,070 検体は実行後直ちに C&C サーバとの通信を試みるが，そのうち 1.6 %の 65 検体しか DoS 攻撃の命令を受け取っていないことが判明した．検体の 95.1 %は実際に DoS 攻撃の機能を有していた．長期観測の結果，C&C サーバとの接続を行おうとするが失敗し，3 日が経過した後に C&C サーバとの接続に成功し DoS 攻撃を開始した検体が 1 検体発見された．

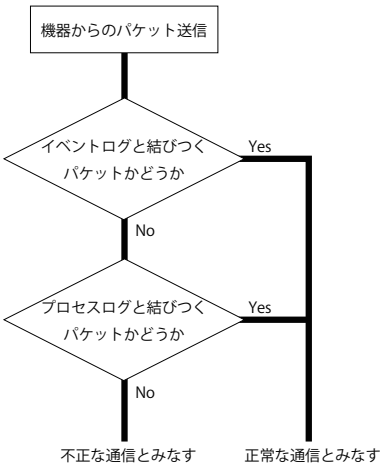

図 1 システムの流れ
Fig. 1 System flow.

本研究では，マルウェアが機器内に長期潜伏した後に DDoS 攻撃に加担する場合を考慮することを目指す．

3. 提案手法

3.1 概要

本研究では，マウスやキー押下などのイベントログや機器自体で正常に動作するプロセスのログを用いてユーザの行動履歴を分析することで，機器から発する通信がユーザが意図した通信であるかどうかを判断し，意図しない通信である場合は DDoS 攻撃への加担が疑われる不正な通信とみなす手法を提案する．イベントログやプロセスログを通信と結びつけることで不正な通信を検知することを目標とする．また，擬似的なシナリオを用いて本提案手法の検証を行う．本研究における通信の分析の流れを図 1 に示す．

3.2 イベントログ

ユーザが機器を操作する際に発生するイベントを syslog 形式で記録する．記録するイベントは，ユーザがマウスを左クリックした際のクリックログと，ユーザが Enter キーを押下した際のエンターログの 2 種類である．これらのイベントの取得には Linux Input Subsystem Userspace API[5] を用いた．また，それぞれのイベントを検知した際の時間を UNIXTIME. マイクロ秒形式で記録し，これを各イベントの識別子とした．記録形式を図 2 に記す．

3.3 プロセスログ

機器上にプリインストールされているソフトウェアのプロセスや，ユーザが意図してインストールしたソフトウェアのプロセスが他の端末へパケットを送信する場合がある．正常なプロセスのリストをあらかじめ取得しておき，正常

© 2018 Information Processing Society of Japan

```
Aug 18 23:33:11 localhost event_log[26892]: Click 1534602791.856777
Aug 18 23:33:14 localhost event_log[27054]: Enter 1534602794.758247
```

図 2 イベントログの例
Fig. 2 event log example

なプロセスが発していると思われる通信については正常な通信とみなす．正常なプロセスのリストの作成に Linux で主に用いられているプロセスアカウンティング機能である pacct を使用した．また，プロセスログには pacct の機能から dump-acct コマンドを使用してプロセスの起動時間を記録する．

3.4 パケットログ

本研究での提案手法の検証のために，ファイアウォールのログ機能を使用し機器が行なっている全ての通信を記録する．ファイアウォールには iptables を使用し，iptables の LOG モジュールを使用して送信する通信と受信する通信それぞれに prefix を付与してパケットのペイロード以外の情報を記録する．

3.5 パケットログへのイベント識別子の付加

上記のイベントログ，プロセスログ，パケットログを用いて各イベントと通信の結びつきについて検証を行った．検証のために簡易なシナリオを用意し，イベント発生後何秒間中の通信がイベントと結びつくものであるか検討する．

3.5.1 軽量な Web サイトを Web ブラウザで閲覧する

軽量な Web サイトである example.com（http://example.com）に Web ブラウザでアクセスし，その際の各ログについてグラフを描画した．グラフを図 3 に示す．また，アクセス方法として Web ブラウザの URL 欄に手打ちで URL を打ち込んだ．経過時間 4 秒ほどにあるパケットは Web ブラウザ上で以前開いていた Web ページが残っていた際のパケットである．

3.5.2 多数のコンテンツを有する Web サイトを Web ブラウザで閲覧する

多数のコンテンツを有する Web サイトとして，動画投稿・閲覧サイトである YouTube（https://www.youtube.com/）に Web ブラウザでアクセスし，その際の各ログの記録数についてグラフを描画した．グラフを図 4 に示す．また，アクセス方法として Web ブラウザの検索欄に YouTube と打ち込み，検索結果から YouTube にアクセスした．また，検証中にプロセスの起動が起こらなかったため，proc は描画されていない．

3.5.3 考察

図 3，図 4 から，イベント周辺にパケットが集中していることがわかる．特に，イベント発生直後 3 秒間ほどにパケットが集中しているように見え，イベントとパケット量の相関関係が推察できる．そこで，イベント発生後の経過時間を閾値として，各パケットにイベントの識別子を付与することで，イベントと関与のないパケットをユーザの意図しないパケットと想定する．評価実験では，イベント発生後の経過時間を N として検証を行う．

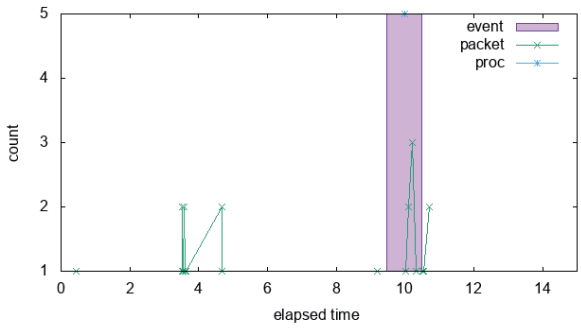

図 3 軽量な Web サイトを閲覧した際の各ログの記録数
Fig. 3 The number of records of each log when browsing a lightweight Web site

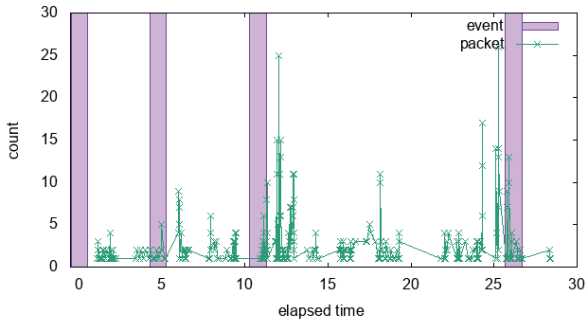

図 4 多数のコンテンツを有する Web サイトを閲覧した際の各ログの記録数
Fig. 4 The number of records of each log when browsing a website with many contents

4. 評価実験

本研究の提案手法について評価実験を行なった．実験環境として Virtual Box 上の VM 環境 CentOS 7 をインストールし，実験を行う前に正常なプロセスのリストを pacct のログ機能を用いて抽出した．前節での考察から，イベント発生後の経過時間 N を 3 として検証を行う．

© 2018 Information Processing Society of Japan

```
wget http://www.kansai-u.ac.jp
```

図 5　スクリプトの例
Fig. 5　script example

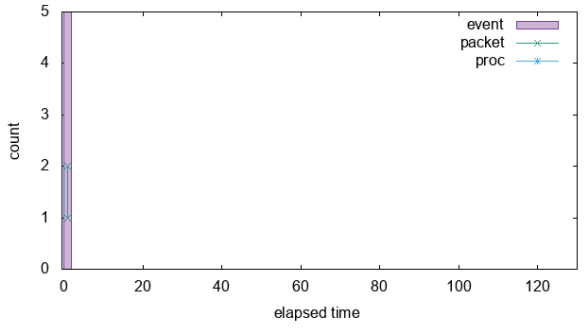

図 6　良性シナリオでの各ログの記録数
Fig. 6　The number of records of each log in benign scenario

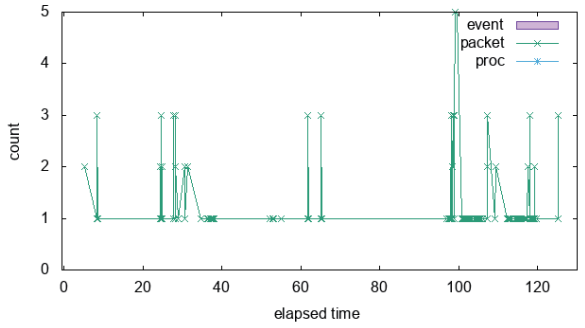

図 7　悪性シナリオでの各ログの記録数
Fig. 7　The number of records of each log in malignant scenario

4.1　良性シナリオでの実験

4.1.1　スクリプトを用いた検証

図 5 のようなスクリプトを用意し，これを正常なユーザが CLI 上で実行した場合のシナリオを検証した．関西大学の Web サイトを wget コマンドで取得するようなスクリプトである．検証結果のグラフを図 6 に示す．

4.2　悪性シナリオでの実験

攻撃者に機器に SSH ログインされ，不正なスクリプトを動作させられた場合のシナリオを検証した．そのシナリオとして，不正なスクリプト（図 5）を GitHib リポジトリからクローンするイベントを考える．検証結果を図 7 に示す．

5.　考察

良性・悪性どちらのシナリオでも同じスクリプトを使用したが，グラフではイベントの有無に差異の出る結果となった．しかし，悪性シナリオの実行時にユーザがアクティブな状態で他のプログラム等を使用している際は差異が現れにくいと考えられる．イベント発生後の経過時間 N を 3 とすると，良性のシナリオでは発生したパケットを正常なものとみなすことができると考えられる．今後ユーザがアクティブな状態での悪性シナリオでの実験を行ない，イベントに付与した識別子を用いた不正な通信の詳細な検知について検証を行なっていく．

6.　まとめ

本研究ではユーザの行動履歴に基づいて DDoS 攻撃への加担を検知することができるかの検証を行なった．今後の展望として，リアルタイムでの DDoS 攻撃への加担検知が挙げられる．また，検証対象として Linux 系の OS を使用したが，今後一般的に利用されている Windows や macOS でも検証を行なっていく．

参考文献

[1] Akamai，“State of the Internet / Security: Web Attack”，https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf，2018 年 8 月 19 日確認．

[2] Silvia Bravo, David Mauricio, “DDoS Attack Detection Mecanism in the Application Layer Using User Features”, IEEE International Conference on Information and Computer Technologies, 2018.

[3] Yi Xie, Shun-Zheng Yu, “A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors”, IEEE/ACM Transaction on Networking, vol.17, NO.1, february 2009.

[4] 鉄 穎，楊 笛，保泉 拓哉，中山 颯，吉岡 克成，松本 勉，“IoT マルウェアによる DDoS 攻撃の動的解析による観測と分析”，情報処理学会論文誌 Vol.59 No.5，pp.1321-1333，2018 年 5 月．

[5] www.infradead.org，“The Linux input driver subsystem”，http://www.infradead.org/mchehab/kernel_docs_pdf/linux-input.pdf，2018 年 8 月 20 日確認．

© 2018 Information Processing Society of Japan