ネットワーク型侵入検知システム 評価用データセットに関する一考察

インターネット上でのサイバー攻撃が頻繁に行われる今日，攻撃を防ぐための手法の開発は急務となっている．その中の一つに，ネットワーク上の通信データをもとにサイバー攻撃を検知するネットワーク型侵入検知システム (Network-based Intrusion Detection System: NIDS）がある．NIDS の研究では，開発した手法を評価用データセットを用いて，その有効性を評価することが行われている．本稿では，現在広く用いられている NIDS 評価用データセットを紹介し，その特徴について考察を加える．

高原尚志[†1]
新潟県立大学[†1]

A Consideration on Datasets for Evaluation of Intrusion Detection System

Hisashi Takahara[†1]
University of NIIGATA PREFECTURE[†1]

1. はじめに

近年，新たなサイバー攻撃が大量に生産され，インターネット上のコンピュータは日々攻撃を受けている．このような中，攻撃を防ぐための手法の開発が盛んに行われている．サイバー攻撃を防ぐための手法のひとつに通信データをもとに攻撃を検知するネットワーク型攻撃検知システム (Network-based Intrusion Detection System: NIDS)がある．NIDS の研究では，開発した手法を評価用データセットで評価するのが一般的である．本稿では，広く用いられている NIDS 評価用データセットを紹介し，その特徴について考察を加える．

2. 評価用データセット

NIDS 評価用データセットには，大きく分けて，通信データ(PCAP データ)をそのまま使用するデータセット（以降，PCAP 型データセットと称す）と通信データをセッション単位で加工して提供するデータセット（以降，セッション型データセットと称す）がある[1]．本稿では，PCAP 型，セッション型それぞれにおいて，広く用いられているデータセットについて紹介し，その特徴について考察を加える．

2.1 PCAP 型データセット

2.1.1 1998 DARPA Intrusion Detection Evaluation Data Set

1998 DARPA Intrusion Detection Evaluation Data Set(以降，DARPA98 と称す)[2]は，米国国防高等研究計画局（DARPA）と米国空軍研究所（AFRL）のもとでマサチューセッツ工科大学（MIT）Lincoln laboratory の The DARPA Intrusion Detection Evaluation Group が作成し配布した世界初の NIDS 評価用標準データセットであり，正常通信や攻撃の種類を示すラベルが付されている．

2.1.2 MWS データセット

日本でデータセットを配布している代表的な団体にマルウエア対策研究人材育成ワークショップ(MWS)[3]がある．MWS では，ポット観測データや研究者コミュニティから提供されたデータを「研究用データセット」として提供している（サイト[3]より引用）．

BOS 2014〜2017　総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験の請負」にて実施し，研究者コミュニティから提供された組織内ネットワークへの侵害活動を観測したデータ

FFRI Dataset 2013〜2017　株式会社 FFRI で収集したマルウェアの動的解析ログ

NICTER Dataset 2013〜2017　サイバー攻撃観測・分析・対策システム NICTER で収集したダークネットトラフィックデータ，メールサーバに届いたダブルバウンスメールのデータ

CCC DATAset 2008〜2013　マルウェア検体を収録したボット観測データ群であり，CCC 運営連絡会が運用するサイバークリーンセンターハニーポットで収集したマルウェア検体とウイルス対策ソフト 6 製品での検知名をリスト化したデータ

D3M (Drive-by-Download Data by Marionette) 2010〜2015　研究者コミュニティから提供された Web 感染型マルウェアデータ

NCD in MWS Cup 2014　MWS Cup 2014 会期中に収集したホワイトデータセット

†1 新潟県立大学
University of NIIGATA PREFECTURE

PRACTICE Dataset 2013　総務省「国際連携によるサイバー攻撃予知・即応に関する実証実験」（略称：PRACTICE）の挙動観察システムで，マルウェアを長期観測した際の通信トラヒック（マルウェア感染後の通信挙動）を示すデータ

PRACTICE (AmpPot) Dataset 2015　インターネット上のオープンなサーバ (DNS, NTP 等) を踏み台にして通信を増幅させることでサービス妨害を行う分散反射型サービス妨害攻撃 (DRDoS 攻撃) を観測したデータセット

上記のデータセットは，最新の通信データという意味で大変有用であるが，PCAP データのため，データごとに攻撃通信と正常通信を区別するのが難しく，ラベルが付されていない．そのため，以下の課題があると考えられる．

① 利用者によって攻撃通信と正常通信の評価が異なる

② ハニーポットによって収集されたデータをすべて攻撃通信として，正常通信は自組織のネットワークから収集することも多く見受けられる．この場合，通信環境が異なるネットワークからのデータが混在する状況となり，攻撃通信の特徴に基づいた判別か，ネットワーク環境の違いに基づいた判別かの区別がつきにくい

③ ②に関連して，正常通信として混在させた通信データは公開されていないことが多いため，②で用いたデータセットをもとに検証することは困難である

2.2 セッション型データセット

2.2.1 KDD Cup 1999 Data

KDD Cup 1999 Data（以降，KDD99 と称す）[4]は，NIDS 評価用データセットとして，現在でも世界で広く使用されているデータセットである．ACM(American Computer Machinery)の研究会である SIGKDD(The community for Data mining, data science and analytics)[5]が毎年開催しているコンテストである KDD Cup の 1999 年に開催されたコンテスト(KDD Cup 1999[6])に使用されたデータセットで，DARPA98 のパケットキャプチャデータをもとに，これをセッションデータに加工して，現在 University of California Irvine, Machine Learning Repository から公開されているデータセットであり，ラベルが付されている．KDD99 に関しては，データが古い，冗長的である，データサイズが大きいなどの欠点が指摘されている．このため，上記の欠点を修正した NSL-KDD dataset[7][8]が University of New Brunswick (UNB)の Canadian Institute for Cybersecurity (CIC)から提供されており，近年広く利用される傾向にある．

2.3 Kyoto2016 Dataset

Kyoto2016 Dataset[1][9]は，Kyoto2006+ Dataset[10][11]に改善を加え引き継いだもので，2006 年 11 月から 2015 年 12 月までに京都大学に設置されているハニーポットにおいて収集した通信データ（パケットキャプチャ形式）をセッションデータに加工したもので，Traffic Data from Kyoto University's Honeypots として公開されている[9][10]．各通信データは，KDD99 に準拠した 14 個の特徴量と独自の 10 個の特徴量からなり，攻撃通信と正常通信などのラベルが付されている．データの新規性，信頼性，他者による検証といった観点から，NIDS 評価用データセットとして非常に優れたものと考えられる．

3. まとめ

本稿では，NIDS の研究において重要な要素である，評価用データセットに注目して，現在広く利用されている評価用データセットを，PCAP 型とセッション型に分けて紹介し，その特徴について考察を加えた．この際，ラベルが付されていない場合の課題についても指摘した．

今後，本稿で紹介したデータセットを用いて NIDS の手法を評価して行く予定である．

謝辞

本研究は JSPS 科研費 JP17K00187 の助成を受けたものです．この場を借りて，感謝の意を表します．

参考文献

[1] 多田竜之介，小林良太郎，嶋田創，高倉弘喜, “NIDS 評価用データセット : Kyoto 2016 Dataset の作成,” 情報処理学会論文誌, Volume 58, No.9, pp1450-1463, (2017).

[2] “MIT Lincoln Laboratory DARPA Intrusion Detection Evaluation (online),” available from <https://www.ll.mit.edu/ideval/data/1998data.html> (accessed 2018-04-26).

[3] “マルウェア対策研究人材育成ワークショップ 2017 (MWS2017),” available from <https://www.iwsec.org/mws/2017/> (accessed 2018-04-30).

[4] “KDD Cup 1999 Data,” available from < http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (accessed 2018-04-26).

[5] “SIGKDD,” available from < http://www.kdd.org/> (accessed 2018-07-23).

[6] “SIGKDD KDD Cup 1999 Computer network intrusion detection,” available from < http://www.kdd.org/kdd-cup/view/kdd-cup-1999/Intro> (accessed 2018-07-23).

[7] “NSL-KDD Datasets Research Canadian Institute for Cybersecurity UNB (online),” available from < http://www.unb.ca/cic/datasets/nsl.html> (accessed 2018-04-26).

[8] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” *Proc. the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications* (CISA 2009), pp.53-58 (2009).

[9] “Traffic Data from Kyoto University's Honeypots (online),” available from <http://www.takakura.com/Kyoto_data/> (accessed 2018-04-30).

[10] Jungsuk SONG, Hiroki Takakura, and Yasuo Okabe, “Description of Kyoto University Benchmark Data (online),” available from < http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf> (accessed 2018-04-26).

[11] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, K. Nakao, “Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation,” Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS’11), pp.29-36. (2011).