社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－IOT－1 (18)
2008 / 5 / 9

パッシブスキャンによる中小規模LAN向けトラフィック分析システムの試作

薄田 昌広† 上田 達也‡ 上原 哲太郎§

†関西電力株式会社電力技術研究所 〒661-0974 兵庫県尼崎市若王寺 3-11-20
‡大阪市立大学大学院創造都市研究科 〒558-8585 大阪市住吉区杉本 3-3-138
§京都大学学術情報メディアセンター 〒606-8501 京都市左京区吉田二本松町
E-mail: †susukita.masahiro@d5.kepco.co.jp, ‡ueda@osaka-cu.ac.jp, §uehara@media.kyoto-u.ac.jp

あらまし TCP/IPによるLAN技術は広く普及しており、扱いも容易であるため、学校や中小企業のように組織内LANが十分に管理をされていない場合には管理者が意図しないような機器がユーザによって接続され、それらがセキュリティ上のリスクとなる場合がある。また、正規に接続された機器であっても、意図しない動作によって組織に被害を与える可能性がある。本論文では、LAN内のトラフィックを監視することにより各機器で用いられているOSやアプリケーションを網羅的に把握し、不正な機器や意図しない利用形態の機器を検出するシステムを提案し、試作した。

キーワード セキュリティ，ネットワーク，トラフィック解析，パッシブスキャン

A prototype of network-traffic analysis system for small and middle-scale LAN by passive scanning

Masahiro SUSUKITA† Tatsuya UEDA‡ and Tetsutaro UEHARA§

† Power Engineering R&D Center ,The Kansai Electric Power Co., Inc. 3-11-20 Nakoji, Amagasaki, Hyogo, 661-0974 Japan
‡ Graduate School for Creative Cities, Osaka City University 3-3-138 Sugimoto, Sumiyoshi-ku, Osaka, 105-0123 Japan
§ Academic Center for Computing and Media Studies, Kyoto University Nihonmatsucho, Sakyo-ku, Kyoto, 606-8501 Japan
E-mail: †susukita.masahiro@d5.kepco.co.jp, ‡ueda@osaka-cu.ac.jp, §uehara@media.kyoto-u.ac.jp

Abstract TCP/IP-based LAN technology is widely spread and it is quite easy to construct a network based on IP networking. Therefore it might be a risk on security when some machines without the administrators' intention are connected to the LAN when it is not managed enough like that of schools and small-to-medium-sized firms. Moreover, there is a possibility of damaging those organizations by the unintended behaviors of officially connected machines. This paper proposes a network-traffic analysis system which grasps the applications and operating-systems used on each machines on the LAN and detects illegally-connected machines and unintended usage of the machines.

Keyword Security, Network, Traffic Analysis, passive scan

1. はじめに

企業や学校などの各種組織において、情報機器をIPによるローカルエリアネットワーク(LAN)で接続した情報システムとして運用するということが一般的になって久しい。IPによるLAN構築は、コストが低く、設計が容易であり、拡張が容易でインターネットとの親和性が非常に高いというメリットがあり、利便性に優れている。ただし、一方では、システム管理者以外でも技術知識さえあれば不正な機器の接続や業務と関連のない利用などが容易であり、システムのパフォーマンスを低下させ、情報の不正な流通を起こすなどセキュリティ面での問題を抱えている。

システムを厳重に管理するソリューションは多数存在するが、導入や運用のコストも高く、中小規模の組織では広く普及しているとは言いがたい。また、LANに存在する機器を正確に把握するためのコストもかけられていない場合が多い。

本研究では、システム管理者がネットワーク内で利用されている情報機器およびOSやアプリケーションなどの利用形態を網羅的に把握し、管理者の意図しない機器や利用形態などの検出を支援するためのトラフィック分析システムの開発を目指す。

ネットワークに接続された情報機器を検索するための方式は大きく二つに分けられる。LANに検索のための通信を流してその応答を分析するactive scan方式

と、ネットワーク内のトラフィックを取り込んで分析することで情報機器を把握する passive scan 方式である。active scan 方式では短時間で情報を収集することが可能であるが、ワームやウィルスの感染の振る舞いと同様であるために応答を拒否する機器が増加しており十分な精度が得られなくなってきている。そのため、本システムでは、情報機器の把握のための手段として passive scan 方式を採用することとした。

2. 分析システムの構成

2.1. システム想定用途

本システムが対象としているネットワークは中小規模の IP ネットワークであり、情報機器は台帳などによる管理ができているが厳格な管理ではないため実態との差異が生じることがある。

また、本システムはリアルタイム監視を目的とするものではなく、トラフィックを中長期的に観測することで緊急性は低くても重要なセキュリティリスクに対応することを目的としている。具体的な用途として想定している例を以下に示す。

- 不正機器の利用
- 不正アプリケーションの利用
- 停止漏れ機器やサービス
- 業務内容と異なるアクセスや大量データ転送など
- OS の更新漏れ
- トラフィック想定の確認

2.2. システム利用形態

本システムはトラフィックデータを取得して分析するパッシブスキャン方式を採用している。そのためトラフィックの収集・蓄積機器であるプローブをネットワーク内に設置する。設置場所としては、例えば、ひとつのスイッチに収容されたフロア内部のトラフィックを分析したい場合には、そのスイッチで利用されているポートをデータ取得用のポートにミラーリングし、プローブへ接続する。あるいは、外部ネットワークとの接続点など 1 本のケーブル上のトラフィックのみを分析したい場合はケーブルを TAP にて分岐し、プローブへ接続することも可能である。

分析を行う場所については、このプローブ自体が PC をベースにした機器であるため、モニタとキーボードを接続すれば単体でトラフィック分析が可能であるが、遠隔地からの分析も可能とするために Web によるリモート分析機能を有している。

Web によるリモート分析については、トラフィック取得とは別の通信伝送路が必要となるが、トラフィック取得のためと別の伝送路へ接続可能なインターフェースを用意している。分析したいトラフィックへの影響をなくすため、理想的には完全に分離された専用の伝送路を利用することが望ましいが、実際にはそのような伝送路を用意することは難しい。ただし、スイッチなど一般のネットワーク機器には一般の情報機器とは別系統の管理用 IP アドレスが割り当てられていることが多く、ネットワークの上位が分離していることもあるのでその IP アドレス系統に所属させることで分析対象への影響を減らすことが可能となる。

3. システムの実装

3.1. ハードウェアおよび OS

ハードウェアとして特に重要な要件は、実時間によるデータベース構築ができるように高速な CPU を採用すること、大量のトラフィックデータを蓄積することができるように大容量の記憶媒体が利用できること、および高速ネットワークインターフェースを接続できることである。一方で、さまざまな場所で長期間稼動させることから、小型で駆動音が小さく、消費電力の少ないものを次の要件とした。

今回は Commell 社の組み込み PC 向け Mini-ITX サイズのマザーボードを採用し、AC アダプタ電源を採用し、3.5 インチ HDD が収容可能な小型ケースにハードウェアを収容した。

全体の構成は以下の通りである。

- CPU: Intel Celeron 1.4GHz
- Memory: 512MBytes(DDR2-400)
- Chipset: Intel 915GM
- Ethernet1: Marvell 8053 or Intel PRO/1000
- Ethernet2: USB-FastEther Adapter
- OS: FreeBSD 6.2

イーサネットはデータ取得用のギガビットイーサネットと Web 用のファストイーサネットの 2 種類あり、ギガビットイーサネットは性能比較のためメーカーの異なるものを採用し、どちらも 1 台につき 2 ポートを用意した。OS はネットワーク性能の安定性とネットワークツールの利便性から実績のある FreeBSD を採用している。FreeBSD の機能により、データ取得用の 2 つのポートをブリッジ接続することができ、イーサネット用タップでネットワークを分割した場合の上りと下りの両トラフィックをひとつのブリッジインターフェースにまとめられ、またプローブ自体をネットワーク機器の間に直接割り入れることも可能となっている。

3.2. トラフィック取得ツール

プローブでは通信パケットに対して複数のトラフィック取得ツールを組み合わせ、ログをデータベースに蓄積してゆく。個々のトラフィックツールについては後述するが、トラフィックの特徴を示すデータのみを保存し、通信内容本文は保存していない。データベースは高速性が特徴であるオープンソースのデータベース MySQL を採用している。

3.2.1. snort

snort はオープンソースのネットワーク型侵入検知システムである。本システムでは、通常の一般的なアプリケーションに対応する検出ルールセットを記述し、トラフィックがどのアプリケーションによるものかを判定するために snort を利用している。

3.2.2. p0f

p0f は TCP オプションなどの特徴を元に OS を同定するツールである。本システムでは p0f を改造し、結果をデータベースに書き込むようにしており、トラフィックを発生させた情報機器の OS を判定するために利用している。

3.2.3. TCPlogger

汎用キャプチャライブラリである libpcap を用いて独自に作成したツールである。すべての TCP セッションについて通信データ量や送受信 IP アドレスおよびポート番号を記録する。

3.3. Web インターフェース

データベースに記録されたトラフィックログは、Web 画面で対話的に分析することが可能である。分析のための動的な画面生成にはスクリプト言語である PHP で記述したプログラムを利用している。

3.4. 中長期トラフィック管理

通信本文を記録していない設計にはなっているが、記録領域には限りがありるためトラフィックログを無限に記録することは不可能である。試作したシステムは役 250GBytes の記憶領域があるが、トラフィック量の激しいネットワークだと 1 ヶ月の記録も不可能である。そこで、時間とともに段階的に集計していくことで中長期間のトラフィック分析を可能としている。具体的には 1 時間を単位として 1 日のトラフィックを日次集計し、1 日を単位として 1 ヶ月のトラフィックを月次集計している。日次集計は日付変更時、月次集計は月初に前日あるいは先月分に対してバッチ処理され、同時に不要なデータは削除される。

4. 複数ネットワークに対する同時分析

システムの特性上、ひとつのサブネット範囲であってったとしても、スイッチで分離される複数のネットワークに対してすべてのトラフィックを分析するためには複数のプローブが必要となる。しかし、ネットワーク内全体の IP アドレスの通信動向など、複数のプローブに蓄積したトラフィックデータに対しては同一の分析を行うことが多く、プローブごとに分析手順を繰り返すことは非効率である。そこで、本システムでは複数ネットワークからのトラフィックデータに対して同時分析を行う機能を付加している。

4.1. 機能設計の方針

同一の分析を複数のプローブのトラフィックデータに対して行う方法については大きく 2 種類に分けることができる。

(a)結果集約：分析のためにデータベースに対して発行する SQL をプローブごとに分散して発行して結果を集約

(b)データベース集約：それぞれのプローブからデータベースを集約しておいて全体データベースに対して分析

どちらの方式においても、プローブ間でデータ転送が可能であることを前提としている。

(a)の結果集約方式では、SQL コマンドを解釈し、それぞれのデータベースに分割した上で結果の集約が必要になり、制限も大きい。本システムでは複雑な分析にも柔軟に対応できるように(b)の集約データベース方式を採用した。ただし、前述のとおりデータの転送量が大きくなることが考えられる。そこで、オリジナルデータではなく日ごとに生成される 1 日の集計データのみを集約対象とすることとした。

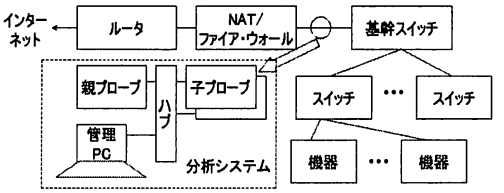
4.2. 機能の実装

プローブの中で、データの集約先を親、データの提供元を子として、親側から子に対してデータを要求する形で集約を行うように実装した。こうすることで親が複数の子からのデータ集約を容易に制御できるようにしている。転送手段としては、Web インターフェースで稼動している HTTP サーバを兼用しており、HTTP の手順に従ってプローブ間でファイル転送を行うしくみとなっている。この際、データ量の増加も考慮して zip による圧縮を選択できるようになっている。

5. 動作検証

5.1. 検証環境

図のような研究用の検証ネットワークにプローブを設置して動作検証を行った。検証ネットワークには約 100 台の PC が接続されており、NAT 兼ファイア・ウォールを介して外部にアクセスできるようになっている。アクセスのほとんどは Web の閲覧であることがわかっている。プローブはファイア・ウォールのすぐ内側に割り入れ、外部へ向かうトラフィックを分析した。データベース集約の検証のために同じ箇所に 2 台の子プローブを設置し、1 台の親プローブ、分析用 PC と共に独立した LAN を構成した。



5.2. 検証結果

通常業務期間 1 ヶ月分の日次集計データ量は約 3G バイトとなった。1 日あたり約 100MB のデータが集約されていることが確認できる。この間どのプローブもは正常に動作しており、zip 圧縮によるデータ集約も行われたことが確認できた。通信量の多い日を選んで圧縮効率を測定したところデータ量が約 1/4 に圧縮されており、圧縮機能の効果も確認できた。

また、いくつかの日について親プローブに対する Web 画面からの分析を実施したところ、すべての分析に対して子プローブ 2 台分の結果が得られていることから正しい集約が行われていることが確認できた。子プローブ 2 台ではイーサネットチップのメーカーが異なっていたが、データ取得に関しては 2 台の差異は認められなかった。

6. まとめ

中小規模の LAN を対象にした passive scan 方式のトラフィック分析システムを試作して検証を行った。このシステムではトラフィックを取得するプローブをネットワーク内に設置してリモートから Web インターフェースを用いて分析が可能となっている。また、複数のネットワークを同時に分析するためのデータベース集約機能をプローブに付加し、検証用ネットワークで正しく稼動することを確認した。

今後はさらに多くの実ネットワークで長期間の動作検証を行い、動作実績を積むことにより新たな知見を得ることを予定している。

文　献

[1] 薄田昌広、上田達也、上原哲太郎、“遠隔ネットワークセキュリティ評価システムの試作,” 電子情報通信学会技術報告、Vol.106,No.173, pp.19-24, 2006.

[2] 薄田昌広、上田達也、上原哲太郎, “中長期トラフィック分析による LAN 内端末検出システムの試作および評価, ” マルチメディア, 分散, 協調とモバイル(DICOMO2007)シンポジウム, pp. 671 – 676, 2007.

[3] Snort: the de facto standard intrusion detection/prevention. http://www.snort.org/

[4] P0F: Passive OS fingerprinting http://lcamtuf.coredump.cx/p0f.shtml

[5] MySQLAB: MySQL Homepage http://www.mlysql.com/