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

2006－ＱＡＩ－18（５）
2006／1／20

未利用アドレスブロックに到達するトラフィックの解析

鈴木 和也† 馬場 俊輔† 高倉 弘喜‡

†横河電機株式会社 セキュリティプロジェクト 〒180-8750 東京都武蔵野市中町 2-9-32
‡京都大学 学術情報メディアセンター 〒606-8501 京都市左京区吉田本町

E-mail: †(Kazuya.S,Shunsuke.Baba)@jp.yokogawa.com, ‡takakura@media.kyoto-u.ac.jp

あらまし ネットワークセキュリティにおいて,スキャン行為や DoS 攻撃などのネットワークトラフィックの異常を発生初期段階で検知することは極めて重要である．我々は,ネットワークのエンドポイントにセンサを設置するタイプのネットワークモニタリングシステムの研究開発を進めている．このシステムに到達するトラフィックを精査するための,トラフィックの分類法を提案し,実証実験を行った．分類方法としては,まずシステムのセンサに到着したパケットを単位時間Δt ごとに送信元 IP アドレス別にまとめ,これをひとつのイベントとみなす．このイベントをさらに解析し,送信先の IP アドレスが単一か複数か,さらには送信元,送信先のポート,さらには送信先ポートの組合せなどを考慮することで分類している．その結果,本提案の分類法を適用することで定常的に存在するトラフィックと未知のものを可能な限りリアルタイムに分離することが可能となったのでこれを報告する．

キーワード 未利用アドレスブロック，トラフィック解析，パケット監視

Analyzing traffic directed to unused IP address blocks

Kazuya SUZUKI† Shunsuke BABA† and Hiroki TAKAKURA‡

† Yokogawa Electric Corporation Security Project 2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750 Japan
‡ Academic Center for Computing and Media Studies Kyoto University Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501 Japan

E-mail: †(Kazuya.S,Shunsuke.Baba)@jp.yokogawa.com, ‡takakura@media.kyoto-u.ac.jp

Abstract In network security, it is very important to detect a security incident such as scanning activity, which often is a precursor to a DoS attack. We have developed a network monitoring system whose sensors are deployed at the endpoints of a network. To provide an understanding of the monitored network traffic, we classify various events by parameters observed from packets comprising a given event. For example, we use the Δt between packets, the number of unique source IPs, destination IPs as well as source and destination ports. In addition we also determine whether or not multiple source/destination IPs/ports occur in a sequence or appear randomly. Using this method we are able to quickly divide events into two primary classes, known events for which pre-defined actions may be taken and/or warnings issued and, suspicious events that may or may not be hostile but in ether case require further analysis.

1. はじめに

セキュリティインシデントの発生が増加している．JPCERT/CC[1]に報告されたセキュリティインシデントの数は，2002/10/01 から 2002/12/31 までは 439 件であったが，2005/07/01 から 2005/09/30 までは 667 件と増加している．最近のインシデントの発生状況，さらにワームの開発速度，伝播速度を考えると常にネットワークの状況を監視し，リスク状況を把握する必要がある．

インターネットのリスク状況を把握するためのシステムの開発が進んできており，日本国内のネットワーク観測システムには財団法人データ通信協会 Telecom-ISAC Japan[2]が運営している広域モニタリングシステム，独立行政法人情報処理推進機構セキュリティセンター[3]が運営している TALOT2，警視庁が運営している@Police[4]，有限責任中間法人 JPCERT コーディネーションセンター[5]が運営している ISDAS などがあり，海外でも Dshield.org[6]が運営している Distributed Intrusion Detection System，SANS[7]が運営している Internet Storm Center，CAIDA[8]が運営している Telescope Analysis，ミシガン大学[9]が研究開発している Internet Motion Sensor などがある．

このようなシステムを通してネットワークの状況を正確に把握することが期待されている．

2. 目的

ネットワークの状態を監視するには様々な技術が存在しており，現在主流となっているものは不正侵入検知システム(Intrusion Detection System)やトラフィックの状態を監視する MRTG(Multi Router Traffic Grapher)などであろう．侵入検知システムは，基本的にはシグネチャベースのシステムであり，既存のワームや攻撃などには有効であるが，未知の攻撃や攻撃の予兆，さらには準備行為等を検出するのは困難である．MRTG に代表されるトラフィックの状態を監視するシステムは，トラフィックの流量や遅延の計測が主な目的であり，微細な攻撃や初期段階の攻撃は通常のトラフィックに埋もれてしまい発見は難しくなってしまう．したがって，微細な攻撃，攻撃の予兆，さらには既存の攻撃ではなく未知の攻撃を発見するためには，トラフィック全体のみを監視するだけでなくパケットそのものも監視し精査する必要が出てくる．パケットそのものを監視する場合において，どこに監視ポイントを設置するのかが重要になってくる．バックボーンやゲートウェイなどの流量の大きいポイントを監視するには，大量のリソースが必要となってしまう．さらに各種法令により通信の秘密を守らなければならないため，バックボーンの監視には大きな制限がある．エンドポイントの監視であれば，通信の秘密に抵触しないとは言い切れないが，制約を受けがたい．したがって，今回の目的はエンドユーザと同じレベルのネットワークのエンドポイントにある未利用アドレスブロックを監視ポイントとし，この監視ポイントに到達するパケットの解析を行うことである．未利用アドレスブロックに到達するパケットは通常のアクセスにかかわるものではなく，間違いアクセス，ワーム，スキャンなどの異常なものとみなすことが可能である．この解析を行うことで，定常的にネットワークに存在しているトラフィックとそうでないものを分離することが可能となり，ネットワークの状態を正確に把握できる．

3. システム

3.1. システム概要

本システムの概要を図 1 に示す．本システムは複数のセンサと解析サーバから構成され，センサはネットワークのエンドポイントのエンドユーザと同じポイントで連続している未利用アドレスブロックに設置する．このポイントに到達するパケットを全てキャプチャし，解析サーバに転送する．この際，センサはアクセス元には一切の応答を基本的には返さないステルスセンサとする．未利用アドレスブロックにセンサを設置した目的としては前節で述べたように，このアドレスブロックには通常のアクセスが到達しないため，これらをトラフィックから分離する必要が無い．さらに複数のポートを同時に対してアクセスを試みるマルウェアのなかには，最初にアクセスしたポートから応答があると次のポートに対してアクセスしないものが存在する．通常のトラフィックを監視している限りにおいてはこの種のアクセスを検出することが不可能であるが，本システムのセンサは応答を一切返さないため検出可能である．ただし，ICMP Echo Request に関しては例外的に取り扱い，Echo Reply を返すようにした．これはマルウェアの中には ICMP Echo Request を送信し，応答があった場合に初めてスキャン行為を行うものが存在しており，これを検出するためである．単一ではなく連続したアドレスブロックにセンサを設置した理由としては単一ホストに対するスキャン行為と複数のホストに渡るネットワークスキャン行為の区別を計るためである．

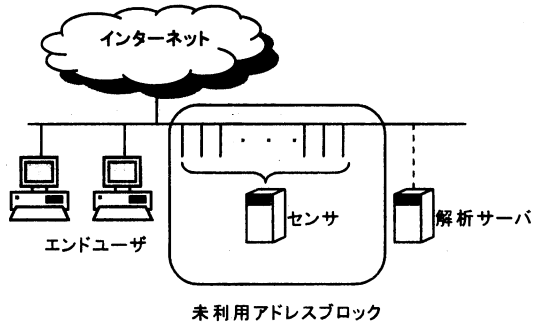

図 1 システム概要

3.2. システム構成

本システムのシステム構成を図 2 に示す．本システムのセンサは未利用アドレスブロックに到達するパケットをフルキャプチャして保存する．その後センサ側から解析サーバへデータを転送する．センサから転送されたデータは解析サーバのイベント生成モジュールに格納される．格納されたデータは後述する分類手法にて解析が開始される．まずイベント生成モジュールでインプットデータは後述する分類手法を用いてイベントに分割される．イベントに分割されたデータは，分類タイプ生成モジュールにてそのイベントがどの分類タイプに属するかの判定を受けて分類タイプが決定される．次にそのイベントに関する送信先ポートの組み合わせよりポートセットが決定される．イベント，ポートセットが確定した後，ログファイルに記録される．

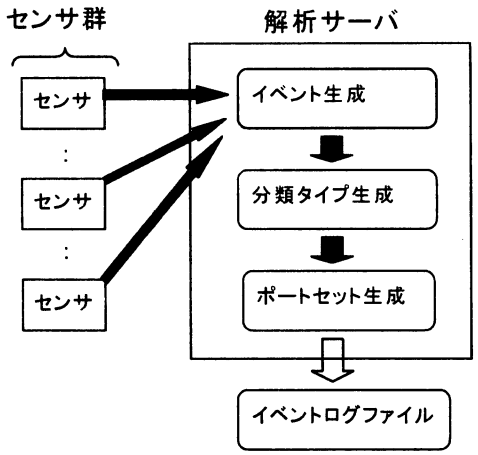

図 2 システム構成

4. 分類手法

4.1. イベント生成

イベント生成モジュールでは，センサに到達したパケットを送信元 IP アドレス毎に分類する．次にその送信元アドレスの一番始めに送信されたパケットから時間(Δt)以内に送信されたパケットまでをひとつのイベントとみなす．このΔtを 30 秒程度に設定することによりリアルタイムにネットワークの状況を把握することが可能となる．仮に時間をかけてゆっくりとしたスキャン行為が発生している場合，このスキャンはひとつのイベントに収束せずに複数のイベントにまたがってしまい，スキャンタイプに分類されなくなる恐れがある．しかし一連の分類が終了した後にこのイベント自体を再度解析する，つまりイベント同士の比較を行うことによりスキャン行為を検出することが可能となる．仮にΔt の値を大きくして分類を行うとこの種のスキャンは検出可能となるが，リアルタイム性が損なわれてしまう．

4.2. 分類タイプ生成

この前節で生成したイベントに属するパケットがどのようなアクセスをしているかを精査する．精査するパラメータとしては，イベントに属するパケットが複数である場合に

- 送信先 IP アドレスの種類数
- 送信先 IP アドレスが複数の場合，
  - ランダムアクセスか
  - シーケンスアクセスか
- 送信元ポートの種類数
- 送信先ポートの種類数

である．これらを考慮して表 2 のように分類を行う．

この分類法ではまず送信先ポートの種類数が単一か複数かでネットワークスキャン系とポートスキャン系に大別する．さらにネットワークスキャン系において，送信先アドレスの種類数が単一か複数かで分類を行う．仮に単一であった場合にはネットワークスキャンとは呼べないため，Normal タイプと Barrage タイプに分類を行う．また複数であった場合には，送信先アドレスがランダムなものになっているか，またはシーケンシャルなものになっているかで分類を行う．一方のポートスキャン系においても同様に送信先アドレスの種類数が単一か複数かでさらに分類を行う．単一であった場合には，通常のポートスキャンとみなすことができ，複数であった場合，つまり複数の送信先アドレスに対して複数の送信先ポートにアクセスするものはネットワークポートスキャンと分類する．

4.3. ポートセット生成

タイプの分類分けが完了した後，さらにこのイベントに含まれる送信先ポートをセンサに到達した順を考慮して，表 1 のようなポートの組合せ(ポートセット)を自動的に生成する．仮に tcp/135 にアクセスがあり次に tcp/445 にアクセスがあると，ポートセットは tcp/135:tcp/445 となる．ただし今回は到着した順番を考慮せずに生成を行った．本来なら，この逆の順番でアクセスがあった場合には，tcp/445,tcp/135 となり別のポートセットとみなすべきである．tcp/135:tcp/445 と tcp/445,tcp/135 は異なるイベントとして，このアクセス順をそのまま保持したイベントログに記録する必要がある．今後，同じイベントか異なるイベントかを判定して行くには，そのイベントに格納されたパケットの到着間隔などを調べればよいと思われるが今回は省略した．さらに UDP プロトコルの場合には略号 U を使用し，ICMP プロトコルの場合には I，TCP プロトコルで SYN フラグがたっている場合には S，SYN-ACK フラグがたっている場合には B，それ以外は O をポート番号に付記する．このポートセットは各イベントに関して自動的に生成するため，全ての組み合わせが自動的に生成される．

表 1 ポートセット

Number	Event
49	U/1434
23	S/445
1	B/2142:B/1697
1	B/4861
1	I/3
1	O/36684:O/45601:O/27243:O/46879
1	O/445

表 2 分類テーブル

		dstPort = 1		
		dstAddr = 1	dstAddr > 1	
			sequence	random
srcPort = 1	packet = srcPort	Normal 1	-	-
	packet > srcPort	Normal N (N > 2)	Network Scan 1	Network Scan 2
srcPort > 1	packet = srcPort	barrage 1	Network Scan 3	Network Scan 4
	packet > srcPort	barrage 2	Network Scan 5	Network Scan 6

		dstPort > 1		
		dstAddr = 1	dstAddr > 1	
			sequence	random
srcPort = 1	packet = srcPort	-	-	-
	packet > srcPort	Normal Port Scan 1	Network Port Scan 1	Network Port Scan 2
srcPort > 1	packet = srcPort	Normal Port Scan 2	Network Port Scan 3	Network Port Scan 4
	packet > srcPort	Normal Port Scan 3	Network Port Scan 5	Network Port Scan 6

(この表において使用している略号は,

- **dstPort**: 送信先ポートの種類数
- **dstAddr**: 送信先アドレスの種類数
- **srcPort**: 送信元ポートの種類数
- **packet**: パケット数

となっており，さらに

- **sequence**: 送信先アドレスが連続しているシーケンシャルアクセスパターン(インクリメント，デクリメント)
- **random**: 送信先アドレスが連続しておらず，ランダムなアクセスパターン

を考慮し分類を行う.)

4.4. イベントログファイル生成

前述したような手法を用いてイベントを精査し，その結果をイベントログに記録する．このとき 1 イベントを 1 行に表現し，各パラメータをデリミタで区切った csv ファイルに書き込む．この際のフォーマット例は以下のようになる．

フォーマット例.

イベント開始時刻,送信元 IP アドレス,国コード,プロトコル,分類タイプ,ポートセット

5. 観測実験

上記の分類手法を用いて実証実験を行った．実際に ISP 数社と ADSL 契約を結び連続した IP アドレスを複数個用意した．本システムの目的には複数のホストに対するネットワークスキャンと単一ホストに対するポートスキャンを区別することがあるためである．それぞれのネットワークに本システムのセンサを設置した．今回は各 ISP の監視対象 IP アドレスは平均 8 個とした．さらにネットワークの状況把握のために可視化を行った．これについては後述する．

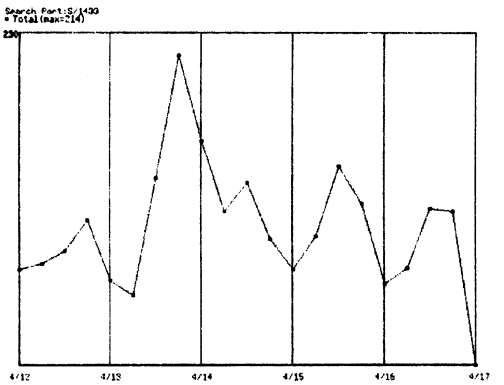

図 3 TCP/1433 に関する総アクセス数

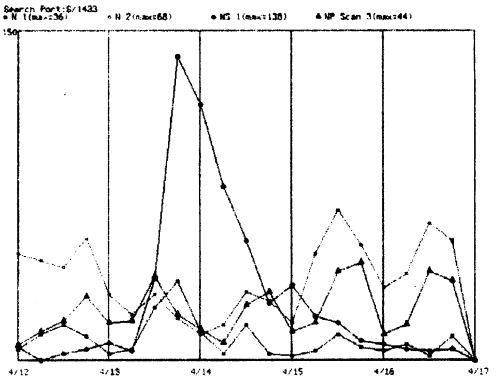

図 4 TCP/1433 に関する分類後のタイプ別グラフ

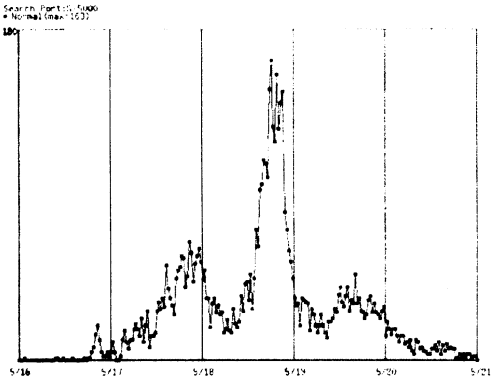

図 5 TCP/5000 に関する総アクセス数

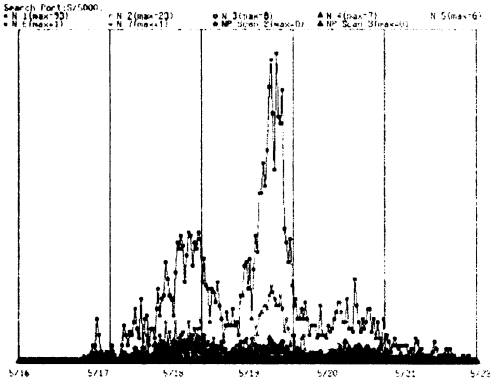

図 6 TCP/5000 のみの分類後のタイプ別グラフ

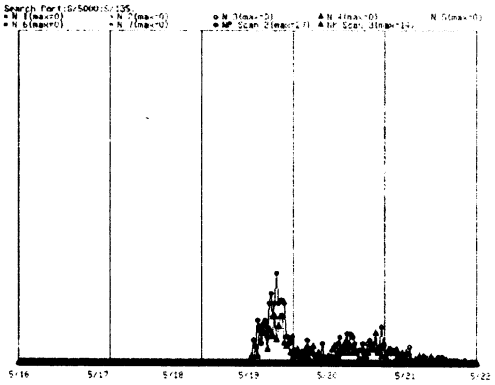

図 7 TCP/5000 と TCP/135 に関するタイプ別グラフ

6. 実験結果

TCP/1433 に関する観測結果を図 3，図 4 に示す．図 3 は TCP/1433 に関する総アクセス数である．また，このトラフィックに分類手法を適用したものが図 4 である．つぎに，TCP/5000 に関する観測結果を図 5–図 7 に示す．

6.1. 分類タイプに着目した観測結果

入力データには 2005 年 5 月に採取したパケットデータを採用し，TCP/1433 に関するトラフィックに着目した観測結果を示す．図 3 は TCP/1433 に関する総アクセス数をグラフ化したものであり，図 4 は入力データを分類しタイプ毎にグラフ化したものである．

6.2. ポートセットに着目した観測結果

入力データには 2004 年 5 月に採取したパケットデータを採用し，TCP/5000 に関するトラフィックに着目した観測結果を示す．図 5 は TCP/5000 に関する総アクセス数をグラフ化したものであり，図 6 は TCP/5000 のみに関するグラフである．そして，図 7 はポートセットに着目し，TCP/5000 と TCP/135 のセットに関するものを分類タイプ毎にグラフ化したものである．

7. 考察

7.1. 分類タイプに着目した観測結果に関する考察

図 3 を見ると 4/13 から 4/14 にかけて TCP/1433 に関する総イベント数が急激に増加している．このグラフだけをみると既存とトラフィックか未知のトラフィックかの区別がつかない．分類手法により分類タイプに区別した後にグラフ化した図 4 をみると，NS 1(Network Scan 1)が増加していることが分かる．これは symantec 社によると[10]digispida ワームであることが判明した．

7.2. ポートセットに着目した観測結果に関する考察

図 5 を見ると 5/18 から 5/19 にかけて TCP/5000 に関する総アクセス数が増加している．このグラフは TCP/5000 を含むイベント数に関するものであるが，TCP/5000 のみのタイプ別グラフが図 6 である．さらにポートセット TCP/5000,TCP/135 に関するものをグラフ化したものが，図 7 となる．図 6 に関しては Normal タイプのものが大半を占めているが，これは symantec 社によると[11], W32.Kibuv.B ワームであることが判明した．さらに図 7 に関する TCP/5000 と TCP/135 を同時にアクセスするものは symantec 社によると[12], bobax.c ワームであることが判明した．

8. 可視化

本システムのセンサに到達するパケットは，前述した方法でイベント化された後，分類が行われる．この結果をネットワーク管理者に効果的に見せるために，実験的に可視化を行った．図 8 に示すように，一画面を真中から 2 つに分割し，左側を送信側，右側を受信側とする．イベントから送信元ポートを抜き出しそれらの中の最小ポート番号，最大ポート番号を左画面の Y 軸の最大値と最小値とする．X 軸は同イベントの開始時刻と終了時刻とした．一方，右画面の Y 軸は送信先ポート番号の最大ポート番号と最小ポート番号とし，X 軸は送信先アドレスの最小アドレスと最大アドレス

とした．さらに描画する際にプロトコル別に色分けを行い，UDP プロトコルは赤色，ICMP プロトコルは白色，TCP プロトコルに関しては，SYN フラグが立っているものは青色，SYN-ACK フラグが立っているものは黄色，それ以外のフラグが立っているものは緑色にした．この描画手法を用いて各イベントを表現すると分類タイプ毎に特徴のあるグラフを作成することができ，発生しているイベントがどのようなものであるのかを素早く理解することが可能となる．例として分類タイプ Network Scan 5 を可視化したものを図 9 に示す．

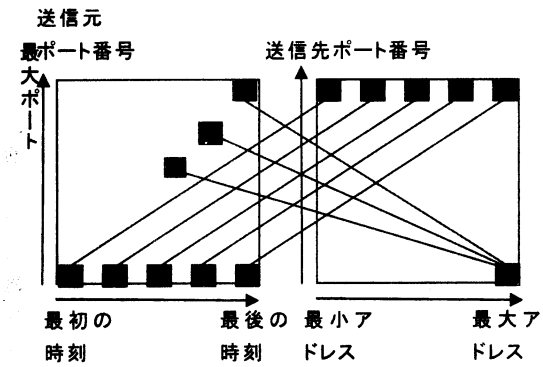

図 8 可視化用グラフの概要

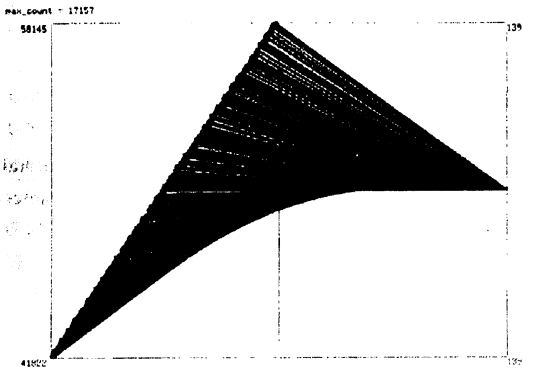

図 9 可視化例(Network Scan 5)

9. まとめ

本報告では，未利用アドレスブロックにセンサを設置し，このアドレスブロックに到達するトラフィックを分類し，既知のトラフィックと未知のものに可能な限りリアルタイムに分類できる可能性があることを示した．今後，ポート番号は同じだが順番だけが異なるポートセットの取り扱いに関して検証を進めていく予定である．現在は到着順に組み合わせを決定しているに過ぎず，この決定法が妥当であるとは言い切れない．この検証の目的としては，単にネットワークを通過する際に到着順が入れ替わったに過ぎないのか，本当にこの順に送信されたのかを確定させることである．これを確定できればさらに既知のものと未知のものに分離できる可能性がある．この検証を行うためにはパケットの到着間隔に注目し，その値の検証から開始する予定である．さらにセンサが監視しているアドレスの範囲の妥当性に関しても検証を行っていく予定である．

文　献

[1] http://www.jpcert.or.jp/stat/reports.html

[2] https://www.telecom-isac.jp/

[3] http://www.ipa.go.jp/

[4] http://www.cyberpolice.go.jp/index.html

[5] http://www.jpcert.or.jp/

[6] http://www.dshield.org/

[7] http://isc.sans.org/

[8] http://www.caida.org/home/

[9] http://ims.eecs.umich.edu/

[10] http://www.symantec.com/region/jp/sarcj/data/d/digispid.b.worm.html

[11] http://securityresponse.symantec.com/avcenter/venc/data/w32.kibuv.b.html

[12] http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.bobax.c.html

[13] 竹森敬祐他，“攻撃イベント数に関する調査および理論統計分布へのモデル化”，信学技報，NS2003-286，pp171-174，2004 年 3 月

[14] 及川達也他，“統計的クラスタリング手法によるネットワーク異常状態の検出”，信学技報，NS2002-143，pp83-88，2002-10

[15] Micheal Bailey et al., A Distributed Blackhole Monitoring System, Network and Distributed System Security Symposium Conference Proceedings: 2005, http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/ims-ndss05.pdf

[16] James Newsom , Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software, Network and Distributed System Security Symposium Conference Proceedings: 2005 , http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/taintcheck.pdf

[17] Sven Krasser et al., Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization , Proceedings of the 2005 IEEE Workshop on Information Assurance 、