様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年　6 月 13 日現在

機関番号：１７１０４
研究種目：若手研究（B）
研究期間：２０１０～　２０１１
課題番号：２２７００００７８
研究課題名（和文）　パケットモニタリングを用いた DNS トラヒック解析による異常検知に関する研究
研究課題名（英文）　Anomaly detection method based on packet monitoring by DNS traffic analysis
研究代表者
中村　豊（NAKAMURA YUTAKA）
九州工業大学・情報科学センター・准教授
研究者番号：４０３４６３１７

研究成果の概要（和文）：
ネットワークを安定運用するためには、ネットワーク異常の早期発見が必要となる。これまでにもネットワークの異常検知について､様々な研究がおこなわれている｡本研究では、ボット・ワームが利用する DNS トラヒックを考慮した DNS トラヒックの解析を行った。DNS トラヒックを解析することによりパケット内の詳細情報を取得することで、DNS プロトコルにおける異常トラヒックを検出することが可能となった。また、実際のネットワークにおいて提案システムを適用し、有効性を示した。

研究成果の概要（英文）：
To steadily maintain a network system, we need early detect an anomaly of the network. In this research, we analyzed DNS traffics used by bots and worms. By obtaining the detail information of DNS packets, we can detect the packets of the DNS protocol error. We also applied for this system to our campus network, and showed the validity.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,400,000	420,000	1,820,000
2011 年度	1,200,000	360,000	1,560,000
年度	0	0	0
年度	0	0	0
年度	0	0	0
総　計	2,600,000	780,000	3,380,000

研究分野：総合領域
科研費の分科・細目：情報学、計算機システム・ネットワーク
キーワード：DNS、異常検知、パケットモニタリング、トラヒック解析

１．研究開始当初の背景

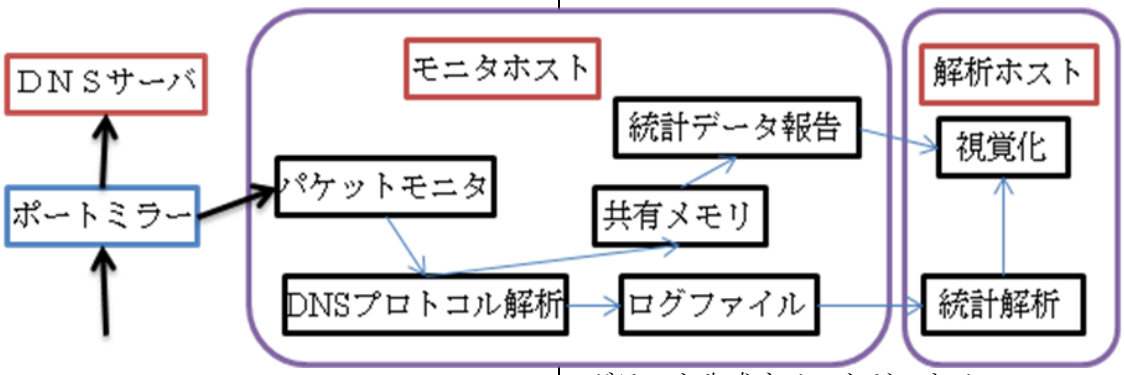
ネットワークを安定運用するためには、ネットワーク異常の早期発見が必要となる。これまでにもネットワークの異常検知について、様々な研究がおこなわれている。本研究ではボット・ワームが利用する DNS を考慮した､DNS トラヒックの解析を行う事で、ネットワークの異常を検出することを目標とした｡この課題を実現するために、本研究では以下の４項目について研究を進めた。

(1) パケットモニタリングを用いたトラヒック計測システムの構築
(2) DNS プロトコル解析システムの構築

(3) 視覚化システムの構築
(4) 実際のサイトへの適応

２．研究の目的
(1) モニタリング負荷を低減させるため、リアルタイム統計情報と、静的統計情報に分割することで、統計解析の負担とモニタリングの負担を低減することを目指している。また、全てのトラヒックを計測しないで、DNS トラヒックに限定することでログ出力の削減することが可能となる。
(2) (1)で得られたパケットを DNS の仕様に従い解析を行うことで、DNS パケット内の詳細な情報を得ることが可能となる。
(3) (2)で解析した結果を既存の視覚化ツールへの入力として与えることで実現できる。
(4) (1)～(3)までで構築したシステムを実際のサイトへ適応し、その有効性を示す。

３．研究の方法
　本提案システムの基本コンポーネントであるモジュール群の構成図を下に示す。ネットワークに流れる DNS トラヒックを収集し、蓄積・解析・視覚化の流れを構築する。



(1) パケットモニタモジュールの構築
　パケットモニタモジュールでは、DNS トラヒックのパケットを計測するために、Berkeley Packet Filter(BPF)を用いたパケットキャプチャライブラリを用いる。このライブラリを用いることによって、IP 層でのパケットが得られる。また、多くの UNIX プラットフォームで動作させることが可能となる。

(2) DNS プロトコル解析モジュールの構築
DNS プロトコル解析モジュールでは DNS パケット内のフィールド毎の解析を行う。このモジュールでは DNS ヘッダの各フィールドから query、reply 等の情報を取得する。プロトコル解析モジュールでは、まず QR フィールドを確認し、DNS パケットが query か reply であるかを確認する。Query であるなら、Opcode から問い合わせのタイプを確認する。また、再帰問い合わせかどうかの確認も行う。その後、QNAME, TYPE, CLASS フィールドから、query の内容を取得する。Reply の場合、RCode から応答のタイプを確認する。また、AA フィールドから権威付き応答であるかどうかも確認する。その後、NAME, TYPE, CLASS 等のフィールドより reply の内容を取得する。

(3) 視覚化モジュールの構築
視覚化モジュールは様々なデータを表示するためのプログラムである。データは統計データ報告モジュールに対してデータを要求することで統計データを取得する。このモジュールにより単位時間当たりの query/reply 数といった性能指標に関するグラフを生成することができる。

(4) 実際のサイトに適用する
　本学（九州工業大学）のキャンパスネットワークに本提案システムを適用し、実環境において本システムの有効性を評価する。

４．研究成果
(1)～(4) 下図に本学における提案システムを適用した出力結果の例を示す。下図に示されるように、DNS パケットの内容について詳細に解析することが可能となっている。また、

```
flags:8410 iplen:191 210.150.XXX.XXX 53 131.206.XXX.XXX 2547 len:171 id:4363 [r0A---10] qdcount:1 anc
ount:1 nscount:3 arcount:3 XXXXX.goo.ne.jp. qtype:0001 qclass:0001
AN answer_n:c0 XXXXX.goo.ne.jp. qtype:0001 qclass:0001 ttl:00000384 rdlength:0004 A 210.165.X.XXX
NS answer_n:c0 goo.ne.jp. qtype:0002 qclass:0001 ttl:00015180 rdlength:0010 NS XXXX.sphere.ad.jp.
NS answer_n:c0 goo.ne.jp. qtype:0002 qclass:0001 ttl:00015180 rdlength:0009 NS XXXX.goo.ne.jp.
NS answer_n:c0 goo.ne.jp. qtype:0002 qclass:0001 ttl:00015180 rdlength:0009 NS XXXX.goo.ne.jp.
AR answer_n:c0 XXXXX.goo.ne.jp. qtype:0001 qclass:0001 ttl:00000384 rdlength:0004 A 210.150.XXX.XX
AR answer_n:c0 XXXXX.goo.ne.jp. qtype:0001 qclass:0001 ttl:00000384 rdlength:0004 A 210.150.XXX.XX
AR answer_n:0  qtype:0029 qclass:1000 ttl:00008000 rdlength:0000 EDNS0
```

1 パケット内に複数の応答内容が含まれていることも明確となっている。
これらの結果を統計解析することにより、周期性を導出し、確率的に異常なトラヒックを分別することが可能となった。また、運用中のシステムを計測できる、計測システムがDNS サーバに影響を与えることはない、といった高い運用性を実現できた。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計　7 件）

① 佐藤彰洋、中村豊、池永全志、フローの特徴に基づく SSH 総当り攻撃の検出手法、電子情報通信学会 IN 研究会、2011 年 12 月 16 日、広島市立大学（広島）
② 中村豊、戸田哲也、反町祐司、技術職員向け講習会の実施、平成 23 年度　大学 ICT 推進協議会年次大会、2011 年 12 月 8 日、福岡国際会議場（福岡）
③ 佐藤彰洋、戸田哲也、福田豊、中村豊、キャンパスネットワークにおける IPv6 の導入とその課題、平成 23 年度　大学 ICT 推進協議会年次大会、2011 年 12 月 8 日、福岡国際会議場（福岡）
④ 東島慶、野林大起、中村豊、池永全志、阿部俊二、漆谷重雄、山田茂樹、多地点観測に基づくスキャン検知手法における候補リストの比較手法に関する検討、電子情報通信学会 2011 総合大会、2011 年 3 月 14 日、東京
⑤ 中村豊、戸田哲也、井上純一、福田豊、侵入検知とモニタリングシステムを組み合わせた異常トラヒックの自動保存、情報処理学会 IOT 研究会、2011 年 3 月 1 日、高知市文化プラザかるぽーと（高知）
⑥ 東島慶、野林大起、中村豊、池永全志、阿部俊二、漆谷重雄、山田茂樹、多地点観測に基づくスキャン検知手法の提案、電子情報通信学会 IA 研究会、2011 年 3 月 1 日、高知市文化プラザかるぽーと（高知）
⑦ 中村豊、戸田哲也、福田豊、対障害を考慮したキャンパス LAN の整備について、平成 22 年度　情報教育研究集会、2010 年 12 月 11 日、京都テルサ（京都）

６．研究組織
(1)研究代表者
中村　豊（NAKAMURA YUTAKA）
九州工業大学・情報科学センター・准教授
研究者番号：40346317