不正パケット遮断システムのホスト特定機能の工学部ネットワークへの適用

06T226 亀岡 志帆 （最所研究室）

本研究室では、不正パケットを発したホストを特定し遮断する、L2 スイッチを用いた不正パケット遮断システムの設計・開発を行ってきた。本研究では、このシステムを工学部ネットワークで実用化することを目標とし、遮断に至るまでのホスト特定機能を工学部ネットワークにおいて適用した。

1 はじめに

現在インターネットは、誰でも利用できるものとなり、知識の乏しいユーザも数多くいる。学校や会社のような組織的なネットワークにおいてもインターネットに接続されたコンピュータが多数存在し、情報流出の危険性が常に付きまとう。組織における情報の重要性は明白だが、不正アクセスやコンピュータウィルスなどにより、個人情報や機密情報を流出させている場合も増加しており、このような被害を防ぐため、ネットワーク管理者に大きな負担がかかっている。

このような問題を解決するため、侵入検知システム (IDS) を利用して不正パケットを送信したホストを特定し、Firewall とポート単位での制御が可能なレイヤ 2 スイッチ (L2 スイッチ) を組み合わせ、通信を遮断する不正パケット遮断システムの研究を行ってきた [1][2][3][4]。昨年度までに自動遮断・解除機能、ポリシ機能の実装までが行われてきたが、実用化には至っていない。

本研究は不正パケット遮断システムを工学部ネットワークで実用化することを目標としている。しかし、現在の工学部ネットワークでは全ての機能を実現できず、ま手違いで実ネットワークを止めてしまう可能性があるので、遮断に至るまでのホスト特定機能を適用し、ポリシ機能と警告メール通知機能も実装した。

2 概要

本システムの構成を図 1 に示す。昨年度までの研究では IDS を用いて不正パケットの検出を行っていたが、現在、工学部ネットワークでは Firewall からアラートメールが管理者に送られてくるので、そのメールを用いてホスト特定を行うことにした。

アラートメールを受信するとメールからアラート情報を解析し、ホスト特定機能によって不正パケット利用者および利用ポートを特定する。不正ホスト情報テーブルからそのホストの不正パケット利用状況を参照し、その情報と不正パケットのプロトコルや発信時刻を基に、ポリシ機能によりアラートレベルを決定する。その決定に基づき、警告メール送信機能によって管理者と利用者に通知を行う。

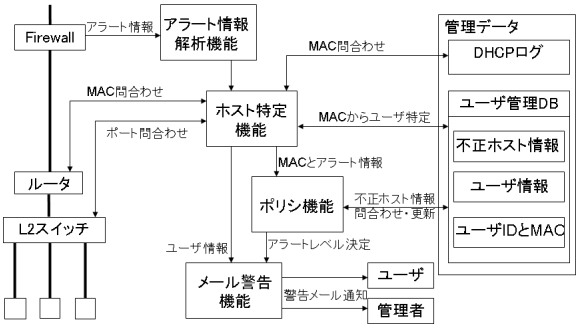

図 1: 本システムの構成

ホストを特定する際は、DHCP が持つ IP アドレスと MAC アドレスの情報や、ユーザ管理データベースの情報を用いる。

3 各機能の設計

3.1 アラート情報解析機能

Firewall によりサーバに送られるアラートメールから、ホスト特定やアラートレベルの決定に必要な、不正パケット検知日時、プロトコル、発信者の IP アドレス、受信者の IP アドレスを抽出する。

3.2 ホスト特定機能

アラート情報解析機能によって抽出した IP アドレスから、SNMP を利用してルータの ARP テーブルに問い合わせ、その IP アドレスに対応する MAC アドレスを取得する。さらに接続している L2 スイッチのポート番号まで調べる。ARP テーブルから MAC アドレスが特定できなかった場合、DHCP のログ情報を参照して MAC アドレスを特定する。

MAC アドレスが特定できれば、ユーザ管理データベースを用いてホストを特定する。予めユーザ ID とユーザの MAC アドレスを登録しておくことによりどのユーザかが分かり、さらにユーザ情報テーブルから連絡先等も取り出すことが出来る。

3.3 ポリシ機能

ポリシ機能では警告メールの送信判断を行い、アラートレベルを決定して、不正ホスト情報テーブルのアラート情報を更新する。

警告メールは、不正ホスト情報テーブルを参照し、最終検知日時から指定時間以上経過、または検知回数が指定回数毎であれば送信する。送信条件を満たした場合、最終検知日時からの経過時間、検知回数、プロトコルの危険度、前回までのアラートレベルを考慮して、アラートレベルを決定する。図 2 は、検知した動作パターンの一例である。

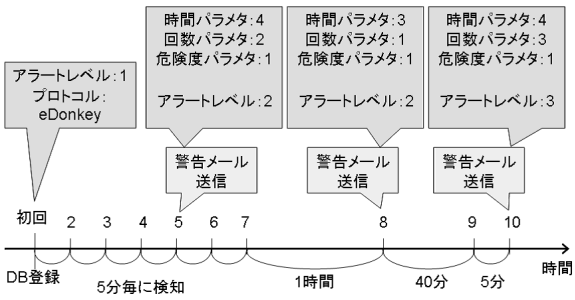

図 2: アラートレベルの変化例

3.4 警告メール送信機能

ポリシ機能によって警告メールの送信が決定された場合、決定したアラートレベルに応じてメールの宛先や本文を決定し、送信する。

メールの宛先は、本人と管理者から始まり、レベルが上がるにつれて直接指導にあたる教員（上司）、さらに上位の教員（上司）にも通知されるようになる。

メール本文には、ユーザ ID と時刻や回数などの検知情報、アラートレベルを警告文と共に記載し、第三者への通知前であればそれを報せることで、不正パケット利用を停止するきっかけとさせる。

4 実装と評価

Firewall から送られるアラートメールを模したダミーメールを送信し、システムの動作を確認した。ダミーメールの本文中には date=2010-01-29、time=20:20:20、proto=eDonkey、laddr=133.92.157.156、raddr=123.456.789.102 といった情報を含ませる。このダミーメールによるホスト特定の結果は図 3 の通りである。ホストの IP アドレスから MAC アドレスを正しく求めることに成功し、同時に L2 スイッチの接続ポート番号が特定されていることが分かる。また、これによってホストの受信した警告メールを図 4 に示す。警告メール送信機能も、正しく動作していることが確認できる。

```
==========================================
2010-01-29 20:20:20 proto=eDonkey
add=133.92.157.156 MAC=00 16 E3 17 7E 17
SW IP:133.92.157.2 PORT:8

add=123.456.789.102
==========================================
```

図 3: ホスト特定結果

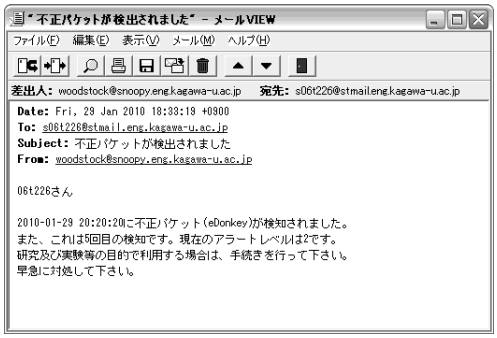

図 4: ホストの受信した警告メール

5 まとめ

不正パケット遮断システムの実用化に必要な、ホスト特定機能とポリシ機能、警告メール通知機能を実ネットワーク上で実現し、正常に動作することを確認できた。

現段階では実際に不正ホスト本人にメールを送るまでは至っていないが、ユーザ管理データベースのユーザ情報テーブルと uid_mac テーブルを作成すれば、運用することが可能である。

今後の課題として、自動遮断および遮断解除機能の実装や、管理のためのインタフェースの作成が挙げられる。

参考文献

[1] 高橋巧, “組織内における不正パケット遮断システムの運用ポリシ設計および実装”, 香川大学大学院工学研究科修士論文, 2007.

[2] 原田知拡, “不正パケット遮断システムにおける自動制御ツールの開発”, 香川大学工学部卒業論文, 2007.

[3] 岡原聖, “不正パケット遮断システムのユーザインタフェース開発,” 香川大学工学部卒業論文, 2007.

[4] 松木崇, “不正パケット遮断システムにおけるポリシ機能の実装と評価”, 香川大学工学部卒業論文, 2008.