5T－6

情報コンセントにおける認証とアドレス偽造防止機構の実現とその評価

阪本晃[1], 石橋勇人[2], 山井成良[3], 安倍広多[2], 大西克実[2], 松浦敏雄[2]
[1]大阪市立大学大学院 工学研究科, [2]大阪市立大学 学術情報総合センター, [3]岡山大学 総合情報処理センター

1 はじめに

最近、大学の図書館や情報センターなどに情報コンセントを設置し、利用者にネットワークアクセスサービスを提供する組織が増加している。このような環境では、利用者の特定が困難なため、悪意を持った利用者に不正利用される可能性がある。本稿では、このような不正利用を防止するシステムの実現方法とその評価について述べる。

2 不正アクセス防止方法

本稿において想定している環境では、利用者が所有する計算機を情報コンセントに接続し、動的にIPアドレスを受け取り、ネットワークにアクセスする。不正アクセスを防止するためには、正規の利用者のみが情報コンセントを使用して外部ネットワークにアクセスできるようにアクセス制御を行い、ネットワーク利用時に誰がいつどこからどのIPアドレスを使ってアクセスしたかを記録できることが必要である。そのためには、次の機能が必要となる[1]。

1. 送信元MACアドレス/IPアドレス偽造防止機能
2. アクセス制御機能
3. 利用者認証機能・アクセス記録機能

3 システムの構成

3.1 概要

LANAシステムは図1に示すように、LANAサーバ、LANAフィルタ、DHCPサーバ、RADIUSサーバ、VLAN機能付きスイッチングハブで構成される。利用者は所有する計算機を情報コンセントに接続し、DHCPサーバからIPアドレスを取得する。次に、LANAサーバとパスワードなどの認証用の情報の交換を行う。認証に成功するとLANAサーバは利用者計算機がバックボーンネットワークへアクセスできるようにハブとLANAフィルタの設定を行う。

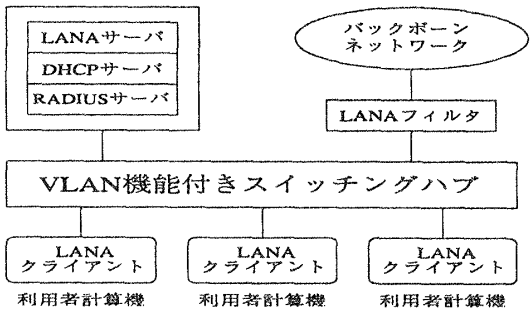

図1: システム構成

LANAサーバは利用者計算機のMACアドレス、IPアドレス、ハブのポート番号の3つ組を管理しており、認証された利用者計算機からのフレームのみがバックボーンへ出ていけるように制御している。実現方法としては、ハブのMACアドレスフィルタ機能を使う方法とIEEE802.1Qに基づくVLANタギング機能を使う方法がある[2]。前者の場合、利用者計算機を情報コンセントに接続した後にはMACアドレスを変更できないようハブのフィルタを設定することによって、ハブの接続ポートと利用者計算機の対応を固定する。そのため、なりすましによる不正アクセスは行えない。また、後者の場合は、それぞれのポート毎にユニークなVLAN IDを割り当てることによって、利用者の計算機が送信するフレームとVLAN IDとを対応づける。VLAN IDは利用者が偽造することが不可能なため、なりすましによる不正アクセスは行えない。

3.2 LANAフィルタ

本稿ではLANAフィルタの性能を中心に評価するため、特にLANAフィルタについて説明する。LANAフィルタはスイッチングハブとバックボーンネットワークにそれぞれ接続され、ルータとして動作する。また、LANAフィルタはフィルタリング機能とアクセス記録機能を持っている。現在は、FreeBSD4.0-CURRENT上でBPF(Berkeley Packet Filter)を用いてユーザレベルプロセスの形で実装している。

3.2.1 フィルタリング機能

LANAサーバによって指定されたフィルタリング条件に基づいて、フレームを選択的に中継する。フィルタ

Implementation and Evaluation of an Authentication/Spoof-protection System for LAN Sockets
A.Sakamoto[1], H.Ishibashi[2], N.Yamai[3], K.Abe[2], K.Onishi[2], T.Matsuura[2]
[1] Graduate School of Engineering, Osaka City University, [2] Media Center, Osaka City University, [3] Computer Center, Okayama University.

リングの条件には不正防止のために必須なもの(送信元IP/MACアドレス、VLAN ID)と管理上設定可能なオプショナルな条件とがある。後者のフィルタリング条件はあらかじめC言語による関数としてクラス毎に作成しておく。LANAサーバは利用者のIDに基づいてクラスを決定し、LANAフィルタに通知することによって利用者クラスに基づくアクセス制御を実現している。

3.2.2 アクセス記録機能

LANAフィルタでは、通過するすべてのフレームをチェックすることが可能であるため、各種のアクセス記録が可能である。現在はTCPセッションのポート番号、開始/終了時刻、利用者IDについて記録している。

4 評価

4.1 フィルタリングの性能

LANAフィルタの性能を評価するために以下の3通りについて実験を行った。

CASE1 すべてのネットワークサービスを利用できる利用者クラス

CASE2 特定のメール・ニュースサーバ、WWWプロキシサーバ、学内へのtelnet、及び、ネームサーバへのアクセスは通し、それ以外は破棄する利用者クラス

CASE3 LANAフィルタを使わずにカーネルでパケットを転送した場合

実験は、利用者計算機とバックボーンネットワーク上に他のルータを介さずに接続された計算機との間で行った。LANAフィルタを動作させた計算機のCPUはIntel社製のCeleron 400MHzのものを使用し、それぞれの計算機とスイッチングハブは100BaseTXで接続している。受け取り側のバッファサイズ64kB, 転送したパケットのサイズ8kB, 測定時間10秒という条件の下で、netperf[3]を用いてネットワークスループットの測定を行った。測定結果(10回の平均)を表1に示す。

表1: LANAフィルタのスループット

	TCP Throughput[Mbps]	UDP Throughput[Mbps]
CASE1	69.6	94.7
CASE2	65.3	95.0
CASE3	63.0	95.1

TCPにおいてCASE2はCASE1よりも複雑なフィルタリング処理をしているため、CASE1に対して6.2%性能が低下している。また、UDPにおいてはほとんどその影響が現れていない。TCPにおいてCASE3が他の2つの場合よりも性能が落ちている理由は、LANAフィルタではTTL(Time to Live)の減算を行わないなど、ルータとしての機能の一部を省略しているためと考えられる。

4.2 アクセス記録機能のオーバーヘッド

アクセス記録機能のオーバーヘッドを測定するために、利用者計算機とLANAフィルタのバックボーン側に直接接続された計算機との間でTCP接続/切断に要する時間を測定した。測定を1万回行った平均値では、アクセス記録を取った場合は2.4[ms]、取らない場合は2.2[ms]であった。したがって、オーバーヘッドは1コネクションあたり9.1%である。

4.3 単位時間あたりの接続処理能力

MACアドレスフィルタ機能を使う方式の場合、スイッチングハブにおいてVLANの切り替えなどの設定をする操作はクライアント毎に排他的に実行する必要がある。このため、排他処理によって時間的制約が生じる。1つのクライアントが認証に成功するまでに必要なハブの設定時間は約0.97秒であり、1秒間に1クライアントの接続処理を行うことができることになる。ただし、これは1つのハブにおける時間的制約であり、また、同時に接続要求が発生する場合のことであるので、実際に問題となることはほとんどないと考えられる。

5 おわりに

本稿では，情報コンセントにおいて利用者の認証を行い，IPアドレスおよびMACアドレスの偽造防止を実現するシステムLANAの実現方法、ならびに、その評価実験の結果を示した。実験の結果、LANAフィルタによるネットワークのスループットの低下は軽微なものであり、実用上差し支えない性能を発揮できることが確認された。

参考文献

[1] 山井 他: 情報コンセントに接続された計算機に対するMACアドレス/IPアドレスの偽造防止手法, 情処シンポジウム CSS'98, pp.141–146, 1998.

[2] 石橋 他: 情報コンセントにおける認証とアドレス偽造防止をVLAN機能により実現するシステムLANA2, 情処研報 99-DSM-14, Vol.99, No.56, pp. 137–142. 1999.

[3] R. Jones, K. Choy, D. Shield, Netperf:A Network Performace Benchmark, http://www.netperf.org/