4F−4 侵入追跡システムIDAにおけるインターネット侵入追跡手法の検討

井上 直[1], 女部田 武史[1], 岡澤 俊士[2], 浅香 緑[1]
情報処理振興事業協会技術センター[1], (株) 日本総合研究所セキュリティ事業推進部[2].

1 はじめに

ネットワーク侵入検出システムIDA[1,2,3]は踏み台アタックの侵入源を見つけるためのLAN上の侵入追跡をモバイルエージェント(D'Agents[4])を用いて実現している。しかし現状のIDAではIPアドレスのみによって侵入追跡を行うため、ファイアウォールなどで保護されたLANへインターネットを介して追跡することはできない。つまり現在のIDAが侵入追跡をするためには侵入追跡対象のLAN上のホストが直接アクセス可能であることが必要になる。IDAにインターネット上の追跡機能を加えるためにはなんらかの工夫をする必要がある。今回はそのための一手法を提案する。

2 現在のIDAの侵入追跡

現在のIDAのLAN上の侵入追跡は次の様に行われる。

1. あるホストで侵入行為が発見される。
2. 侵入行為が発見されたホストにモバイルエージェントが派遣される。
3. モバイルエージェントは侵入行為が発見されたホストのログを調べて、侵入源のホストであるかを判定し、侵入源である場合は追跡を終了する。侵入源でない場合は侵入元のホストを特定する。
4. 侵入元ホストへモバイルエージェントが移動する。
5. 3.へ戻る。

実際の侵入追跡はIPアドレスに基づいて行われる。この事がインターネット、特にインターネットに接続されファイアウォールなどで保護されたLAN内のホストに侵入追跡を行う際に問題となる。この問題はモバイルエージェントによる追跡が原因ではなくIPアドレスに基づく追跡から生じるものである。よって以降は追跡手段をモバイルエージェントに限定することなく一般的に考察する。

3 インターネット上の侵入追跡の問題点

ここでは現在のIDAで侵入追跡を阻害する主な技術を2つ述べる。

- **ファイアウォール**
  インターネットに接続されたLANを守る基本的な手法。パケットフィルタリングによってネットワーク経由のアクセスを遮断する。
- **ネットワークアドレス変換(NAT)**
  少数のアドレスを多数のホストで使いまわすための手法。使用できるグローバルIPアドレスが少ない場合によく使用される。内部ネットワークの隠蔽を目的として使われることもある。

他にも代理サーバ経由のアクセス、動的IPアドレス割当(DHCP)などもIPアドレスによる侵入追跡の障害になるがここでは詳細は述べない。

3.1 ファイアウォールがある場合

侵入元のホストがファイアウォール内部にある場合は、ファイアウォールがパケットのフィルタリングを行うため侵入元のホストに侵入追跡に必要なアクセスができない。そのため現状のIDAではファイアウォールから先は侵入追跡が行えなくなる。

3.2 ネットワークアドレス変換されている場合

ネットワークアドレス変換(NAT)が行われている場合では、侵入のためのアクセスの経路上のNATルータ(実際にアドレス変換を行うルータ)でパケットのソースアドレスが侵入元のホストのIPアドレスからNATルータのIPアドレスに変換される。そ

A Study of IDA's Intrusion Route Tracing Method on Internet
Tadashi Inoue[1], Takefumi Onabuta[1], Shunji Okazawa[2], Midori Asaka[1]
Information Technology Promotion Agency[1], The Japan Research Institute, Limited[2]
Bunkyo Green Court Center Office. 2-28-8. Honkomagome. Bunkyo-ku. Tokyo 113-6591. Japan

のため侵入されたホストからは NAT ルータから侵入された様に見える。以上の理由から NAT が導入されているLANで侵入追跡を行うことはできない。また現状のIDA にはIPアドレスが変換されたホストを追跡する機能はないため、たとえ NAT ルータに IDA が導入されている場合でも NAT ルータから先に侵入追跡する事はできない。

4 代理サーバを用いた侵入追跡手法

以上の理由からインターネット上の侵入検出のため、LAN の侵入追跡を代理するサーバを用いて IP アドレスのみによって侵入追跡する手法を考案した。

- LAN の侵入追跡の代理をするサーバをインターネット側から見える場所に置き、外部からの侵入追跡リクエストは全てこのサーバで処理する。
- この侵入追跡代理サーバに LAN 内のアクセス情報を置く。
- 外部からの侵入追跡リクエストは、LAN 内にアクセスせず、外部から見える代理サーバに集められたアクセス情報だけで侵入判定する。
- 外部からの侵入追跡リクエストは代理サーバの情報によって追跡先の LAN が侵入源であるかどうかを判定し、もし侵入源であるなら追跡を終了し、侵入源でないなら追跡を続行する。

LAN に外部からのモバイルエージェントを受け入れる事は危険である。またモバイルエージェントそのものを代理サーバが LAN 内の別のモバイルエージェントを仲介し協調して侵入追跡を行うという手法も考えられるが、セキュリティ面の不安が大きい。そのため今回は外部の代理サーバに LAN のアクセス情報を集める手法を提案する。

この手法の実現には解決すべき以下の 3 つの問題点がある。

- どのように侵入先 IP アドレスに対応する侵入検出代理サーバを見つけ出すのか。
- どのように代理サーバ同士で侵入追跡情報をやり取りするのか。
- どのように侵入検出代理サーバへの内部ネットワークのアクセス情報の集め、どのように保護するのか。

以下、各問題についてどのように解決するか述べる。

4.1 侵入検出代理サーバの検索

IDA は侵入追跡を行うためそのサイトの IDA がインストールされている全てのホストを記録する必要がある。これにならって、IP アドレスの範囲に対応する侵入検出代理サーバをあらかじめ登録しておく。これでは不便なので、実用にするためには DNS のような仕組みが必要である。

4.2 代理サーバ同士の通信

通信プロトコルを決め、なんらかのアクセス認証方式を導入する必要がある。モバイルエージェントを利用するならばIDA の方式を拡張し対応できる。

4.3 アクセス情報収集と内部情報の保護

内部ネットワークのアクセス情報を、外部からアクセス可能な侵入追跡代理サーバに置く方式が必要となる。Syslog を用いて必要なログを外部に置く事で対応する。ただし、これでは侵入追跡判定に必要のない情報まで外部からアクセスできる場所に置かれてしまうので、外部に出す侵入追跡に情報の削減とその情報を保護する仕組みが必要である。

5 おわりに

ファイアウォールなどで守られた LAN に対して外部から侵入追跡を行う手法について検討した。実際にネットワーク侵入検出システム IDA に組み込む事を目標としてここで提案した手法を改良していく。

[参考文献]

[1] http://www.ipa.go.jp/STC/IDA/

[2] 浅香 緑「モバイルエージェントによる侵入検出システムのための情報収集方式」,電気情報通信学会論文誌 Vol.J81-D-I No.5 pp.532-539 (1998)

[3] M.Asaka,M.Tsuchiya,T.Onabuta,S.Okazawa, and S.Goto, "Local Attack Detection and Intrusion Route Tracing",IEICE Transaction on Communications,Vol.E82-B No.11 pp1826-1833,November 1999.

[4] http://agent.cs.dartmouth.edu/

[5] R.Gray,D.Rus,andD.Kotz,"Transportable information agents",TR96-278, Department of Computer Science,Dartmouth College