おとり誘導による不正アクセス対策システム*

2H－04

藤井 誠司、大越 丈弘、河内 清人、北澤 繁樹、勝山 光太郎、芦沢 賢、木下 洋輔[1)]
三菱電機(株) 情報技術総合研究所[2)]、三菱電機(株) 通信機製作所[3)]

1. はじめに

近年増加しているインターネットにおける組織内ネットワークへの不正侵入やシステムの破壊などの犯罪行為に対する対策技術のひとつとして、おとりシステムが注目されている。おとりシステムは外部のネットワークに、計算機またはサービスを公開し、不正アクセスを試みる攻撃者の挙動を記録する。記録された挙動から、不正アクセス手法の解析などを行う。

現在、我々はおとりを利用した不正アクセス対策システムを検討している。検討中のシステムは、動的に不正アクセスをおとりサーバへ誘導する機能[1]、ネットワークおよび計算機上でのログから攻撃元を追跡する機能[2]を提供することを特徴とする。

本稿では、おとりシステムの利用について検討を行い、おとり誘導による不正アクセス対策システムを実現するための課題および検討中のシステムの構成について報告する。

2. おとりシステムの要件

おとりシステムを研究開発する組織として、Honeynet [3]プロジェクトがある。Honeynetプロジェクトでは、おとりに必要とされる機能を以下のように定義している。

2. 1. データ制御

正規のサーバが不正アクセスを受けるリスクを避けるために、自動的な方式で、おとりシステムへのデータの流れを制御する。

2. 2. データ取得

おとりへのアクセスを監視し、攻撃者に知られずに、おとりへのすべての入出力データ(ログ)を取得する。

2. 3データ解析

攻撃者の目的、不正アクセスの手法等を知るために、データの適切な解析を行う。

3. システム実現上の課題

3. 1. データ制御およびデータ取得

おとりにはHoneypot型の実装が多いが、正規のサーバが不正アクセスを受けるリスクの低減および不正アクセスのデータの取得という点が確実ではない。

一方、誘導(Trap)型[4]は、正規サーバが不正アクセスを受けるリスクが小さく、確実にデータが取得される。誘導型としては、以下の実装方式がある。

- ルータ、Firewallにより固定的におとりへ誘導
- 不正アクセス検知時にプロキシにより強制的に誘導[5]

ただし、これらの方式には、おとりサーバが提供できるサービスに制限があるという問題がある。

3. 2. データ解析

以下の点を考慮して、不正アクセスされたシステムのデータ解析として、侵入経路追跡を行うこととした。

- 侵入元を発見することは、不正アクセスの防止策となる。
- おとりは踏み台化される可能性が高いため、侵入追跡に適したデータが収集できる。

侵入経路追跡には、攻撃者の情報を収集するツール(ping, finger 等)を使用する方式があるが、以下のような方式も研究されている。

- IP アドレスの発信元IPアドレスを元にする方式(ホストレベル追跡)[6]
- Ether アドレスを元にする方式(ルータレベル追跡)[7]

これらの方式は、複数の踏み台を経由した攻撃者の追跡が困難であるといった課題がある。

---

* Study of the defensive system for unauthorized system using an intrusion trap
1) Seiji Fujii, Takehiro Ohkoshi, Kiyoto Kawauchi, Shigeki Kitazawa, Kotaro Katsuyama, Satoshi Ashizawa, Yosuke Kinoshita
2) Information Technology R&D Center Mitsubishi Electric Corporation
3) Communication Systems Center Mitsubishi Electric Corporation

4. おとり誘導による不正アクセス対策システム

上記の課題を考慮して、以下の設計方針を設定した。

- 正規のサーバの不正アクセスを受けるリスクの低減から、誘導型おとりシステムとする。
- 多種で、大量の攻撃者の活動記録データを取得するために、サーバ上で提供するサービスを制限しない。
- 複数の踏み台計算機があっても侵入経路追跡できるように、ホストレベル追跡およびルータレベル追跡の利点を組み合わせた侵入経路追跡方式とする。

上記の設計方針を満たすおとり誘導による不正アクセス対策システムを実現するにあたり、図1に示すシステム構成とした。

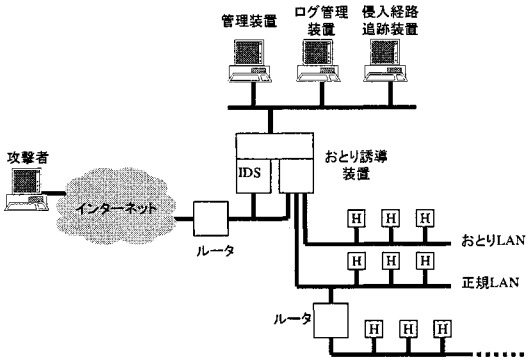

図1 おとり誘導による不正アクセス対策システムの構成

本システムは、構成要素である装置および計算機を集中管理する管理装置、侵入検知装置(IDS)、おとり誘導装置、正規 LAN、おとり LAN、ログ管理装置、侵入経路追跡装置から構成される。以下では、個々の構成要素について説明する。

4. 1. IDS

正規 LAN の外で不正アクセスを監視する。不正アクセスを検知した場合、その不正アクセスパケットをおとり誘導装置に通知する。

4. 2. おとり誘導装置

正規 LAN およびおとり LAN へ誘導するパケットを制御する。侵入検知装置から通知された不正アクセスパケットに含まれるソースIPアドレスからのパケットをすべておとり LAN へ誘導する。

おとり LAN 内の計算機がソースとなる場合の通信について、管理ネットワーク外との不整合が生じないように変換を行う。

4. 3. おとり LAN

不正アクセスの目標となることを想定したネットワークであり、正規 LAN と同一のネットワーク構成およびサービスを提供する。攻撃者に知られずに、各計算機上および LAN を監視し、ログを取得し、ログ管理装置へ集積する。

4. 4. ログ管理装置

正規 LAN およびおとり LAN から送信されるログを蓄積する。

4. 5. 侵入経路追跡装置

管理装置からの指示によって、ログ管理装置に蓄積されるログを使用して、攻撃元を追跡するための解析を行う。

5. おわりに

本稿では、おとり誘導を用いた不正アクセス対策システムを検討し、その構成要素について報告した。

本システムにおいて、侵入検知装置については、専用ハードウェアによる実装が終了している。現在、おとり誘導装置および侵入経路追跡装置について、実装方式の検討および試作を実施している。今後は、本システムを試験運用し、その有効性の評価を実施する。

参考文献

[1]河内他、“おとり誘導装置の試作“, 情処 64 全大, 2H-03, March 2002.

[2]北澤他、“パケット情報と通信ログ情報を用いた侵入経路追跡の検討“, 情処 64 全大, 3H-05, March 2002.

[3]The Honeynet Project, “Know Your Enemy”, ADDISON-WESLEY, Sep. 2001

[4]E. G. Amoroso, ”Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response”, Intrusion. Net Books, Sparta, NJ, 1999.

[5]竹森他,”Intrusion Trap System の実装および評価”,CSEC, pp415-420, 2001 年 10 月.

[6]M. Asaka, “Information-Gathering with Mobile Agents for an Intrusion Detection Systems”, Systems and Computers in Japan, Vol.30 No.2, pp.31-37, 1999

[7]小久保他、“不正アクセス発信源追跡システムのモデルの検討“, 情処 60 全大, 6Q-04, March 2000