侵入検出システムにおける誤判別率の改善

2G−4

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

実効性のある侵入検出システムは誤検出が多く運用に労力がかかるため、誤検出の少ない侵入検出システムが求められてきている。

本論文で対象とする侵入検出システム IDA[1]では、侵入の際にはなんらかの痕跡が残る事を利用して、この痕跡をトリガーにしてシステムログを検証し、侵入検出を行う。IDA では侵入の痕跡を

- セキュリティ上重要なファイルの変更
- 実効 uid が root になっていて、suid されていないコマンドの実行

と定義している[1]。この「痕跡に基づく検出手法」は現在公開されている IDA で実装されている[2]。

しかし、痕跡発見後のログの検証が不十分なため、侵入を検出する事はできるが、正常な行為を侵入と誤って検出する場合がある。それは以下の場合である。

1. suid コマンドによって一般ユーザがセキュリティ上重要なファイルを変更する。
2. suid コマンドから suid されていないコマンドを実行する。

上記の 1.については[3]において、セキュリティ上重要なファイルがどのコマンドから変更されるかを予め登録しておいた、正規手続きデータベースを用いる事で解決されている。しかし 2.については考慮されていない。

本論文では、システムにできるだけ余計な負荷を与えずに、侵入検出システムが誤って検出する侵入報告を削減する手法を提案する。

2　痕跡に基づく侵入検出手法の問題

具体的に問題になるのは以下のようなログが残った場合である。

	コマンド	パーミッション	UID	実効 UID
1	Xwrapper	104711	t-inoue	root
2	X	100755	t-inoue	root

表 1　問題となるログ

上記の表は Vine Linux 2.0 上で startx を実行した場合のログの一部である。startx は 1 で suid コマンドである Xwrapper を実行し、2 で Xwrapper から suid されていないコマンド X が実効 UID が root で起動されている。

IDA では、実効 UID が root になっていて、suid されていないコマンドの実行された場合、su によって一般ユーザが root にスイッチした場合には正常行為であると判断する。そのため startx の実行の場合では suid されていコマンド X が、su を実行されずに、実効 UID が root で実行されているため、この Xwrapper の実行を侵入と判断してしまう。

また上記のように su を特別視しているため、su の脆弱性をついた攻撃は検出できない。

3 正規手続きデータベースによる解決

[3]では、一般ユーザによる suid コマンドを用いたセキュリティ上重要なファイルの変更が、誤検出される事を問題としている。この問題を、セキュリティ上重要なファイル毎に、一般ユーザが

An Improvement of Misdetection rate on Intrusion Detection Systems
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

変更に用いるコマンドを正規手続きデータベースに登録する事で、解決している。

ここでは[3]と同様に suid コマンドの振舞仕様をデータベースに登録することで解決する事を試みた。具体的には、以下のような方針で誤検出をできるだけ防ぐ事にした。

- 一般ユーザの suid コマンド実行によって exec されるコマンドを正規手続きデータベースに登録する。登録されたコマンド以外の実行を侵入とみなす。(Xwrapper など)
- 引数によって実行するコマンドが変わるような、何を実行するか決まっていないコマンドは、正規手続きデータベースに何も登録しない。この suid コマンドによる痕跡があがった場合は即座に侵入とみなす。(suidperl, sudo など)

この仕組みを実現するには suid コマンドの仕様を調べる事と、suid コマンドの仕様を利用する正規手続きデータベースを拡張する事が必要である。以下、この 2 点について述べる。

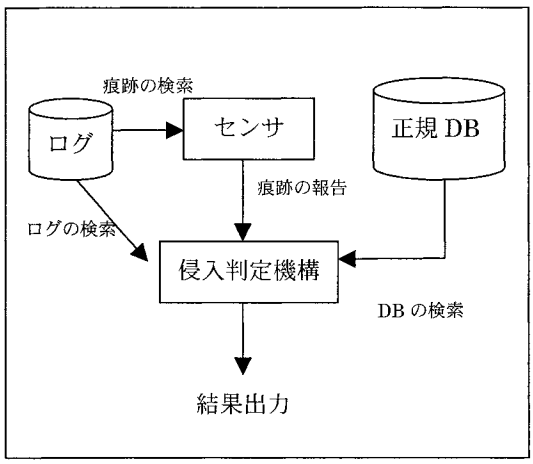

図 1　侵入検出機構の概要

3.1 suid コマンドの仕様の調査

ここでは suid コマンドの仕様を網羅的に調査した。具体的には

- suid コマンドのマニュアル
- suid コマンドを実行したログ
- suid コマンドのソースコード

を調査し、正常時にどのようなコマンドを実行するかを調べた。

3.2 正規手続きデータベースの拡張

[3]で定義された正規手続きデータベースではセキュリティ上重要なファイルとそのファイルを変更する suid コマンドの関係しか記述していない。これを suid 自身の正規手続きを記述できるように拡張する。具体的には以下のような情報を登録できるように拡張した。

suid コマンド	実行が許されるコマンド
Xwrapper	/etc/X11/X
su	/usr/X11R6/bin/xauth

表 2　正規手続きデータベースの例

ここで「suid コマンド」と「実行が許されるコマンド」に登録されたコマンドは、痕跡として検出されても侵入とはみなさない。

4　評価と今後の課題

上記の機構を実装して評価したところ、正規手続きデータベースに登録された suid コマンドについては誤検出は行われなくなった。また実装する前と同じく侵入行為の判定が正しく行えた。

今後は sudo,suidperl などの振舞が不定なコマンドの正常行為の判定と、負荷の大きな実環境で評価した上での実装の改良が挙げられる。

[参考文献]

[1] 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.

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

[3] 原田 慎介,浅香 緑「痕跡を用いた侵入検出手法への正規手続きデータベースを利用した侵入判定の適用」,情報処理学会論文誌 Vol.41 No.8 pp.2208-2215 (2000)