情報通信

SSHパスワードクラッキング攻撃の検出

用途・応用分野

- SSHサーバへのパスワードクラッキング攻撃対策および可視化
- 小型UNIXマシンへの不正アクセス防止　等

本技術の特徴・従来技術との比較

小型のUNIXマシンやエッジコンピューティング従来型の制限ではIPアドレスでしか行うことはできなかったが、本システムではパスワードの入力時間やアクセス時間帯等も加味することができる。

技術の概要

【SSHパスワードクラッキング攻撃の検知】

本技術において、攻撃アクセスのみを受け付けるサーバ（ハニーポットサーバ）と、正規アクセスが含まれる、実際に運用するサーバ（運用サーバ）の2つのSSHサーバを並行運用する。この2つのサーバは、ネットワーク的に近い2ホストで運用するか、1ホスト上で異なるポートで構築する。SSHサーバデーモンには認証情報の取得・転送および認証情報を元に攻撃を検知・遮断する機能を追加したSSHサーバを実装し、これを動作させる。

ハニーポットサーバは攻撃アクセスの認証情報を取得し、 DB サーバへ送信、格納する。十分な攻撃アクセスが蓄積された後、解析サーバは DB サーバから取得した認証情報 ログを元に検知モデルを構築し DB サーバに格納する。解析が完了した時点で、解析サーバは運用サーバに解析完了通知を送り、通知を受け取った運用サーバは DB サーバから検知モデルを取得する。運用サーバは SSH アクセスを受け取った際、その認証情報を取得し、検知モデルを用いて悪性を判断する。攻撃だと判断した場合、その認証試行を遮断する。解析処理と運用サーバの解析結果の取得、検知モデルの更新は定期実行させ、検知率の向上を図っている。

また、過大に多くのログイン試行を行う送信元に対しては別の手段で拒否を行い、比較的少数の接続元からのログイン試行について、正規・攻撃の判別を行なっている。

特許・論文

＜論文＞

大歳・中原・波多・小林他、グラフ理論に基づくSSHサーバログの統合管理およびリアルタイム可視化システムの提案、FIT2023講演論文集、D-1，2023

研究者

小林　孝史
総合情報学部　総合情報学科
小林研究室

お問合わせ先
関西大学 社会連携部 産学官連携センター
TEL：06-6368-1245
MAIL：sangakukan-mm@ml.kandai.jp