L-015

認証時間に基づいた SSH パスワードクラッキング攻撃検知手法の提案
An Approach of SSH Password Cracking Attack Detection Method Based on Authentication Time

坂東 翼† 上原 拓也 小林 孝史‡
Tsubasa Bando Takuya Uehara Takashi Kobayashi

1. はじめに

遠隔地の計算機にアクセスするための手段として SSH プロトコルが広く利用されている．しかし，SSH はログインに成功すると計算機に対して直接操作を行えるという特徴から，攻撃者の標的となりやすい側面を持つ．

SSH に対する代表的な攻撃手法としてパスワードクラッキング攻撃が挙げられる．攻撃者は一般的に，攻撃対象のサーバに対しパスワードクラッキングツールを用いて膨大な回数の認証を試行する．このような攻撃は近年増加の一途を辿っており，計算機に対する不正アクセス事件が相次いでいる．著者らの研究室で運用する SSH サーバでも日々パスワードクラッキング攻撃を観測しており，それらの攻撃アクセスを収集・分析した結果を報告している[1].

本研究ではパスワードクラッキング攻撃への対策として，認証に要する時間（以下，認証時間）を用いた検知手法を提案する．また，提案手法を既存の OpenSSH サーバに実装し，関西大学の小林研究室に割り当てられたグローバル IP アドレスで運用することで，パスワードクラッキング攻撃に対する提案手法の有効性を検証する．

2. 関連研究

小刀稱らの研究[2]では，TCP コネクション 1 回あたりにおけるパケット送受信回数に基づいた，SSH パスワードクラッキング攻撃検知システムの運用結果が述べられている．小刀稱らは 1 コネクションにおいてパケット送受信回数 50 回というしきい値を設定することで高精度の攻撃検知を可能とした．しかし，しきい値の超過が 10 回観測された場合に攻撃者と判定することから，10 回以下の攻撃コネクションを異なる IP アドレスから行う“分散型”の攻撃に対応できないという問題点が挙げられていた．

佐藤らの研究[3]では，トラフィックにおけるフローの特徴に基づいた，SSH 総当たり攻撃検出手法が提案されている．フローの特徴とはフローを構成する個々のパケットから計測可能な，パケットのサイズ，到着順，および到着時間間隔に代表される統計的特徴を指す．佐藤らは独自のデータセットを用いた実験により，総当たり手法による攻撃の特徴がパスワードの入力に要する時間に現れることを明らかにした．さらに，機械学習により SSH サブプロトコルの推移箇所を識別することでパスワード入力時間を推定する手法を提案した．

SSH サーバが出力するログメッセージを監視することで，攻撃を検知する手法が実用化されている．代表的なソフトウェアに fail2ban や denyhosts が存在する．これらのソフトウェアはさまざまなサービスに対するアクセス状況に応じて，動的なファイアウォールの設定変更を支援するツールである．攻撃検知の指標としては，ホワイトリスト外のホストからの接続，認証方法による検知，存在しないユーザへのアクセス，一定時間内における同一ホストからの繰り返しアクセスなどが挙げられる．

しかし，ホワイトリストや認証方法による検知手法は接続できる IP アドレスや認証方法を制限するという特性上，利用形態や組織の運用ポリシーによる制約を受けるという問題がある．さらに一定時間内における同一ホストからのアクセス数による検知手法は，複数のマシンを協調させることで一つの IP アドレスあたりの認証試行数を削減し，単位時間あたりの認証試行数による検知を回避する“分散型”の攻撃に対応できないという問題も存在する．

3. 提案手法

SSH サービスの利用において，正規ユーザによる認証試行ではユーザがパスワード入力プロンプトを認識し，キーボードからパスワードを入力する必要がある．それに対し，パスワードクラッキングツールによる認証試行では認証に必要な処理を自動化しているため，正規ユーザによる認証試行と比較して認証時間が短くなる傾向があると考えられる．そこで本研究では，SSH アクセスにおける認証時間に着目し，計測した認証時間と事前に決定したしきい値と比較することでパスワードクラッキング攻撃の検知を行う手法を提案する．

SSH プロトコルではまず，接続が開始された際，プロトコルバージョンやセキュリティ機能に関するパラメータネゴシエーションが行われる．次にディフィー・ヘルマン鍵交換法による共通鍵の共有が行われ，暗号化が開始される．暗号化の開始と同時にユーザ認証に関するネゴシエーションが開始される．本研究における認証時間の定義は，サーバがユーザ認証サービスの認可メッセージをクライアントに送信してから，パスワード情報などを含む認証リクエストを受信するまでの時間とする．

4. 実装

本提案手法を実装するため，既存の OpenSSH のプログラムを改変し，認証時間計測機能を追加した．

まず，クライアントからの“ユーザ認証開始リクエスト”に対して，サーバは“ユーザ認証認可”のメッセージを返信する．“ユーザ認証認可”のメッセージ送信後，サーバはその時点での時刻を取得し認証開始時間とする．クライアントからパスワードを含む認証情報を受信したサーバは認証成否の判定を行い，その時点での時刻を認証終了時間とする．

次に，現在の認証試行がコネクション中において 1 回目の試行であるかの判定を行う．これは最初に認証開始時間を記録した関数が，1 コネクションにつき一度しか実行さ

†関西大学大学院総合情報学研究科
‡関西大学総合情報学部

れない関数であることに基づいている．コネクション中の 2 回目以降の認証開始時間は，サーバからクライアントに対して“ユーザ認証失敗”のメッセージを送信する際に記録する．認証時間を測定し終えると，サーバはあらかじめ sshd_config 内で設定されたしきい値と認証時間を比較し，SSH アクセスが悪性のものであるか判定を行う．

最後に，認証が成功であった場合は認証を終了し，認証が失敗であった場合は次の認証情報を待ち受ける．また，SSH プロトコルでは 1 コネクション中で可能な最大認証試行数が，サーバ側の設定とクライアント側の設定のどちらか少ない方に合わせられる．そのため，どちらかの最大認証試行数に達した場合，認証が成功していなくてもコネクションは切断される

5. 調査と評価

本章では，攻撃を検知するしきい値として最適な認証時間を設定するために行った調査と，設定したしきい値による攻撃検知率の検証結果について述べる．なお，SSH アクセスを収集するための SSH デーモンには OpenSSH6.6p1 を使用し，サーバの OS には CentOS7.2.1511 を使用した．OpenSSH はソースコードの改変が必要となるため，ソースコードをダウンロードし，ビルドを行った．

5.1 通常の認証時間に関する調査

本提案手法では認証時間によって通常の SSH アクセスと異常な SSH アクセスを分類するため，二種類のアクセスを分類するために有効なしきい値が必要となる．また，しきい値の性能を検証するには，攻撃アクセスと通常のアクセスをそれぞれ正しく識別できた割合を調査する必要がある．

そこで，本システムを用いて 9 名の協力者に指定したパスワードでの認証を 1 回ずつ試行させ，一般ユーザによる SSH アクセスにおける認証時間を計測した．計測用のパスワードには，設定可能なパスワード長が多様であることを考慮し，長さの異なる文字列“a”，“root”，“password”を使用した．その結果，最短認証時間は 0.385 秒，最長認証時間は 3.32 秒を記録した．

5.2 最適なしきい値に関する調査

前節の調査にて収集した通常の SSH アクセスにおける認証時間と，本提案手法を実装したシステムを用いて収集した関西大学宛ての異常な SSH アクセスを用いて，最適なしきい値を調査する実験を行った．本実験では，2016 年 12 月 27 日から 2017 年 2 月 10 日までの期間収集した 1,592,525 件の攻撃アクセスと，前節の調査で収集した 9 人の被験者による合計 27 件の認証試行データを用いた．前節での調査結果により，通常の認証試行における最短の認証時間が 0.3 秒台であったことから，調査を行う最短の秒数を 0.3 秒とした．また，長すぎるしきい値は検知性能を低下させると考えられたため，最長のしきい値を 1.2 秒とした．

最適なしきい値を調査するため，0.3 秒から 1.2 秒の調査範囲でしきい値を変化させ，それぞれのしきい値において独自の性能評価値を算出した．性能評価値には，しきい値を下回った攻撃アクセスの割合（以下，真陽性率）と前節の調査によって収集した通常のアクセスがしきい値を上回った割合（以下，真陰性率）を合計した値を利用する．また，しきい値の変化の粒度は 0.01 秒ずつとした．

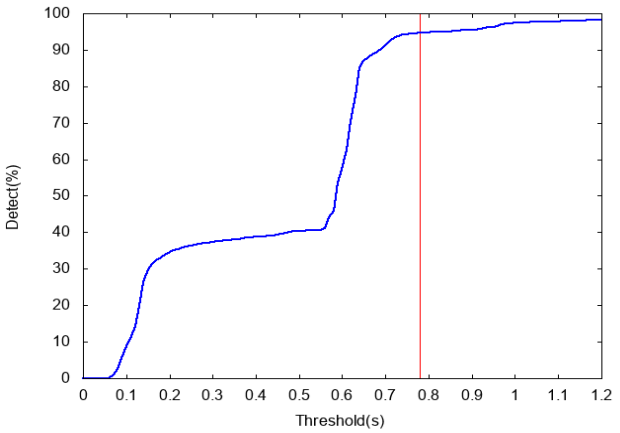

図 1　しきい値変動時の検知率の推移

最も性能評価値が高かったしきい値の秒数は 0.78 秒であった．0.78 秒のしきい値において真陽性率は 95.41%，真陰性率は 85.19%，性能評価値は 180.6 であった．このことから，本研究では 0.78 秒を運用時のしきい値として決定した．

5.3 決定したしきい値による攻撃検知率の検証

本提案手法を実装したシステムを 2017 年 3 月 1 日から 2017 年 5 月 31 日までの期間，関西大学小林研究室に割り当てられたグローバル IP アドレスで運用し，SSH アクセスを収集した．その結果，攻撃アクセスの総認証試行数は 2,025,182 回，認証を試行した IP アドレスの総数は 4,057 個をそれぞれ記録し，平均認証時間は 0.482 秒，認証時間標準偏差は 0.625 秒，最短認証時間は 0.00913 秒，最長認証時間は 97.9 秒であった．また，認証時間が仮のしきい値である 0.78 秒を下回ったアクセスは 1,917,311 回となり，検知率は 94.7%であった．

しきい値を 0.0 秒～1.2 秒の間で変動させた際の検知率の推移を図 1 に示す．横軸にしきい値である認証時間を，縦軸に攻撃の検知率をそれぞれ示している．

6. おわりに

本研究では，仮に決定したしきい値によって約 94.7%の SSH パスワードクラッキング攻撃が検知可能であることを明らかにした．パスワードクラッキング攻撃の判別の指標として認証時間を用いることで，従来の検知手法の問題点である分散型の攻撃への対応も可能であると考えられる．また，佐藤らの研究にて提案されていた機械学習を用いた手法より低い計算コストでパスワード入力時間の差異に基づいた検知手法を実装した．

今後の展望として伝送時間を考慮し，しきい値を変動させる機能の実装を検討している．

参考文献

[1] 中田恭平, 吉井章, 坂本要, 小林孝史, “関西大学における SSH アクセスの収集と分析”, 情報処理学会研究報告セキュリティ, インターネットと運用技術(IOT) 2015-IOT-31, No.8 (2015).
[2] 小刀稱知哉, 中本菜桜美, 清水光司, 池辺実, 吉田和幸, “SSH パスワードクラッキング攻撃検知システムの改善とその運用結果”, 情報処理学会研究報告, インターネットと運用技術(IOT) 2014-IOT-26, No.4 (2014).
[3] 佐藤彰洋, 中村豊, 池永全志, “フローの特徴に基づく SSH 総当り攻撃の検出手法”, 信学技報.IN 情報ネットワーク, Vol.111, No.346 (2011).