様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ８ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１５４

研究課題名（和文）ステルシーSSH辞書攻撃のフローベース検出手法に関する研究

研究課題名（英文）Stealthy SSH Dictionary Attack Detection based on Flow Analysis

研究代表者
中村　豊（YUTAKA, NAKAMURA）

九州工業大学・情報科学センター・准教授

研究者番号：４０３４６３１７

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：SSH総当たり攻撃による被害は深刻さを増していることから、管理者にとってその攻撃への対策は急務である。従来手法としてアクセスログやトラヒックから得られる情報を元にSSH総当たり攻撃の発生を検出してきた。本研究ではSSHフローの特徴に基づくSSH総当たり攻撃手法を提案する。本学におけるトラヒック計測及びハニーポットを用いたデータ解析により、我々の提案手法を用いることにより、通常の通信と総当たり攻撃の分別に加え、攻撃による被害の有無を高精度で識別できるようになった。

研究成果の概要（英文）：SSH brute force attack has become more seriously, so administrators are desired to implement its countermeasures. In the traditional ways, the SSH brute force attack has been detected by analyzing access logs and network traffic. However, the former way must check a huge quantity of the logs in all servers, and the latter cannot find victims of the attacks. To solve these problems, we propose SSH brute force attack detection based on the flow features analysis. As the experimental results, we showed to be able to identify the attacks and their victims.

研究分野：ネットワークセキュリティ

キーワード：ネットワークセキュリティ　総当たり攻撃　SSH

１．研究開始当初の背景

SSH サーバに対するパスワード総当たり攻撃によりパスワードが取得されると、情報漏洩、フィッシングサイトの構築、スパムの送信など、その被害の影響範囲は甚大なものとなる。

従来手法ではサーバのアクセスログやトラヒックから得られる情報をもとに SSH 総当たり攻撃の発生を検出してきた。しかしながらすべてのサーバのアクセスログを確認することは困難である。また、トラヒックからの情報では攻撃の検出はできたとしても、パスワードが奪取されたかどうかの被害の有無は確認できない。さらに、slow-motion SSH 辞書攻撃では攻撃の検出も困難である。

２．研究の目的

従来の異常検知・侵入検知システムにおいて slow-motion SSH 辞書攻撃や分散辞書攻撃を検出するシステムは存在しない。そこで本研究では個別の SSH セッションにおいて SSH 認証が成功したか、失敗したかの判断が可能であり、かつ、それらの判断をサーバのログファイルではなくネットワークトラヒックのモニタリングデータのみを用いて実現することを目的とする。

３．研究の方法

本研究では SSH 辞書攻撃に対して、トラヒックモニタリングを用いて実現するために、以下の 3 つのテーマについて取り組む。

(1) SSH セッションにおけるフローの抽出

SSH セッションにおけるフローの抽出では、本学のインターネット接続の出入り口において、SSH 通信のフローを抽出するためのモニタリング環境を構築する。また、外部からの攻撃を誘導するハニーポットを設置して、実際の攻撃トラヒックがどの様なパターンで攻撃を実施しているのかを把握する。

(2) SSH 通信におけるサブプロトコルの解析

(1)で構築したトラヒックデータおよびハニーポットのデータを用いて、SSH サブプロトコル解析を行う。具体的に SSH フローを、攻撃成功、攻撃失敗、通常の SSH 通信と分類し、得られたデータセットがどれに相当するかを解析する。

(3) ユーザ認証パケットにおける inter-arrival time の解析

(1)で構築したトラヒックモニタリングデータを用いて解析を行う。また(2)での識別において通常の SSH 通信と SSH 辞書攻撃を含んだデータを解析し、その違いを識別する。

４．研究成果

(1) SSH セッションにおけるサブプロトコル解析

SSH 総当たり攻撃の識別における SSH フローの特徴を明らかにするために、分析を行った。フローとは、パケットの送信元および宛先アドレスやポート番号、プロトコル番号に基づいて識別可能な、クライアント・サーバ間の双方向通信である。

SSH では仕様として 3 つのサブプロトコルが存在する。トランスポート層プロトコル、認証プロトコル、コネクションプロトコルである。トランスポート層プロトコルでは暗号化された通信路をクライアント・サーバ間で確立することで、データの機密性、安全性を実現する。認証プロトコルでは、トランスポート層プロトコルで確立した通信路において、その利用の可否を認証によって判断する。

図１はハニーポットへ到着した SSH 通信におけるパケット数の解析結果である。S は成功、U は失敗、T はトランスポート層プロトコル、A は認証プロトコル、C はコネクションプロトコルである。攻撃が成功した時の C は 4～6 パケットであるが、攻撃が失敗した時の C は 0 である。また、他のサブプロトコルの違いは見られない。これにより、コネクションプロトコルの存在の有無が攻撃の成功の判断基準であると言える。

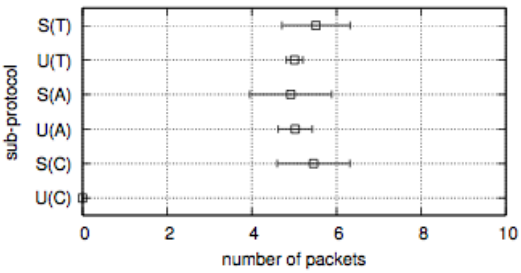

図１　SSH サブプロトコル解析

(2)通常の通信と総当たり攻撃の識別

通常の通信と総当たり攻撃におけるパスワードの入力に要する時間の違いを明らかにするために、通常の SSH 通信と SSH 辞書攻撃を含んだデータの解析を行った。図２に認証パケットの到着時間間隔の累積分布を示す。認証パケットとは、クライアントからサーバに送られる認証方法と認証情報を保持するパケットである。認証方法の例としては、パスワード認証、チャレンジレスポンス認証、公開鍵認証などがある。認証情報とはユーザ名やパスワードである。パケットの到着時間間隔とはフローにおいて、i 番目のパケットが到着した時刻 T_i と、i+1 番目のパケットが到着した時刻 T_{i+1} の時刻の差分 T_{i+1}-T_i で求められる。図２における横軸は認証パケットの到着時間間隔、縦軸は累積確立を示す。図２から認証パケットの到着時間間隔が通常の通信では2～5秒の間に99%以上含まれていること、そして総当たり攻撃では 0.1～0.5 秒の間に 99%以上含まれていることが明らかとなった。これは総当たり攻撃では、パスワードを破るために辞書データベースに基づい

た機械的な入力を行うため、人間がパスワードを入力する時間と大きく隔たりがあることが原因であると思われる。

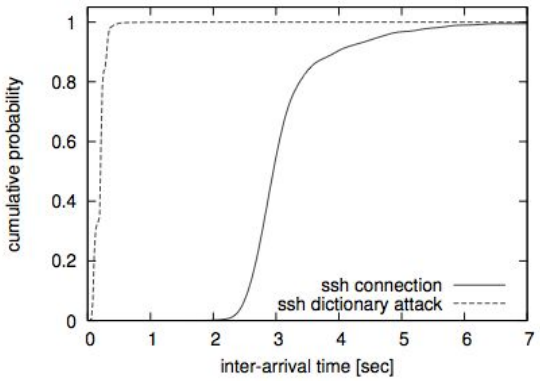

図２　認証パケットの到着時間間隔

(3)SSH セッションにおけるフローの特徴
本学のパケットモニタリングシステムより得られたデータから、任意に選択した SSH フローを対象に、それらを構成する個々のパケットについて、(i)パケットの到着順、(ii)パケットサイズ、(iii)パケットの通信方向、(iv)パケットの種類を計測し、それらの関係の可視化を行った。その結果を図３に示す。横軸はパケットの到着順、縦軸における値の大きさはパケットサイズ、その正負は通信方向を示す。クライアントからサーバに向けた通信の場合は正の値、サーバからクライアントへ向けた場合は負の値となっている。図３では(1)から(10)までのそれぞれのパケットにおける役割について示している。(1)が 3-way handshake で通信の確立である。(2)および(3)でサーバ、クライアントがそれぞれサポートしている暗号化アルゴリズムの情報の開示を行っている。(4)～(7)および(8)～(10)において、SSH 暗号化通信の暗号方式の交換を行っている。(10)以降で暗号化が開始されており、パケットの内容の解析が不可能となる。

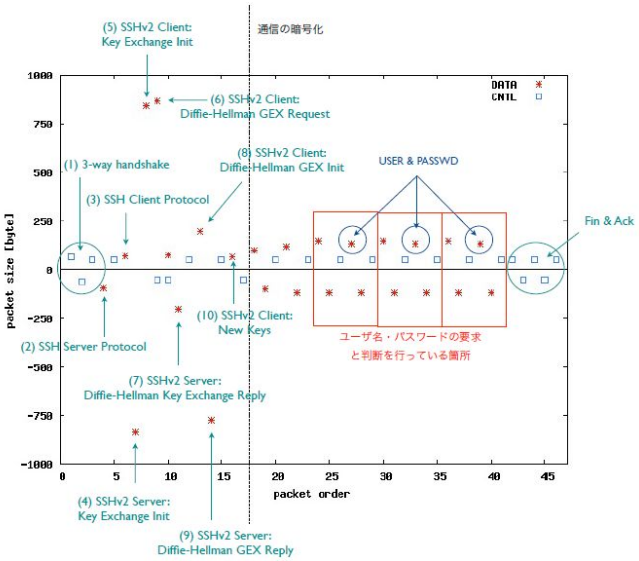

図３パケット順とパケットサイズ

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　2 件）

① Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, A Flow-Based Detection Method for Stealthy Dictionary Attacks against Secure Shell, Journal of Information Security and Application, Vol 21 Issue C, April 2015,pp.31-41,DOI:10.1016/j.jisa.2014.08.003, 査読あり

② Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, A New Approach to Identify Authentication Methods toward SSH Dictionary Attack Detection, IEICE Transactions on Information and Systems, Vol. E98-D, No. 4 April 2015, pp.760-768,DOI:10.1587/transinf.2014ICP0005, 査読あり

〔学会発表〕（計　3 件）

① Yasutaka Shindo, Akihiro Satoh, Yutaka Nakamura, Katsuyoshi, Iida, Lightweight Approach to Detect Drive-by Download Attacks Based on File Type Transition, CoNEXT Student Workshop 2014, Dec 2-5, Sydney, Australia

② Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, Analysis for Identifying User Authentication Methods on SSH Connections, The International Workshop on Smart Technologies for Energy, Information and Communication, 2013, Aug 21-22, Incheon, Korea

③ Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, Identifying User Authentication Methods on Connections for SSH Dictionary Attack Detection, The Annual International Computers Software & Applications Conference, 2013, July 22-26, Kyoto, Japan

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：

権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
中村　豊（NAKAMURA, Yutaka）
九州工業大学　情報科学センター・准教授
研究者番号：４０３４６３１７

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：