2003年日本オペレーションズ・リサーチ学会
秋季研究発表会

周波数分析を用いた ハッキングトラヒックアナリシス

申請中 日本大学生産工学部 ○ 内山 貴夫
Nihon University Uchiyama Takao
01205220 日本大学生産工学部 篠原 正明
Nihon University Shinohara Masaaki

1 はじめに

今日、PCは一家に一台といわれるほど普及している。常時接続をするPCも増え、ハッキング及びクラッキング（本稿では以後、ウィルスも含めハッキングとする。）などからPCを守ることは必要不可欠になってきた。

最近では、アンチウィルスソフトなども普及をはじめ、ウィルスに対するユーザの関心は高まりつつある。これらには、ファイアーフォール機能が付加されているものが多くPCを守ることができる。ただし、これだけではPCを守りきることはできない。

そこで本稿では、ハッキングを検出する新たな方法を提案し、ハッキングが検出できるかについて検証したい。

2 ハッキング

ハッキングとは、コンピュータシステムにおいて技術的な解析を行うことである。そして、技術的な解析を行う人をハッカーという。このような技術を悪用する行為、または人を、クラッキング、クラッカーという。ただ、現在ではハッキングとクラッキングは同値として考えられることが多いのが現状である。

本稿ではハッキング、クラッキングをまとめて「ハッキング」とする。ハッカー、クラッカーについても同様である。

3 ハッキング検出

ハッキングからPCを守るためにはハッキングを検出する必要があります。ハッキングを検出するには、「IDS」、「ファイアウォール」などのシステムの利用やアクセスログをとることでハッキングの足跡を記録するなどの方法がある。本論では「トラヒック周波数解析」という新たなシステムを提案する。

トラヒック周波数解析とはトラヒックを周波数分析し、周期的な攻撃を検出する方法である。本システムは攻撃を防ぐことはできないが、早期発見することで被害を最小限に抑えることができると考えられる。

このシステムの最大の利点は「ファイアウォール」、「IDS」などにあげたいくつかの欠点を補えると考えられる点である。

方法としてはトラヒックログを周波数分析し、周期成分を見つけることでハッキングを検出する。ただし、攻撃に周期性が見られないと検出不可能であるため、他の検出方法との併用が好ましい。

4 トラヒック周波数解析

周波数解析にはフーリエ変換、ウェーブレット変換など多数の方法が存在するが、本稿ではフーリエ変換でトラヒック解析を行う。

フーリエ変換とは、われわれが直接得ることのできる時間領域に属する信号を周波数領域に属する信号に変換するものである。

フーリエ変換は下記の式によって定義されている。

$$F(\omega) = \int_{-\infty}^{\infty} f(t)e^{-j\omega t}\,dt \qquad (1)$$

$$F(\omega) = R(\omega) + jX(\omega) = A(\omega)e^{j\phi(\omega)} \qquad (2)$$

$A(\omega)$ はf(t)のフーリエスペクトル、$A^2(\omega)$ はそのエネルギースペクトル、また $\phi(\omega)$ はその位相角と呼ばれている。

本稿では以上の計算を離散データでも可能なFFTを利用し計算する。

5 解析モデル

実際にパケットのログを取り、周波数解析を行うとモデル及び解析結果が複雑化するため、本稿では、単純なトラヒックでシミュレーションしてみることにする。

トラヒックシミュレーションにはプログラムを利用する。トラヒックは基本的に周期性のあるトラヒックとランダムなトラヒックを混ぜて生成されている。

このようなルールを元に次のような解析モデルを用意した。

- ランダムなトラヒック
- 周期的なトラヒック
- 周期的な攻撃が潜んでいるランダムトラヒック

周期的な攻撃が潜んでいるランダムトラヒックに関しては、ランダムなトラヒックの周期やトラヒックサイズなどを変えた様々なモデルを用意した。

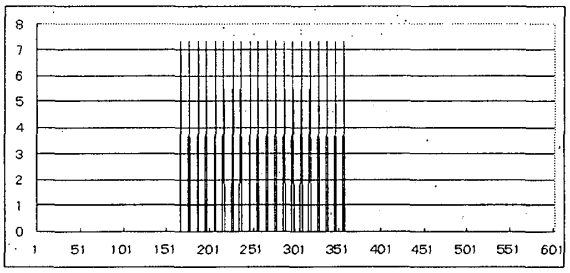

図 1: 周期的なトラヒック

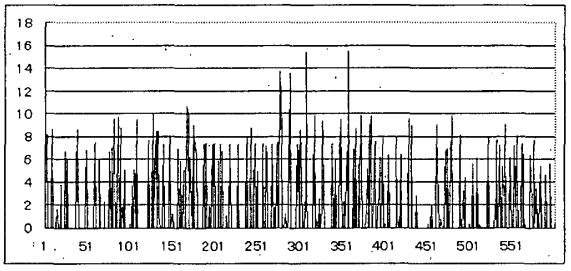

図 2: 周期的な攻撃が潜んでいるランダムトラヒック

6 解析結果

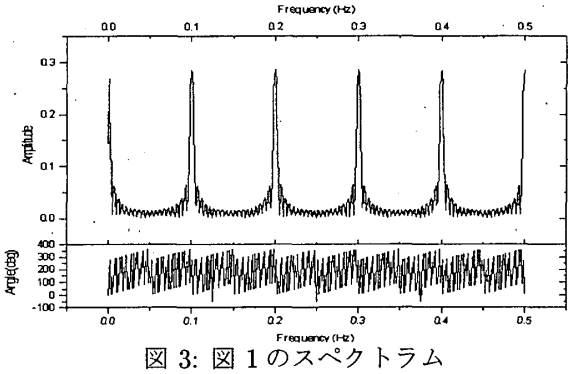

図 3: 図 1 のスペクトラム

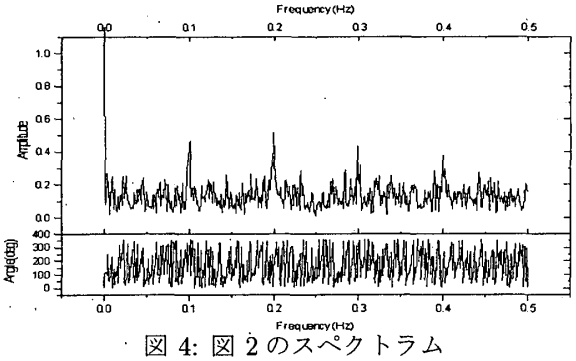

図 4: 図 2 のスペクトラム

7 考察・まとめ

様々なシミュレーションモデルの中から解析可能であったモデルとそのモデルの周期的なトラヒックのサイズのみを小さくしたモデルを比較した結果、ランダムトラヒックに対して周期的なトラヒックのサイズが小さい場合にはスペクトラムに顕著な結果が現れなかった。しかし、周期的なトラヒックのサイズが小さい場合でも解析データのはじめから最後まで連続して周期的なトラヒックがある場合、顕著な結果が表れることもあった。これは周期的なトラヒックがランダムトラヒックに埋もれてしまうこと、定常性を仮定するフーリエ変換では解析データの一部分の周波数をうまく解析できないことが原因と考えられる。

フーリエ変換では、通常のアクセスのトラヒックに対して攻撃トラヒックが小さい、また、一度に連続して攻撃する回数が少ないと周期的なハッキングを検出できないということである。これでは、ほとんどの場合ハッキングを検出することはできないということになってしまうため他の周波数分析方法で可能か検討する必要がある。

シミュレーション結果からこのハッキングの検出方法は通常のトラヒックが混雑しているネットワークで直接に実現するのは難しいと考えられる。つまり、ISP や IX 網などでそのまま利用するのは難しい。このシステムは、アクセスのあまり多くないサーバやログを取っていない一般のクライアント PC でのハッキングの検出、あるいは選択的トラヒックでの検出が主な利用方法になると考える。

8 今後の課題

本稿ではスペクトラムの解析には FFT を利用したが、結果としてスペクトラムに顕著な結果は表れなかった。そこで、時間軸と周波数の両方の解析を行える STFT、ウェーブレット変換を利用することで顕著な結果が現れるのではないかと考えられる。このような手法で解析を試みたいと思う。

トラヒックに顕著な結果が表れた時、攻撃なのか、たまたま周期的なアクセスなのか、判別することができないが、スペクトラムに時間軸が付くことにより、アクセスログを参照することで攻撃かどうか調べられると考えている。

最終的には実データでの解析を行い、ハッキングからサーバを守るトータルのシステム構築をしたい。具体的には、トラヒック周波数解析ハッキングされた時間と特定し、その時間のログを参照。そしてそのログの発信者、つまり IP アドレス及びにログの特徴を IDS の攻撃パターンのデータベースに追加し、以後そのハッキング及びその相手からのアクセスを禁止させる。このようなシステムによって、既存のシステムの弱点を埋めることができる。

このような作業を自動化させることでこれまでにない新しいセキュリティ対策としていきたい。

参考文献

[1] 中野隼人, 周波数スペクトラム分析に基づくハッカートラヒック検出, 日本大学生産工学部 34 学術講演会, 数理情報部会 (2001.12)