大量プロセス生成によるOOM Killerを用いた攻撃への対策

高 橋 秀 明† 大 山 恵 弘†

1. はじめに

Linuxカーネルには OOM Killer というシステムが存在する。これは、メモリ不足に陥った際に、消費メモリと優先度より算出されたスコアの最も大きいプロセスを殺すことでメモリを確保する。

OOM Killerは、スコアによって優先的に殺すプロセスを決定しているので、低スコアのプロセスを悪意のあるプログラムで大量に作ることでユーザーが意図しないプロセスを攻撃者が殺せてしまう。そのため、OOM Killerを用いた攻撃が可能になってしまうという問題点が存在する。

そこで本研究では、大量プロセス生成による OOM Killer を用いた攻撃を防ぐ方法を提案する。

2. OOM Killerの性質

OOM Killer のスコアはプロセスの消費しているメモリと、プロセスに設定された優先度により決まる。優先度は-16から15の範囲で設定でき、デフォルトは0であり、優先度が小さいほど OOM Killer の対象になりにくくなる。一方で、あまりに消費メモリが多いと、低優先度に設定していても、スコアが高くなってしまう。例えば、消費メモリが200MBで優先度-16のプロセスは、消費メモリが100KBで優先度0のプロセスよりもスコアが高い。

OOM Killer が作動するのは、メモリ不足で必要量のメモリが確保できない時のみである。OOM Killer はプロセスをそのユーザーによって区別せず、スコアのみによって殺すプロセスを決定する。その為、あるユーザーの生成したプロセスを、そのプロセスより低スコアのプロセスを別のユーザーが大量生成して OOM Killer を作動させることで殺せてしまう可能性がある。

3. 実際の攻撃の検証

実験環境は VMware 上の Ubuntu11.10 で行った。メモリは 1GB、swap はオフにした。

実験 1 100KB を消費するプロセスを無限に生成

100KB を消費するプロセスを無限に生成して OOM Killer を作動させた。最終的に画面が暗転し、ログイン画面へ戻った。これは重要なプログラムが KILL された可能性があると考えられる。

実験 2 別のユーザーに対する攻撃

Ubuntu 上に A と B という 2 つのユーザーを作成した後、B でログインして 200MB のプロセスをを起動した。その後 A でログインして 100KB のプロセスを OOM Killer が作動するまで生成した。結果として B で起動したプログラムも KILL されていた。

実験 3 優先度を変えたプロセスへの影響

まず、200MB のプロセスを起動し、そのプロセスの優先度を-16 に設定し、OOM Killer の対象になりにくくした。その後、100KB のプロセスを OOM Killer が作動するまで生成した。結果として優先度を-16 に設定した 200MB のプロセスが KILL されていた。

† 電気通信大学 電気通信学部 情報工学科

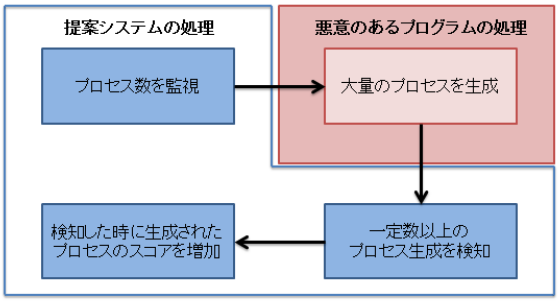

図 1 提案する方法の簡略図

4. 対策の方針

提案する方法は、短時間に大量に生成されたプロセスを優先して KILL する、というものである。本研究では、提案する方法を実現するためのカーネルモジュールを実装する。

提案する方法は、単位時間ごとのプロセス数を監視し、ある隣合った単位時間あたりのプロセス数の差が一定値以上ならば、その単位時間内に作られたプロセスのスコアを増加させる。図 1 は、提案する方法の簡単な流れである。この方法により、大量に低スコアのプロセスが生成されても、それらのスコアを増加させることで、他のプロセスよりも高スコアになる。そのため、結果として OOM Killer の対象になりやすくなるのである。

この方法の検討課題として、最適な、単位時間と、攻撃と判断する単位時間内のプロセス生成数を決める必要がある。これらは安易に決めることはできず、実験等により検討する必要がある。

5. 関 連 攻 撃

本研究で取り上げた攻撃に似た攻撃として、fork bomb または fork 爆弾と呼ばれる攻撃が存在する。この攻撃は、fork により高速に多数のプロセスを生成することで、OS の管理するプロセステーブルを埋め尽くす。それにより、新しいプロセスを作れなくするというものである。

この攻撃には予防法がとられており、一般的には 1 ユー

ザーあたりが生成できるプロセス数を制限するという方法である。Ubuntu11.10 では約 8000 個というプロセス生成数の制限が存在する。

また rexFBD [1] という Linux 用のカーネルモジュールも存在する。これは 1 秒あたりの fork 回数と 1 ユーザーあたりの fork 回数から fork bomb を OS にて検出するものである。

本研究と比べて、単位時間に注目している点等では共通点があるが、本研究ではメモリ不足が原因でプロセスが殺される点が大きく異なる。それにより、プロセスの生成数だけを制限しても、研究対象としている攻撃の対策にはならない。

6. 現状と今後

現状では、OOM Killer を用いた攻撃の検証実験を行い、加えて、これらの攻撃に似た関連攻撃の調査を行った。提案する方法を実現するためのカーネルモジュールの開発は、割り込みタイマーを用い、一定間隔ごとにプロセスリストを取得し、線形リストを用いて動的に情報を保持する手法を用いて行っている。これにより、本研究で必要となるスコアを増やすべきプロセスのリストを取得できるようになっている。今後としては関連研究の調査を行いつつ、開発中のカーネルモジュールを完成させ、その後各パラメーターの最適値を実験等により調査する予定である。

参 考 文 献

1) rexFBD
http://rexgrep.tripod.com/rexfbdmain.htm