Internet Protocol における More Fragment フラグの立ったパケットによる攻撃と各 OS の対応状況

HAYASHI yu-ichi
Core and Information Technology Center

1 はじめに

IP[1]の潜在的な脆弱性の原因の１つとしてパケットのフラグメントという問題がある．MTU の異なる 2 つのネットワーク間をルーティングする際，ルータは末端部を除いて 8 の倍数となるようにパケットを分割する．この作業がフラグメントである．フラグメントを利用した攻撃として RFC[2][3]でも考察されている．

2 More Fragment を利用した攻撃手法

More Fragment の flag を利用した攻撃方法は非常に簡単なものである

攻撃手法１

・IP Header 内の Flags フラグメントのビットを立てる

・それに加えフラグメント後続のフラグを立て次々と別の IP address から目的のマシンに対してパケットを送信する．

攻撃手法２

・同一内容の IP フラグメントデータグラムを攻撃目標マシンに対して連続して多量に送りつける

まず攻撃手法１に関する考察より行う

3 攻撃手法１における各 OS の挙動

対象の OS は Linux, FreeBSD, NetBSD, OpenBSD, Windows2000 である．

Windows2000 に関してはソースコードがないため攻撃を行ってみた際の OS の挙動を観察するしかないわけであるが，それ以外の OS に関してはソースコードもザッと読んだ上で考察を述べることとする．

まず Windows2000 以外の OS について各統一の挙動をここに記述します．

手順１： カーネルは到着した IP パケットがフラグメントされているか，いないかをヘッダのフラグを見て振り分けます

手順２： フラグメントされているパケットは再構築されるために Queue に格納され再構築されるのを待ちます

手順３： Queue の限界がセットされている OS もしくは Queue に入ったフラグメントパケットにタイマーが設定される OS の場合フラグメントのパケットは破棄され ICMP が送信側にエラーメッセージを送ります

上記の OS のなかでこの手順すべてを確認できたものは Linux と OpenBSD(ICMP の送信は確認していません)の２つでした．

攻撃方法１に各 OS の対処をまとめると次になります．

OS	攻撃方法１に対する対応
Linux	Queue にタイマーが仕掛けられており時間内に残りのフラグメントパケットが到着しなかった場合はパケットを破棄し送信元に対し ICMP でエラーを通知する．Queue の制限時間は一定なのでその時間内にある程度帯域のあるネットワークに対しフラグメントを大量に送りつけると CPU のロードアベレージを上げることができる．
FreeBSD	未実験
NetBSD	大量の fragment したパケットを受け取った時に毎回 Queue に積まれたフラグメントされたパケットのリストを辿るので 8000 個くらいで CPU をビジー状態に陥らせることができる．
OpenBSD	フラグメントされたパケットを格納する Queue のサイズの上限を決めているので，それ以上のフラグメントされたパケットが来た場合は順次待ち行列内のパケットは破棄される．
Windows	CPU に関しては変化なし，帯域に関しては大量のフラグメントパケットが来ているので Ping が Timeout することもあり．

攻撃１に対する各 OS の挙動

これらの OS の挙動を観察して浮かぶ疑問点は，このようなフラグメントの攻撃を受けた時に悪意ない，通常の通信の確立も困難になるという点である．現状ではフラグメントの起こる確立は前トラフィックの中で微少量でしかないことが多いが，802.11b などを利用した通信においてフラグメントは日常茶飯事に起こることが観測されている．このように悪意ないフラグメントパケットをその他のパケットをどのように分けそれを判別するかの手法に関しては現状ではまったく言及されていない．

またコンピュータウイルス等で OS の MTU を調整できれば非常に広範囲に対してフラグメント化されたパケットを引き起こすことができる．これに関しては感染しても特段影響がないためこのようなウイルスが開発されバラまかれた場合上記の問題は非常に深刻である．

4 攻撃手法２に OS の挙動

この攻撃に関しては Windows2000 のみにしか確認を行っていないため他の OS への言及はさけることとする．またこの攻撃は通常起こりえないフラグメントの形式をとっているためフィルタは簡単でありここでは問題にならない．

通常，同じ内容のフラグメント化 データグラムを連続して送りつけられた場合，明らかにそのような現象に対して OS 側で処理を講じておくべきであるが，Windows2000 にはこの機能が備わっていない．Windows2000 はこのようなパケットを 1 秒間に 150 個近く受け取ると CPU の使用率が 100％になりネットワーク周りや Windows2000 上のアプリケーションが利用できない状態になる．送りつけるデータグラムは ICMP や TCP いずれでもかまわない．

マイクロソフトの製品のなかで該当するものは Windows2000 だけ

ではなく

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT 4.0 Workstation
- Microsoft Windows NT 4.0 Server
- Microsoft Windows NT 4.0 Server, Enterprise Edition
- Microsoft Windows NT 4.0 Server, Terminal Server Edition
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server

となっている[7]

攻撃方法は 2000 年に勧告がだされ現在ではサービスパック２を使用しているユーザには問題がないがこのような脆弱性を持っている OS があるということに注意していただきたい.

5 おわりに

攻撃手法１の各 OS の対応状況に関する場面で述べたように今後の課題としてフラグメント化の起こる通信を悪意ある攻撃からどのように守るかという点が大きな課題である．最初にも書いたようにフラグメントというそれ自体に対する脆弱性がある以上防ぎようのない攻撃であることはいうまでもなく，それらからマシンを守るためには特定の相手とのみ通信を許すような仕組みをとるしかないことが予測されよう.

参考文献

[1] M. Rey, “Internet Protocol,” RFC791, September 1981

[2] G. Ziemba, D. Reed and P. Traina, “Security Considerations for IP Fragment Filtering,” RFC1858, October 1995

[3] I. Miller “Protection Against a Variant of the Tiny Fragment Attack.” RFC3128, June 2001

[4] IP Fragment Reassembly: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-029.asp