Slow HTTP DoS Attackに対する検知と防御の研究

尾崎, 航一 / OZAKI, Koichi

(出版者 / Publisher)
法政大学大学院理工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
60
(開始ページ / Start Page)
1
(終了ページ / End Page)
3
(発行年 / Year)
2019-03-31
(URL)
https://doi.org/10.15002/00022042

Slow HTTP DoS Attack に対する検知と防御の研究

A METHOD FOR DETECTING AND DEFENDING SLOW HTTP DOS ATTACKS

尾崎航一
Koichi OZAKI
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Slow HTTP DoS Attacks keeps all TCP session by sending packets little by little to a Web server with a wait time in between, and it interfere so that genuine users cannot access it. Over the past few years, how to defend against Slow HTTP DoS Attacks has been studied, but many problems remain to be solved. In the proposed method, when a number of sessions exceeds a certain number, the session is closed in descending order of session time. This method prevents false detection of authorized users and prevents attacks that could not be prevented by existing methods. As a result of the evaluation, the proposal method proved to be superior to the existing method from the viewpoint of the high detection rate for Slow HTTP DoS Attacks and the reducing load on the server.

***Key Words** : Slow HTTP DoS Attack*

１．序論

害を行う．同攻撃手法は，TCP セッションの維持の仕方によって，三つに分類されるが，うち二つの対策方法が十分に確立されていない．その一つが Slow HTTP Headers Attack で，この攻撃は待機時間を挟みながら，長大な HTTP リクエストヘッダを送信し続けることにより，TCP セッションを占有する. もう一つが Slow HTTP BODY Attack で, この攻撃は HTTP リクエストヘッダの代わりに HTTP リクエストボディを送信し続ける．本研究では，既存の方法で防げなかった Slow HTTP DoS Attack に対して有効な防御手法を新たに提案する．

２．関連研究

先行研究では, Slow HTTP DoS Attack に対する検知や防御の方法が幾つか知られているが，問題点も多い．例えば，同 IP アドレスからの同時セッション数を制限する方法がある[3]．しかし，複数の正規ユーザと攻撃者が共通の NAT を使い，同じグローバルアドレスで同時に Web サーバを利用した場合，Web サーバは正規ユーザを攻撃者であると誤認識して，アクセスを制限してしまう可能性がある．また攻撃者が IP アドレスの偽装，BOT など複数の IP アドレスを使った攻撃を行った場合，Web サーバを守ることはできない[4].

他の防御方法として，最長パケット間隔や最長セッション時間などパラメータ制限をいくつか行うことで検知率をより高めることが可能である[5]．しかし，最長パケット間隔の制限をしても，その制限値よりパケット間隔が短い攻撃は防げない．また最長セッション時間を制限しても，制限した時間内に Web サーバにアクセスできる最大セッション数(MaxClient)を越えるセッション数の攻撃は防げない．つまり，パラメータ制限をいくつか行っても，パケット間隔が短く，単位時間当たりに張るセッション数が多い攻撃は防ぎきることはできない．

３．提案手法

先行研究では, Slow HTTP DoS Attack に対する検知や防御の方法が幾つか知られているが，問題点も多い．例えば，同 IP アドレスからの同時セッション数を制限する方法がある[3]．しかし，複数の正規ユーザと攻撃者が共通の NAT を使い，同じグローバルアドレスで同時に Web サーバを利用した場合，Web サーバは正規ユーザを攻撃者であると誤認識して，アクセスを制限してしまう可能性がある．また攻撃者が IP アドレスの偽装，BOT など複数の IP アドレスを使った攻撃を行った場合，Web サーバを守ることはできない[4].

他の防御方法として，最長パケット間隔や最長セッション時間などパラメータ制限をいくつか行うことで検知率をより高めることが可能である[5]．しかし，最長パケ

ット間隔の制限をしても，その制限値よりパケット間隔が短い攻撃は防げない．また最長セッション時間を制限しても，制限した時間内に Web サーバにアクセスできる最大セッション数(MaxClient)を越えるセッション数の攻撃は防げない．つまり，パラメータ制限をいくつか行っても，パケット間隔が短く，単位時間当たりに張るセッション数が多い攻撃は防ぎきることはできない．

4．検証方法

検証は大きく分けて二種類の検証をする．一つ目の検証 1 から 5 では，既存の方法である最長パケット間隔や最長セッション時間を制限する手法と提案手法で，どちらの方法が防御に有効かを比較，検証する．検証の際，既存の方法や提案手法を実装した Web サーバに対し，攻撃テストツールを用いてパケット間隔が短いもしくは，単位時間当たりに張るセッションが多い Slow HTTP DoS Attack を行う. 最長パケット間隔や最長セッション時間の制限値は低速または大きな遅延を生じる回線を使用している正規ユーザに配慮した値である．提案手法では，セッション数 100 以上のとき，セッション時間の長いものから順にセッションを切っていく．検証 1 から 5 の設定をまとめたものを表 1 に示す．二つ目の検証 6 から 9 では，低速または大きな遅延を生じる回線を使用している正規ユーザに対して，既存の方法と提案手法で，正規ユーザを誤検知するか否かを検証する．検証 6 から 9 の設定をまとめたものを表 2 に示す.

Web サーバの OS は CentOS 6.5 とし，サーバ機能として Apache 2.2.27 を使用する．MaxClient は 256 とする．既存の防御手法である最長パケット間隔による制限は Apache の Timeout により，最長セッション時間による制限は mod_reqtimeout により実装する．提案手法は Perl5.22 で書いたスクリプトにより実装する．攻撃側クライアントや正規ユーザの OS は Ubuntu 14.04 とする. 攻撃テストツールとして slowhttptest 1.7 を使用し, セッション数の推移の記録も行う．正規ユーザは Chrome のディベロッパーツールを使用し，低速または遅延が大きい通信を行う．

表 1 検証 1 から 5 の設定

	Web サーバの設定			攻撃クライアントの設定	
検証番号	パケット間隔の制限値(s)	セッション時間の制限値(s)	perl script	パケット間隔(s)	セッション数/s
1		10		1	20
2		10		1	40
3	3			5	40
4	3			1	40
5			on	1	40

表 2 検証 6 から 9 の設定

	Web サーバの設定			正規ユーザの設定		
検証番号	セッション時間の制限値(s)	パケット間隔の制限値(s)	perl script	ダウンロード(kb/s)	アップロード(kb/s)	遅延時間(ms)
6	10	3		600	200	125
7	10	3				4000
8			on	600	200	125
9			on			4000

5．結果と評価

検証 1，3，5 ではサービス利用可，検証 2，4 ではサービス利用不可となった．これらの結果から，最長セッション時間を制限する方法は，パケット間隔の短い Slow HTTP DoS Attack に対しては有効だが，単位時間当たりに張るセッション数が多い Slow HTTP DoS Attack に対しては有効ではないことが分かる．また逆に，最長パケット間隔を制限する方法は，単位時間当たりに張るセッション数が多い Slow HTTP DoS Attack に対しては有効だが, パケット間隔の短い Slow HTTP DoS Attack に対しては有効ではないことがわかる．提案手法では，パケット間隔や単位時間当たりに張るセッション数に関係なくセッションを切っていくので，パケット間隔が短く，かつ単位時間当たりに張るセッション数が多い Slow HTTP DoS Attack に対しても有効であることが分かる．

検証 6 から 9 では，全ての検証において，正規ユーザは Web サーバにアクセスすることができた．検証 6，7 では，正規ユーザが低速な回線や大きな遅延を生じる回線を使用していると，パケット間隔が長く，セッション時間も長くなるので，最長セッション時間と最長パケット間隔を制限する方法による正規ユーザの誤検知の対象になると思われたが，そうはならなかった．検証 8，9 では，提案手法で設定した一定のセッション数 100 を超えていないので，セッションは切られなかった．

6．考察

検証 6, 7 において正規ユーザがアクセスできたのは，現在各ブラウザ側で，セッションが切られた際，繋ぎ直す仕様になっているためである．セッションの繋ぎ直しが多くなるとサーバへ負荷がかかるので，サーバへの負荷が少ない点においても提案手法は優れているといえる．しかし，この技術が攻撃者に応用された場合，提案手法でも攻撃を防ぐことはできなくなる．

7．結論

提案方法は, Slow HTTP DoS Attack に対する検知率の高さやサーバへの負荷の観点から，既存の方法より優れていることがわかった．今後の課題は，提案手法の実装方法の改良と，更なる Slow HTTP DoS Attack に対する検知率の向上や正規ユーザの誤検知率の低下，サーバへの負担低減を実現できる理論や実装方法を提案することである．

参考文献

1) AndMen, “About DoS/DDoS Attack,” [online]. Available: http://andmem.blogspot.jp/2014/02/dosattack.html. [retrieved: 1, 2019].

2) E. Cambiaso, G. Papaleo, G. Chiola, and M. Aiello, “Slow DoS attacks: definition and categorisation,” Int. J. Trust Management in Computing and Communications, Volume 1, Number 3-4, pp.300-319, 2013.

3) Jieren Cheng, Jianping Yin, Yun Liu, Zhiping Cai, and Min Li, “DDoS attack detection algorithm using IP address features,” In Frontiers in Algorithmics, pages 207–215. Springer, 2009.

4) Esraa Alomari, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, and Rafeef Alfaris, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers,” Classification and Art. International Journal of Computer Applications, July 2012. Published by Foundation of Computer Science, New York, USA.

5) Koichi Ozaki, Astushi Kanai, Shigeaki Tanimoto, “A Method for Preventing Slow HTTP DoS attacks,” Proceedings of SECUREWARE 2017, Rome, Itary, September 2017, pp.2-6.