L-007

DNS 水責め攻撃効果に関する一考察

Study on effectiveness of DNS water torture

ボルド ムンフバートル * 三村 守 * 田中 秀磨 *
Bold Munkhbaatar Mamoru Mimura Hidema Tanaka

1. はじめに

DNS はドメイン名から IP アドレスへ変換する仕組みであり、ドメインツリーと呼ばれる階層構造で管理されている。これは、ノードでいくつかの階層に区切りを持たせたもので、各階層を分散担当することで負荷を軽減している (図 1)[3]。DNS の問い合わせはまず、ユーザがアクセスできるキャッシュDNS に対して行われる。もし頻繁な問い合わせ内容であればキャッシュDNS で解決されるが、そうでなければドメイン名に対応する権威サーバへの問い合わせが生じる。DNS 水責め攻撃の場合は、故意に存在しない問い合わせ (無効な問い合わせ) を行うことで、権威サーバに対して問い合わせが生じるように仕向ける [6]。さらにボットネットなどを利用して大量の無効な問い合わせを発生させ、権威 DNS を過負荷に陥らせるだけでなく、キャッシュDNS もダウンさせることで、ネットワークをサービス不能な状態に陥らせる。

本研究では DNS 水責め攻撃の効果を向上させるため、三種類の手法を考えそれぞれの効果を調査する。

手法 A) 各 DNS での検索に時間をかけさせる。

手法 B) 物理的に離れた地点のドメイン名を探索させる。

手法 C) ドメイン名登録の仕組みを悪用する。

手法 A) の方法は典型的な DNS 水責め攻撃の手法であり、有効なドメイン名にランダムなサブドメイン名を追加することで実行される。しかしながら攻撃対象のドメイン名と追加するランダムなサブドメイン名の効果の関係は明らかにされていない。

手法 B) の方法は攻撃者の地理的な要素が大きくなる上、DNS に過負荷がかかるというよりは通信自体に負荷を与える攻撃であって、主にキャッシュDNS の通信のリソースへの負荷となる。このため DNS 水責め攻撃としてではなく、別の攻撃手法として対処されている可能性もある。

手法 C) の方法は本論文の主題であり、明示的な指摘がこれまでのところ見られていない。

*防衛大学校情報工学科

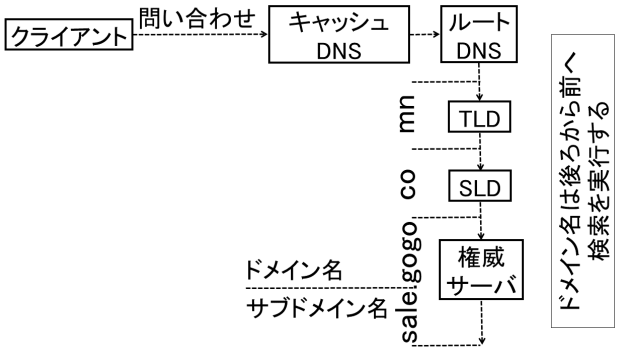

図 1: ドメインツリー

2. 実験環境

DNS 水責め攻撃の効果を観測するためには、ルート DNS、TLD、SLD など各 DNS サーバでの負荷状態の観測を必要とする。しかしながら、これを実現するのが困難なため、攻撃者側から見て、DNS 要求に対する返事が到達するまでの時間 (問い合わせ時間) を DNS 全体に対する負荷と見積る。

本実験では実験用キャッシュDNS を用意し、攻撃者が最初に利用するサーバにおける処理状況を観測する。実験用キャッシュDNS の上流 DNS は所属する防衛大学校の DNS サーバとした。実験用のドメイン名は 563Mbyte であり news.ycombinator.com[1]からダウンロードした。

3. 手法 A に関する実験

図 2 にドメイン名の構成を示す。この仕組みからランダムなサブドメイン名を生成には以下の 2 通りが考えられる。

A-1) 各ノードにおけるサブドメイン名の長さに注目し、検索に負荷をかける。

A-2) ノード数に注目し、権威サーバーにおけるループ検索に負荷をかける。

実験対象として、www.[A].gogo.mn という正規のドメイン名を用いた。A-1 に対し[A]へ 2 文字から 63 文字ま

[1]https://news.ycombinator.com/item?id=10367342

Copyright © 2017 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

表 1: サブドメインの長さとノード数の平均時間

長さ	平均時間 (秒)	ノード数	平均時間 (秒)
2	0.11182	2	0.12413
5	0.11165	5	0.11409
8	0.11121	10	0.11812
9	0.11262	15	0.11316
10	0.11162	20	0.11217
20	0.11199	25	0.11316
30	0.11256	30	0.11511
40	0.11132	35	0.11616
63	0.11191	37	0.11713

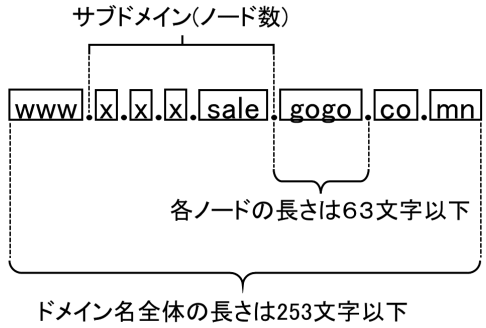

図 2: ドメイン名構成

でランダムなサブドメイン名を 10,000 個生成し問い合わせ時間を測定した。結果の一部を表 1 に示す。次に A-2 に対し A へ 1 文字 (“X”) だけのサブドメインを 1 個から 121 個まで与えて、問い合わせ時間を測定した。ただしノード数が 37 を超えると正常な問い合わせが成立しなかった。結果の一部を表 1 に示す。これらの結果から、長さもノード数増加させても効果がないと結論できる。従って、現時点で手法 A は既に対策が取られている可能性があり、DNS 水責め攻撃において有効な手法ではない。

4. 手法 B に関する実験

問い合わせ時間が長い方がキャッシュDNS の通信リソースを効率的に占有できるので、キャッシュDNS から物理的に距離が遠い権威サーバへの問い合わせを生じさせることで DoS 状態を生じさせることができると考えられる。問い合わせ時間の差を観測するため、国内から近い国として韓国、遠い国としてアルゼンチンを対象とした。実験用のドメイン名から co.kr 及び com.ar のドメイン名をそれぞれ 100 個ずつランダムに選び、平均時間を算出した。この結果、韓国へは平均 0.20 秒、アルゼンチンへは平均 0.46 秒となった。この結果から前述の予想通り、2 倍程度の問い合わせ時間の差が生じている。従って、一般的には手法 B は有効的と考えられるが、場合によって、国名を表すドメイン名を持つサーバーが対象国に存在せず、実際にはもっと物理的に近い場所に設置されていることがあることを実験中に発見した。従って、必ずしも手法 B が成立しないケースもあることを留意する必要がある。

表 2: ドメイン登録仕組み

登録	IP アドレス	説明
あり	あり	正常用途 (タイプ 1)
	なし	先取りドメイン (タイプ 2)
なし	ありで使用中	Web サービスを利用しない用途
	割振済みだが未使用	Darknet 等
	なし	空きアドレス

5. 手法 C に関する実験

ドメイン名の取得においては、高額転売目的とした、先取りに代表されるドメイン名紛争問題がある。そのためドメイン名の登録利用状態は表 2 のようにまとめられる。DNS 水責め攻撃の対象となるのは登録がある場合であるから、正常用途 (タイプ 1) と先取りドメイン (タイプ 2) を対象とする。実験用のドメイン名からタイプ 1 とタイプ 2 をそれぞれ 100 個ずつ選び、これまでと同様に問い合わせ時間を測定した。尚、タイプ 2 はこれまでの実験から想定外に時間がかかることを発見し、WHOIS により登録状態を確認した。その結果、タイプ 1 で平均 0.74 秒、タイプ 2 で平均 10.88 秒を要した。タイプ 2 の結果は UDP 通信の仕様からの異常であり、パケット解析を実行したところ、クライアント側では約 2 秒で Timeout しており、合計 4 回の再送を実行していることが分かった。

この状況が上流 DNS へどのような影響があるかを解析するため、実験用のドメイン名から各タイプの 1000 個ドメイン名を実験用キャッシュDNS に問い合わせし処理状況を観測した。その結果を表 3 に示す。この結果から実際に使用されているタイプ 1 は検索に時間がかからず CPU 負荷も小さいが、検索結果がキャッシュされるためメモリ負荷が増加することが分かる。一方、タイプ 2 は上述のように 4 回検索を実行するので CPU 負荷が増加していると考えられる。これは表 3 の CPU 負荷の結果からも確認できるが、詳細な解析は今後の課題である。一方で、タイプ 2 の検索結果はキャッシュされることはないのでメモリ負荷が増加することはない。タイプ 1 とタイプ 2 の同じドメイン名を 100 回問い合わせる実験を行った場合、それぞれ平均 0.11 秒、平均 10.25 秒という結果

Copyright © 2017 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

表 3: 各タイプのキャッシュDNS 最大負荷

	CPU 負荷 (%)	メモリ負荷 (%)
タイプ 1	3.795	0.466
タイプ 2	13.372	0.229

が得られ、キャッシュ効果に関する予想がおおよそ正しいと結論した。タイプ 2 のドメイン名の問い合わせを実行した場合、明らかにキャッシュDNS では解決できないので、図 1 に示したようにルート DNS ⇒ TLD ⇒ SLD の順に負荷を与えると考えられる。その時、表 3 に示したようにメモリ負荷は与えないが大きい CPU 負荷を与えることが可能と考えられる。

6. 発見した新たな脆弱性

タイプ 2 の問い合わせを実行すると上述のようにクライアント側で Timeout していることを確認した。これは Timeout 設定時までに DNS からの返答がなかったことを意味しているため、ルート DNS 以下へ負荷をかけられるものと考えられる。また後述のように登録済みであるが未使用のドメイン名は大量に存在するため、攻撃者にとって有利な状況となっている。実験に用いたクライアントの OS は Windows8.1 であり、再送回数の default 値は 4 であるため、第 5 節で示した結果が得られた。再送回数の設定は OS に依存すると考えられ攻撃効果に影響するので今後、調査する予定である。

タイプ 2 の背景には、商標関係などで第三者利用を防ぐ目的がある。これは誤解を招きやすいサイトを開設することによるサギ行為などが行われることで、信用問題へ発展させないためである。そのため、実際に使用しないがイメージを損なう可能性があるドメイン名は一通り取得する。このような事情により、タイプ 2 のドメイン名は実際には大量に存在する。ここでのポイントは、これらタイプ 2 のドメイン名は保持者が必ず存在する点にある。この攻撃は検知されやすいと考えられるが、一方で攻撃が検知された場合、このような攻撃に利用されたタイプ 2 のドメイン保持者には少なからずペナルティが発生する可能性がある。例えば、利用していないドメイン名が DNS 利用負荷の原因として公表されることによるイメージダウンである。この結果生じ得るドメイン名放棄は前述のサギサイト開設などのリスクを増大させ、結果的に個人への攻撃としても成立できる。逆にこのようなリスクを無視できるのであれば、大量にタイプ 2 のドメイン名を取得することで特定の TLD もしくは SLD に対する攻撃環境を整えることができる。

尚、同様の状態はランダムに生成したドメイン名でも生じることができると予想したが、このような問い合わせ時間の長期化はできなかった。これは TLD と SLD で登録状態を確認しているためと考えられるが、詳細な解析は今後の課題である。

7. まとめ

本研究では DNS 水責め攻撃の効果を向上させるため、三種類の手法を考えそれぞれの効果を調査した。手法 A は従来手法の発展であるが、ほとんど効果が見られなかった。手法 B はネットワーク環境からおよそ予想できる結果であるものの、現実的な脅威になるとは考えにくい結果を得た。手法 C は本研究での新たな発見であり、具体的な脆弱性であると考えられる。今後はより詳細な攻撃効果の解決と新たな攻撃手法への発展について取り組む予定である。

参考文献

[1] Elz, Z: Clarifications to the DNS Specificaion, University of Melborne (online), available from (https://tools.ietf.org/html/rfc2181)

[2] Joe, M: Random dns queries with random sources, The Tri Tech Group (online), available from (http://www.gossamer-threads.com/lists/nanog/users/169123)

[3] Mockapetris, P: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, The Internet Engineering Task Force (online), available from (http://www.ietf.org/rfc/rfc1035.txt)

[4] Nominum: Latest Internet Plague Random Subdomain Attacks (online), available from (https://nominum.com/wp-content/uploads/2014/10/Nominum-Whitepaper-Latest-Internet-Plague-Random-Subdomain-Attacks.pdf)

[5] Secure64: Water Torture: A Slow Drip DNS DDos Attack, Secure64 Software Corporation (online), available from (https://secure64.com/water-torture-slow-drip-dns-ddos-attack/)

[6] Yuya Takeuchi, Takuro Yoshida, Ryotaro Kobayashi, Masahiko Kato, Hiroyuki Kishimoto, “Detection of the DNS Water Torture Attack by Analyzing Features of the Subdomain Name” Journal of Information Processing Vol.24 No.5 p.p.793-801 (Sep. 2016)

Copyright © 2017 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.