technische universität
dortmund

Bachelorarbeit

Auswirkungen von autoritativen DNS-Infrastrukturausfällen

Ege Girit

22. August 2022

Begutachtung:
Prof. Dr. Christian Rossow
Jonas Bushart

Technische Universität Dortmund
Fakultät für Informatik
Lehrstuhl V - Programmiersysteme
Fachgruppe Softwaretechnik sicherer Systeme
https://sse.cs.tu-dortmund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Struktur der Arbeit

Diese Bachelorarbeit ist in 6 Teilen gegliedert. Der erste Teil gibt eine Zusammenfassung von Domain Name System. Darauf aufbauend wird dann erklärt, warum wir glauben, dass es Forschungsbedarf an Resolververhalten bei einem Cyberangriff gibt. Die Merkmale, die wir untersuchen möchten, die Möglichkeiten der Testquellen und Metriken für einen Angriffserfolg werden in Teil 2 angegeben. In Teil 3 wird die Testumgebung vorgestellt und der Ablauf der Simulationen sowie Analyseverfahren deutlich gemacht. Die erzielten Ergebnisse werden in Teil 4 mithilfe graphischer Darstellungen angezeigt. Diese Ergebnisse werden dann in Teil 5 evaluiert um Schlussfolgerungen zu ziehen, was die Tests zeigen. Abschließend wird diskutiert, ob und wie viel unsere Ergebnisse von der Realität abweichen und ob es mehr Forschung in diesem Bereich nötig ist.

1.2 Domain Name System

Der Bedarf für Domain Name System entstand aus der Notwendigkeit, dass man die IP Adressen von Servern, die für Menschen kompliziert zum Merken sind, gerne unter einem leicht merkbaren Namen ansprechen möchte. Mithilfe DNS kann man dann die Namen eines Servers zu ihren zugehörigen IP Adresse auflösen.

Vor Domain Name System gab es nur eine zentralisierte Textdatei (hosts.txt), die aus statischen Zuordnungen bestand, die es Benutzern ermöglichten, die gespeicherten Webseiten zu ihren zugehörigen IP Adressen zu auflösen. Diese Textdatei musste nach jeder Änderung aktualisiert und an alle Computer verteilt werden, um eine Zuordnung zwischen diesen Namen und ihren entsprechenden Netzwerkadressen bereitzustellen. Aufgrund der wachsenden Anzahl von Hosts und Websites ist es heute unmöglich, ein derart zentralisiertes System zu verwalten. Der Verwaltungsaufwand, der mit der Verwaltung aller möglichen Domainnamen im Internet verbunden ist, wäre zu groß und diese zentrale Datenbank wäre nicht gut skalierbar. Angesichts dieser Herausforderungen wandten sich die Designer von DNS vom flachen Namensansatz ab und übernahmen daher ein dezentralisiertes Modell mit einer hierarchischen Namensarchitektur, das 1986 zum Internetstandard wurde. Die offizielle Dokumentation dieser Standards ist in RFC 1034 und 1035 beschrieben. Die hosts.txt-Datei existiert jedoch immer noch für verschiedene Zwecke wie Leistungsverbesserung und URL-Filterung.

Heute haben wir eine global verteilte Sammlung von Datenbanken, die eine Baumstruktur bilden. Die Systemadministration wird vollständig dezentralisiert und die Delegation an Organisationen abgegeben. Es gibt 3 Hauptfunktionen von DNS:

1. Namensraum (Überprüfung, ob der Syntax/Struktur der Domain gültig ist)
2. Namensregistrierung (Ob der zu registrierenden Namen eindeutig ist)
3. Namensauflösung

Bei dieser Arbeit konzentrieren wir uns auf die Namensauflösung in DNS. Bei der Auflösung von Namen zu ihren dazugehörigen IP Adressen, spielen mehrere Aktoren eine Rolle. Diese Aktoren sind:

- Der Client, der eine Anfrage sendet
- Recursive Resolver
- Root Name Server
- TLD Server
- Authoritative Name Server

Da es sich in diesem Prozess viele Server beteiligen, kann eine Anfrage von einem Client viel Netzwerkressourcen gebrauchen, bis die Auflösung erfolgt oder fehlschlägt. Daher gibt es Optimisationsmechanismen wie caching, die die Laufzeit verkürzt und Ressourcen spart. Der Zweck des Cachings besteht darin, zuvor angefragte Daten vorübergehend zu speichern, damit zukünftige Anforderungen für diese Daten schneller bedient werden können, ohne alle Server in der DNS-Hierarchie zu kontaktieren.
... [Rollen von Root/Recursive/TLD/Auth Resolver kurz beschreiben]

1.3 Motivation der Arbeit

DNS ist ein relativ grundlegendes Protokoll und wurde nicht im Hinblick auf Sicherheit entwickelt. Es gibt viele Arten von Angriffen, die darauf abzielen, Schwachstellen im DNS auszunutzen. Falls es Probleme bei der Namensauflösungen gibt, gibt es kein alternatives Protokoll und die Konnektivität zwischen den Benutzern und dem Server ist gefährdet. Dies macht das DNS ein beliebtes Ziel für Hacker. Viele Systeme zählen darauf, dass das DNS funktionstüchtig bleibt. Deswegen sind Fehler oder Angriffe auf DNS besonders von Bedeutung für alles darauf aufbauende. Wenn DNS ausfällt, fällt das Internet aus.
Falls ein autoritativer Name-Server unerreichbar ist, muss der Client in der Regel mit Wartezeiten und Fehlern rechnen. Es fehlt uns jedoch das Wissen über Resolververhalten während eines Cyberangriffs/Ausfalls.

In dieser Arbeit wird das Verhalten von Resolver bei einem (teilweisen) Ausfall von kritischen autoritativen DNS-Server untersucht. Unsere Aufgabe ist es, aus den Ergebnissen unserer Tests verstehen zu können, ob das Verhalten von Resolvern bestimmte Mustern verfolgt.

Die Erkenntnisse dieser Verhaltensanalyse könnten helfen, den Einfluss der einzelnen Parameter bei der Kommunikation mit Name-Server besser zu verstehen und das Verhalten der Resolver vorherzusagen.

In diesem Bereich existieren ähnliche/ansatzweise Forschungen, die die Seite der Clients untersuchen. Unsere Arbeit unterscheidet sich ...

2 Struktur des Experiments

2.1 Zu testende Parameter

Da wir keinen echten Cyberangriff auf unserem authoritativen Nameserver durchführen können, werden wir einen Angriff durch variieren der verschiedenen Metriken an unserem Server simulieren. Bei einem DDoS Angriff entsteht beim Server eine hohe Netzwerklast und dadurch wird verursacht, dass einige Netzwerkpakete nicht erfolgreich gesendet werden können. Diese Situation simulieren wir, indem wir **packetloss** bei unserem Server simulieren. Dabei verwenden wir verschiedene raten an packetloss (10, 20, 40, 60, 80, 90, 95) für unsere Experimente... Wir messen die rate an TCP **Truncations**. Mit Truncation diktiert der Server, dass er ab dem Zeitpunk nur komplett über TCP angesprochen wird. Das ist wichtig um sicherzustellen, dass der Resolver immer Antworten bekommt.
DNS Cookies: DNS Cookies provide protection for the clients, domain name owners , the innocent and DNS Servers. It is a lightweight mitigation and not a complete solution for all security problems. There are certain attacks they don't protect against. The client who makes a DNS query can get a false answer/response. If an attackers answers the client query before the legitimate DNS server, attackers response is accepted on the client side (if client is a recursive resolver -> cache poisoning.) Cookies protect an innocent victim against spoofed IP address attacks. An attacker can forge a DNS query using a victims IP address, and the DNS Servers will respond to the victims IP address (The response will be bigger than the query because of UDP(amplification), many dns servers will contact the victim IP like a botnet -> Reflection attack). An authoritative name server can protect itself from DDoS attacks, they identify spoofed IP's and the server limits its misuse in a reflection, responding with TC bit (TCP).
Response Rate Limiting: No response vs. truncation.. DNSSEC NSEC3 Caching: ..

2.2 Testquellen

Da es (im freien?) viele Arten von Resolvern gibt, möchten wir unsere Experimente so durchführen, dass wir eine möglichst große Überdeckung an alle Arten von Resolvern haben, um eine Verallgemeinerung des Resolververhaltens festzustellen. Die Arten von Resolvern, die wir bei unseren Experimenten getestet haben, sind folgende:

- RIPE Atlas
- "Wild" Open Resolvers (found via DNS scans)
- "Popular" Open Resolvers (e.g., from Wikipedia)...

[Beschreibung von Ripe Atlas, Wild open resolvers, populer open resolvers...]

2.3 Metriken für einen Angriffserfolg

In unseren Experimenten möchten wir wissen, ob der simulierte Cyberangriff gegen die Abwehrmechanismen von DNS erfolgreich ist. Dafür messen wir folgende Metriken: ... DNS response failure rate (client side), DNS response rate (server side), DNS response latency, Rate of stale records, Name server migrations (and reasons thereof), Multiple NS records, One NS with multiple A/AAAA records, (Anycast), Page load time (Web context), Attack amplification, Query duplicates, Switch-over rate to TCP...

3 Details der Testumgebung

3.1 Serveraufbau

Für die Simulation der DNS-Infrastruktur haben wir an der Universität Saarland eine eigene Nameserver ausgesetzt. Zu diesem Zweck wird ein authoritativer Name Server auf einem Linux Rechner konfiguriert. Um mit DNS interagieren zu können, verwenden wir BIND9 als Software. Die Konfigurationsdateien der Server, die wir bei unseren Experimenten verwendet haben, sind auf unseren Repository verfügbar. Ein Angriff auf dem Server wird mit (iptables?) simuliert, das eine beliebige Rate an Paketen ignoriert. Unser authoritativer Name Server agiert sowohl als ein Server, der die DNS-Antworten an einen Resolver gibt, als auch ein Client, der die DNS-Anfragen stellt. Damit wir zwischen den Client und Server Netzwerkverkehr unterscheiden können, verwenden wir für den Client und den Server unterschiedliche IP Adressen.

3.2 DNS Anfragen erstellen

DNS Python zum erstellen und senden der DNS Anfragen, random source port, destination port 53...

3.3 Paketerfassung und Analyse

Zum Protokollieren von DNS-Abfragen/-Antworten und Datenpaketen wird das linux Software tcpdump verwendet. Um die Netzwerkverkehr für die jeweilige Resolverkommunikationen zu isolieren, verwenden wir wireshark filter...

3.4 Plotten von Ergebnissen

Nachdem wir die Experimente durchgeführt haben, werden die gespeicherten Log-Dateien mithilfe eines Skirpts evaluiert. Diese gespeicherte Log-Daten werden in JSON Format umgewandelt und die interessierende Teile extrahiert. Um die Daten visualisieren zu können, wird das matplotlib Bibliothek verwendet.

3.5 Vorgehensweise

[Was machen die Skripte...]

4 Ergebnisse

Packet loss Tests: ...
Truncation Tests: ...
DNS Cookies Tests: ...
Response Rate Limiting Tests: ...
DNSSEC NSEC3 caching Tests: ...

5 Schlussfolgerungen/Evaluation

...

6 Fazit/Diskussion

...

Literaturverzeichnis

Eidesstattliche Versicherung

(Affidavit)

Name, Vorname
(surname, first name)

Matrikelnummer
(student ID number)

☐ Bachelorarbeit
(Bachelor's thesis)

☐ Masterarbeit
(Master's thesis)

Titel
(Title)

Ich versichere hiermit an Eides statt, dass ich die vorliegende Abschlussarbeit mit dem oben genannten Titel selbstständig und ohne unzulässige fremde Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

I declare in lieu of oath that I have completed the present thesis with the above-mentioned title independently and without any unauthorized assistance. I have not used any other sources or aids than the ones listed and have documented quotations and paraphrases as such. The thesis in its current or similar version has not been submitted to an auditing institution before.

Ort, Datum
(place, date)

Unterschrift
(signature)

Belehrung:
Wer vorsätzlich gegen eine die Täuschung über Prüfungsleistungen betreffende Regelung einer Hochschulprüfungsordnung verstößt, handelt ordnungswidrig. Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 50.000,00 € geahndet werden. Zuständige Verwaltungsbehörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten ist der Kanzler/die Kanzlerin der Technischen Universität Dortmund. Im Falle eines mehrfachen oder sonstigen schwerwiegenden Täuschungsversuches kann der Prüfling zudem exmatrikuliert werden. (§ 63 Abs. 5 Hochschulgesetz - HG -).

Die Abgabe einer falschen Versicherung an Eides statt wird mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe bestraft.

Die Technische Universität Dortmund wird ggf. elektronische Vergleichswerkzeuge (wie z.B. die Software „turnitin") zur Überprüfung von Ordnungswidrigkeiten in Prüfungsverfahren nutzen.

Die oben stehende Belehrung habe ich zur Kenntnis genommen:

Official notification:
Any person who intentionally breaches any regulation of university examination regulations relating to deception in examination performance is acting improperly. This offense can be punished with a fine of up to EUR 50,000.00. The competent administrative authority for the pursuit and prosecution of offenses of this type is the Chancellor of TU Dortmund University. In the case of multiple or other serious attempts at deception, the examinee can also be unenrolled, Section 63 (5) North Rhine-Westphalia Higher Education Act (*Hochschulgesetz, HG*).

The submission of a false affidavit will be punished with a prison sentence of up to three years or a fine.

As may be necessary, TU Dortmund University will make use of electronic plagiarism-prevention tools (e.g. the "turnitin" service) in order to monitor violations during the examination procedures.

I have taken note of the above official notification:*

Ort, Datum
(place, date)

Unterschrift
(signature)

***Please be aware that solely the German version of the affidavit ("Eidesstattliche Versicherung") for the Bachelor's/ Master's thesis is the official and legally binding version.**