Computers & Security 135 (2023) 103426

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Configuration anormaly detection and resolution risk assessment of authoritative domain name server

Chao Li, Yanan Cheng, Zhaoxin Zhang *, Ping Yu *

Faculty of Computing, Harbin Institute of Technology, Harbin, 150001, China

ARTICLE INFO

Keywords:
Anomaly detection
Authoritative domain name server
Risk assessment
Configuration anomaly
Active measurement

ABSTRACT

Authoritative domain name servers (referred to as authoritative servers) play a critical role in the Domain Name System (DNS) by resolving domain names to specific IP or CNAME records, ensuring seamless internet access. However, misconfigurations in authoritative servers can introduce risks to domain name resolution. This paper proposes a comprehensive approach to analyze and evaluate the configuration risks of authoritative servers. We develop a tool called "AuthDetect" to detect configuration anomalies in authoritative servers, and leveraging this tool, we conduct anomaly detection and analyze resolution risks from three perspectives: resolution latency, content, and reliability. Our evaluation indicates that 90% of the domains have a favorable overall resolution risk (below 0.13), but varying levels of risks exist: (1) 60% face resolution latency risk, (2) only 8.33% of domain names exhibit content risk, and (3) almost all domain names (99.8%) experience resolution reliability risk, primarily due to inadequate server configuration. These findings offer valuable data support for domain name managers, providing insights into the current configuration status of authoritative servers and contributing to maintaining a healthy and stable DNS system operation.

1. Introduction

The Domain Name System (DNS) plays a vital role in resolving domain names into IP addresses and is crucial for numerous network applications like CDN, load balancing, and service discovery. DNS is a distributed database organized hierarchically through a delegation structure. Within the DNS system, the DNS authoritative domain name server (hereinafter referred to as "authoritative server") holds all DNS records for specific domain names and provides domain name resolution services to users. The stability and reliability of the DNS system rely on the trustworthiness and security of authoritative servers. As reported by Verisign, there are 351.5 million registered domain names across all top-level domains (TLDs) in the second quarter of 2022 (Verisign, 2022). With the increasing number of registered domain names, the scale of the DNS system grows, making authoritative servers more susceptible to security attacks such as DDOS (Perlroth, 2016; Williams, 2019), Cache poisoning (Alharbi et al., 2019), and domain name hijacking (Rascagneres, 2019; Hirani et al., 2019). These attacks disrupt normal domain name resolution, adversely affecting the regular operation of the DNS system. Additionally, inadequate or abnormal configuration of authoritative servers themselves can also impact the DNS system's normal resolution services, leading to downtime (Fryman, 2014; Tung, 2019) and security risks (Kovacs, 2018; Rashid, 2016). This research focuses on investigating internal configuration anomalies and aims to detect such anomalies, conducts in-depth analysis, and evaluates domain name resolution risks. This serves as the motivation for this study. Previous studies have examined various configuration anomalies of authoritative domain name servers, including zone dependency in domains (Xu et al., 2022; Moura et al., 2021; Jiang et al., 2018), lame delegation (Pappas et al., 2004; Sato et al., 2022), and Glue RRs configuration detection (Kakarla et al., 2022; Kakarla, 2022). However, these studies primarily focus on specific configuration properties' anomalies. There is a lack of comprehensive analysis and evaluation of the domain name resolution risks caused by configuration anomalies. In this paper, we address this gap by performing a risk assessment of configuration anomalies from three perspectives: resolution latency, resolution content, and resolution reliability. By integrating risk assessments from these perspectives, we provide an overall evaluation of each domain name's authoritative server configuration risk.

Our key contributions are as follows:

* Corresponding authors.
E-mail addresses: 20B903094@stu.hit.edu.cn (C. Li), chengyn@hit.edu.cn (Y. Cheng), zhangzhaoxin@hit.edu.cn (Z. Zhang), yuping0428@hit.edu.cn (P. Yu).

https://doi.org/10.1016/j.cose.2023.103426
Received 10 April 2023; Received in revised form 27 July 2023; Accepted 8 August 2023
Available online 16 August 2023