



(51) International Patent Classification:
H04L 61/4511 (2022.01) *H04L 9/40* (2022.01)

(21) International Application Number:
PCT/US2023/071170

(22) International Filing Date:
28 July 2023 (28.07.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/370,135 02 August 2022 (02.08.2022) US

(71) Applicant: **CENTURYLINK INTELLECTUAL PROP-
ERTY LLC** [US/US]; 1025 Eldorado Blvd., Broomfield,
Colorado 80021 (US).

(72) Inventors: **WOODWORTH, John R.B.**; c/o CenturyLink
Intellectual Property LLC, 1025 Eldorado Boulevard,

Broomfield, Colorado 80021 (US). **BALLEW, Dean**; c/
o CenturyLink Intellectual Property LLC, 1025 Eldorado
Boulevard, Broomfield, Colorado 80021 (US).

(74) Agent: **LEIBOLD, Gregory D.**; LEWIS ROCA
ROTHGERBER CHRISTIE LLP, P.O. Box 29001, Glen-
dale, California 91209-9001 (US).

(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,
KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA,
NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO,
RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

(54) Title: SYSTEMS AND METHODS FOR MITIGATING DOMAIN NAME SYSTEM AMPLIFICATION ATTACKS

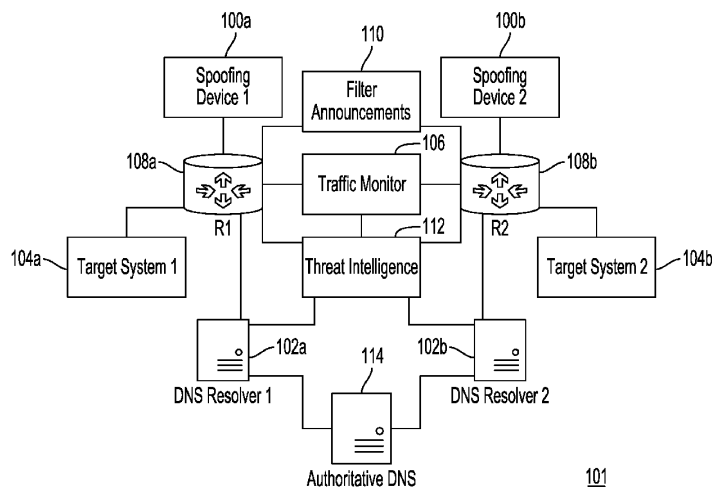


FIG. 1

(57) Abstract: Systems and methods for mitigating DNS amplification attacks are provided. In one example, a threat intelligence system collects data about the requests received by a DNS server, and/or responses generated by the DNS server. The threat intelligence system triggers a threat mitigation action upon detecting evidence (in one or more forms) of a DNS amplification attack. The threat mitigation action may include filtering DNS responses generated by the DNS server. The filtering rule may indicate that a DNS response in which the payload size is above a threshold payload size is to be dropped. In examples, the payload threshold size is dynamically set by the threat intelligence system using a machine learning model to minimize the filtering of DNS responses for valid DNS queries, while maximizing filtering of DNS responses for malicious DNS queries

[Continued on next page]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*