Παραγωγική Τεχνητή Νοημοσύνη (Generative Artificial Intelligence) για την Αυτόματη Παραγωγή Κώδικα Αντιμετώπισης Δικτυακών Επιθέσεων σε Επίπεδο Δεδομένων

Οι επιθέσεις άρνησης παροχής υπηρεσιών (Distributed Denial of Service, DDoS) αποτελούν ένα από τα επικρατέστερα προβλήματα για τους διαχειριστές δικτυακών υποδομών. Οι επιθέσεις αυτές στοχεύουν σε δίκτυα, εφαρμογές ή/και υπηρεσίες, προσπαθώντας να παρεμποδίσουν την ομαλή λειτουργία τους. Για την ανίχνευση (detection) και αντιμετώπιση (mitigation) επιθέσεων DDoS έχουν αναπτυχθεί πολυάριθμα συστήματα ασφαλείας [1].

Ωστόσο, η επεξεργασία δικτυακής κίνησης στο user space εισάγει σημαντικές καθυστερήσεις στην ανίχνευση και αντιμετώπιση των επιθέσεων DDoS. Ως αποτέλεσμα, οι user space μηχανισμοί ασφαλείας αδυνατούν να ανταποκριθούν στο διαρκώς αυξανόμενο μέγεθος των σύγχρονων επιθέσεων DDoS. Για το σκοπό αυτό αναζητούνται λύσεις σε σύγχρονες τεχνολογίες προγραμματισμού στο επίπεδο δεδομένων (data plane) δικτυακών συσκευών (switches) ή καρτών δικτύου που επεξεργάζονται τη δικτυακή κίνηση χωρίς να την προωθήσουν στο user space [2].

Μία διαδεδομένη μέθοδος προγραμματισμού στο επίπεδο δεδομένων είναι το eXpress Data Path (XDP) [3]. Ωστόσο, η ανάπτυξη προγραμμάτων σε XDP απαιτεί εξοικείωση με τις ιδιαιτερότητες της τεχνολογίας. Το γεγονός αυτό συνήθως δυσκολεύει την υιοθέτηση νέων τεχνολογιών σε παραγωγικά περιβάλλοντα.

Στη διπλωματική αυτή θα χρησιμοποιηθούν αλγόριθμοι παραγωγικής τεχνητής νοημοσύνης (Generative Artificial Intelligence) και Large Language Models (LLM's) για την αυτοματοποίηση της παραγωγής κώδικα σε XDP με σκοπό την ανίχνευση και αντιμετώπιση επιθέσεων DDoS. Συγκεκριμένα, θα πραγματοποιηθεί αναζήτηση/δημιουργία κατάλληλων κειμένων (prompts) που θα δοθούν στο ChatGPT [4] με σκοπό την ταχύτερη παραγωγή κώδικα σε XDP. Μέρος της διπλωματικής θα είναι και ο έλεγχος της ορθής λειτουργίας των παραγόμενων προγραμμάτων μέσω κατάλληλων τυπικών μεθόδων (formal methods) [5], καθώς και η αξιολόγηση της απόδοσής τους μέσω πειραμάτων στην υποδομή του εργαστηρίου NETMODE. Για την πειραματική αξιολόγηση των παραπάνω μοντέλων θα χρησιμοποιηθούν δημόσια διαθέσιμα σύνολα δεδομένων καλόβουλης και κακόβουλης δικτυακής κίνησης, τα οποία χρησιμοποιούνται ευρέως στη βιβλιογραφία, π.χ. [6].

[1] S.T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, Volume 15, pp. 2046-2069, March 2013
[2] R. Bifulco and G. Rétvári, "A Survey on the Programmable Data Plane: Abstractions, Architectures, and Open Problems", 19th IEEE International Conference on High Performance Switching and Routing (HPSR), pp. 1-7, June 2018
[3] T. Høiland-Jørgensen et al., "The Express Data Path: Fast Programmable Packet Processing in the Operating System Kernel", in the 14th international conference on emerging networking experiments and technologies, December 2018
[4] ChatGPT, https://openai.com/chatgpt/
[5] J. Liu et al., "P4v: Practical Verification for Programmable Data Planes", Conference of the ACM Special Interest Group on Data Communication, pp. 490-503, August 2018
[6] DDoS Evaluation Dataset (CIC-DDoS2019), https://www.unb.ca/cic/datasets/ddos-2019.html