Ανάπτυξη Κατανεμημένης Πλατφόρμας με Χρήση Blockchain και Smart Contracts για την Ιδιωτική Ανταλλαγή Πληροφοριών Ασφαλείας

Οι σύγχρονοι μηχανισμοί για την ανίχνευση δικτυακών απειλών βασίζονται σε αφθονία δεδομένων για την ορθή λειτουργία τους. Ωστόσο, πολλοί οργανισμοί δε διαθέτουν τον απαραίτητο όγκο δεδομένων για την ανάπτυξη έγκυρων συστημάτων ανίχνευσης επιθέσεων. Κατά συνέπεια, καθίσταται αναγκαία η συνεργασία πολλών διαφορετικών οργανισμών για την ανταλλαγή δεδομένων καλόβουλης και κακόβουλης δικτυακής κίνησης.

Παρά την αναγκαιότητα για συνεργασία ανάμεσά τους, πολλοί οργανισμοί αρνούνται την παροχή πρόσβασης σε ευαίσθητα δεδομένα τους, καθώς φοβούνται για την ασφάλεια των πελατών τους. Έτσι, πολλοί οργανισμοί δεν δέχονται να συμμετάσχουν σε πλατφόρμες ανταλλαγής πληροφοριών ασφαλείας, π.χ. Indicators of Compromise (IoC), όπως είναι η πλατφόρμα MISP [1].

Στην κατεύθυνση αυτή, οι τεχνολογίες του Blockchain και των Smart Contracts έχουν αποδειχθεί πολλά υποσχόμενες για την ανάπτυξη πλατφορμών ανταλλαγής δεδομένων ασφαλείας [2]. Οι τεχνολογίες αυτές εξασφαλίζουν ότι η ταυτότητα των οργανισμών που συμμετέχουν σε αυτές δεν αποκαλύπτεται άμεσα στους άλλους συμμετέχοντες, ευνοώντας την ιδιωτική ανταλλαγή δεδομένων. Ο συνδυασμός τέτοιων τεχνολογιών με πιθανοτικές δεδομένων, οι οποίες αποθηκεύουν πληροφορίες σε hashed μορφή, αυξάνουν την προστασία της ιδιωτικότητας των δεδομένων των οργανισμών.

Η διπλωματική θα εξετάσει τεχνολογίες Blockchain και Smart Contracts με σκοπό την ανάπτυξη μιας κατανεμημένης πλατφόρμας για την ανταλλαγή IoC's ανάμεσα σε συνεργαζόμενους οργανισμούς με έμφαση στην προστασία της ιδιωτικότητας (privacy) των οργανισμών αυτών. Για την ενίσχυση της ιδιωτικότητας των ανταλλασσόμενων δεδομένων, θα εξεταστεί η χρήση πιθανοτικών δομών δεδομένων, π.χ. Cuckoo Filters [3] και MinHashes [4], ώστε να καθίσταται δύσκολη η άμεση εξαγωγή δεδομένων από αυτές.

Ως εφαρμογή θα εξεταστεί η ανταλλαγή δεδομένων για την προστασία του συστήματος DNS. Συγκεκριμένα, θα εξεταστεί η ανταλλαγή ζωνών DNS μέσω Cuckoo Filters [5] για τη συνεργατική αντιμετώπιση επιθέσεων DDoS που απειλούν Authoritative DNS Servers. Παράλληλα, θα εξεταστεί η ανταλλαγή περιλήψεων δικτυακής κίνησης μέσω MinHashes για την ανίχνευση δικτυακών πόρων που έχουν μολυνθεί από κακόβουλο λογισμικό που βασίζεται στη χρήση Domain Generation Algorithms (DGA's) [6].

Στα πλαίσια της διπλωματικής θα γίνει χρήση γλωσσών προγραμματισμού ειδικού σκοπού για την ανάπτυξη των απαραίτητων Smart Contracts, π.χ. Solidity [7], Smart Python [8], καθώς επίσης θα απαιτηθεί η εγκατάσταση ενός τοπικού Blockchain για την εκτέλεσή τους, π.χ. Ethereum node [9].

[1] MISP Project, https://www.misp-project.org/
[2] E. Bandara et al., "LUUNU: Blockchain, MISP, Model Cards and Federated Learning Enabled Cyber Threat Intelligence Sharing Platform", in IEEE Annual Modeling and Simulation Conference (ANNSIM), 2022
[3] B. Fan et al., "Cuckoo filter: Practically Better than Bloom", in the Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies, 2014

[4] MinHash, https://en.wikipedia.org/wiki/MinHash
[5] N. Kostopoulos, “Enabling Privacy-Aware Zone Exchanges Among Authoritative and Recursive DNS Servers”, in Proceedings of the Applied Networking Research Workshop, 2020
[6] D. Plohmann et al., “A Comprehensive Measurement Study of Domain Generating Malware”, in the 25th USENIX Security Symposium, 2016
[7] Solidity, https://docs.soliditylang.org/en/v0.8.17/
[8] SmartPy, https://smartpy.io/
[9] Ethereum, https://ethereum.org/en/