ΕΙΣΗΓΗΣΗ ΘΕΜΑΤΟΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

ΠΡΟΣ ΤΟ ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΟΥ ΔΙΕΘΝΟΥΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΕΛΛΑΔΟΣ

Προτεινόμενος τίτλος διατριβής:

"Ευφυείς Τεχνικές για την Ανίχνευση και Ανάλυση Κοινωνικής Φύσεως Κυβερνοαπειλών"

Θεματική Περιοχή / Πεδίο: Κυβερνοασφάλεια, Διάγνωση Απάτης, Μηχανική Μάθηση στην Ασφάλεια Πληροφοριών, Επιθέσεις Κοινωνικής Μηχανικής

Λέξεις κλειδιά:

- Κοινωνική Μηχανική (Social Engineering)
- Phishing (Ηλεκτρονικό "Ψάρεμα")
- Μηχανική Μάθηση (Machine Learning - ML)
- Βαθιά Μάθηση (Deep Learning - DL)
- Ανίχνευση Απάτης (Fraud Detection)
- Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing - NLP)
- Κυβερνοασφάλεια (Cybersecurity)
- Spear Phishing
- URL Analysis (Ανάλυση URL)
- Αυτοματοποιημένη Ανίχνευση (Automated Detection)

Συνοπτική περιγραφή του προτεινόμενου θέματος:

Η Ανίχνευση Επιθέσεων Κοινωνικής Φύσεως είναι μια διαρκώς εξελισσόμενη πρόκληση στον τομέα της κυβερνοασφάλειας, καθώς οι επιτιθέμενοι υιοθετούν συνεχώς νέες τακτικές για να παρακάμψουν τους παραδοσιακούς μηχανισμούς ασφαλείας. Η Κοινωνική Μηχανική παραμένει ένας από τους κυριότερους φορείς παραβιάσεων πληροφοριακών συστημάτων, εκμεταλλευόμενη την ανθρώπινη ψυχολογία για την απόκτηση εμπιστευτικών δεδομένων. Αυτή η έρευνα επικεντρώνεται στην ανάπτυξη και αξιολόγηση προηγμένων τεχνικών για την αυτοματοποιημένη ανίχνευση και την αποτροπή επιθέσεων, όπως τα phishing emails και οι παραπλανητικές ιστοσελίδες.

Θα εξεταστούν μέθοδοι Μηχανικής Μάθησης (ML), Επεξεργασίας Φυσικής Γλώσσας (NLP) και τη χρήση Βαθιάς Μάθησης (Deep Learning), για την ανάλυση χαρακτηριστικών όπως το περιεχόμενο κειμένου, οι επικεφαλίδες ηλεκτρονικού ταχυδρομείου, και η δομή URL, με στόχο την κατασκευή ενός ανθεκτικού και αποτελεσματικού συστήματος έγκαιρης προειδοποίησης. Στόχος είναι η εξαγωγή σύνθετων, μη εμφανών χαρακτηριστικών από το περιεχόμενο και τα μεταδεδομένα των επικοινωνιών. Έμφαση θα δοθεί στην ανάπτυξη μοντέλων ανίχνευσης σε πραγματικό χρόνο που μπορούν να ενσωματωθούν σε υπάρχουσες υποδομές email gateways, βελτιώνοντας δραστικά την ανθεκτικότητα του πληροφοριακού συστήματος έναντι αυτών των διαρκών και ύπουλων απειλών.

Ενδεικτικές Βιβλιογραφικές αναφορές:

1. Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep learning for phishing detection: Taxonomy, current challenges and future directions. *Ieee Access*, *10*, 36429-36463.

2. Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, Banu Diri, Machine learning based phishing detection from URLs, Expert Systems with Applications, Volume 117, 2019, Pages 345-357, https://doi.org/10.1016/j.eswa.2018.09.029.
3. Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing detection system through hybrid machine learning based on URL. *IEEE Access*, *11*, 36805-36822.
4. Yun Lin, Ruofan Liu, Dinil Mon Divakaran, Jun Yang Ng, Qing Zhou Chan, Yiwen Lu, Yuxuan Si, Fan Zhang, Jin Song Dong, Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages, 30th USENIX Security Symposium, Proceedings of the, August 11–13, 2021, pp 3793-3810
5. Kytidou, E., Tsikriki, T., Drosatos, G., & Rantos, K. (2025). Machine learning techniques for phishing detection: A review of methods, challenges, and future directions. Intelligent Decision Technologies, 18724981251366763.
6. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
7. Alhogail, A., & Alsabih, A. (2021). Applying machine learning and natural language processing to detect phishing email. Computers & Security, 110, 102414.