Προτεινόμενα θέματα για εκπόνηση μεταπτυχιακής διατριβής					
α/α	**Περιγραφή Θέματος**	**Προαπαιτούμενα**	**Πηγές**	**Υπεύθυνος Θέματος**	**email**
1	Ανάπτυξη κατανεμημένου συστήματος διαχείρισης δεδομένων σε φυσικό δίκτυο με χρήση raspberry pi's και τεχνολογιών Blockchain, (υποδομή αντίστοιχη με το Inter-Planetary File System -IPFS). Στην παρούσα εργασία θα γίνει μια σύντομη επισκόπηση της διεθνούς βιβλιογραφίας σχετικά με κατανεμημένα συστήματα δεδομένων και θα αναπτυχθεί μια υποδομή σε Raspberry pi - model 4.	Blockchain (Ethereum or Hyperledger), Programming skills (Solidity or Go), Dockers	(1) x0001_Nizamuddin, Nishara, et al. "Decentralized document version control using ethereum blockchain and IPFS." Computers & Electrical Engineering 76 (2019): 183-197. (2) x0001_Vimal, S., and S. K. Srivatsa. "A new cluster p2p file sharing system based on ipfs and blockchain technology." Journal of Ambient Intelligence and Humanized Computing (2019): 1-7. (3) x0001_Kumar, Randhir, and Rakesh Tripathi. "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain." 2019 Fifth International Conference on Image Information Processing (ICIIP). IEEE, 2019.	Μάλαμας Βαγγέλης	bagmalamas@unipi.gr
2	**Δημιουργία Εικονικής Πλατφόρμας IoT στο Metaverse: Μελέτη σεναρίου ασφάλειας** Βήματα Υλοποίησης: 1. Δημιουργία Εικονικών Συσκευών IoT στο Unity. 2. Χρήση 3D μοντέλων για τις IoT συσκευές. 3. Ανάπτυξη Scripts για Αλληλεπίδραση. 4. Δημιουργία κλάσεων για τη συμπεριφορά των συσκευών. 5. Ενσωμάτωση >2 Πρωτοκόλλων (MQTT/CoAP/WIFI/BLE etc). 6. Χρήση βιβλιοθηκών όπως MQTTnet ή CoAP.NET. (red blue team σενάριο)	Unity ή υλοποίηση σε τοπική τοπολογία με έτοιμα εργαλεία και scripts	https://www.sciencedirect.com/science/article/pii/S1084804523000942 https://ar5iv.labs.arxiv.org/html/2212.13993 https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/ https://create.unity.com/road-to-metaverse	Κούτρας Δημήτρης	dkoutras@unipi.gr
3	Ανάλυση και εφαρμογή μεθοδολογίας αυτοματοποιημένης ανάλυσης binaries. Τα βασικά βήματα υλοποίησης περιλαμβάνουν: Καθορισμός Σκοπού: Ορισμός των χαρακτηριστικών (π.χ. metadata, συναρτήσεις, κώδικας). Γλώσσα Προγραμματισμού: Χρήση Python ή Bash για την ανάπτυξη του script. Ανάπτυξη Script : Δημιουργία κώδικα που να: Εξετάζει τα binaries για metadata (π.χ. version, author). Ανιχνεύει εξαρτήσεις (π.χ. βιβλιοθήκες). Εκτελεί στατική ανάλυση (π.χ. strings, entropy). Ενσωμάτωση Εργαλείων Ανάλυσης: Χρήση εργαλείων όπως objdump, strings, ή radare2 για εξαγωγή πληροφοριών. Δημιουργία Αναφοράς: Δημιουργία αναφοράς με τα αποτελέσματα της ανάλυσης σε μορφή JSON ή CSV. Δοκιμή και Βελτιστοποίηση: Δοκιμή του script σε διάφορα binaries με σκοπό την επαλήθευση της αποτελεσματικότητας και τη βελτιστοποίηση του κώδικα.	Binaries automation	https://ieeexplore.ieee.org/abstract/document/9766127 https://www.cisa.gov/sites/default/files/2022-02/ICSJWG%20-%20Vulnerability%20Identification%20in%20Binary%20Files.pdf https://www.infosecinstitute.com/resources/vulnerabilities/binary-exploitation-techniques/ https://link.springer.com/chapter/10.1007/978-3-642-22540-6_1 https://dl.acm.org/doi/abs/10.1145/3304082.3304083	Κούτρας Δημήτρης	dkoutras@unipi.gr
4	Ανάλυση μονοπατιών επιθέσεων (Attack path analysis). Ανάπτυξη/βελτίωση και υλοποίηση μεθοδολογίας ανάλυσης επικινδυνότητας για μονοπάτια επιθέσεων σε κυβερνο-φυσικά συστήματα (cyber-physical attack path risk assessment). Συνδιαστική εκμετάλλευση ευπαθειών (vulnerability chaining) με την χρήση τεχνικών μηχανικής μάθησης και τεχνητής νοημοσύνης: Δημιουργία μεθοδολογίας /εργαλείου που θα κάνει χρήση υφιστάμενων οντολογιών ασφάλειας προκειμένου να προβαίνει σε: Αναγνωριση ευπαθειών με την χρήση αυτοματοποιημένων εργαλείων εργαλειών ή/και custom scripts Σειριακή εκμετάλλευση ευπαθειών από/προς διαφορετικές πλατφόρμες λογισμικού (CPEs) με την χρήση προκαθορισμένων τεχνικών εκμετάλλευσης (e.g. ATT&CK) Σειριακή εκμετάλλευση ευπαθειών από/προς διαφορετικές πλατφόρμες λογισμικού (CPEs) με την χρήση τεχνικών μηχανικής μάθησης και τεχνητής νοημοσύνης Δημιουργία τελικών διανυσμάτων (cummulative CVSS vectors) κατά το πρότυπο CVSS 3.1 & 4.0 Στα παραπάνω θα πρέπει να περιλαμβάνεται και η σχετική έρευνα για ήδη υπάρχουσες σχετικές μεθοδολογίες (research papers) αλλά και μεθοδολογία επαλήθευσης των αποτελεσμάτων Το εργαλείο θα πρέπει να περιλαμβάνει γραφική διεπαφή και οδηγίες για τις βασικές λειτουργίες του	Πολύ καλή γνώση python. Καλή γνώση μεθοδολογιών ανάλυσης επικινδυνότητας Καλή γνώση εφαρμογής LLMs (LLM/OPS) Επιθυμητά: micro-services (dockers) micro-services orchestration (Kubernetes)	https://link.springer.com/chapter/10.1007/978-3-030-95484-0_2 https://www.sciencedirect.com/science/article/abs/pii/S0167404821001401 https://link.springer.com/chapter/10.1007/978-3-030-95484-0_13	Στέλλιος Ιωάννης	jstellios@unipi.gr
5	Ανάπτυξη αυτοματοποιημένου μηχανισμού χαρτογράφησης και καταγραφής πληροφοριακών αγαθών ενός πληροφοριακού συστήματος. Σε αυτή την εργασία θα μελετηθούν οι τεχνικές μοντελοποίησης και χαρτογράφησης αγαθών (asset modeling and asset inventorying). Θα αναπτυχθεί αυτοματοποιημένο εργαλείο για την καταγραφή αγαθών (h/w, s/w assets)	Bash scripting, powershell scripting, python, Network and endpoint logging(eg. Windows Security Events, sysmon), EDR technologies, Asset Inventory Tools, Familiarity with MITRE Frameworks and databases Επιθυμητά: micro-services (dockers) micro-services orchestration (Kubernetes)		Χρήστος Γρηγοριάδης	cgrigoriadis@unipi.gr
6	Ανάπτυξη βάσης δεδομένων αδυναμιών, απειλών και άλλων δεδομένων κυβερνοασφάλειας. Αναζήτηση και απτικοποίηση δεδομένων σε μορφή γράφου	Python, Εμπειρία σε API-parsing scripts, neo4j, open-source vector databases (eg Qdrant), Γνώση σχετικών Open Source Cybersecurity Threat Intelligence (OSCTI) και ειδικά των MITRE και NIST Frameworks/Databases Επιθυμητά: micro-services (dockers) micro-services orchestration (Kubernetes)		Χρήστος Γρηγοριάδης	cgrigoriadis@unipi.gr
7	Ανάπτυξη συστήματος ανίχνευσης κλοπής ταυτοτήτων (identity theft) στο Metaverse βασισμένο σε μοντέλα Τεχνητής Νοημοσύνης. Περιγραφή: Καθώς οι χρήστες αποκτούν εικονικές ταυτότητες και συμμετέχουν σε κοινωνικές, οικονομικές και επαγγελματικές δραστηριότητες, η ασφάλεια των ψηφιακών τους δεδομένων είναι κρίσιμη. Το προτεινόμενο σύστημα θα χρησιμοποιεί μοντέλα Τεχνητής Νοημοσύνης (AI) για την ανάλυση συμπεριφορών και μοτίβων χρήσης, με στόχο να εντοπίζει ύποπτες δραστηριότητες που υποδηλώνουν κλοπή ή πλαστοπροσωπία. Το σύστημα θα βασίζεται σε αλγόριθμους μηχανικής μάθησης για την ανίχνευση ανωμαλιών (anomaly detection) και θα συνδυάζει δεδομένα από πολλαπλές πηγές, όπως η ανάλυση συμπεριφοράς των χρηστών (User Behaviour Analytics - UBA), η αναγνώριση μοτίβων αλληλεπιδράσεων, καθώς και η σύγκριση με κανονικές δραστηριότητες των ταυτοποιημένων χρηστών. Το μοντέλο AI θα εκπαιδευτεί με τη χρήση δεδομένων τόσο πραγματικών όσο και συνθετικών, για να αναγνωρίζει τα σενάρια στα οποία υπάρχει πιθανότητα κλοπής ταυτότητας. Ο φοιτητής θα χρειαστεί να: Διερευνήσει τις υπάρχουσες τεχνολογίες ασφάλειας και ανίχνευσης κλοπής ταυτοτήτων στο Metaverse. Μελετήσει μοντέλα τεχνητής νοημοσύνης, όπως οι αλγόριθμοι ανίχνευσης ανωμαλιών και οι τεχνικές ανάλυσης συμπεριφοράς. Σχεδιάσει και να αναπτύξει το σύστημα ανίχνευσης με χρήση εργαλείων και πλατφορμών AI (π.χ. Python, TensorFlow).			Μάλαμας Βαγγέλης	bagmalamas@unipi.gr
8					
9					