Τα προτεινόμενα θέματα για εκπόνηση πτυχιακής εργασίας ταξινομούνται για ευκολία σε 3 υποκατηγορίες του χώρου της Ασφάλειας: (Α) Ασφάλεια Δικτύων, (Β) Ασφάλεια Πληροφοριακών Συστημάτων και (Γ) Ερευνητικά Θέματα.

α/α	Επιστ. Περιοχή	Περιγραφή Θέματος	Προαπαιτούμενα	Πηγές	Υπεύθυνος Θέματος	email
1	(Α)	Σχεδιασμός και μελέτη ασφάλειας IoT συστήματος. Σε αυτή την εργασία καλείστε να αναπτύξτε μία μικρή υποδομή για την απομακρυσμένη διαχείριση, παρακολούθηση και έλεγχο συστήματος καταγραφής θερμοκρασίας, καθώς και να μελετήσετε την ασφάλεια του συστήματος. Η ανάπτυξη της υποδομής μπορεί να βασίζεται σε έτοιμα kit ή σε DIY εξοπλισμό (raspberry pi, arduino). Θα σχεδιαστεί και θα υλοποιηθεί μηχανισμός για την ασφάλεια της απομακρυσμένης διαχείρισης και επικοινωνίας.	Python Scripting/PHP scripting Debian Based OS Raspberry Pi / Arduino Networking	https://retropie.org.uk/	Χρήστος Γρηγοριάδης	cgrigoriadis@unipi.gr
2	(Α)	Τα firewalls, ids, honeypots αποτελούν τις βασικότερες τεχνολογίες για την προστασία ενός δικτύου. Σκοπός της εργασίας είναι η δημιουργία μίας ολοκληρωμένης τοπολογίας δικτύου και η ενσωμάτωση των παραπάνω τεχνολογιών πάνω σε αυτή. Η εργασία περιλαμβάνει τα παρακάτω: 1) Δημιουργία εικονικού δικτύου το οποίο θα περιλαμβάνει κατ ελάχιστο ζώνες ITZ, DMZ, καθώς και εξωτερικό (μη έμπιστο) δίκτυο. 2) Υλοποίηση τεχνολογιών ασφάλειας δικτού (firewall, IDS και honeypot) της επιλογής σας, ανάλογα με την τοπολόγια και τις υπηρεσίες δικτύου που έχετε δημιουργήσει. 3) Υλοποίηση και καταγραφή τουλάχιστον δύο επιθέσεων (π.χ. botnets, DoS, scannning, unauthorized access κτλ) από το εξωτερικό δίκτυο προς το εσωτερικό (ITZ και DMZ). Στη διαδικασία της καταγραφής μπορούν να χρησιμοποιηθούν forensics analysis tools. 4) Ανάλυση αποτελεσμάτων, σύγκριση και πιθανή διόρθωση των μηχανισμών ασφάλειας που υλοποιήσατε στο βήμα 1. Σύγκριση για το πώς ανταποκρίθηκαν οι μηχανισμοί ασφάλειας σε κάθε επίθεση υπό διαφορετικές συνθήκες (πριν και μετά την υλοποίηση των μηχανισμών ασφάλειας). Όλα τα εργαλεία που θα χρησιμοποιηθούν θα είναι εργαλεία ανοικτού λογισμικού.	Debian based OS, Linux internals, Good networking knowledge	https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/ https://linux.die.net/man/8/iptables https://wiki.debian.org/iptables https://www.ossec.net/ https://www.comparitech.com/net-admin/network-intrusion-detection-tools/ https://www.hackingarticles.in/configure-suricata-ids-ubuntu/ https://medium.com/@jeremiedaniel48/install-and-setup-cowrie-honeypot-on-ubuntu-linux- https://github.com/paralax/awesome-honeypots https://null-byte.wonderhowto.com/forum/bypassing-ids-firewall-using-meterpreter-over-ss https://www.kalilinux.in/2018/12/bypassing-firewalls-nmap.html https://tools.kali.org/information-gathering/fragrouter https://adsecurity.org/?p=2921 https://www.verodin.com/post/bypassing-antivirus-for-your-antivirus-bypass https://www.packetaddict.com/post/intrusion-detection-using-powershell	Κούτρας Δημήτρης	dkoutras@unipi.gr
3	(Γ)	Το BLE το Z-Wave και το ZigBee αποτελούν μέχρι στιγμής ορισμένα από τα βασικότερα πρωτόκολλα στην λειτουργία ενός δικτύου διασυνδεδεμένων συσκευών (IoT). Σκοπός της εργασίας είναι η ανάλυση των πρωτοκόλλων, ο τρόπος λειτουργίας τους, το προτεινόμενο περιβάλλον για την εφαρμογή τους, τα πλεονεκτήματα, τα μειονεκτήματα, οι διαφορές, οι ευπάθειες αλλά και τα μέτρα αντιμετώπισης αυτών. Στο πρακτικό μέρος, καλείστε να υλοποιήσετε δύο ή και παραπάνω επιθέσεις που σχετίζονται σε ένα από τα παραπάνω πρωτόκολλα. Οι επιθέσεις μπορούν είτε να υλοποιηθούν μέσω ειδικού εξοπλισμού είτε μέσω κάποιου script σε Python μαζί με την βοήθεια έτοιμων εργαλείων για Bluetooth “hacking”. Βασικά βήματα: 1. Καθορισμός τοπολογίας που θα γίνουν οι επιθέσεις 2. Υλοποίηση των δύο ή και παραπάνω επιθέσεων (Η MIA ΘΑ ΕΙΝΑΙ Man In The Middle) 3. Αναλυτικό Report με τις καταγεγραμμένες ευπάθειες (CVE) της συσκευής (θύματος) 4. Ανίχνευση της ευπάθειας που εκμεταλλευτήκατε (εάν υπάρχει) κατά τη διάρκεια της επίθεσης Τα ζητούμενα μπορούν να αλλάξουν και να προσαρμοστούν στις δυνατότητες αλλά και στον αριθμό των φοιτητών.	IoT, protocol infrastructure, Protocol Security.	https://gattack.io/ https://www.hackers-arise.com/getting-started-with-bluetooth-hack https://duo.com/decipher/bluetooth-hacking-tools-comparison https://linuxhint.com/bluetooth_security_risks/ https://nis-summer-school.enisa.europa.eu/2018/cources/IOT/nis-summer-school-damien-ca https://github.com/crypt0b0y/BLUETOOTH-DOS-ATTACK-SCRIPT https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf https://ieeexplore.ieee.org/abstract/document/6295953 http://ijeecs.iaescore.com/index.php/IJEECS/article/view/23100/14495 https://francozappa.github.io/about-bias/ https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf https://www.link-labs.com/blog/bluetooth-zigbee-comparison https://www.iwavesystems.com/iot-future-ble-zigbee-embeddedtechnology https://www.digi.com/blog/post/zigbee-vs-bluetooth-choosing-the-right-protocol https://www.link-labs.com/blog/zigbee-vs-bluetooth Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Securit	Κούτρας Δημήτρης	dkoutras@unipi.gr

4	(Γ)	Στα IoT networks (δίκτυα διασυνδεδεμένων συσκευών), το LoraWAN αποτελεί ένα από τα πιο διαδεδομένα πρωτόκολλα. Σκοπός της εργασίας είναι •Η ανάλυση του πρωτοκόλλου, ο τρόπος λειτουργίας του, η σύγκριση με άλλα πρωτόκολλα αλλά και η ανάλυση των χαρακτηριστικών του. •Να γίνει κατανοητό τι είναι τα LoraWAN stacks και να γίνει εφαρμογή τους. Σαν δεύτερο μέρος προτείνεται η υλοποίηση μίας τοπολογίας σε κάποιον προσομοιωτή όπως Opnet, ns3, ns2, OMNeT++ . Η τοπολογία έχει θέμα την τοποθέτηση αισθητήρων με σκοπό την πρόληψη πυρκαγιών. Αρχικά θα πρέπει να παρουσιαστεί ο τύπος της τοπολογίας που έχει επιλεχθεί σε σχέση με άλλες (πχ. κεντρικοποιημένη) Στον προσομοιωτή θα πρέπει να φαίνονται: •Οι κόμβοι της τοπολογίας ανάλογα με τον ρόλο που θα έχουν •Οι συνδέσεις μεταξύ τους •Τα τεχνικά χαρακτηριστικά του κάθε κόμβου Με τα επιπλέον features του προσομοιωτή (μετρήσεις γραφήματα) 1.Οι τιμές των αισθητήρων (θερμοκρασία υγρασία κλπ) 2.Η αποδοτικότητα της επικοινωνίας (ταχύτητα, αξιοπιστία) μετά από πειραματικές τιμές (Fuzzing), Αλλαγές στην τοπολογία κλπ 3.Ζητήματα ασφάλειας a.Τεχνικά που προκύπτουν από τα παραπάνω TEST b.Θεωρητικά που προκύπτουν από ευπάθειες που έχουν καταγραφεί σε τέτοιου είδους τοπολογίες που βασίζονται στο πρωτόκολλο LoraWAN.	IoT, protocol infrastructure, Communication protocols, Simulation tools.	https://lora-alliance.org/about-lorawan https://tech-journal.semtech.com/open-source-stacks-for-lorawan https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/ https://github.com/TheThingsNetwork/lorawan-stack https://github.com/Lora-net/LoRaMac-node https://omnetpp.org/download-items/FLoRA.html https://link.springer.com/chapter/10.1007/978-981-10-5041-1_88 https://www.researchgate.net/publication/334616557_Design_and_Implementation_of_Op https://ieeexplore.ieee.org/abstract/document/8090518 https://dl.acm.org/doi/epdf/10.1145/3199902.3199913 Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Securit	Κούτρας Δημήτρης	dkoutras@unipi.gr
5	(Γ)	Τα συστήματα κατανεμημένου καθολικού (blockchain) έγιναν περισσότερο γνωστά μέσα από τις διάφορες εφαρμογές ψηφιακών νομισμάτων (π.χ. Bitcoin, Litecoin, Stellar etc) ενώ πλέον η εφαρμογή τους εκτείνεται σε πολλούς διαφορετικούς τομείς όπως η εφοδιαστική αλυσίδα, η υγεία, η ανταλλαγή κεφαλαίων κ.α. Η παρούσα εργασία έχει σαν σκοπό την αξιοποίηση εργαλείων ελέγχου ασφάλειας (Securify, Mythril, Slither) και σχετικής βιβλιογραφίας για την ανάλυση ευπαθειών σε ενεργά έξυπνα συμβόλαια του δικτύου Ethereum. Η εργασία πέρα απο την θεωρητική τεκμηρίωση σχετικά με την ανάλυση ευπαθειών σε έξυπνα συμβόλαια θα περιλαμβάνει και πρακτικό μέρος στο οποίο μέσω της εφαρμογής των εργαλείων ανάλυσης ευπαθειών σε ενεργά έξυπνα συμβόλαια θα γίνεται κατηγοριοποίηση των συχνά εμφανιζόμενων ευπαθειών.	Blockchain and Cryptography basics, Open source Security tools, Code analysis	(1) Parizi, R. M., Dehghantanha, A., Choo, K. K. R., & Singh, A. (2018). Empirical vulnerability analysis of automated smart contracts security testing on blockchains. arXiv preprint arXiv:1809.02702. (2)_x0001_He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart contract vulnerability analysis and security audit. IEEE Network, 34(5), 276-282. (3)Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654. (4)_x0001_Rameder, H. (2021). Systematic review of ethereum smart contract security vulnerabilities, analysis methods and tools. (5) Feist, J., Grieco, G., & Groce, A. (2019, May). Slither: a static analysis framework for smart contracts. In 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (pp. 8-15). IEEE. (6) Vivar, A. L., Orozco, A. L. S., & Villalba, L. J. G. (2021). A security framework for Ethereum smart contracts. Computer Communications, 172, 119-129.	Μάλαμας Βαγγέλης	bagmalamas@unipi.gr
6	(Γ)	Η αναζήτηση λύσεων για την ιχνηλάτηση προϊόντων στην εφοδιαστική αλυσίδα ήταν και παραμένει στο επίκεντρο των τεχνολογικών εξελίξεων και απασχολεί μεγάλες εταιρίες ανάπτυξης λογισμικού. Τα προηγούμενα χρόνια η δημιουργία cloud υπηρεσιών σε συνδυασμό με την χρήση αισθητήρων ενσωματώθηκαν από την πλειοψηφία των εταιριών του κλάδου. Πλέον αναζητούνται κατανεμημένες λύσεις που θα μειώνουν περαιτέρω το κόστος και θα αυξάνουν τις δυνατότητες. Σκοπός της παρούσας εργασίας είναι η ανάπτυξη συστήματος για την ιχνηλάτηση εμπορευμάτων στην εφοδιαστική αλυσίδα (supply chain tracking system) βασισμένη σε τεχνολογίες Blockchain. Συγκεκριμένα για τις ανάγκες της εργασίας ζητήται να αναπτυχθεί μια web-based υποδομή για την διαχείριση πληροφοριών προερχόμενα απο το οικοσύστημα της εφοδιαστικής αλυσίδας με εφαρμογή μηχανισμών ασφάλειας όπως για παράδειγμα μηχανισμός για την ακεραιότητα των δεδομένων.	Blockchain basics, Programming skills	(1)_x0001_Tian, Feng. "An agri-food supply chain traceability system for China based on RFID (2)_x0001_Casino, Fran, et al. "Blockchain-based food supply chain traceability: a case study i (3)_x0001_Dasaklis, Thomas K., Fran Casino, and Constantinos Patsais. "A traceability and auc (4)_x0001_Mondal, Saikat, et al. "Blockchain inspired RFID-based information architecture fo	Μάλαμας Βαγγέλης	bagmalamas@unipi.gr
7	(Γ)	Ανάπτυξη αρθρώματος (module) για την γραφική αναπαράσταση δικτυακών επιθέσεων. Σε αυτή την εργασία θα αναπτυχθεί ένα module για ένα γραφικό περιβάλλον περιγραφής και οπτικοποίησης (visualization) δικτυακών διαδρομών επίθεσης (attack paths). 1) Δημιουργία διεπαφής για την περιγραφή των διασυνδέσεων/αλληλεπιδράσεων μεταξύ συστημάτων. Ο χρήστης θα μπορεί να σχεδιάζει γραφικά ένα δίκτυο από διασυνδεδεμένες συσκευές. 2) Δημιουργία διαπεφής για την περιγραφή των δικτυακών διαδρομών επίθεσης. Οι διαδρομές επίθεσης θα δίνονται ως είσοδος (π.χ. σε δομημένο κείμενο, xml κτλ) και το υπό ανάπτυξη module θα πρέπει να δημιουργεί μία γραφική αναπαράσταση των επιθέσεων με τη μορφή γράφων ή/και δένδρων. Π.χ. προβολή κάθε διαδρομής επίθεσης για ένα σύστημα-στόχο. Προβολή όλων των διαδρομών επίθεσης, κτλ.	Προγραμματισμός σε γλώσσα python	Networkx (python library for creating graphs and networks) https://pypi.org/project/network py2neo, https://py2neo.org/2020.0/ Matplotlib, https://python-graph-gallery.com/matplotlib/	Χρήστος Γρηγοριάδης	cgrigoriadis@unipi.gr