|  |  |  |
| --- | --- | --- |
| **Περιγραφή Θέματος** | **Προαπαιτούμενα** | **Πηγές** |
| **Στατική και δυναμική ανάλυση κινητών εφαρμογών:** Η εργασία αυτή αφορά τη στατική και δυναμική ανάλυση κινητών εφαρμογών σε Android και iOS περιβάλλοντα. Για την ανάλυση θα γίνει εφαρμογή τεχνικών αντίστροφης μηχανικής (reverse engineering) και ανάλυσης πηγαίου κώδικα (source code audit) για τον εντοπισμό και την αξιολόγηση μηχανισμών ασφαλείας [1], [2] σε αρχεία APK και IPA.[1]: <https://source.android.com/security>[2]: <https://support.apple.com/guide/security/welcome/web> | Καλή γνώση Java.Καλή γνώση του Λειτουργικού Συστήματος Linux. Καλή γνώση του TCP/IP stack και των πρωτοκόλλων DHCP, DNS, HTTP. | [1]: <https://source.android.com/security>[2]: <https://support.apple.com/guide/security/welcome/web> |
| **Πολιτικές Ασφάλειας – Ανάλυση κανόνων firewall**Η μελέτη των κανόνων που υλοποιούνται στα τείχη προστασίας αποτελούν τον βασικό τρόπο ελέγχου εφαρμογής των πολιτικών ασφαλείας που αφορούν την κίνηση των πακέτων μέσα και έξω από το δίκτυο του οργανισμού.Σκοπός της εργασίας είναι η μελέτη των κανόνων firewall τύπου IPTABLES ή NFTABLES με στόχο την σύγκριση των αποτελεσμάτων της μελέτης αυτής με την υπάρχουσα πολιτική[14][17].Βήμα1:\*Δημιουργία κανόνων που αφορούν την κίνηση πακέτων μέσω διαφόρων πρωτοκόλλων και τεχνολογιών, π.χ.: HTTP/HTTPS, FTP, SMTP, SSH. Oι κανόνες αυτοί [ΚΠ – κανόνες Πολιτικής] θα αποτελούν την βέλτιστη πολιτική του οργανισμού και δίδονται σε φυσική γλώσσα.\*Δημιουργία Δοκιμαστικών κανόνων [ΔΚ] και εξαγωγή αυτών απομακρυσμένα με bash scriptΒήμα2 :\*Δημιουργία python script για text data analysis – regex. To script θα αναγνωρίζει για ποια πρωτόκολλα υπάρχουν κανόνες – πολιτικές [02][03][04][05] στους [ΔΚ].! Εάν η αναγνώριση των κανόνων και ο διαχωρισμός τους ανά πρωτόκολλο γίνει με αλγόριθμο ML classification [ Logistic Regression- Naive Bayes- K-Nearest Neighbors- Decision Tree- Support Vector Machines ή NLP [Policy->Segmentation->(Text Cleaning)->Vectorization->(Interpretation)] η υλοποίηση μπορεί να σταματήσει εδώ!Βήμα3 : Έλεγχος των [ΔΚ] για κάθε πρωτόκολλο ξεχωριστά σε σχέση με τους [ΚΠ] με σκοπό να αξιολογηθεί σε κάποιο βαθμό (π.χ. ποσοστιαία) η συμβατότητα των κανόνων (επαλήθευση δηλαδή ότι οι κανόνες υλοποιούν σωστά την πολιτική ασφαλείας που έχει τεθεί από την αρχή).O έλεγχος μπορεί να υλοποιηθεί με δύο τρόπους είτε με έτοιμα εργαλεία [01][10][11], είτε με πολλαπλούς ελέγχους μέσω python script, είτε μετατρέποντας τους κανόνες [ΔΚ] και [ΚΠ] σε XML και συγκρίνοντάς τους.[06][07][08][09]. | Καλή γνώση δικτυακών πρωτοκόλλων και τεχνολογιών ασφάλειας δικτύωνΚαλή γνώση python ή άλλης scripting γλώσσας | [01] <https://github.com/diekmann/Iptables_Semantics>[02] <https://towardsdatascience.com/python-text-analysis-with-the-schrutepy-package-234bc70f3916>[03] <https://www.nltk.org/>[04] <https://textblob.readthedocs.io/en/dev/>[05] <https://spacy.io/>[06] <https://numpy.org/>[07] <https://matplotlib.org/stable/tutorials/introductory/pyplot.html>[08] <https://bokeh.org/>[09] <https://pypi.org/project/gensim/>[10] Marmorstein, R., & Kearns, P. (2005). A tool for automated iptables firewall analysis. USENIX 2005 Annual Technical Conference, 71–81.[11] Diekmann, C., Hupel, L., Michaelis, J., Haslbeck, M., & Carle, G. (2018). Verified iptables Firewall Analysis and Verification. Journal of Automated Reasoning, 61(1-4), 191–242.[12] Al-Shaer, E., & Hamed, H. (2004). Modeling and Management of Firewall Policies. IEEE Transactions on Network and Service Management, 1(1), 2-10.[13] Golnabi, K., Min, R., Khan, L., & Al-Shaer, E. (2006). Analysis of Firewall Policy Rules Using Data Mining Techniques. In 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006 (pp. 305-315).[14] Al-Shaer, E. (2014). Automated Firewall Analytics.[15] Katic, T., & Pale, P. (2007). Optimization of Firewall Rules. In 2007 29th International Conference on Information Technology Interfaces (pp. 685-690).[16] Shanbhag, S., & Wolf, T. (2011). Automated composition of data-path functionality in the future internet. IEEE Network, 25(6), 8-14.[17] El-Atawy, A., Samak, T., Wali, Z., Al-Shaer, E., Lin, F., Pham, C., & Li, S. (2007). An Automated Framework for Validating Firewall Policy Enforcement. In Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07) (pp. 151-160).[18] Khelf, R., & Ghoualmi-Zine, N. (2018). IPsec/Firewall Security Policy Analysis: A Survey. In 2018 International Conference on Signal, Image, Vision and their Applications (SIVA) (pp. 1-7). |
| ΙοΤ πρωτόκολλα επικοινωνίας MQTT – COAP – HTTP/2 – HTTP/3 – XMPPΘεωρητικό κομμάτι Ανάλυση λειτουργίας των πρωτοκόλλων Σύνδεση και σύγκριση των πρωτοκόλλων μεταξύ τουςΑνάλυση ασφάλειαςΠρακτικό κομμάτι Client – MQTT proxy – Server implementation1. Αναζήτηση κατάλληλου data set για ΙοΤ sensors data2. Δημιουργία service στον client σε οποιαδήποτε γλώσσα με σκοπό την αποδοχή, την διαμόρφωση και την αποστολή των δεδομένων στον MQTT server3. Set up a default MQTT broker service4. Δημιουργία Server σε οποιαδήποτε γλώσσα που καταναλώνει τα δεδομένα που περνάνε από τον MQTT και έπειτα τα εμφανίζει.5. MQTT service hardening6. Attack implementation into the system | Καλή γνώση πρωτοκόλλων επιπέδου εφαρμογής και τεχνολογιών ασφάλειας δικτύωνΚαλή γνώση Java ή GOlang ή Python | [01] Labouardy, M. (2021). Building Distributed Applications in Gin: A Hands-on Guide for Go Developers to Build and Deploy Distributed Web Apps with the Gin Framework. Ανακτήθηκε από <https://books.google.gr/books?id=n-mHzgEACAAJ>[02] <https://wiki.xmpp.org/web/Tech_pages/IoT_systems>[03] <https://www.researchgate.net/publication/290379207_Context-based_search_engine_for_industrial_IoT_Discovery_search_selection_and_usage_of_devices>[04] <https://www.datasetlist.com/>[05] <https://www.kaggle.com/search?q=iot>[06] <https://www.kaggle.com/datasets/shaivyac/gps-iot-data-for-data-visualization>[07] <https://hub.packtpub.com/25-datasets-deep-learning-iot/>[08] [https://www.amazon.com/MQTT-Essentials-Lightweight-IoT-Protocol/dp/1787287815/ref=sr\_1\_1?crid=11L2L96R8PTC&keywords=mqtt&qid=1666281544&qu=eyJxc2MiOiI1LjA3IiwicXNhIjoiNC4wMyIsInFzcCI6IjMuMzQifQ%3D%3D&s=books&sprefix=mqtt%2Cstripbooks-intl-ship%2C319&sr=1-1](https://www.amazon.com/MQTT-Essentials-Lightweight-IoT-Protocol/dp/1787287815/ref%3Dsr_1_1?crid=11L2L96R8PTC&keywords=mqtt&qid=1666281544&qu=eyJxc2MiOiI1LjA3IiwicXNhIjoiNC4wMyIsInFzcCI6IjMuMzQifQ%3D%3D&s=books&sprefix=mqtt%2Cstripbooks-intl-ship%2C319&sr=1-1)[09] [https://www.amazon.com/Practical-IoT-Hacking-Fotios-Chantzis/dp/1718500904/ref=d\_pd\_sbs\_sccl\_2\_8/133-2500231-2573029?pd\_rd\_w=JzrXR&content-id=amzn1.sym.3676f086-9496-4fd7-8490-77cf7f43f846&pf\_rd\_p=3676f086-9496-4fd7-8490-77cf7f43f846&pf\_rd\_r=65YFFCMRX0MGK4YEKVCE&pd\_rd\_wg=3kEJH&pd\_rd\_r=e484584e-7496-4239-80e6-a36a72e4a2a4&pd\_rd\_i=1718500904&psc=1](https://www.amazon.com/Practical-IoT-Hacking-Fotios-Chantzis/dp/1718500904/ref%3Dd_pd_sbs_sccl_2_8/133-2500231-2573029?pd_rd_w=JzrXR&content-id=amzn1.sym.3676f086-9496-4fd7-8490-77cf7f43f846&pf_rd_p=3676f086-9496-4fd7-8490-77cf7f43f846&pf_rd_r=65YFFCMRX0MGK4YEKVCE&pd_rd_wg=3kEJH&pd_rd_r=e484584e-7496-4239-80e6-a36a72e4a2a4&pd_rd_i=1718500904&psc=1)[10] [https://www.amazon.com/MQTT-Complete-Beginners-Basics-Protocol-ebook/dp/B08HDCWDSG/ref=sr\_1\_2?crid=11L2L96R8PTC&keywords=mqtt&qid=1666281544&qu=eyJxc2MiOiI1LjA3IiwicXNhIjoiNC4wMyIsInFzcCI6IjMuMzQifQ%3D%3D&s=books&sprefix=mqtt%2Cstripbooks-intl-ship%2C319&sr=1-2](https://www.amazon.com/MQTT-Complete-Beginners-Basics-Protocol-ebook/dp/B08HDCWDSG/ref%3Dsr_1_2?crid=11L2L96R8PTC&keywords=mqtt&qid=1666281544&qu=eyJxc2MiOiI1LjA3IiwicXNhIjoiNC4wMyIsInFzcCI6IjMuMzQifQ%3D%3D&s=books&sprefix=mqtt%2Cstripbooks-intl-ship%2C319&sr=1-2) |
| Ανάπτυξη κατανεμημένου συστήματος εξουσιοδότησης και αυθεντικοποίησης βασισμένη σε τεχνολογίες Blockchain (Ethereum ή Hyperledger). Στην παρούσα εργασία θα αξιοποιηθούν εργαλεία ανάπτυξης και δοκιμής Έξυπνων Συμβολαίων (Smart Contracts) για να κατασκευαστεί μια υποδομή εξουσιοδότησης και αυθεντικοποίησης. Συγκεκριμένα θα χρησιμοποιηθούν τα Truffle Suit και Ganche εφόσον επιλεγεί η πλατφόρμα Ethereum ή το Remix εφόσον επιλεγεί η πλατφόρμα Hyperledger. Η εφαρμογή θα αξιοποιεί ένα frontend της επιλογής σας. | Blockchain (Ethereum or Hyperledger), Programming skills (Solidity or Go – similar to javascript), Cryptography basics | (1) Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers & Security 78 (2018): 126-142.(2) Fisher, Justin, and Maxwell Henry Sanchez. "Authentication and verification of digital data utilizing blockchain technology." U.S. Patent Application No. 15/083,238.(3) Malamas, Vangelis, et al. "A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data." IEEE Access 8 (2020): 134393-134412.(4) Malamas, Vaggelis, et al. "A forensics-by-design management framework for medical devices based on blockchain." 2019 IEEE World Congress on Services (SERVICES). Vol. 2642. IEEE, 2019.(5) Wang, Jing, et al. "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure." IEEE Transactions on Industrial Informatics 16.3 (2019): 1984-1992. |
| 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 – similar to javascript), Dockers | (1) Nizamuddin, Nishara, et al. "Decentralized document version control using ethereum blockchain and IPFS." Computers & Electrical Engineering 76 (2019): 183-197.(2) 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) 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. |
| **Harvesting Information from open sources to develop concrete threat agent profiles.**OSCTI - Web Scraping - Machine LearningThere are multiple approaches to identify and assess threat agent profiles along with their characteristics. OWASP, NIST and Intel provide their own taxonomies and sets of characteristics to define threat agents, while MITRE’s ATT&CK framework catalogues events related to specific threat groups. In the context of this thesis you are called to:• Research existing threat agent profiling methodologies• Research different threat groups active in different environments• Discover the common characteristics amongst threat agent taxonomies• Develop scripts to pull existing repositories • Develop NLP module to harvest information from social media (e.g. Twitter, Linkedin) and CVs related to threat agent groups or individuals that will support later classification**Goals:**• Create a custom threat agent profiling methodology utilizing existing taxonomies and known characteristics.• Create a knowledge base for the methodology using harvested information |  |  |