# Περίληψη

Προκειμένου να υφίσταται η ασφάλεια σε ένα κατανεμημένο σύστημα, είναι άκρως σημαντικό να αξιολογηθεί η αξιοπιστία των συμμετεχόντων οντοτήτων, καθώς η εμπιστοσύνη είναι, γενικότερα, βασική προϋπόθεση για επικοινωνία και συνεργασία. Σε αυτή την εργασία, παρουσιάζουμε ένα ολοκληρωμένο πλαίσιο (framework), το οποίο παρέχει ένα σύνολο εργαλείων, βιβλιοθηκών και υπηρεσιών για την ανάπτυξη ασφαλών κατανεμημένων συστημάτων και εφαρμογών, ονόματι *Vanadium*.

Η διάρθρωση της παρούσας εργασίας εστιάζει στην εξερεύνηση του συγκεκριμένου framework. Το *Vanadium* αποτελεί ένα open-source framework, με το οποίο είναι δυνατή η κατασκευή ασφαλών και κατανεμημένων cross-platform εφαρμογών. Πιο συγκεκριμένα, μελετώνται το *πρωτόκολλο κλήσης απομακρυσμένης διαδικασίας Vanadium* (RPC), το μοντέλο ασφάλειας του *Vanadium*, το οποίο καθορίζει *μηχανισμούς αναγνώρισης* (identification mechanisms), *ελέγχου ταυτότητας* (authentication mechanisms), υποστηρίζοντας, έτσι, μία πλήρως αποκεντρωμένη, λεπτομερή και ελεγχόμενη εξουσιοδότηση όταν επικοινωνούν δύο ή και περισσότερες οντότητες (π.χ. αυτόνομες διεργασίες). Σε ό,τι αφορά τους προαναφερθέντες μηχανισμούς, γίνεται περιγραφή των ιδιοτήτων τους, των υλοποιήσεων που παρέχονται από το *Vanadium Framework* και ορισμένων λεπτομερειών σχεδίασης που σχετίζονται με τα πρωτόκολλα αυτά καθ’ αυτά. Επιπλέον, εξηγείται εκτενώς η έννοια και η υλοποίηση της ονοματοδοσίας στο framework και ο τρόπος με τον οποίο το σύστημα ονομάτων του *Vanadium* επιτρέπει την ανακάλυψη συσκευών, ανεξάρτητα από τη φυσική τους θέση - με ή χωρίς σύνδεση στο διαδίκτυο. Τέλος, προκειμένου να αναδειχθούν στην πράξη ορισμένες από τις λειτουργίες και δυνατότητες του *Vanadium Framework,* παρέχεται συμπληρωματικά και μία εφαρμογή επίδειξης (σε γλώσσα προγραμματισμού *Go*), η οποία κάνει χρήση των περισσότερων λειτουργιών του framework, και συγκεκριμένα εκείνες που αφορούν την επικοινωνία, την αυθεντικοποίηση, αλλά και την αναγνώριση οντοτήτων.

Συνοψίζοντας, η συμβολή της παρούσας εργασίας εντοπίζεται, κυρίως, στο επίπεδο της μελέτης της δομής και της λειτουργίας του *Vanadium Framework.* Επεκτείνεται, όμως, και στο επίπεδο της προγραμματιστικής υλοποίησης μίας demo εφαρμογής, με την οποία μπορεί να γίνει αντιληπτό το πώς μπορεί κανείς να χρησιμοποιήσει τις δυνατότητες που προσφέρει το *Vanadium Framework* στην πράξη.

# Περιεχόμενα

[Εξώφυλλο](#_Toc57145658)

[Πρόλογος](#_Toc57145659)

[Περίληψη](#_Toc57145660)

[Περιεχόμενα](#_Toc57145661)

[Ευρετήριο Σχημάτων](#_Toc57145662)

[Ευρετήριο Πινάκων](#_Toc57145663)

[1. Εισαγωγή](#_Toc57145664)

[2. Ερευνητικό Υπόβαθρο](#_Toc57145665)

[2.1 Κρυπτογραφία](#_Toc57145666)

[2.2 Αυθεντικοποίηση Machine to Machine (M2M)](#_Toc57145667)

[3. Συναφείς Έρευνες](#_Toc57145669)

[4. Vanadium](#_Toc57145670)

[4.1 Δομή Πελάτη - Διακομιστή](#_Toc57145671)

[4.2 Μοντέλο Ασφάλειας](#_Toc57145672)

[4.2.1 Γενικά](#_Toc57145673)

[4.2.2 Principals & Blessings](#_Toc57145673)

[4.2.3 Αναθέσεις](#_Toc57145673)

[4.2.4 Περιορισμοί](#_Toc57145673)

[4.2.5 Επαλήθευση των Blessings](#_Toc57145673)

[4.2.6 Αυθεντικοποίηση](#_Toc57145674)

[5. Υλοποίηση](#_Toc57145676)

[5.1 Εκίνηση Πελάτη - Διακομιστή](#_Toc57145677)

[5.2 Δικαιώματα](#_Toc57145678)

[6. Αποτέλεσματα](#_Toc57145680)

[7. Συμπεράσματα (ίσως και προτάσεις βελτίωσης)](#_Toc57145681)

[8. Βιβλιογραφία](#_Toc57145682)

[9. Παραρτήματα](#_Toc57145683)

# Βιβλιογραφία

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2017, 9). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks, 2017*. doi:10.1155/2017/6562953

Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Towards Viable Certificate-Based Authentication for the Internet of Things. *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy* (σσ. 37–42). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2463183.2463193

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IT Professional, 19*, 27-33. doi:10.1109/MITP.2017.3680960

Lee, J., Lin, W., & Huang, Y. (2014). A lightweight authentication protocol for Internet of Things. *2014 International Symposium on Next-Generation Electronics (ISNE)*, (σσ. 1-2). doi:10.1109/ISNE.2014.6839375

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013, 3 10). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility, 1*, 309–348.

Ramos, J. H., Jara, A., Marín, L., & Gómez-Skarmeta, A. F. (2013). Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur., 3*, 1-16.

Taly, A., & Shankar, A. (2016). Distributed Authorization in Vanadium. Στο A. Aldini, J. Lopez, & F. Martinelli (Επιμ.), *Foundations of Security Analysis and Design VIII: FOSAD 2014/2015/2016 Tutorial Lectures* (σσ. 139–162). Cham: Springer International Publishing. doi:10.1007/978-3-319-43005-8\_4

Wu, D. J., Taly, A., Shankar, A., & Boneh, D. (2016). Privacy, Discovery, and Authentication for the Internet of Things. Στο I. Askoxylakis, S. Ioannidis, S. Katsikas, & C. Meadows (Επιμ.), *Computer Security – ESORICS 2016* (σσ. 301–319). Cham: Springer International Publishing.

Taly, A., Practical Distributed Authorization, Two day course at the 2016 International School on Foundations of Security Analysis and Design, Bertinoro, Italy (Aug. 29 - Sep. 2)

[Vanadium Official WebSite](https://vanadium.github.io/)

[Προσπελάστηκε 29/11/2020]