ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Αναγνώπουλος Γεώργιος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Επικ. Καθηγητής, Π. Πρατικάκης

Σ. Ιωαννίδης (επιβλέπων)

Δευτέρα, 29 Μαρτίου 2021 , ώρα 11:00 π.μ.

Join Zoom Meeting

https://zoom.us/j/93820796126

"ΑΤΛΑΣ: Αυτοματοποιημένη κλιμάκωση μη-ασφαλών συστημάτων σε Αξιόπιστα Περιβάλλοντα Εκτέλεσης"

Περίληψη

Τα Αξιόπιστα Περιβάλλοντα Εκτέλεσης προσφέρουν αξιοσημείωτα οφέλη ασφαλείας σε εφαρμογές που είτε τα χρησιμοποιούν άμεσα είτε συνδυάζουν ένα σύνολο από τα στοιχεία τους. Αποκομίζοντας αυτά τα οφέλη, ωστόσο, απαιτούν απαιτητικές προσπάθειες του προγραμματιστή για τον εντοπισμό και την διαμόρφωση των στοιχείων που χρειάζονται να εκτελεστούν σε αξιόπιστο περιβάλλον. Η έλλειψη εργαλείων για αξιόπιστα περιβάλλοντα γραμμένα σε γλώσσες προγραμματισμού υψηλού επιπέδου αναγκάζει τους προγραμματιστές να υλοποιούν τις εφαρμογές τους σε χαμηλό επίπεδο, αντιμετωπίζοντας παράλληλα και όλες τις πολυπλοκότητες που συνοδεύουν αυτές τις γλώσσες, όπως ο προσεκτικός χειρισμός μνήμης, εντοπισμός σφαλμάτων ή συντήρηση των εργαλείων αυτών. Επιπλέον, η ενίσχυση της ασφάλειας της εκτέλεσης συμβάλλει στην μείωση της βέλτιστης απόδοσης, λόγω της προστιθέμενης κρυπτογράφησης/αποκρυπτογράφησης, δοκιμών ακεραιότητας ή περιορισμών δικαιωμάτων της μνήμης.

Αυτή η εργασία παρουσιάζει ένα σύστημα για την αυτόματη κλιμάκωση μή ασφαλών στοιχείων με τη χρήση γλώσσας προγραμματισμού υψηλού επιπέδου, JavaScript, σε Αξιόπιστα Περιβάλλοντα Εκτέλεσης. Χρησιμοποιεί μετασχηματισμούς στο ίδιο το πρόγραμμα με σκοπό την εκφόρτωση και διανομή φορτίου μιας δεδομένης εφαρμογής μεταξύ αξιόπιστων κόμβων. Αυτή η λειτουργία επιγχάνεται με την ενσωμάτωση ενός συστήματος εκτέλεσης υψηλού επιπέδου γλώσσας προγραμματισμού σε αξιόπιστο περιβάλλον. Η αξιολόγηση πραγματοποιήθηκε σε ένα σύνολο αλγόριθμων βασισμένο στην ίδια την γλώσσα προγραμματισμού, μια κρυπτογραφική σουίτα αλλά και 3 πραγματικές εφαρμογές γραμμένες εξ' ολοκλήρου σε JavaScript. Η αυτόματη κλιμάκωση των εφαρμογών δείχνει θετικά αποτελέσματα και σημαντικές επιταχύνσεις σε σχέση με την απλή ενίσχυση της εφαρμογής με μέσο όρο της τάξεως του 6 επί με σύστημα αποτελούμενο από 10 κόμβους.

University of Crete

Computer Science Department

M.Sc. Thesis presentation / examination

Anagnopoulos Georgios

Master's Thesis Supervisor: Assistant Professor, P. Pratikakis

S. Ioannidis (Thesis CO-Advisor)

Monday, 29 March 2021, 11:00 a.m.

Join Zoom Meeting

https://zoom.us/j/93820796126

"Atlas: Automated Scale-out of Trust-Oblivious Systems to Trusted Execution Environments"

Abstract

Trusted Execution Environments (TEEs) offer notable important security benefits to applications that combine on- and off-premise components. Reaping these benefits, however, requires burdensome developer effort to identify and rewrite TEE-executing components. The lack of high-level TEE APIs enforces the developing community to limit their implementations to only low-level interfaces, dealing with the complexities that low-level programming languages come with; i.e. memory handling, debugging and/or maintenance. The security enforcement of the execution

though, comes with a trade-off against optimal performance, due to the added encryption/decryption, integrity tests and/or memory limitations.

This work presents Atlas, a system for automatically scaling out components on TEEs with the use of a high-level programming language, JavaScript. It uses program transformations to offload function calls of a given application and distribute load among trusted nodes. A TEE-embedded language run-time environment and associated optimizations complete the picture, supporting the run-time execution of offloaded fragments. Atlas evaluation applies on a set of language-specific algorithms and cryptographic suites but also 3 real-world applications written in native JavaScript. This evaluation shows success at TEE scale-out of legacy applications not written for TEE's, substantial speedups over naïve decomposition with an average of 6x with a 10-node cloud and attractive elasticity characteristics, all achieved with minimal developer effort.