ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Καρνίκης Δημήτριος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Επικ. Καθηγητής, Π. Πρατικάκης

Σ. Ιωαννίδης (επιβλέπων)

Τετάρτη, 27 Ιανουαρίου 2021 , ώρα 13:00 μ.μ.

Join Zoom Meeting
https://zoom.us/j/8496458640?pwd=OGZKVUROYld3R25kalNsanByd3dDQT09

"LuaGuardia: Ένα σύστημα εκτέλεσης κρίσιμου κώδικα για Περιβάλλοντα Ασφαλούς Εκτέλεσης"

Περίληψη

Οι εφαρμογές εκτελούν κώδικα κρίσιμο για την ασφάλεια ενός συστήματος και διαχειρίζονται ευαίσθητα ή προσωπικά δεδομένα. Συχνά υποστηρίζονται από Περιβάλλοντα Ασφαλούς Εκτέλεσης (ΠΑΕ), τα οποία γίνονται όλο και πιο διαδεδομένα στον χώρο των υπολογιστών. Ωστόσο, η ανάπτυξη και η εφαρμογή τους παραμένουν μία πρόκληση για διάφορους λόγους. Αρχικά, η έλλειψη διεπαφών υψηλού επιπέδου στα ΠΑΕ περιπλέκει την ανάπτυξη εφαρμογών και αναγκάζει τη χρήση γλωσσών που δε προσφέρουν ασφαλείς διεπαφές μνήμης και τύπων. Αυτές οι προκλήσεις επιδεινώνονται από τεχνικά ζητήματα που αφορούν την επεκτασιμότητα του περιβάλλοντος εκτέλεσης, την διαχείριση των κρυπτογραφικών λειτουργιών αλλά και τις περιορισμένες διαθέσιμες διεπαφές. Επίσης, η μεταφορά των υπαρχόντων εφαρμογών

σε διαφορετικά συστήματα/πλατφόρμες απαιτεί χειροκίνητη τμηματοποίηση της εφαρμογής, εκ νέου μεταγλώττιση του πηγαίου κώδικα και την υλοποίηση των απαραίτητων βημάτων σύνδεσης για την τελική δημιουργία του εκτελέσιμου προγράμματος. Αυτή η εργασία παρουσιάζει το LuaGuardia, ένα σύστημα που απλοποιεί την ανάπτυξη εφαρμογών βασισμένων σε ΠΑΕ. Το LuaGuardia αντιμετωπίζει τις προαναφερθείσες προκλήσεις προσφέροντας ένα σύνολο διεπαφών υψηλού επιπέδου γύρω από ένα περιβάλλον εκτέλεσης σε γλώσσα υψηλού επιπέδου. Αυτές οι διεπαφές απλοποιούν την ανάπτυξη τέτοιων προγραμμάτων με γνώμονα τη διατήρηση της ασφάλειας των τύπων και την προστασία της μνήμης. Ακόμη, προσφέρει μια βιβλιοθήκη που επιλύει τεχνικές δυσκολίες όπως την υπογραφή του εκτελέσιμου κώδικα, τη διαχείριση των κλήσεων συστήματος, τον έλεγχο πρόσβασης σε δεδομένα και τη δυναμική φόρτωση κώδικα. Ακόμη, προσφέρει μια σειρά βελτιστοποιήσεων που επιταχύνουν την εκτέλεση προστατευμένου κώδικα. Επιπλέον, σε αυτή την εργασία αξιολογούμε την επίδοση του LuaGuardia σε ένα σύνολο από αλγορίθμους, κρυπτογραφικές συναρτήσεις αλλά και εμπορικές εφαρμογές. Μέσω πειραμάτων παρατηρούμε ότι το σύστημά μας προσφέρει τα παραπάνω πλεονεκτήματα, αυξάνοντας κατά μέσο όρο τον χρόνο εκτέλεσης κατά 18%, με την πλειονότητα των χρονικών επιβαρύνσεων να οφείλεται σε καθυστερήσεις εισόδου/εξόδου.

University of Crete

Computer Science Department

M.Sc. Thesis presentation / examination

Dimitros Karnikis

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

S. Ioannidis (Thesis CO-Advisor)

Wednesday, 27 January 2021, 13:00 p.m

Join Zoom Meeting

https://zoom.us/j/8496458640?pwd=OGZKVUROYld3R25kalNsanByd3dDQT09

“LuaGuardia: A Confidential Computing Framework for Trusted Execution Environments”

Abstract

Confidential computing applications are enabled by Trusted Execution environments (TEEs) that are becoming increasingly widespread in the computing landscape. However, their development and deployment remains challenging due to several reasons. The lack of high-level TEE abstractions complicates application development and forces the use of low-level memory- and type-unsafe abstractions. These challenges are exacerbated by technical issues regarding runtime extensibility, management of cryptographic operations, and restricted interfaces: even porting existing applications requires manual partitioning, re-compilation, and linking steps. This work presents LuaGuardia, a system simplifying the development of confidential computing. LuaGuardia addresses the aforementioned challenges by offering a set of abstractions around a TEE-embedded runtime environment of a high-level programming language. LuaGuardia’s abstractions simplify the development and deployment of such applications in a type- and memory-safe manner. It also offers a runtime library solving technical challenges such as code signing, system-call offloading, access control, and dynamic code loading. A series of optimizations is also provided that accelerate protected code execution. Our evaluation applies LuaGuardia to a diverse set of applications, cryptographic functions but also real-world commercial applications, with an average overhead of 18%, the majority of which is due to I/O delays.