ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Κλεφτογιώργος Κωνσταντίνος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Καθηγητής, Ε. Μαρκάτος

Παρασκευή, 06/07/2018, 13:00
Αίθουσα B108,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

" Ανακατασκευή της Ροής Εκτέλεσης Προγράμματος σε Περιβάλλοντα JIT με τη Χρήση Υλικού "

ΠΕΡΙΛΗΨΗ

Η ανακατασκευή της Ροής-Εκτέλεσης είναι ένα σημαντικό κομμάτι πολλών μηχανισμών ασφάλειας, δημιουργίας προφίλ και ανάλυσης. Ένας αξιοσημείωτος περιορισμός σε προηγούμενες δουλειές, είναι ότι δεν υποστηρίζουν την παρακολούθηση προγράμματος σε περιβάλλοντα JIT. Ήδη υπάρχοντες μηχανισμοί, για την απόκτηση της Ροής-Εκτέλεσης μιας διαδικασίας, περιλαμβάνουν τη χρήση παραμετροποίησης του πηγαίου κώδικα, είτε δυναμικά είτε στατικά. Ωστόσο, αυτές οι προσεγγίσεις υποφέρουν από ορισμένα μειονεκτήματα. Η λήψη της ροής ελέγχου μέσω δυναμικής παραμετροποίησης κατά την εκτέλεση μιας διαδικασίας, προκαλεί σοβαρή επιβράδυνση, ενώ η στατική μπορεί να οδηγήσει σε ανακριβή αποτελέσματα.

Χρησιμοποιούμε την τεχνολογία Intel Processor Trace, μια νέα δυνατότητα υλοποιημένη στο υλικό των σύγχρονων επεξεργαστών της Intel, προκειμένου να αποκτηθεί η Ροή-Ελέγχου μιας διαδικασίας σωστά, ελαχιστοποιώντας τις επιπτώσεις στην απόδοση. Προηγούμενες δουλειές έχουν δείξει την αποτελεσματικότητα της αξιοποίησης του Intel PT για την ανασυγκρότηση της Ροής-Εκτέλεσης μιας διαδικασίας. Ωστόσο, κανένας από αυτούς, εξ όσων γνωρίζουμε, δεν έχει

προσπαθήσει να εκτελέσει ανασυγκρότηση της Ροής-Εκτέλεσης σε μια διαδικασία που εκτελείται μέσα σε περιβάλλοντα JIT.

Για να δείξουμε τη λειτουργία του μηχανισμού μας, βρίσκουμε τη Ροή-Εκτέλεσης ενός προγράμματος που εκτελείται μέσα στον παραμετροποιητή κώδικα Intel Pin. Γι' αυτό το λόγο, υλοποιήσαμε έναν οδηγό υλικού για το Intel PT καθώς και ένα νέο αποκωδικοποιητή, ο οποίος μας επιτρέπει να ανασυγκροτήσαμε της Ροή-Εκτέλεσης κατά τη διάρκεια της εκτέλεσης και όχι μετά το τέλος του προγράμματος. Αυτή η προσέγγιση επιβάλλει σημαντικά λιγότερες καθυστερήσεις, σε σύγκριση με τη δυναμική παραμετροποίηση κώδικα, και είναι περισσότερο ακριβής από τη στατική.

Τέλος, χρησιμοποιήσαμε τη σουίτα μέτρησης επιδόσεων SPEC CPU2006, προκειμένου να αξιολογήσουμε την αποτελεσματικότητά του πρωτοτύπου μας και να μετρήσουμε τις επιδόσεις του. Τα αποτελέσματα μας αποδεικνύουν ότι η επιβράδυνση του μηχανισμού μας είναι τάξης μεγέθους χαμηλότερη από τους προηγούμενους μηχανισμούς, καθώς παράλληλα επιτυγχάνει την ανακατασκευή της Ροής-Εκτέλεσης του προγράμματος.

Kleftogiorgos Konstantinos
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Professor, E. Markatos

Friday, 06/07/2018, 13:00
Room B108, Computer Science Dept., University of Crete

“Hardware Accelerated Control-Flow Reconstruction in JIT Environments”

ABSTRACT

Control-Flow reconstruction is a critical part of many security, profiling and analysis mechanisms. A challenging limitation in previous works is that they do not support tracing in JIT environments.

Already existing mechanisms of obtaining the Control-Flow of a process, include the use of instrumentation, either dynamic or static. However, these approaches suffer from certain drawbacks.

Obtaining the Control-Flow through dynamic instrumentation during the execution of a process, imposes severe slowdowns, while static instrumentation can lead to inaccurate results. We leverage Intel Processor Trace, a new hardware feature of modern Intel CPUs, in order to acquire the Control-Flow of a process correctly, while at the same time minimizing the impact on the performance.

Previous works have shown the effectiveness of utilizing Intel PT in order to reconstruct the Control-Flow of a process. However, none of them, to the best of our knowledge, has attempted to perform Control-Flow reconstruction on a process executing inside a JIT environment. To showcase our mechanism in JIT environments, we trace the execution of a process in Intel Pin dynamic instrumentation framework. To achieve this we implemented a custom Intel PT driver and a new decoder which enables us to reconstruct the Control-Flow at runtime and not after the completion of the process. This approach imposes significantly less overhead, compared to dynamic binary instrumentation, while being more accurate than the static one.

Finally, we evaluate the correctness of our mechanism and measure its performance by running SPEC2006 benchmark suit. Our results indicate that the overhead imposed by our mechanism, is marginally lower than previously developed mechanisms, while the Control-Flow is accurately reconstructed.