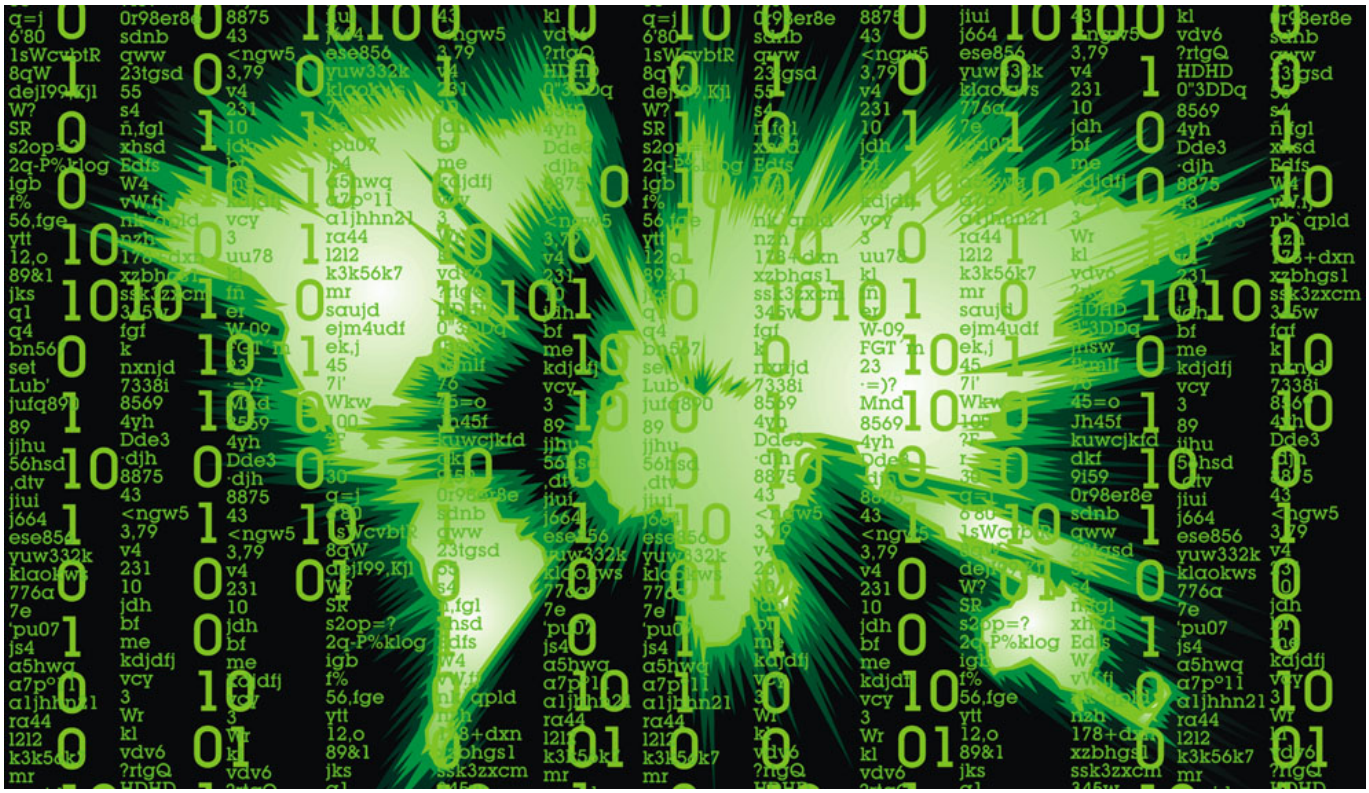
4 Ιουνίου 2016

Η κρυπτογράφηση απογειώνεται! Νέος τρόπος παραγωγής τυχαίων αριθμών

/ Πεμπτουσία

Image not found or type unknown



Δύο ερευνητές από το Πανεπιστήμιο του Τέξας έχουν δημοσιεύσει ένα έγγραφο που περιγράφει με λεπτομέρειες ένα νέο αλγόριθμο για το συνδυασμό δύο πηγών εντροπίας για να επιτύχουν καλύτερη ποιότητα τυχαίων αριθμών που μπορεί να χρησιμοποιηθεί για να ενισχύσει εργασίες κρυπτογράφησης με λιγότερη χρήση υπολογιστικών πόρων.

Ο κόσμος της επιστήμης των υπολογιστών και της κρυπτογράφησης φλέγεται με συζητήσεις για την «Explicit Two-Source Extractors and Resilient Functions» μελέτη που δημοσιεύθηκε τον Ιούλιο του 2015, αλλά πρόσφατα ενημερώθηκε, το Μάρτιο, η οποία αναφέρει λεπτομερώς μια θεωρητική ανακάλυψη σε σχέση με την παραγωγή τυχαίων αριθμών.

Για πολύ, πολύ καιρό, η αδυναμία στις CSPRNGs (Cryptographically-Secure Pseudo-

Random Numbers Generators) ήταν η προέλευση του τυχαίου αριθμού, που ονομάζεται πηγή εντροπίας ή αλλιώς entropy pool. Στις περισσότερες περιπτώσεις, για πολλά συστήματα ηλεκτρονικών υπολογιστών, αυτό λαμβάνεται από τις κινήσεις του ποντικιού του χρήστη, τις εισροές του πληκτρολογίου, τα disk IO events, τις διακοπές του σήματος, τις inter-arrival φορές του πακέτου δικτύου ή από άλλα events με βάση το hardware.

Ανάλογα με την υπάρχουσα entropy pool κατά τη δεδομένη στιγμή όταν ένα κρυπτογραφικό σύστημα «τραβά» τον τυχαίο αριθμό για τις δραστηριότητές του, η πηγή αυτού του αριθμού υπαγορεύει έμμεσα την ποιότητα της κρυπτογράφησης. Οι περισσότερες επιθέσεις σε συστήματα κρυπτογράφησης βασίζονται στις αδύναμες ακολουθίες τυχαίων αριθμών και πηγών.

Αυτό που οι δύο ερευνητές κατάφεραν να κάνουν είναι να επινοήσουν έναν αλγόριθμο που εξαλείφει την ανάγκη για μια υψηλής ποιότητας πηγή τυχαίων αριθμών. Ο αλγόριθμος επιτρέπει στους προγραμματιστές, θεωρητικά προς το παρόν, να συγχωνεύσουν δύο πηγές χαμηλότερης ποιότητας και να αποκτήσουν έναν αριθμό υψηλής ποιότητας.

Το έργο του David Zuckerman, ενός καθηγητή της επιστήμης των υπολογιστών και του Eshan Chattopadhyay, ενός μεταπτυχιακού φοιτητή, και οι δύο στο Πανεπιστήμιο του Τέξας, έγιναν δεκτοί με ανοιχτές αγκάλες από την κοινότητα τηςεπιστήμης των υπολογιστών.

Ο Xin Li, Επίκουρος Καθηγητής στο Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου Johns Hopkins, έχει αρχίσει ήδη να καταβάλει προσπάθεια για να κάνει τον αλγόριθμο για να συνεργαστεί με περισσότερες πηγές.

Λαμβάνοντας υπόψη ότι ο αλγόριθμος αυτός είναι resource-light και ισχυρότερος ταυτόχρονα, η τεχνική εφαρμογή του μπορεί να είναι μόνο θέμα χρόνου, με αμέτρητα smartphones και συσκευές IoT να περιμένουν την ενίσχυση στον τομέα της ασφάλειας.

Πηγή: secnews.gr