Πανεπιστήμιο Αθηνών	Εαρινό 2016
ΥΣ13 Ασφάλεια Υπολογιστικών Συστημάτων	ΚΙΑΓΙΑΣ
Due: `20.05.2016`	Project #3

Rainbow-Tables

Στόχος στο project 3 είναι να αποκτήσετε πρόσβαση σε ένα service το οποίο λειτουργεί (όχι απαραίτητα διαρκώς) στο sbox.di.uoa.gr. Συγκεκριμενα το service αυτό ζητάει απο κάθε χρήστη που συνδέεται, ένα κωδικό και στην περίπτωση που ο κωδικός αυτός είναι σωστός τότε στέλνει στον χρήστη ένα μυστικό κλειδί το όποιο και θα πρέπει να αποκτήσετε σε αυτή την εργασία.

Για να μεγιστοποιήσει την ασφάλεια του συστήματος το service επικοινωνεί με μια άλλη διεργασία η οποία εκτελείται στο ίδιο μηχάνημα και το οποίο παράγει ένα νέο κωδικό σε τακτά χρονικά διαστήματα. Για να είναι ο κωδικός εύκολος για να τον μάθει κάποιος χρησιμοποιείται ως κωδικός μια συμβολοσειρά 6 χαρακτήρων που διαλέγονται απο τους παρακάτω

`ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@`

Παρότι η ιδέα φαίνεται καλή, προκύπτει το ζήτημα της επικοινωνίας μεταξύ των διεργασιών. Πράγματι, για την αποστολή των κωδικών τα processes χρησιμοποιούν το D-BUS daemon [1] και συγκεκριμένα D-BUS signals αγνοώντας το γεγόνός οτι όλες οι διεργασίες του συστήματος έχουν πρόσβαση σε αυτό.

Παρά το λάθος στο σχεδιασμό η διεργασία παραγωγής των κωδικών έχει προνοήσει να μην στέλνει τον κωδικό απλά μέσα στο κανάλι επικοινωνίας (το D-BUS στην περίπτωση μας[2]) αλλα στέλνει ενα hash του κωδικού. Γνωρίζοντας τα τελευταία αποτελέσματα κρυπτανάλυσης στις πιο διαδεδομένες συναρτήσεις hash οι προγραμματιστές του service αποφάσισαν να χρησιμοποιήσουν μια συνάρτηση απο τις finalist του διαγωνισμού SHA-3 και συγκεκριμένα την συνάρτηση **Blake**.

Τα ζητούμενα απο το project είναι τα εξής:

1. Η υλοποιήση ένος πρόγραμματος το οποίο θα υποκλέπτει την μετάδοση του κωδικού απο το D-BUS.

2. Η υλοποιήση ενος προγραμμάτος που θα σπάει το hash και θα συνδέεται επιτυχώς στο service.

Για την υλοποιήση του δεύτερου μέρους της εργασίας θα πρέπει να υλοποιήσετε ένα rainbow table[3], το οποίο θα πρέπει να καταφέρνει να σπάσει τον κωδικό που υποκλάπηκε προτού αυτός αλλάξει πάλι.
Οδηγίες παράδοσης του project. Πρέπει να δουλέψετε μόνοι σε αυτό το project. Πρέπει να γράψετε την αναφορά σας ηλεκτρονικά και να την παραδώσετε ηλεκτρονικά στη διεύθυνση :

`csec.di@gmail.com`

σε μορφή doc, ps η pdf αρχείου. Το e-mail πρέπει να έχει subject "project 3." Θα πρέπει να συμπεριλάβετε στην αναφορά όλο τον κώδικα που γράψατε και να εξηγήσετε όλο το συλλογιστικό σας για το πως κάνατε την κατασκευή του.

---

[1] Διαβάστε σχετικά με το D-BUS στο εξής link: `http://dbus.freedesktop.org/doc/dbus-tutorial.html`. Για να κάνετε την υλοποίηση πρόσβασης στο D-BUS μπορείτε να χρησιμοποιήσετε python: περισσότερες λεπτομέρειες στο http://dbus.freedesktop.org/doc/dbus-python/doc/tutorial.html. Τα παραδείγματα που αναφέρονται στο tutorial μπορείτε να τα βρείτε εδώ (σε python): `http://www.gnu-darwin.org/www001/src/ports/devel/py-dbus/work/dbus-python-0.82.4/examples/`. Αντίστοιχα παραδείγματα υπάρχουν και για Java αν προτιμάτε (google it!).

[2] Η πρόσβαση στο D-BUS με αυτόν τον τρόπο έχει χρησιμοποιηθεί και σε πραγματικές επιθέσεις εναντίον εφαρμογών βλέπετε το `http://census-labs.com/news/2012/02/25/libpurple-otr-info-leak/`.

[3] Ενα project το οποίο μπορεί να δείτε για rainbow tables είναι το `http://project-rainbowcrack.com/`. Για το project πάντως θα πρέπει να κάνετε την δική σας υλοποίηση για τα tables.

Καθυστερημένες Υποβολές Project. Μπορείτε να χρησιμοποίησετε μέχρι 10 μέρες για να καθύστερησετε την παράδωση ενος project (συνολικά για όλο το εξάμηνο). Η ημερομηνία υποβολής κρίνεται η ημερομηνία που παραδίνεται το e-mail σας στον server.
Εξώφυλλο Project. Το εξώφυλλο του project σας πρέπει να περιέχει το όνομα σας, το ΑΜ σας, καθώς και τα στοιχεία "Project #3", "ΥΣ13 ΕΑΡΙΝΟ 2016" καθώς και μια ένδειξη για το πόσες μέρες καθυστέρησης χρησιμοποιήθηκαν (0 αν καμμία).