Αναφορά project HY335b

Τσιριμώνας Γεώργιος
AM:2977
tsirimon@csd.uoc.gr
Αμηρίδης Γεώργιος
AM 2993
amirid@csd.uoc.gr

Στο project αυτό η υλοποίηση των ζητουμένων έγινε με 2 αρχεία: τα client.py και relay_nodes.py. Στο πρώτο έχουμε το direct mode και το relay mode, ενώ στο δεύτερο μόνο το relay. Όλα τα ζητούμενα υλοποιήθηκαν, εκτός του traceroute στα relay nodes, καθώς το traceroute στα μηχανήματα της σχολής δεν ανταποκρίνοταν, παρόλο που σε end_servers δουλεύει κανονικά. Το bonus δεν υλοποιήθηκε, καθώς υπήρχε έλλειψη χρόνου λόγο πολλαπλών υποχρεώσεων. Το project δουλεύει με threads, για όλες τις λειτουργίες που εκτελεί. Όλα τα μηνύματα μεταξύ client και relay, εκτός του αρχικού είναι κρυπτογραφημένα με RSA assymetric cipher και η αποστολή του αρχείου γίνεται με AES symmetric cipher. Η ακεραιότητα του αρχείου ελέγχεται μέσω ενός SHA512 hash το οποίο κρυπτογραφείται μαζί με το αρχείο. Παρακάτω δίνεται η ανάλυση των αρχείων.

Client.py

Functions

ping_server(hostname, iterations):

Η συνάρτηση εκτελεί το ping και επιστρέφει το μέσο RTT η -1 σε περίπτωση αποτυχίας

trace_server(hostname):

Η συνάρτηση εκτελεί το traceroute και επιστρέφει το μέσο hops η -1 σε περίπτωση αποτυχίας

download_file (file_url, filename):

Η συνάρτηση εκτελεί το download και τυπώνει τον χρόνο που πήρε η εκτέλεση του

get_sha512_signature (private_key, hash):

Η συνάρτηση παίρνει ένα private key και ένα hash δημιουργεί ένα signiature

verify_sha512_signature (public_key, signature, hash):

Η συνάρτηση παίρνει ένα public key και ένα hash και επικαιροποιεί το signiature. Εάν είναι,τότε παίρνουμε true, διαφορετικά false

check_signature (client_signature, relay_signature):

Η συνάρτηση αυτή παίρνει 2 signatures και τα επικαιροποιεί

Threads

class ping_Thread (threading.Thread):

Thread το οποίο εκτελεί ping σε end servers

class trace_Thread (threading.Thread):

Thread το οποίο εκτελεί traceroute σε end servers

class latency_Thread (threading.Thread):

Thread το οποίο εκτελεί ping & traceroute σε end servers

class server_latency_Thread (threading.Thread):

Thread το οποίο στέλνει σήμα στα relays να εκτελέσουν ping & traceroute σε end servers

class relay_Thread (threading.Thread):

Thread το οποίο στέλνει σήμα στα relays να εκτελέσουν ping η traceroute σε end servers

class relay_latency_Thread (threading.Thread):

Thread το οποίο εκτελεί ping στα relays

class relay_optimal_path_Thread (threading.Thread):

Thread το οποίο τυπώνει το πιο γρήγορο μονοπάτι προς ένα end server

class download_Thread (threading.Thread):

Thread το οποίο κατεβάζει ένα αρχείο

class relay_download_Thread (threading.Thread):

Thread το οποίο στέλνει σήμα σε ένα relay προκειμένου να κατεβάσει ένα αρχείο,να το κρυπτογραφήσει και να το στείλει στον client

Επιπλέον υλικό

select mode():

Εκτελεί την εναλλαγή μεταξύ direct & relay mode

Επίσης συμπεριλαμβάνεται ένα state machine που εκτελείται στο main thread και δέχεται είσοδο απο τον χρήστη. Ανάλογα με την είσοδο και την κατάσταση του δημιουργεί τα κατάλληλα threads για να εκτελεστούν οι εντολές του χρήστη

Relay_node.py

functions

ping_server(hostname, iterations):

Η συνάρτηση εκτελεί το ping και επιστρέφει το μέσο RTT η -1 σε περίπτωση αποτυχίας

trace_server(hostname):
Η συνάρτηση εκτελεί το traceroute και επιστρέφει το μέσο hops η -1 σε περίπτωση αποτυχίας

download_file (file_url, filename):
Η συνάρτηση κατεβάζει το αρχείο και τυπώνει τον χρόνο που πήρε η διαδικασία

encrypt_file (filename, key, mode, iv, private_key):
Κρυπτογραφεί ένα αρχείο βάση ενός AES symmetric cipher

get_sha512_signature (private_key):
Επιστέφει ένα SHA512 signature βάση ενός private key

get_signature ():
Επιστέφει το signature ενός relay

verify_signature (public_key, signature):
Επικαιροποιεί ενα signature βάση ενός public key

check_signature (signature):
Επικαιροποιεί το signature

threads
class ping_Thread (threading.Thread):
Thread το οποίο εκτελεί ping σε end server και επιστρέφει το αποτέλεσμα στον client

class trace_Thread (threading.Thread):
Thread το οποίο εκτελεί traceroute σε end server και επιστρέφει το αποτέλεσμα στον client

class latency_Thread (threading.Thread):
Thread που εκτελει ping & traceroute σε end servers και επιστρέφει το αποτελέσμα στον client

class download_Thread (threading.Thread):

Thread που κατεβάζει ένα αρχείο,το κρυπτογραφεί,το υπογράφει και το στέλνει στον client

class relay_Thread (threading.Thread):

Thread το οποίο παρακολουθεί το port εισόδου του relay, ανταλλάζει RSA asymmetric encryption keys με τον client,αποκωδικοποιεί τις εντολές του client και δημιουργεί άλλα threads για να τις εκτελέσουν