ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
http://www.cslab.ece.ntua.gr

Εργαστήριο Λειτουργικών Συστημάτων

7ο εξάμηνο, Ακαδημαϊκή περίοδος 2020–2021

Οδηγός Χρήσης του cryptodev module

Εργαστήριο Υπολογιστικών Συστημάτων Ε.Μ.Π.
os-lab@lists.cslab.ece.ntua.gr

Δεκέμβριος 2020

Περιεχόμενα

Επιμέλεια: Ευ. Αγγέλου, Στ. Γεράγγελος, Δ. Σιακαβάρας, Ευ. Κούκης

1 Εισαγωγή - Ασφάλεια στο Διαδίκτυο

Καθημερινά γίνονται εκατομμύρια συναλλαγές μέσω του διαδικτύου, επομένως αντ-αλλάσονται άπειρα bytes προσωπικών και ευαίσθητων δεδομένων. Η ανάγκη για ασφαλή επικοινωνία μέσω διαδικτύου οδήγησε στη δημιουργία διαφόρων κρυπτογραφικών πρωτοκόλλων που εγγυόνται την ασφαλή μετάδοση των δεδομένων. Για παράδειγμα, η χρήση του SSL (Secure Sockets Layer) και της σύγχρονης εκδοχής του, του TLS (Transport Layer Security) είναι κοινός τόπος για ιστοσελίδες ηλεκτρονικών καταστημάτων, συστημάτων ηλεκτρονικών πληρωμών, αλλά και για προσωπικές πλέον χρήσεις, όπως το webmail.

Το πρωτόκολλο TLS επιτρέπει σε εφαρμογές client-server να επικοινωνήσουν πάνω από ένα δημόσιο δίκτυο χωρίς τον κίνδυνο να παρέμβει κάποιος στη συνομιλία, πιθανά καταγράφοντας ή μετατρέποντας την. Για να δείξει κάποιος client ότι επιθυμεί ασφαλή σύνδεση συνήθως ζητά σύνδεση σε ένα διαφορετικό αριθμό πόρτας από τον σύνηθες για ένα πρωτόκολλο (π.χ. για την ασφαλή μορφή του HTTP, HTTPS, στην πόρτα 443 αντί της 80). Αφού ο client και ο server συμφωνήσουν στον τύπο TLS που θα χρησιμοποιηθεί, χρησιμοποιούν τα κλειδιά τους για την κωδικοποίηση/αποκωδικοποίηση των δεδομένων. Αν και η ακριβής διαδικασία έχει περιγραφεί πολύ συνοπτικά εδώ, δεν θα μας απασχολήσει περισσότερο[1].

Στόχος μας είναι να εξασφαλίσουμε την ασφάλεια της επικοινωνίας ανάμεσα σε ένα πελάτη κι έναν εξυπηρετητή. Το παράδειγμα που θα χρησιμοποιήσουμε είναι ένα εργαλείο για συνομιλία (chat) πάνω από BSD sockets, το οποίο τροποποιούμε ώστε τα μηνύματα που ανταλλάσσονται να στέλνονται στο δίκτυο κρυπτογραφημένα.

2 Κρυπτογραφικές Συσκευές

Για να χρησιμοποιήσουμε κρυπτογραφία σε ένα πρόγραμμα που τρέχει σε χώρο χρήστη έχουμε τρεις επιλογές:

- Μπορούμε να αναπτύξουμε τον αλγόριθμο κωδικοποίησης (π.χ. DES, 3DES, AES) κατευθείαν στο πρόγραμμά μας. Φυσικά, αυτό προϋποθέτει ότι είμαστε ειδικοί στην κρυπτογραφία, είμαστε διατεθειμένοι να επενδύσουμε τον κόπο και τον χρόνο που απαιτείται για τη σωστή υλοποίηση του αλγορίθμου, και εμπιστευόμαστε ότι η υλοποίησή μας δεν θα περιέχει σφάλματα που θα την κάνουν ευάλωτη σε κρυπτογραφικές επιθέσεις. Προφανώς, αυτός δεν είναι πρακτικός τρόπος να εξασφαλίσουμε την ασφάλεια της επικοινωνίας.

[1] Για περισσότερες πληροφορίες, δείτε το εισαγωγικό υλικό εδώ: https://developer.mozilla.org/en-US/docs/Introduction_to_SSL

- Μπορούμε να χρησιμοποιήσουμε ελεύθερες, υψηλού επιπέδου βιβλιοθήκες, όπως για παράδειγμα την OpenSSL, http://www.openssl.org/. Αυτός είναι ο πιο πρακτικός τρόπος. Η υλοποίηση των αλγορίθμων κρυπτογράφησης γίνεται σε λογισμικό, και είναι υπολογιστικά απαιτητική.

- Θα μπορούσαμε να χρησιμοποιήσουμε κατάλληλο hardware, του οποίου η χρήση από διεργασίες χώρου χρήστη γίνεται δυνατή μέσω ενός οδηγού συσκευής. Κρυπτογραφικοί επιταχυντές σε υλικό μπορούν να επιτύχουν πολύ υψηλότερους ρυθμούς επεξεργασίας απ'ότι μια υλοποίηση σε λογισμικό.

Αν και οι συγκεκριμένες συσκευές είναι πιο κοινές σε ενσωματωμένα συστήματα, σιγά-σιγά μεγάλοι κατασκευαστές ολοκληρωμένων κυκλωμάτων όπως π.χ. η Intel, παρέχουν hardware για κρυπτογράφηση ακόμα και σε συστήματα που προορίζονται για desktops. Για παράδειγμα κάποιες γενιές επεξεργαστών Intel παρέχουν εντολές assembly που επιταχύνουν την κρυπτογράφηση και αποκρυπτογράφηση block δεδομένων[2].

Στο πλαίσιο της άσκησης, θα χρησιμοποιήσουμε τον οδηγό συσκευής cryptodev-linux. Ο οδηγός αυτός αναπτύχθηκε ώστε να επιτρέπει τη χρήση κρυπτογραφικών συσκευών από βιβλιοθήκες όπως η OpenSSL ή και κατευθείαν από προγράμματα χρηστών μέσω κατάλληλων κλήσεων I/O στο ειδικό αρχείο `/dev/crypto`. Αν στο σύστημα δεν υπάρχει κάποια πραγματική κρυπτογραφική συσκευή, το cryptodev-linux χρησιμοποιεί αλγορίθμους υλοποιημένους σε λογισμικό, ως μέρος του πυρήνα του Linux, για την πραγματοποίηση των κρυπτογραφικών λειτουργιών.

3 Χρήση του cryptodev-linux

Για τους σκοπούς της παρούσας άσκησης θα χρησιμοποιήσουμε την έκδοση 1.10 του cryptodev-linux την οποία μπορείτε να βρείτε στον βοηθητικό κώδικα που σας δίνεται.

Έχετε ήδη εξοικοιωθεί με τη διαδικασία μεταγλώττισης και δυναμικής εισαγωγής ενός module στον πυρήνα του Linux, άρα δε θα πρέπει να αντιμετωπίσετε κάποιο πρόβλημα σε αυτό το στάδιο. Μετά την μεταγλώττιση του cryptodev module πρέπει να εκτελέσετε και `make install` ώστε να αντιγραφεί το αρχείο `cryptodev.h` στο `/usr/local/include/crypto/cryptodev.h` και να μπορεί να χρησιμοποιηθεί από τα προγράμματά σας. Εναλλακτικά, μπορείτε να ρυθμίσετε το μονοπάτι αναζήτησης του `gcc` ώστε να περιλαμβάνει τον κατάλογο όπου έχετε μεταγλωττίσει το

[2] http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/advanced-encryption-standard-new-instructions-set-paper.html

cryptodev module, παράμετρος `-I`.

Αφού έχετε φορτώσει επιτυχώς το module θα πρέπει να βλέπετε μία συσκευή χαρακτήρων `/dev/crypto`. Από αυτό το σημείο μπορούμε να χρησιμοποιήσουμε όλες τις γνωστές κλήσεις συστήματος για συσκευές χαρακτήρων (`open()`, `close()`, `ioctl()`). Το cryptodev userspace API, το οποίο υλοποιεί ο οδηγός cryptodev-linux, βασίζεται στην κλήση `ioctl()`. Για τους σκοπούς του παρόντος οδηγού θα ασχοληθούμε με τις εξής κλήσεις:

- **CIOCGSESSION:** Αρχίζει ένα session με τη συσκευή. Από εκεί και πέρα, κάθε κλήση χρειάζεται να αναφερθεί σε αυτό το session, που περιέχει όλες τις πληροφορίες για τις κλήσεις κρυπτογράφησης/αποκρυπτογράφησης. Ως όρισμα δέχεται μία δομή `struct session_op`.
- **CIOCFSESSION:** Η κλήση αυτή τερματίζει ένα session με τη συσκευή, όταν πλέον δεν χρειαζόμαστε τη χρήση της.
- **CIOCGSESSINFO:** Παρέχει πληροφορίες για τις δυνατότητες της συσκευής στο πρόγραμμα.
- **CIOCCRYPT:** Η συγκεκριμένη κλήση ζητά από τη συσκευή να κρυπτογραφήσει ή να αποκρυπτογραφήσει δεδομένα.

Για περισσότερες πληροφορίες σχετικά με τη χρήση του cryptodev-linux, δείτε τον βοηθητικό κώδικα που σας δίνεται και την τεκμηρίωση του οδηγού στο http://cryptodev-linux.org/documentation.html.