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

8ο εξάμηνο, Ακαδημαϊκή περίοδος 2017–2018

Κρυπτογραφική συσκευή VirtIO για QEMU-KVM

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

Απρίλιος 2018

Περιεχόμενα

1 Εισαγωγή

Αντικείμενο της παρούσας άσκησης είναι η ανάπτυξη εικονικού *υλικού* στο περιβάλλον εικονικοποίησης QEMU-KVM.

Στο πλαίσιο της άσκησης, θα σχεδιάσετε και θα υλοποίησετε εικονική κρυπτογραφική συσκευή VirtIO, η οποία θα αποτελεί πλέον μέρος του QEMU.

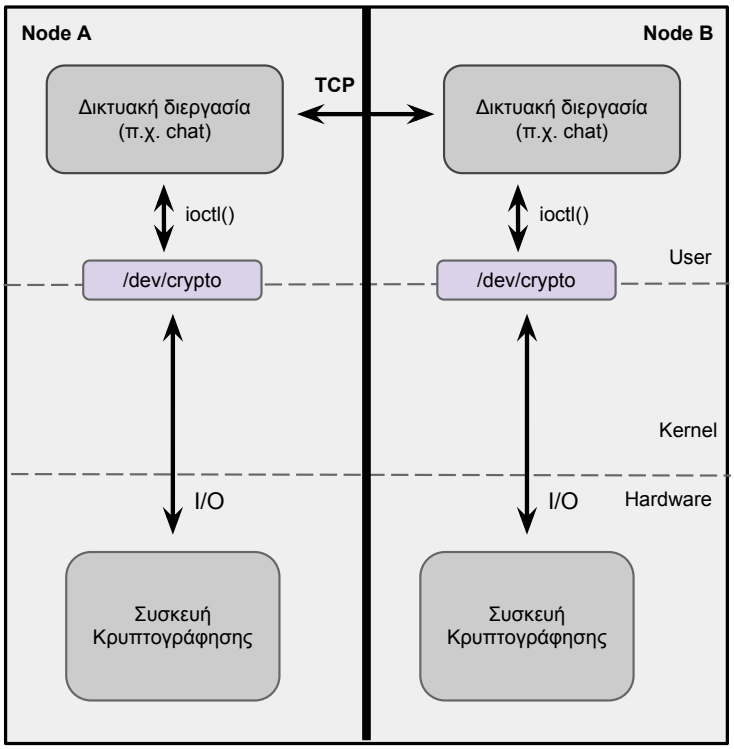
Η εικονική κρυπτογραφική συσκευή θα επιτρέπει σε διεργασίες που εκτελούνται μέσα στην εικονική μηχανή να έχουν πρόσβαση σε πραγματική κρυπτογραφική συσκευή του host, τύπου cryptodev-linux, με χρήση τεχνικής *παρα-εικονικοποίησης* (paravirtualization).

Η συσκευή cryptodev-linux επιτρέπει σε εφαρμογές να έχουν πρόσβαση σε επιταχυντές υλικού για κρυπτογραφία (hardware crypto accelerators), κάνοντας κλήσεις σε ειδικό αρχείο `/dev/crypto`. Περισσότερα για τον τρόπο πρόσβασης σε συσκευές cryptodev-linux και το προσφερόμενο API μπορείτε να διαβάσετε στον οδηγό προγραμματισμού cryptodev-linux που σας δίνεται, καθώς και στο `http://cryptodev-linux.org/`.

Το σενάριο χρήσης του οδηγού σας, με το οποίο και θα επαληθεύσετε τη σωστή λειτουργία του, είναι η υλοποίηση ενός εργαλείου για κρυπτογραφημένη επικοινωνία (encrypted chat) πάνω από TCP/IP sockets, όπως φαίνεται στο Σχήμα 1.

2 Κρυπτογραφημένη επικοινωνία πάνω από TCP/IP

Η κατασκευή της εφαρμογής chat είναι μέρος της άσκησης. Τα δύο άκρα στα οποία εκτελείται η εφαρμογή θα επικοινωνούν μέσω TCP/IP, κάνοντας χρήση του BSD



Σχήμα 1: Κρυπτογραφημένο chat πάνω από TCP/IP

Sockets API. Περισσότερα για το BSD Sockets API μπορείτε να βρείτε στον οδηγό προγραμματισμού με BSD Sockets που σας δίνεται. Η κρυπτογράφηση των μηνυμάτων θα γίνεται μέσω του cryptodev userspace API (`/dev/crypto`).

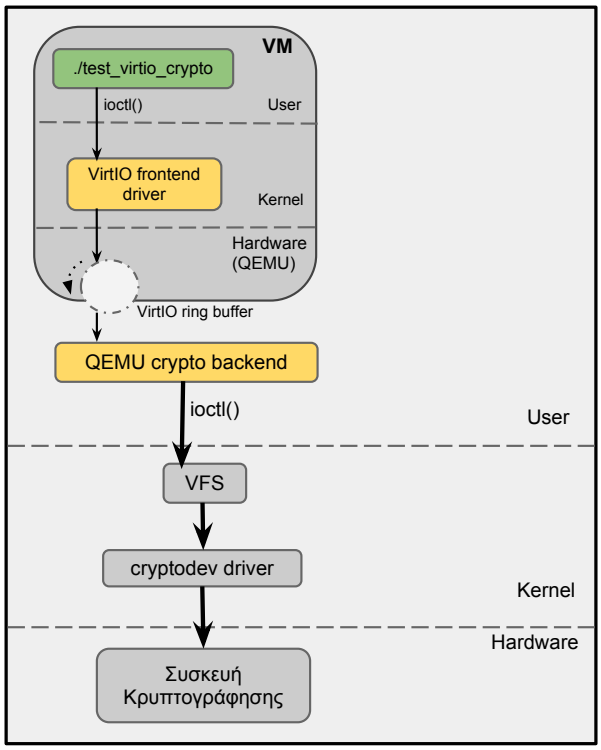
Η εφαρμογή chat θα μπορεί να τρέξει είτε χρησιμοποιώντας απευθείας συσκευή cryptodev-linux, όταν εκτελείται στον host, είτε χρησιμοποιώντας τη δική σας κρυπτογραφική συσκευή VirtIO, όταν εκτελείται μέσα σε εικονική μηχανή QEMU-KVM.

3 Κρυπτογραφική συσκευή VirtIO

Για την υποστήριξη πρόσβασης σε κρυπτογραφικούς επιταχυντές μέσα από VMs, θα σχεδιάσετε και θα υλοποιήσετε δική σας κρυπτογραφική συσκευή VirtIO για cryptodev (εικονικό hardware στο QEMU), και αντίστοιχο οδηγό συσκευής για τον guest πυρήνα Linux, μέσα στην εικονική μηχανή.

Η συσκευή θα υλοποιηθεί σε δύο μέρη, σύμφωνα με το split-driver model: Ένα

frontend (μέσα στο VM) κι ένα backend (μέρος του QEMU), τα οποία θα χρησιμοποιούν το VirtIO ως μηχανισμό επικοινωνίας ανάμεσά τους, όπως φαίνεται και στο Σχήμα 2.



Σχήμα 2: Αρχιτεκτονική λογισμικού της (paravirtualized) συσκευής virtio-crypto

Πιο συγκεκριμένα, σας ζητείται υλοποίηση του οδηγού συσκευής για τον guest πυρήνα του Linux, ο οποίος θα εξάγει στις εφαρμογές το ίδιο cryptodev userspace API που εξάγει η συσκευή cryptodev του host, ουσιαστικά η υλοποίηση της κλήσης `ioctl()` σε κατάλληλη εικονική συσκευή.

Αντίστοιχα, στην πλευρά του backend, μέσα στον κώδικα του QEMU, σας ζητείται να λαμβάνετε τις κλήσεις του frontend και να τις προωθείτε για επεξεργασία από τη συσκευή cryptodev του host.

Η υλοποίηση της κρυπτογραφικής συσκευής VirtIO θα βασιστεί στον κώδικα της συσκευής `virtio-console` που υποστηρίζεται ήδη από το QEMU.

Περισσότερα για τη λειτουργία του VirtIO και την υλοποίηση συσκευών VirtIO μπορείτε να βρείτε στον οδηγό της εργαστηριακής άσκησης που σας δίνεται.

4 Ζητούμενα

Τα ζητούμενα της άσκησης, σε χρονολογική σειρά είναι:

Z1: Εργαλείο chat πάνω από TCP/IP sockets
: Το εργαλείο αυτό θα επιτρέπει αμφίδρομη επικοινωνία πάνω από TCP/IP, με χρήση του BSD Sockets API, χωρίς κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται.

Z2: Κρυπτογραφημένο chat πάνω από TCP/IP
: Επέκταση του εργαλείου chat, ώστε τα δεδομένα που μεταφέρονται πάνω από TCP/IP να είναι κρυπτογραφημένα με προσυμφωνημένο κλειδί. Χρήση του cryptodev-linux API, από userspace, για την κρυπτογράφηση των δεδομένων. Είναι απαραίτητο να ελέγξετε ότι σε αντίθεση με το Z1 εδώ τα δεδομένα μεταφέρονται κρυπτογραφημένα. Για να το κάνετε αυτό θα χρησιμοποιήσετε την εντολή `tcpdump` του linux. Η εγκατάσταση του `tcpdump` μπορεί να γίνει μέσω εκτελώντας `sudo apt-get install tcpdump`. Ένα παράδειγμα χρήσης της `tcpdump` είναι: `tcpdump -ni eth0 -vvv -XXX`

Z3: Υλοποίηση συσκευής cryptodev με VirtIO
: Σχεδίαση και υλοποίηση εικονικής συσκευής cryptodev, με χρήση του πλαισίου VirtIO, έτσι ώστε το προηγούμενο εργαλείο να μπορεί να εκτελείται μέσα σε VM κάνοντας χρήση κρυπτογραφικών επιταχυντών σε υλικό, οι οποίοι ως τώρα ήταν προσβάσιμοι μόνο από τον host. Το εργαλείο πρέπει να εκτελείται ακριβώς με το ίδιο API, αλλάζοντας μόνο τη συσκευή την οποία χρησιμοποιεί για κρυπτογράφηση των δεδομένων. Για την εργαστηριακή εξέταση του παρόντος ζητήματος είναι απαραίτητο να έχετε σιγουρευτεί ότι το chat που υλοποιήσατε στα Z1 και Z2 δουλεύει χωρίς πρόβλημα και μέσω της virtio συσκευής.

Προαιρετικά, μπορείτε να διερευνήσετε τη δυνατότητα επικοινωνίας πολλών ταυτόχρονων πελατών με κοινό server, σε σενάριο παρόμοιο με αυτό της υπηρεσίας Internet Relay Chat (IRC).

5 Εξέταση άσκησης και αναφορά

Η προθεσμία για την εξέταση της άσκησης έχει ανακοινωθεί στη σελίδα του μαθήματος.

Μετά την εξέταση κάθε ομάδα θα πρέπει να συντάξει σύντομη αναφορά, η οποία θα περιγράφει τις βασικότερες επιλογές που κάνατε, τα προβλήματα που προέκυψαν και τον τρόπο με τον οποίο τα επιλύσατε, κατά τη σχεδίαση και υλοποίηση του εργαλείου chat και της κρυπτογραφικής συσκευής VirtIO.