ERASMUS+ KA-2 STRATEGIC PARTNERSHIP PROJECT IN HIGHER EDUCATION
Project no. 2020-1-RS01-KA226-HE-094550, 01.03.2021-28.02.2023

Repository of Open Educational Resources for Laboratory Support in Engineering and Natural Science-RELAB

ВЕБ-Лабораторија: пројектовање, имплементација, одржавање

„Омогући конверзију “off-line” лабораторијског модела у лабораторијски модел који се може користити путем Интернета“

вер 1.0, јануар 2022

Интелектуални исход 5
пројекта
Репозиторијум отворених садржаја образовања ради лабораторијске подршке у природним и техничким наукама – РЕЛАБ 2020-1-RS01-KA226-HE-094550

https://github.com/Erasmus-RELAB
www.relab.kg.ac.rs

Twitter@RELAB2023 *Facebook@ReLab2021* *Instagram@relab.2021*

„Овај пројекат је финансиран уз подршку Европске комисије. Ова публикација одражава само ставове аутора и Комисија не може бити одговорна за било какву употребу информација садржаних у њој“

ОСНОВНИ ПОДАЦИ О ПРОЈЕКТУ

Наслов:

Репозиторијум отворених садржаја образовања ради лабораторијске подршке у природним и техничким наукама

Акроним: РЕЛАБ

Трајање: 01.03. 2021. – 28.02.2023. (24 месеца)
Национална агенција: RS01 Tempus Foundation https://tempus.ac.rs

Буџет: 143.295,00 EUR

Партнери:	
Универзитет у Крагујевцу, Крагујевац, Србија	Национални универзитет за учење на даљину, UNED, Мадрид, Шпанија
Универзитет у Тарту, Естонија	Универзитет Сингидунум, Београд, Србија
Универзитет у Београду, Београд, Србија	Cognipix doo, Београд, Србија

Главни циљеви РЕЛАБ пројекта:

1. Подржати дигитално образовање и лабораторијске видове наставе кроз иновативне концепте стварања и коришћења заједничког репозиторијума висококвалитетних кратких видео записа репрезентативних експеримената и програмабилних дигиталних копија експерименталних реализација.
2. Израдити свеобухватно упутство за развој егземпларне Веб лабораторије за програмирање и примену специјализованог хардвера, и израда, и пуштање у рад примера једне такве лабораторије.

Циљ пројекта

- Циљ пројекта је развој стратешког партнерства високошколских установа ради стварања и објављивања отворених садржаја образовања у оквиру заједничких или умрежених репозиторијума отворених садржаја образовања
- Предмет овог пројекта су следећи типови отворених садржаја образовања:
  1) „Једноминутни” експерименти
  2) Дигитални близанци експерименталних реализација
  3) Веб лабораторије

  - https://youtube.com/@relabvideos
  - https://relab.kg.ac.rs/dist/#/Home
  - https://relab.kg.ac.rs/docs/intelectualoutputs/io4/

УВОД

Често се дешава да се лабораторијски експерименти прво развијају на ad-hoc начин користећи доступну опрему и познате рачунарске ресурсе, за лабораторијски рад на лицу места. Иако није идеалан, овај приступ је веома чест, па и уобичајен.

Али глобалне пандемије, као и све веће интересовање и потребе за учење на даљину, као и хибридни приступи учења, померају захтеве ка различитим лабораторијским концептима, укључујући и коришћење лабораторија на даљину, или веб лабораторија. Наш циљ, у овом делу РЕЛАБ пројекта, је да понудимо инкрементални приступ и помогнемо наставном особљу да искористе претходне напоре у креирању лабораторијских модела, али их учине и доступним за рад са удаљених локација путем Интернета, а да су при том испуњени безбедносни стандарди.

Под претпоставком изнад, овај документ неће покривати веб-лабораторије створене од нуле са искључивом намером о даљинској доступности. Ове веб-лабораторије треба да узму у обзир ову захтевану карактеристику од самог почетка, да одаберу одговарајућу платформу/оквир/API на неколико нивоа: сервер за подешавање лабораторије, Proxy Server и клијента (радну станицу студента). Постоји много предности, као што је добро контролисано окружење које омогућава продуктивно коришћење лабораторије, повећане аспекте безбедности. Такође, предложено решење је намењено да се користи од стране наставног особља или мале групе наставника без значајне ИТ подршке - ово је основни покретач наших одлука у погледу архитектуре веб лабораторије (тим пре, јер је много различитих путева могуће).

Инкрементални приступ ће укључити три елемента заснована на стандардним, отвореним, готовим технологијама. Међутим, неки елементи као што су регистрација лабораторијског модела, регистрација студената, алокација ресурса у реалном времену, проксирање видео стриминга и SSH приступ преко прегледача би захтевали додатне развојне напоре.

Овај интелектуални исход РЕЛАБ пројекта биће доступан под условима либералних лиценци (коначни избор лиценци MIT, BSD или GPL лиценци биће дискутован са Националном агенцијом). Неопходне скрипте, софтверски пакети и документација биће хостовани на GITHUB и relab.kg.ac.rs, да би омогућили лаку дисеминацију.

За конфигурацију веб лабораторијског модела **потребно је имати средњи ниво познавања Linux оперативног система**. За веб лабораторију/Бастион сервер, потребно је поедовати познавање Linux оперативног система на средњем/напредном нивоу, док сервер је може послужити за више лабораторијских модела, па чак и за више институција у оквиру истог или више универзитета.

Увод у РЕЛАБ веб лабораторијску архитектуру за ”online” приступ

Ово решење је креирано са следећим критеријумима које смо имали на уму:

- Једноставност за крајње кориснике, или за студенте, како би се омогућио брз приступ, лака инсталација, а опет слично искуство као да су физички присутни у реалном лабораторијском простору.
- Већ постоје лабораторијски модели који користе Linux подршку, са прикљученим припадајућом лабораторијском опремом, EVM-овима или слично - и користе се за ”off-line” рад ван мреже, уз физичко присуство студената.
- Конверзија ”off-line” лабораторијског модела (као што је описано у претходном наводу) у ”online” лабораторијски модел, не би требало да захтева много времена и велику ИТ експертизу наставног особља.
- Решење би требало да користи само ” open source ”софтверске пакете са либералним лиценцама – а не ”freeware” или комерцијалне опције.
- WebLab/Bastion сервер инсталација и подешавање може бити комплекснија, али се може делити између више лабораторијских модела, укључујући лабораторијске моделе са различитих локација. Ово је једнократни напор, заснован на корацима и описима у овом документу.
- Избегавајте стављање више лабораторијских модела на јавни Интернет, како бисте смањили “surface-of-attack” на само на један Бастион сервер. Будући да различити делови лабораторијске опреме могу бити на интерном LAN-у, само и излагање лабораторијских модела са јавном IP адресом, може отворити питања конфигурације мреже.
- Међу различитим ”open-source” бесплатним решењима, ми смо изабрали X2GO као поуздано, безбедно решење и решење са малим кашњењем за примену на клијентској радној станици и лабораторијском серверу. Све мрежне везе установљене су на основу SSH или обрнутог SSH-а.

РЕЛАБ архитектура веб лабораторије

Предложена архитектура укључује 3 елемента.

Лабораторијски модел са свим придруженим лабораторијским уређајима, као у конвенционалном лабораторијском простору. Примера ради, уобичајено могу бити ту као посебни елементи Ардуино микроконтролери, мотори, сензори, лабораторијски модели управљаних и мерених процеса, камера, итд. Ови елементи система су обично већ доступни и изван опсега описивања су овог документа.

- **Лабораторијски сервер** је део лабораторијског модела у ширем смислу. Претпостављамо да је то Ubuntu/Debian базиран на ”лаком” рачунару (x86-заснован или ARM-заснован попут RPi). Даћемо детаљно објашњење о његовој конфигурацији и неопходним софтверским додацима. Важна претпоставка овде је да лабораторијски сервер нема (IPv4 или IPv6) јавну адресу. Претпостављамо да је ова конфигурација иза NAT-а, у већини типичних локалних мрежа у лабораторијском окружењу. Осим тога, нећемо дискутовати о VPN опцији јер захтева комплексније IT поставке, које могу створити додатне безбедносне проблеме.

Јавни **веб лабораторијски** (тј. ”Bastion”) **сервер** је у некој мери произвољан термин, али се углавном односи на виртуелни приватни сервер (VPS) доступан ”у облаку”, који пружа услуге IT сервиса у оквиру универзитета, или који се изнајмљује од јавног провајдера информатичког облака (AWS, DigitalOcean, Azure, Google или неког локалног провајдера информатичког облака). Може се користити за различите сврхе, као што су сервер, веб странице, сервер за четовање/блоговање, сервер за датотеке, сервер за видео преност, итд. У овом документу ћемо ограничити обим дискусије на додатне (врло мале) сервисе/конфигурације потребне за предложено решење. Овај сервер је углавном базиран на Linux. граничићемо обим дискусије у овом документу на додатне (врло мале) сервисе/конфигурације потребне за предложено решење. Овај сервер је такође углавном базиран на Линуксу.

- У следећем кораку, ми ћемо предложити софтверско решење за веб-базирану регистрацију нових ресурса лабораторијског окружења и нових студената. Биће омогућена расподела ресурса (термина) за одређеног студента и одређено лабораторијско окружење. Неопходно је укључити логовање/журналисање активности рада студената за потребе праћења, као и механизам за преглед. Коначно, неопходно је дизајнирати пажљиво прилагођено (chroot/jailed ssh) безбедносно решење, што је такође предмет овог решења.
- У овој конкретној улози сервера који се излаже јавности, назива се "Бастион" или "Proxy Jump" сервер.
- Специфични захтеви за Weblab/Bastion сервер се односе пре свега на пропусни капацитет мреже, јер овај сервер већином функционише као комуникациони чвор.

Радна станица клијента/студента захтева веома мало измена на софтверском плану. Може бити базирана на оперативним системима Windows или Linux. Потребна су само два додатна софтверска пакета која могу лако да се инсталирају (<5 минута).

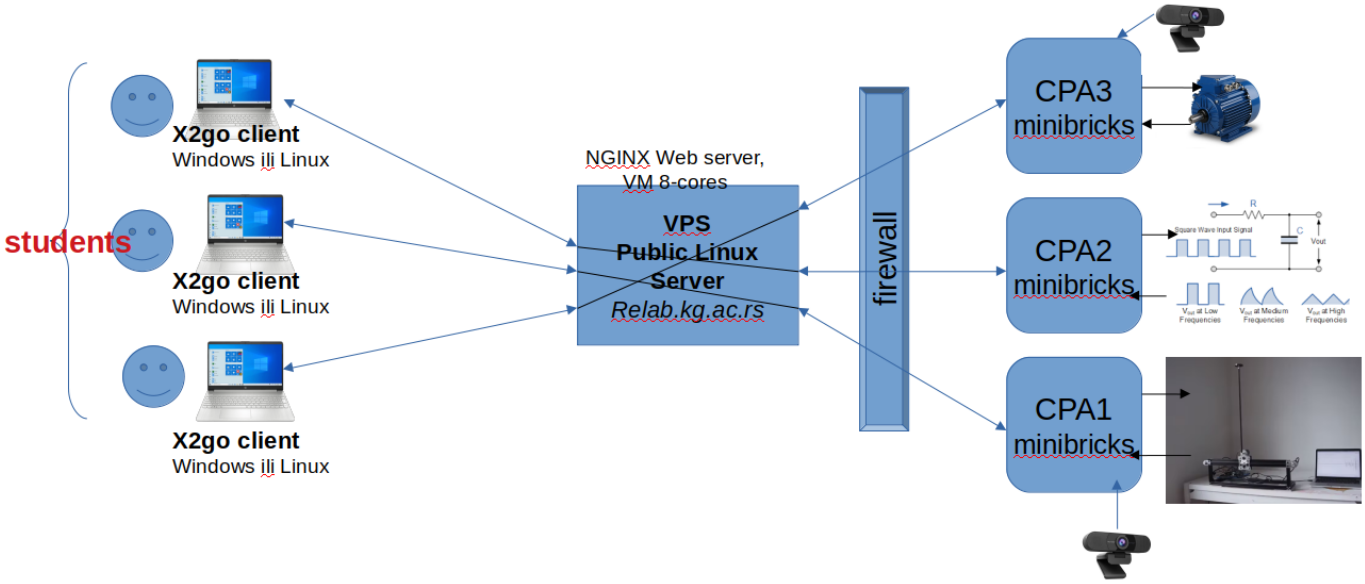
- Као додатни циљ, ми ћемо предложити решење базирано на веб претраживачу, које би требало да омогући студентима да приступе удаљеном лабораторијском окружењу без инсталирања новог софтвера, осим пријављивања и давања додељених акредитива. У следећој фази пројекта, као алтернативу, ми ћемо

предложити решење базирано на Apache Guacamole, са неопходно укљученим изменама.

РЕЛАБ ВЕБ ЛАБ СА ВИШЕ LINUX+ARDUINO СТАНИЦА

Конфигурација која је илустративно приказана испод је примењена на Универзитету у Крагујевцу.

Приступ овим лабораторијским сетовима је имплементиран путем VPS-а, који такође покреће веб сајт relab.kg.ac.rs. Захваљујући Linux оперативном систему, више сервиса може да се покрене истовремено.



Ова пилот инсталација се састоји од:

- 5 лабораторијских модела
  - Користе се мини рачунари Gigabyte Minibricks са Ubuntu 20.04 оперативним системом, сваки са Arduino микрокотролером и протоборд плочом која је повезана на Arduino I/O (аналогни и дигитални улази и излази). Додатни детаљи су наведени у одвојеном документу.
  - Свака лаб конфигурација има USB камеру повезану са мини рачунаром тако да студенти могу да прате реално понашање, као што је укључивање/искључивање LED-диода, кретање DC мотора итд.
- Бастион сервер покреће веб сајт relab.kg.ac.rs
  - VPS са Ubuntu 20.04 LTS функционише као веб сервер. Ова конфигурација има 4 језгра и 8GB RAM-а, заједно са 80GB HDD/SSD.
- Рачунари (PCs/laptops) клијената/студената
  - Коришћењем овог почетног решења, око 100 - 120 студената у семестру је приступало посредством Интернета лабораторијским моделима, уместо да дође у лабораторију и изврши кратке лабораторијске експерименте (<10-15 минута).
  - Не постоје специјални захтеви за рачунаре студената: то могу бити стандардни рачунари или лаптопови са оперативним системом Windows или Linux. Тренутно

решење је засновано на X2GO сервер/клијент решењу, тако да приступ са IoS или Android уређајима није могућ.

Кратак опис конфигурације лабораторијског сервера (Linux, Ubuntu)

Кроз овај документ, ми ћемо претпоставити да лабораторијска подешавања укључују ”танки” сервер базиран на Linux-у (на пример x86 MiniBricks или RPI4). За пример ћемо користити конфигурацију базирану на Debian-у, Ubuntu. Упутства која следе приказују процес уопштено - тачне команде су дате у додатку.

- Први корак је конфигурација, повезивање и провера почетног лабораторијског модела који користе студенти када дођу у лабораторију. Ово укључује инсталацију више стандардних Debian пакета на Ubuntu 20.04LTS.
- Други корак је генерисање SSH кључева и њихова инсталација на 'Bastion' серверу.
    - Овај корак креира приватне кључеве id_rsa и њихове јавне кључеве id_rsa.pub.
- Ове кључеве је потребно трансформисати у јавни сервер веб лабораторије и укључти ауторизоване кључеве (од јавног серевера веб лабораторије)

Кратак опис конфигурације Bastion/Weblab јавних сервера (Linux, Ubuntu)

- VPS Linux сервери обично су већ конфигурисани за јавно излагање, са неопходно инсталираним пакетима и неким нивоом мрежне сигурносне заштите. Ово је случај како за комерцијална решења типа AWS, Google, Digital Ocean, Linode, Azure, тако и за услуге сервера у облаку које нуде универзитети. Ово значи да је SSH приступ већ омогућен, са неколико креираних налога, при чему један од њих има привилегије за извршавање додатних корака користећи sudo команду.
- Потребно је креирати корисничке налоге за сваки лабораторијски модел са ограниченим привилегијама, именоване по узору на weblabcpaX (где је X редни број лабораторијског модела).
- Треба да проверимо мрежну повезаност од Bastion/Weblab сервера ка лабораторијским моделима, како у једном, тако и у обрнутом смеру.

Кратак опис конфигурације радне станице Client / Студента (Windows or Linux)

- Да бисмо омогућили удаљени рад радне станице, користићемо X2GO софтверски пакет инсталирањем серверске стране на лабораторијском серверу, и клијентске стране X2GO-а на студентској радној станици. X2GO серверска страна је доступна само за Linux, док је клијентска страна доступна за оба оперативна система - Windows и Linux.
- Доступан је додатни ZIP пакет са неопходним скриптама и конфигурационим фајловима да би се омогућила повезаност путем једног клика између студентске радне станице и лабораторијског модела.

Детаљна конфигурација Bastion (познатог и као 'proxy jump') сервера

Bastion сервер је јавно доступан (тј. сервер са јавном IP адресом), ојачани систем који служи као улазна тачка до система иза заштитног зида или друге ограничене локације. Ти системи могу бити у истој LAN мрежи, или у различитим LAN мрежама, па чак и иза различитих заштитних зидова.

Један бастион сервер је довољан за више група лабораторијских модела, а ограничен је доступним пропусним капацитетом и рачунарском моћи у мањој мери.

Сервер Bastion је једини Linux сервер који прихвата јавне SSH везе. Ово смањује "површину напада" на само један сервер.

Ако корисник жели да приступи "скривеној" (од јавног Интернета) рачунарској машини у лабораторијском моделу, прво мора да се повеже на Bastion сервер, а затим да направи још једну SSH везу од Бастион сервера до крајње дестинације. Овај процес се понекад назива "proxy jump" и може бити аутоматизован.

У нашем решењу, лабораторијски модели такође установљују SSH реверзни тунел (односно, лабораторијски модел иницира и одржава везу са Бастион сервером), и на тај начин ствара могућност за спољне кориснике (Student/Client радне станице) да приступе лабораторијским моделима који нису изложени на јавном интернету.

Кориснички налози посвећени лабораторијском моделу

Bastion сервер има посебно креиране корисничке налоге за повезивање са лабораторијским моделима, са ограниченим скупом дозвола: "weblabcpa", "weblabcpa2", ..., "weblabcpa5".

Ово се постиже коришћењем стандардних Linux команди 'chroot'. На овај начин, ови кориснички налози могу користити само подскуп команди на Bastion серверу.

У нормалном раду, не очекује се да се студенти логују на Bastion сервер. Уместо тога, користиће аутоматизоване скрипте које ми обезбеђујемо, како би приступили лабораторијским моделима користећи једну команду (на пример, за студенте или клијенте су понуђене датотеке за обраду за Windows или Linux оперативни систем).

Ово се постиже са Linux командом adduser:

```
sudo adduser weblabcpa
sudo adduser weblabcpa2
...
sudo adduser weblabcpa5
```

За сваког корисника морамо да наведемо лозинку, али за све ове налоге, дозволићемо само пријављивање без лозинке, тј. без w/o лозинке, али са SSH кључем (стога је добра навика да се користи јака лозинка, али није обавезна).

Да бисмо омогућили пријаву са ограниченим привилегијама, креираћемо специјални "chroot" директоријум, у овом случају, "/home/testjailed".

Chroot представља начин изоловања апликација од остатка рачунара, стављајући их у *jail (затвор)*. Ово је посебно корисно ако тестирате апликацију која би потенцијално могла изменити важне системске датотеке или која може бити небезбедна. Ово се може урадити за

подскуп корисничких налога на датој конфигурацији. Овај начин ће бити коришћен за weblabcpaX налоге.

```
mkdir -p /home/testjailed/{bin,lib64,etc,home}
cp -v /bin/bash /home/testjailed/bin
```

Сада морамо да пронађемо све библиотеке које су потребне за *bash*. Ово се ради помоћу команде *ldd*:

```
ldd /bin/bash
```

У случају Ubuntu 20.04LTS-а, овај списак добијамо:

```
linux-vdso.so.1 (0x00007ffe901d7000)
libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007fdbb22a7000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007fdbb22a1000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fdbb20af000)
/lib64/ld-linux-x86-64.so.2 (0x00007fdbb2416000)
```

Све наведене библиотеке треба да се копирају (из /lib) у директоријум "/home/testjailed/lib":

```
cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2} /home/testjailed/lib64/
```

Затим морамо копирати фајлове налога:

```
mkdir /home/testjailed/etc
cp -vf /etc/{passwd,group} /home/testjailed/etc/
```

Напослетку, можемо изменити фајл „/etc/ssh/sshd_config“, да би конфигурисали SSH да користи chroot затворени систем (у овом случају „testjailed“):

```
Match User weblabcpa
   ChrootDirectory /home/testjailed
   PasswordAuthentication no

Match User weblabcpa2
   ChrootDirectory /home/testjailed
   PasswordAuthentication no

Match User weblabcpa3
   ChrootDirectory /home/testjailed
   PasswordAuthentication no

Match User weblabcpa4
   ChrootDirectory /home/testjailed
   PasswordAuthentication no

Match User weblabcpa5
   ChrootDirectory /home/testjailed
   PasswordAuthentication no
```

И поново покрените ssh сервис: sudo systemctl restart ssh.service

Како бисмо омогућили приступ без шифре, потребно је да копирамо јавне кључеве id_rsa.pub, генерисане на лабораторијским моделима (са ssh-keygen) у датотекама .ssh/authorized_keys за све налоге weblabcpaX.

Ове кључеви могу бити копирани/прилепљени/пренесени са лабораторијских модела, било као редовна (*scp* базирана) трансфер датотека, или коришћењем ssh-copy-id алата.

Да би били сигурни да су све SSH везе омогућене, можете ручно проверити користећи SSH команду у командној линији (од лабораторијског модела до WebLab/Bastion сервера).

Надзор операција на Bastion серверу

Тренутно установљене везе могу бити надзиране у стандардним датотекама "/var/log/auth.log".

```
grep "weblabcpa" /var/log/auth.log
```

и број успело остварених веза од стране лабораторијских модела користећи следећу команду:

```
relab_user@relabserver01:~/LOGS$ sudo lsof -iTCP -sTCP:LISTEN | grep sshd

[sudo] password for relab_user:
sshd     2142135          root    3u  IPv4 26149991     0t0  TCP *:ssh (LISTEN)
sshd     2142135          root    4u  IPv6 26149993     0t0  TCP *:ssh (LISTEN)
sshd     2340265     weblabcpa2   10u  IPv6 28404097     0t0  TCP ip6-localhost:42287 (LISTEN)
sshd     2340265     weblabcpa2   11u  IPv4 28404098     0t0  TCP localhost:42287 (LISTEN)
sshd     2340265     weblabcpa2   12u  IPv6 28404101     0t0  TCP ip6-localhost:22026 (LISTEN)
sshd     2340265     weblabcpa2   13u  IPv4 28404102     0t0  TCP localhost:22026 (LISTEN)
sshd     2340967      weblabcpa   10u  IPv6 28409371     0t0  TCP ip6-localhost:41310 (LISTEN)
sshd     2340967      weblabcpa   11u  IPv4 28409372     0t0  TCP localhost:41310 (LISTEN)
sshd     2340967      weblabcpa   12u  IPv6 28409375     0t0  TCP ip6-localhost:22024 (LISTEN)
sshd     2340967      weblabcpa   13u  IPv4 28409376     0t0  TCP localhost:22024 (LISTEN)
sshd     2425492     weblabcpa4   10u  IPv6 29142437     0t0  TCP ip6-localhost:56902 (LISTEN)
sshd     2425492     weblabcpa4   11u  IPv4 29142438     0t0  TCP localhost:56902 (LISTEN)
sshd     2425492     weblabcpa4   12u  IPv6 29142441     0t0  TCP ip6-localhost:22030 (LISTEN)
sshd     2425492     weblabcpa4   13u  IPv4 29142442     0t0  TCP localhost:22030 (LISTEN)
sshd     2510791     weblabcpa5   10u  IPv6 29690310     0t0  TCP ip6-localhost:49842 (LISTEN)
sshd     2510791     weblabcpa5   11u  IPv4 29690311     0t0  TCP localhost:49842 (LISTEN)
sshd     2510791     weblabcpa5   12u  IPv6 29690314     0t0  TCP ip6-localhost:22032 (LISTEN)
sshd     2510791     weblabcpa5   13u  IPv4 29690315     0t0  TCP localhost:22032 (LISTEN)
sshd     2550356     weblabcpa3   10u  IPv6 29982993     0t0  TCP ip6-localhost:33894 (LISTEN)
sshd     2550356     weblabcpa3   11u  IPv4 29982994     0t0  TCP localhost:33894 (LISTEN)
sshd     2550356     weblabcpa3   12u  IPv6 29982997     0t0  TCP ip6-localhost:22028 (LISTEN)
sshd     2550356     weblabcpa3   13u  IPv4 29982998     0t0  TCP localhost:22028 (LISTEN)
```

Конфигурација сервера лабораторијских модела (заснована на Linux оперативном систему)

Сервери лабораторијских модела су јефтини мини рачунари са 4 GB RAM-а, 2 језгра и 80 GB SSD простора. Исти приступ може да се користи и са Raspberry PI4, чија је Linux дистрибуција такође заснована на Debian-u.

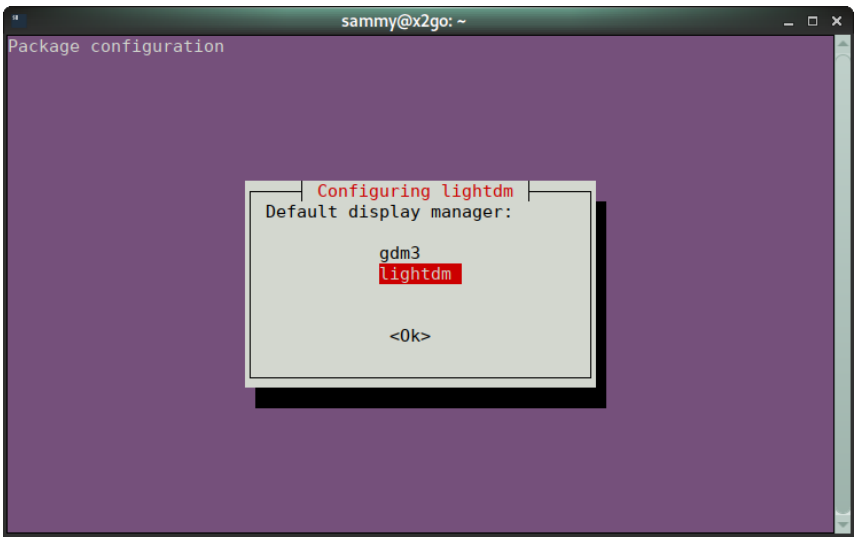
Linux оперативни систем је коришћен за сервере лбораторијских модела, и то Да би прирпемили miniPC за ову улогу, следеће модификације су захтеване:

SSH сервис

- Конзола (терминал, тастатура, миш) су потребни само током инсталације оперативног система и омогућавања SSH приступа, а после тога нису неопходни, што омогућава компактнију конфигурацију (такозвана безглава конфигурација).
- Повежите miniPC за лабораторијски модел на локалну LAN мрежу, а затим ажурирајте пакете на најновију верзију.
  - sudo apt update
- SSH је потребно да буде омогућена
  - sudo apt install openssh-server
  - После овог корака, можете прећи на 'headless' конфигурацију, тј. уклонити монитор, тастатуру и миша.

Додавање радног окружења

- Инсталирајте *Desktop* окружење да бисте омогућили неограничену удаљену употребу апликација на miniPC рачунарима који су повезани за лабораторијским моделима:
  - Инсталирајте и подесите потпуно *Desktop* окружење (пријатна опција, која избегава многе експлицитно изабране пакете). Имајте на уму да овај корак може трајати до 5 минута због многих зависних пакета који се инсталирају:
    - sudo apt-get install xubuntu-desktop
  - Када се од вас затражи да изаберете менаџер приказа, изаберите lightdm:



X2GO сервис

- Инсталирајте X2GO сервер на miniPC рачунару за рад са лабораторијским моделом:
  - sudo apt-get install x2goserver x2goserver-xsession

После овог корака, требало би да верификујете конекцију коришћењем X2GO (од локалног Linux или Windows подешавања оперативног система).

- Следећи корак је омогућавање постојаног SSH обрнутог тунела, омогућавањем autossh сервиса. Овај сервис отвара и поново установљава обрнути тунел при покретању система, а такође и током рада уколико не успе из било ког разлога. На овај начин имамо трајну везу са Бастион сервером (relab.kg.ac.rs).

Процедура подешавања је следећа:

- Прво морамо припремити SSH кључеве за безлозинску везу од сервера лабораторијског модела до Бастион сервера. Ови кључеви се генеришу коришћењем команде:
  - mkdir -p $HOME/setupPROXY/sshkeys/weblabcpa2/
  - ssh-keygen -f $HOME/setupPROXY/sshkeys/weblabcpa2/ -t rsa
  - ssh-keygen -t rsa -b 4096 -C "weblabcpa2@example.com" -f $HOME/setupPROXY/sshkeys/weblabcpa2/id_rsa
  - Сада копирајте кључеве на Бастион серверу, ручно или користећи команду:
    - ssh-copy-id -i $HOME/setupPROXY/sshkeys/weblabcpa2/id_rsa.pub
  - Верификујте да ли SSH веза са сервера лабораторијског модела па до Бастион сервера може да се успостави.
    - ssh -i $HOME/setupPROXY/sshkeys/weblabcpa2/id_rsa `weblabcpa2@relab.kg.ac.rs`
  - Такође, можете проверити на Бастион серверу да ли су кључеви за CPA2 додати у фајл /home/weblabcpa2/.ssh/authorized_keys.
- Инсталирајте AUTOSSH пакет:
  - sudo apt install -y autossh
- Креирајте autossh.service фајл у основном директоријуму (vi ~/autossh.service)

```
[Unit]
Description=Autossh, keeps a reverse tunnel to 'relab.kg.ac.rs' open
After=network.target
[Service]
User=cpa2
Environment="AUTOSSH_GATETIME=0"
Restart=always
RestartSec=30
Type=simple
ExecStart=/usr/bin/autossh -o "ServerAliveInterval 10" -o "ServerAliveCountMax 3" -o "ExitOnForwardFailure=yes" -i /home/cpa2/setupPROXY/sshkeys/weblabcpa2/id_rsa  -N -R 22026:localhost:22 weblabcpa2@relab.kg.ac.rs
StandardOutput=journal

[Install]
WantedBy=multi-user.target
```

- cp ~/autossh.service /lib/systemd/system/autossh.service
- sudo ln -s /lib/systemd/system/autossh.service \
  /etc/systemd/system/autossh.service
- sudo systemctl daemon-reload
- sudo systemctl start autossh
- sudo systemctl status autossh
    - Претходне команде проверавају статус autossh сервиса и приказују излаз сличан следећем:

```
● autossh.service - Autossh, keeps a reverse tunnel to 'relab.kg.ac.rs' open
   Loaded: loaded (/lib/systemd/system/autossh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-01-13 20:47:08 CET; 2 weeks 4 days ago
 Main PID: 682 (autossh)
    Tasks: 2 (limit: 4545)
   Memory: 1.5M
   CGroup: /system.slice/autossh.service
           ├─ 682 /usr/lib/autossh/autossh -o ServerAliveInterval 10 -o ServerAliveCountMax 3 -o ExitOnForwardFailure=yes -i
/home/cpa2/setupPROXY/sshkeys/weblabcpa2/id_rsa -N -R 22026:localhost:22 webl>
           └─1118 /usr/bin/ssh -L 42287:127.0.0.1:42287 -R 42287:127.0.0.1:42288 -o ServerAliveInterval 10 -o ServerAliveCountMax 3 -o
ExitOnForwardFailure=yes -i /home/cpa2/setupPROXY/sshkeys/weblabcpa>
...
јан 13 20:47:19 cpa2-GB-BACE-3000 autossh[682]: starting ssh (count 8)
јан 13 20:47:19 cpa2-GB-BACE-3000 autossh[682]: ssh child pid is 1118
```

- sudo systemctl enable autossh
    - Претходна команда је потребна да би се сервис омогућио при покретању система.

У овом примеру смо користили порт 22026 за обрнуту SSH везу са Бастион серверском страном. То може бити верификовано коришћењем мониторинг команди на Бастион серверу, као што је описано у претходном поглављу.

Такође, са Бастион серверске стране, требало би да можете да се повежете са CPA2 користећи:

ssh -p 22026 `cpa2@127.0.0.1`, и обезбеђујући лозинку.

Ажурирање Ubuntu 20.04 ради превенције потенцијалних проблема (Ubuntu-специфичних)

Како би се избегао проблем закључавања екрана у вези са *screensaver*-ом током удаљене сесије, потребно је додати xorg.conf у фолдер /etc/X11/:

```
Section "Monitor"
Option        "DPMS"
EndSection


Section "ServerLayout"
Option        "BlankTime"    "0"
Option        "StandbyTime"   "0"
Option        "SuspendTime"   "0"
Option        "OffTime"      "0"
EndSection
```

Један још Ubuntu 20.04/20.10 специфичан проблем се појављује само при удаљеној радној станици (у овом случају X2GO), увек (пријављивање) тражећи потврду "Потребна је аутентикација за креирање боје профила/управљаног уређаја".

Ово се покреће помоћу Polkit-а, који је оквир за одобрење апликација. Када се повежете на Ubuntu са удаљеног рачунара, видећете горе наведене грешке, јер Polkit политика датотека не може да се приступи без аутентикације суперкорисника.

Решење за овај проблем је:

```
sudo vi /etc/polkit-1/localauthority.conf.d/02-allow-colord.conf
```

и укључује следеће:

```
polkit.addRule(function(action, subject) {
 if ((action.id == "org.freedesktop.color-manager.create-device" ||
 action.id == "org.freedesktop.color-manager.create-profile" ||
 action.id == "org.freedesktop.color-manager.delete-device" ||
 action.id == "org.freedesktop.color-manager.delete-profile" ||
 action.id == "org.freedesktop.color-manager.modify-device" ||
 action.id == "org.freedesktop.color-manager.modify-profile") &&
 subject.isInGroup("{users}")) {
 return polkit.Result.YES;
 }
});
```

Пилот веб лабораторија на Универзитету у Крагујевцу

Ограничење X2GO времена сесије

Коначно, да бисмо ограничили време сесије X2GO-а, морамо да додамо CRON задатак, извршен сваких 5 минута. Он ће проверити да ли је X2GO сесија установљена, израчунати њено трајање и прекинути је након ~15 минута. Ово се постиже додавањем специјалне скрипте (x2golimittime) заједно са другим X2GO алатима (при инсталацији X2GO серверског пакета, као што је описано раније) - у директоријум /usr/lib/x2go/.

```
#!/bin/bash
# Below constant defines timeout
maxSESSION=800
string1=`/usr/bin/x2golistsessions | cut -f6 -d'|'`
if [ -z "$string1" ]
then
   echo "x2go session list is empty" > /dev/null
else
```

```
  string2=`date -Iseconds | cut -f2 -d'T' | cut -f1 -d'+'`
  StartDate=$(date -u -d "$string1" +"%s")
  FinalDate=$(date -u -d "$string2" +"%s")
  tdiff=`date -u -d "0 $FinalDate sec - $StartDate sec" +"%H:%M:%S"`
  #echo $tdiff
  tdiffIN=(${tdiff//:/ })
  tHOURS=${tdiffIN[0]}
  tMINS=${tdiffIN[1]}
  tSECONDS=${tdiffIN[2]}
  #echo "$tHOURS $tMINS $tSECONDS"
  totSECONDS="$(($tHOURS*3600 + $tMINS*60 + $tSECONDS))"
  #echo $totSECONDS
  if [ "$totSECONDS" -gt "$maxSESSION" ]; then
    stringSESSION=`/usr/bin/x2golistsessions | cut -f2 -d'|'`
    #echo "Terminate session $stringSESSION"
    /usr/bin/x2goterminate-session $stringSESSION
  fi
fi
```

Затим треба да додамо овај задатак на листу CRON задатака, користећи: sudo crotab -e

```
...
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/5 * * * * /usr/lib/x2go/x2golimittime
```

Остатак подешавања удаљеног лабораторијског сервера је идентичан подешавању локалног лабораторијскг сервера, на пример додавање Arduino IDE-a, инсталирање USB камере и апликација као што је "cheese" за снимање слика са USB камере.

Подешавање радне станице клијента/студента (Windows and Linux)

Студентско или клијентско подешавање радне станице захтева инсталацију само два пакета: X2GO клијента и одређени скуп фајлова са прилагођеним SSH кључевима, X2GO сесијски фајл и BATCH / SHELL скриптне фајлови.

На овај начин, један клик или наредба је довољна да иницира конекцију ка удаљеном лабораторијском моделу – потребно је унети само лозинку пре него што се успостави веза са удаљеном радном станицом преко Бастион сервера.

X2GO инсталација клијента

- Подешавање Windows клијента: http://code.x2go.org/releases/X2GoClient_latest_mswin32-setup.exe
- Подешавање Linux клијента: то је расположиво у стандардном Ubuntu репозиторијумима, тако да је следећа команда довољна: sudo apt-get install x2goclient
- Важно је одабрати XFCE као тип сесије (јер је то одабрано у типу X2GO сервера).

Инсталација прилагођених датотека и процедура пријављивања описани су у посебном документу „Приручник за приступ лабораторијским подешавањима преко X2GO сервера“ (или у издању за студенте „Упутство за приступање лабораторијским вежбама преко X2GO сервера“).

Прилагођени пакет укључује следеће датотеке:

- Унапред дефинисане X2GO сесије (за свих 5 лабораторијских модела)
  - cpa_sessions.txt (below is listed only for the 1st session i.e. setup)

```
[20211118132048980]
applications=WWWBROWSER, MAILCLIENT, OFFICE, TERMINAL
autologin=true
clipboard=both
command=XFCE
defsndport=true
directrdp=false
directrdpsettings=
directxdmcp=false
directxdmcpsettings=
display=1
dpi=142
export=
fstunnel=true
fullscreen=false
height=600
host=127.0.0.1
icon=:/img/icons/128x128/x2gosession.png
iconvfrom=ISO8859-1
iconvto=UTF-8
key=
krbdelegation=false
krblogin=false
maxdim=false
multidisp=false
name=RelabMiniBricsCPA
pack=16m-jpeg
print=true
published=false
quality=9
rdpclient=rdesktop
rdpoptions=
rdpport=3389
rdpserver=
rootless=false
setdpi=true
sndport=4713
sound=true
soundsystem=pulse
soundtunnel=true
speed=2
sshport=22024
sshproxyautologin=true
sshproxyhost=147.91.209.60
sshproxykeyfile=id_rsa_weblabcpa.txt
sshproxykrblogin=false
sshproxyport=22
sshproxysamepass=false
sshproxysameuser=false
sshproxytype=SSH
sshproxyuser=weblabcpa
startsoundsystem=true
type=auto
useiconv=false
usekbd=true
user=cpa
usesshproxy=true
width=800
xdmcpclient=Xnest
```

```
xdmcpserver=127.0.0.1
xinerama=false

[20211118132048981]
applications=WWWBROWSER, MAILCLIENT, OFFICE, TERMINAL
autologin=true
clipboard=both
command=XFCE
defsndport=true
directrdp=false
directrdpsettings=
directxdmcp=false
directxdmcpsettings=
display=1
dpi=142
export=
fstunnel=true
fullscreen=false
height=600
host=127.0.0.1
icon=:/img/icons/128x128/x2gosession.png
iconvfrom=ISO8859-1
iconvto=UTF-8
key=
krbdelegation=false
krblogin=false
maxdim=false
multidisp=false
name=RelabMiniBricsCPA2
pack=16m-jpeg
print=true
...
```

- SSH јавни кључеви, различити кључеви за сваки лабораторијски модел (генерисани на подешавању лабораторијског модела коришћењем ssh-keygen)
  - id_rsa_weblabcpa2.txt
  - id_rsa_weblabcpa3.txt
  - id_rsa_weblabcpa4.txt
  - id_rsa_weblabcpa5.txt
  - id_rsa_weblabcpa.txt
- Windows batch датотеке за директан приступ лабораторијском моделу 1, 2, ..., 5
  - to_cpa.bat
  - to_cpa2.bat
  - to_cpa3.bat
  - to_cpa4.bat
  - to_cpa5.bat
- Linux batch датотеке за директан приступ лабораторијском моделу 1, 2, ..., 5
  - to_cpa.sh
  - to_cpa2.sh
  - to_cpa3.sh
  - to_cpa4.sh
  - to_cpa5.sh

Веза се иницира са командне линије / терминала: to_cpa.bat (или to_cpa2.bat …). Само је потребно да се унесе претходно постављена лозинка за лабораторијски модел при пријави, и Студент ће добити приступ рачунару који управља лабораторијски модел.

АУТОРИ

Ђорђе Сеничић, ***главни аутор***, Cognipix, Београд, Србија, djordje@cognipix.com
Luis de la Torre Cubillo, National University of Distance Education - UNED, Madrid, Spain, ldelatorre@dia.uned.es
Милан Матијевић, Универзитет у Крагујевцу, Србија, matijevic@kg.ac.rs
Марко Танасковић, Универзитет Сингидунум, mtanaskovic@singidunum.ac.rs