Raport științific si tehnic in extenso pentru proiectul *Canal securizat între dispozitivele I/O și unitatea de procesare pentru extinderea securității software (SABOTORE)*

Etapa IV – Dezvoltare, testare și validare prototipuri
L4.1 Documentație tehnică pentru cele trei prototipuri realizate
L4.2 Raportul de testare a prototipurilor
L4.3 Documentație de utilizare pentru fiecare prototip

Cuprins

1 Introducere

Noile medii de execuție de încredere (TEE – Trusted Execution Environment) integrate în procesoare (de exemplu, Intel Software Guard Extensions) permit izolarea aplicațiilor critice pentru securitate de restul software-ului care rulează pe sistem. Cu toate acestea, le lipsește suportul pentru I/O de încredere, cum ar fi tastatura sau afișajul. Acest lucru este ceea ce face ca acele tehnologii să nu fie considerate sigure în cazul aplicațiilor centrate pe utilizator. În acest sens am creat token-ul SABOTORE, un modul hardware practic care creează un canal securizat între orice dispozitiv USB HID (de exemplu, tastatură/mouse) și un TEE (de exemplu, Intel SGX) folosind doar autentificare și atestare locală.

Prezentul raport prezintă activitățile realizate în etapa 4, fiind realizat pe baza livrabilelor din cadrul acestei etape.

Obiective

Etapa curenta, etapa numărul 4 a avut doua obiective:

O4.1 Realizarea prototipurilor pentru cele trei scenarii de business

O4.2 Validarea prototipurilor realizate in mediul industrial

Activități

Principalele activități desfășurate în cadrul acestei etape au fost de dezvoltare, testare și validare pentru cele trei scenarii de business:

1. Sistem de autentificare a dispozitivelor de Intrare / Ieșire (Input/Ouput - I/O)
2. Printarea securizată direct din enclava SGX
3. Criptarea datelor stocate extern

Pentru îndeplinirea obiectivelor au fost realizate următoarele activități:

A4.1 Dezvoltarea și testarea sistemului de securizare a accesului la dispozitivul criptografic de păstrare a cheilor criptografice

A4.2 Dezvoltarea si testarea sistemului de securizare a imprimării fizice a documentelor electronice

A4.3 Dezvoltarea si testarea sistemului de acces la mediile periferice de stocare a datelor

A4.4 Validarea prototipurilor in condiții de utilizare reală

2 Documentație tehnică pentru cele trei prototipuri realizate

Scenariul 1 - Autentificare dispozitive I/O

SABOTORE este un modul hardware care este capabil să creeze o cale de comunicatie sigură între un dispozitiv USB și un mediu de execuție de încredere. În special, utilizează un Intel SGX ca TEE și o tastatură ca dispozitiv USB I/O. Proiectul pilot promite că acest strat suplimentar de securitate nu va afecta eficiența și viteza conexiunii. Acest modul funcționează transparent și nicio întârziere nu va fi notificată de către utilizatorul final.

Modulul hardware folosește standardul USB pentru a se conecta la computer și, de asemenea, se conectează la un dispozitiv periferic (o tastatură) folosind același standard USB. Soluția prezentată în această lucrare rezidă pe trei componente esențiale: un firmware care este instalat pe modulul hardware terț, o enclavă Intel SGX și alte drivere și aplicații care rulează pe sistemul de operare de bază.

Enclava Intel SGX este compusă din două părți: Device Provisioning Enclave (DPE), care este responsabilă pentru protocolul de schimb de chei și Application Enclave (AE), care va comunica în continuare cu modulul USB. Deci, DPE este factorul cheie pentru procesul de autentificare și AE pentru comunicarea prin calea securizată cu dispozitivul periferic.

Configurarea constă în crearea unui canal securizat între DPE și AE (cele două enclave): prima enclavă creează un raport, iar a doua primește raportul și își creează propriul raport și o cheie; apoi prima enclava primește datele finale și se face schimbul de chei. In schimbul de chei (cu Diffe-Hellman) se folosesc cheile specifice, cea hard-codata in hardware-ul token-ului SABOTORE si cea folosita de enclava, salvata in sistemul de fișiere al sistemului de operare. Următorul pas este inițializarea căii de încredere care este făcută de DPE. Acest pas se face prin verificarea autorității AE și apoi prin negocierea unei chei efemere cu modulul hardware. După aceea, cheia efemeră este schimbată cu AE și canalul securizat este creat și gata de

utilizare. Ca o privire de ansamblu: cele două enclave: AE și DPE comunică și se autentifică reciproc.

Pentru sistemele bazate pe Linux, exista o funcționalitate in care se pot bloca sau accepta dispozitive periferice USB ce sunt conectate la un calculator gazda. Utilizând aceasta metoda din interiorul enclavei SGX, putem controla astfel, ce dispozitive au voie sa se conecteze si ce dispozitive nu. De asemenea, se pot instaura politici de izolare, in care nu se mai accepta niciun tip de dispozitiv USB. În mod implicit, dispozitivele USB cu fir sunt autorizate pentru a se conecta. Gazdele USB wireless revoca autorizarea tuturor dispozitivelor noi conectate, fiind necesara o etapa de autentificare înainte de a le autoriza. Există o abordare similară pentru a permite sau a refuza anumite interfețe USB. Acest lucru permite blocarea doar a unui subset al unui dispozitiv USB.

În acest fel autentificarea unui dispozitiv USB se poate face doar prin intermediul token-ului SABOTORE si a canalului securizat pana la enclava de pe calculatorul folosit.

Scenariul 2 - Printare securizată

Tehnologia Intel SGX este folosită pentru a ne securiza driverul de sistemul de operare in care nu avem încredere. Driverul acesta este implementat pentru imprimanta specificata într-o enclavă. Acest tip de măsuri de protecție se pot aplica și asupra documentelor tipărite. Un alt tip de securitate aplicat la tipărire și fișierelor tipărite, cere utilizatorului să treacă printr-un proces de autorizare, folosind un PIN sau un smart-card, înainte de inceperea tiparirii documentului.

Desi sistemul de operare este adesea considerat a fi credibil, el nu este sigur și nu există nimic care să garanteze ca este sigur, deoarece codul sau sursă este uriaș.

Obiectivul a fost crearea unei modalități de comunicare între dispozitivul I/O (o imprimanta in cazul de fata) și o entitate de încredere care rulează ca o aplicație în spațiul utilizatorului (userspace). Scopul este de a crea o cale sigură între driver-ul imprimantei și imprimanta în sine, pentru a face procesul de imprimare mai sigur și în același timp reduce suprafața de atac. Astfel sunt folosite capabilitățile criptografie ale TEE împreuna cu cele ale token-ului extern SABOTORE pentru a atinge acest obiectiv de decriptare a datelor.

Microcontrolerul de pe token și enclava vor rula algoritmul Diffe-Hellman, astfel încât fiecare să aibă cheia de criptare/decriptare. Datele transmise prin sistemul de operare sunt criptate folosind AES128, astfel încât sistemul să nu poată înțelege conținutul informațiilor trimise.

Pe gazdă există două componente: un client și un server. Secțiunea de conversie a programului este rulată pe partea clientului, într-un TEE, astfel încât să fie protejat de posibilul sistem de operare rău intenționat. În plus, protocolul de schimb de chei și protocolul de criptare fac, de asemenea, parte din mediul de încredere. Toate aceste procese sunt rulate deasupra stratului de abstracție a platformei, în mediul de execuție de încredere. Procedura de autentificare, inclusiv schimbul de chei și criptarea sunt integrate cu proiectul TIO.

Documentul este convertit într-un fișier de tip PDL (PCL sau PostScript), este criptat și este trimis prin socket, către serverul care rulează în zona non-trusted. Serverul preia documentul, stabilește comunicarea prin USB către MCU și o trimite mai departe. În al doilea rând,

microcontrolerul sau platforma dongle USB primește documentul, îl descifrează și îl trimite la imprimantă.

Scenariul 3 - Criptarea datelor stocate extern

SABOTORE folosește un modul hardware personalizat cu o interfață gazdă USB pentru conectarea dispozitivelor terțe și un port USB separat pentru interacțiunea cu computerul compatibil Intel SGX. Astfel, dispozitivul acționează ca un firewall transparent, stabilind un canal securizat între enclavă și un dispozitiv utilizator care altfel nu este conștient, pentru schimbul de pachete USB. Când stabilim canalul securizat între o enclavă și modulul hardware TIO, trebuie să folosim un protocol de autentificare adecvat care să protejeze utilizatorul împotriva atacurilor de tip man-in-the-middle prin autentificarea reciprocă a părților. Platforma Intel SGX oferă o atestare de la distanță care poate fi utilizată pentru a verifica dacă o enclavă rulează în siguranță în mediul protejat al platformei. Atestarea la distanta nu este folosita in cazul nostru, fiind necesară conectarea la serverele Intel. Rezolvăm acest lucru introducând o condiție prealabilă de configurare unică: dispozitivul de încredere trebuie să fie asociat cu computerul utilizatorului. Acest lucru se realizează prin pornirea unui sistem de operare special, doar pentru citire (stocat în interiorul dispozitivului), care va inițializa enclava pentru prima dată și va schimba cheile necesare pentru autentificarea reciprocă în timpul utilizării normale a sistemului.

Firmware-ul de pe token-ul SABOTORE se ocupă de inițializarea hardware-ului și a interfețelor USB gazdă/dispozitiv, conform cerințelor aplicațiilor. A fost folosit cadrul STM32 Hardware Abstraction Layer și bibliotecile USB STM32 (gazdă și dispozitiv) pentru a ușura dezvoltarea programului. Token-ul acționează atât ca gazdă USB (fiind implementat un driver generic pentru perifericele HID care va captura și filtra rapoartele) cât și ca dispozitiv USB (pentru conectarea lui ca dongle la un computer).

Pentru a putea intelege transferul de date necesar schimbului si gestionarii de fisiere a fost necesara implementarea unei clase custom de Mass Storage: o clasă de stocare în masă care să conțină sistemul de operare bootabil doar cu permisiuni de citire utilizat pentru configurarea unică (poate stoca și alte drivere/programe instalabile, pentru ușurința implementării);

Pentru a scrie date pe mediul de stocare, presupunând ca SGX are deja in memorie datele decriptate ce urmează a fi scrise, este nevoie in primul rând de un canal securizat intre token

si enclava SGX. Cheia folosita pentru criptarea datelor este una compusa, jumătate aflându-se pe enclava, cealaltă jumătate fiind pe token. Schimbul de chei si negocierea unei chei comune de criptare/decriptare se face folosind algoritmul Diffie-Hellman. Având cheia comună corecta, datele sunt criptate in pe enclava si trimise pe canalul securizat, urmând a fi scrise pe mediul de stocare. Procesul invers (de citire) este similar, datele fiind transferate in enclava si apoi decriptate.

3 Raportul de testare a prototipurilor

Strategia de testare a fost realizata pe baza exemplelor din literatura de specialitate pentru testare si având in vedere cele mai bune practici in acest domeniu. Această strategie a fost mai departe adaptata și aplicata, pentru a se potrivi pe cazurile specifice SABOTORE.

A fost astfel realizat un model de testare. Rezultatele in urma execuției incluzând următoarele informații:

1. Numele testului și scenariul testului
2. Criterii de acceptare
3. Rezultate
4. Stare

Validarea fiecărei cerințe se realizează în cel puțin unul dintre următoarele moduri:

- Testare
- Inspecție
- Analiza datelor de performanță

Tipuri de teste

Categoriile următoare au fost aplicate pe fiecare scenariu in parte:

- **Testele de funcționare** au fost realizate pentru a testa cazurile in care toate condițiile necesare sunt îndeplinite și funcționalitatea scenariului poate fi îndeplinită.
- **Testele de blocare** au fost realizate pentru a garanta ca un transfer nu poate fi realizat daca unul dintre componente nu este prezent, astfel transferul fiind blocat sau negocierea unei conexiuni sa fie posibila.

Dintre testele realizate le reamintim pe următoarele:

- Autentificare pentru un dispozitiv, cu enclava si cu token
- Autentificare pentru un dispozitiv, fără enclava si fără token
- Autentificare pentru un dispozitiv, cu enclava, dar fără token
- Autentificare pentru un dispozitiv, fără enclava, dar cu token
- Printare document necriptat, cu token si cu enclava

- Printare document necriptat, fără token si fără enclava
- Printare document criptat, cu token si enclava
- Printare document criptat, fără token sau fără enclava
- Citire date de pe dispozitiv extern, cu token si cu enclava
- Scriere date pe dispozitiv extern, cu token si cu enclava
- Citire date de pe dispozitiv extern, cu token si fără enclava
- Citire date de pe dispozitiv extern, fără token, dar cu enclava

Șablon de test

Acesta este șablonul folosit pentru a descrie fiecare test in parte:

Nume test: Test scenariu 1
Număr scenariu: S1
Criteriu de trecere: Realizare transfer de date
Pași urmați/ Rezultate: 1. **Pas urmat 1** 2. **Pas urmat 2** 3. **etc**
Status: TRECUT/PICAT

Validare

Tehnologia creată in proiect a fost validată în mediul industrial, cu utilizatori reali din rândul utilizatorilor în cadrul certSIGN si UPB.

In luna decembrie se va organiza o intalnire de lucru cu utilizatori reali participanti la proiect dar si din afara acestuia, in cadrul careia se va urmari, pe de o parte diseminarea rezultatelor proiectului, iar pe de alta parte testarea si validarea sistemului realizat impreuna cu utilizatori noi.

Data fiind situatia pandemica actuala si restrictiile aplicate, intalnirea de lucru va avea loc online; o parte din utilizatori vor avea acces la dispozitive periferice (token SABOTORE,

imprimanta, etc), dispozitive ce vor fi folosite in procesul de validare. Personalizarea enclavei de va realiza pe laptopurile de lucru sau personale ale utilizatorilor si vor avea preinstalate sistemul de operare Linux.

Trebuie menționat că pentru fiecare scenariu am folosit protocoale standard, nemodificate, dispozitivul SABOTORE putând fii integrat ușor în orice mediu existent, astfel:

1. Pentru scenariul în care datele criptate sunt stocate pe dispozitiv extern, tokenul SABOTORE a fost actualizat pentru a funcționa cu protocol USB 2.0. Există totuși o constrângere dată de proprietățile microcontroller-ului folosit, și anume acesta are o singură interfață USB2.0 și una USB2.1. Folosind tokenul SABOTORE se poate accesa orice dispozitiv de tip USB și se pot stoca datele, criptate în prealabil de către enclava SGX. La testele pentru scenariul de stocare pe Mass Storage au fost folosite mai multe brand-uri de memorii flash USB de la Kingston, Corsair si Samsung.
2. Pentru scenariul de printare securizată am folosit protocolul PCL, protocolul standard pentru imprimare. Majoritatea imprimantelor din zilele de astăzi oferă suport pentru acest protocol. A fost folosita o imprimantă Samsung pentru a face unele teste intermediare.
3. Pentru scenariul de securizare a dispozitivelor de intrare/ieșire, validarea a fost realizată folosind un kernel nemodificat de Linux. Acesta a fost configurat astfel încât să nu accepte decât tokenul SABOTORE prin USB. Validarea a fost realizată pe mai multe sisteme de operare ce folosesc un kernel de Linux (Arch, Ubuntu și Debian).

4 Documentație de utilizare pentru fiecare prototip

Testarea a fost făcută pe o configurație preexistenta si necesara pentru funcționarea corecta a soluției cu SABOTORE. Aceasta configurație presupune blocarea implicita din kernel a tuturor dispozitivelor periferice de tip USB, cu excepția token-ului SABOTORE, cu care se va realiza autentificarea acestora. Pentru a seta canalul securizat este necesara rularea enclavei specifice, care este pereche a cheii de pe token.

Acesta este un exemplu de cum se poate deautoriza un dispozitiv conectat (in cazul de fata mouse si tastatura) pe un calculator cu Linux:

Output dmesg

```
...
usb 1-1: new low-speed USB device number 5 using xhci_hcd
...
input: PixArt HP USB Optical Mouse as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.0/0003:03F0:134A.0002/input/input22
...
```

Urmând sa blocam acest dispozitiv:

```
# echo 0 > /sys/bus/usb/devices/usb1/1-1/1-1:1.0/authorized
```

In urma acestei comenzi mouse-ul a fost deautorizat si input-ul generat de catre acesta nu a mai fost primit de catre calculator.

In aceasta maniera se pot deautoriza in mod implicit toate dispozitivele USB conectate.

```
for host in /sys/bus/usb/devices/usb*
  do
    echo 0 > $host/authorized_default
  done
```

Acest script ar trebui rulat odata cu etapa de boot la fiecare pornire (in rc.local spre exemplu sau alta solutie), pentru a asigura ca niciun dispozitiv nu se poate conecta inainte.

Astfel se poate implementa o politica de verificare a fiecarui dispozitiv conectat:

```
if device_is_my_type $DEV
 then
  echo 1 > $device_path/authorized
 done
```

In acest fel putem salva id-ul token-ului într-un fișier local, doar cu drepturi de read, pentru a putea interoga acest id

In urma acestor pași ar trebui sa avem o politica funcțională de acceptare a dispozitivelor. Pașii de configurare ramași in acest punct fiind instalarea si rularea enclavei pentru a putea realiza canalul securizat atunci când se introduce un dispozitiv cu token.

Procesul de imprimare constă de obicei în următoarele: a avea un document de tipărit pe sistemul de fișiere al sistemului de operare, fișierul este convertit într-un format PDL și în cele din urmă este transferat prin protocolul USB către imprimantă. După conexiunea cu dispozitivul USB este stabilită, imprimanta a fost identificată și configurată, documentul este trimis în serie, de obicei în vrac către dispozitivul de imprimare.

Criptarea datelor pe un dispozitiv de stocare extern (ex. USB flash, HDD extern) necesită următoarele componente: un calculator cu SGX, token-ul SABOTORE si dispozitivul de stocare.

In acest fel daca un atacator face rost de token si mediul de stocare, acesta nu poate citi acele date, in lipsa cheii de pe enclava. Același lucru este valabil si in cazul in care se obține acces la un calculator cu o enclava valida, dar fără token.

5 Diseminarea rezultatelor obținute

O data cu finalizarea celui mai important pas in conceperea soluției, si anume Arhitectura hardware si software, pentru diseminarea rezultatelor am completat site-ul proiectului https://sabotore.ro unde am publicat rezultatele obținute pana in prezent. Aici putem găsi, pe lângă aspectele informative ale proiectului, precum partenerii ce alcătuiesc consorțiul, sau planul de execuție a proiectului in cinci etape, si aspectele tehnice ale proiectului, precum arhitectura conceputa in etapa curentă.

Totodată, pe pagina web a certSIGN am completat secțiunea „Proiecte” (https://www.certsign.ro/ro/despre-noi/cercetare-si-inovare/proiecte/) cu câteva aspecte importante referitoare la proiectul nostru. Aceasta adăugare este importanta pentru etapa de diseminare a rezultatelor, deoarece site-ul web al partenerului coordonator este vizitat zilnic de mulți utilizatori, având, conform ultimelor statistici Google Analytics, 3.4 milioane de vizitatori dintre care 1,8 milioane, unici de la inceputul anului 2021, pana la data 10 decembrie.

Pornind de la livrabilele dezvoltate pentru etapa 1, "L1.1 Raport de cercetare privind tehnologiile și implementările mecanismelor tehnice de securizare a transferului de date intre sistemul de operare si dispozitivele periferice” , echipa UPB a trimis un articol spre revizie la jurnalul UPB (Seria C Inginerie Electrică și Știința Calculatoarelor - https://www.scientificbulletin.upb.ro/) cu denumirea “Systematization of Trusted I/O solutions for Isolated Execution Environments”.

6 Concluzii

Etapa 4 a fost etapa în care, pornind de la cerințele de business dezvoltate în etapa 2 și arhitecturile hardware și software dezolvate în etapa 3, s-a realizat îmbunătățirea prototipului pentru a ajunge la nivelul de TRL dorit. Pentru aceasta s-a început cu dezvoltarea codului existent (de la care a pornit proiectul actual) și s-a obținut printarea securizată a unui document direct din enclava SGX. Mai mult, s-au identificat mecanismele puse la dispoziție de un sistem de operare pentru a limita accesul la porturile USB doar dispozitivelor SABOTORE (prin intermediul canalului securizat USB-enclavă SGX). Ultima componentă dezvoltată și

testată a fost aceea de criptare a unor documente, criptarea se realizează în enclavă, cheia folosită este stocată pe sistemul de calcul fiind protejată sub forma unei anvelope de către tokenul SABOTORE, iar datele sunt scrise pe disc, în mod transparent, de către sistemul de operare (prin intermediul driverelor deja existente). Prin intermediul activităților evidențiate succint în prezentul raport, echipa a atins toate obiectivele propuse în cadrul acestei etape.