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

Etapa II – Elaborare cazuri de utilizare si cerințe tehnice.

L2.2 - Cerințele tehnice de dezvoltare a componentelor software si hardware

Cuprins

1 Introducere

Protejarea datelor personale a fost mereu una dintre cele mai importante componente atunci când vorbim de securitate în mediul online. Spre exemplu, conceptul de virtualizare a fost introdus nu doar pentru a putea utiliza simultan un dispozitiv de calcul, dar și pentru a putea separa datele fiecărui utilizator. Astăzi, într-o lume interconectată, securitatea datelor a devenit chiar și mai importantă prin utilizarea conturilor în tot mai multe platforme online. Proiectul de față își propună să aducă o îmbunătățire a modului în care sunt folosite datele confidențiale din cadrul unei companii, cum ar fi un fișier care conține unul dintre contractele foarte importante ale companiei.

Majoritatea sistemelor de securitate au o bază de încredere („root of trust") în software, spre exemplu unul dintre cele mai folosite protocoale de securitate, Transport Layer Security (TLS), se folosește de existența în sistemele de operare a unei chei publice (am simplificat foarte mult pentru o explicare mai facilă). Această cheie publică va fi folosită ulterior la tot ce înseamnă o comunicare securizată în Internet, iar compromiterea ei duce la compromiterea întregii securități.

Principala motivație pentru care securitatea are ca bază unelte software este dată de ușurința cu care un produs software se dezvoltă față de un produs hardware. Spre exemplu, apariția unui nou protocol criptografic este prima dată implementată în software, și apoi în hardware, unde evident volumul de date care poate fi procesat este mai mare.

Proiectul SABOTORE vine în contextul în care majoritatea calculatoarelor sunt echipate cu echipamente hardware dedicate ce oferă Execuție Protejată („Trusted Execution Environment - TEE), Intel furnizând începând cu anul 2014 procesoare cu suport Intel Software Guard Extensions (SGX) iar procesoarele AMD oferă din 2016 Secure Encrypted Virtualization (SEV). Aceste soluții hardware oferă garanția execuției unui program în contextul unui sistem de operare malițios, putând fi folosite ca baza de încredere.

Mai mult, în domeniul Internet of Things (IoT) se poate observa o creștere a numărului de echipamente disponibile, estimările actuale arată că până în anul 2025 vom avea peste 75 de miliarde de astfel de echipamente conectate la Internet. Odată cu această explozie a echipamentelor, costurile de fabricare au scăzut, fiind posibilă construirea de hardware particularizat cu o ușurință mai mare.

SABOTORE își propune să se folosească de aceste noi tehnologii pentru a permite o comunicare sigură. Echipa Universității Politehnica din București împreună cu cei de la CertSign au dezvoltat trei posibile scenarii în care tehnologiile prezentate mai sus pot oferi o securitate ridicată:

1. Pentru a proteja accesul la dispozitivele de intrare/ieșire în mediile de lucru unde acest acces trebuie controlat. Spre exemplu, placa de rețea va trebui să folosească un secret stocat în TEE pentru a se autentifica la rețea.
2. Pentru a folosi la distanță token-ul SABOTORE. Mai concret, am putea pune un astfel de la intrarea într-o imprimantă sau într-un video proiector și să permitem accesul la aceste dispozitive doar de la dispozitive autorizate și autentificate.

3. Pentru a cripta datele de pe dispozitive, locale sau la distanță. Spre exemplu, un stick USB poate fi criptat cu cheia care rezidă în TEE, iar decriptarea se poate face doar folosind același calculator (cu migrare facilă folosind token-ul hardware).

Etapele principale în cadrul proiectului sunt:

1. Studii de piață interne și internaționale, privind securitatea transferului de date (I/O) între un sistem de calcul și sistemele periferice acestuia și posibilitatea folosirii platformelor de tip Intel SGX
2. Elaborare cazuri de utilizare și cerințe tehnice
3. Arhitectura de referință și etică
4. Dezvoltare, testare și validare prototipuri
5. Transferul tehnologic al rezultatelor de dezvoltare experimentală și diseminarea rezultatelor

În prezentul raport ne propunem să arătăm care sunt principalele mecanisme care ar trebui implementate in cele 3 scenarii propuse, mecanisme necesare atât pentru buna funcționare cat si pentru asigurarea securitatea.

2 Descrierea etapei și a activităților

Obiectivele acestei etape sunt:

1. Identificarea și stabilirea tuturor componentelor din cele 3 scenarii care vor fi implementate
2. Studiu asupra componentelor hardware ce vor compune dongle-ul SABOTORE
3. Identificarea tuturor resurselor existente (mai ales externe) ce vor fi integrate în proiect

Cele 5 activități din Etapa II descrise in cadrul acestui raport sunt:

1. A2.1 Elaborare business-case-uri pentru implementarea unui sistem sigur de acces la dispozitivele de stocare a cheilor criptografice.
2. A2.2 Elaborare business-case-uri pentru implementarea unui sistem sigur de tipărire a documentelor electronice.
3. A2.3 Elaborare business-case-uri pentru implementarea unui sistem sigur de acces la mediile periferice de stocare a datelor.
4. A2.4 Elaborare cerințe tehnice pentru implementarea transferului securizat de date intre unitatea centrala de procesare si dispozitivele periferice.
5. A2.5 Elaborare cerințe tehnice pentru implementarea sistemului securizat de stocare si transfer de date folosind enclava SGX.

Au fost obținute următoarele livrabile:

1. L2.2 Cerințele tehnice de dezvoltare a componentelor software si hardware

3 Cerințe tehnice pentru implementarea transferului securizat de date intre unitatea centrala de procesare si dispozitivele periferice.

Din punct de vedere al cerințelor tehnice, am tratat implementarea transferului securizat de date intre unitatea centrala de procesare si dispozitivele periferice atât pentru a putea oferi un grad ridicat de utilizabilitate si integrare in cat mai multe medii posibile, dar si din punct de vedere al

securității. Vom prezenta in continuarea specificațiile tehnice necesare astfel încât dispozitivul SABOTORE sa poată atinge nivelul TRL dorit. De menționat ca cerințele tehnice din aceasta secțiune sunt aplicabile atât scenariului 1 (de securizare a dispozitivelor intrare/ieșire atașate calculatorului), cat si scenariului 2 (de securizare a accesului la dispozitive aflate la distanta precum o imprimantă).

Din punct de vedere al procesării informațiilor, in acest scenariu datele se vor aflat atât in procesare ("data at execution") cat si in transfer ("data in transit"). Obiectivele de securitate care trebuie atinse vor fi tratate separat pentru fiecare dintre cele doua stări.

Cerințe tehnice necesare pentru oferirea unui grad de utilizabilitate:

1. Software-ul realizat trebuie sa fie independent si sa nu necesite modificarea componentelor deja existente într-un calculator (de exemplu sistemul de operare).
2. Software-ul creat trebuie validat printr-o serie de teste in diferite contexte de utilizare.
3. Software-ul va oferi o interfață (tip bibliotecă) cu un API ce va putea activa/dezactiva token-ul SABOTORE și stabili un canal de comunicație confidențial autentificat cu acesta.
4. Software-ul să aibe o arhitectură modulară (e.g., să se refolosească codul cât mai mult posibil), facilitând astfel integrarea de noi aplicații și dispozitive periferice;
5. Este necesar un mecanism de auto-activare/dezactivare a securizării transferului (de exemplu, introducerea unui token SABOTORE in calculator (sau activarea unui buton hardware al acestuia) ar trebui sa activeze automat comunicarea securizata; respectiv îndepărtarea acestuia să dezactiveze comunicarea securizata si să permită portului de intrare sa fie folosit normal).
6. Software-ul care rulează pe calculator sa nu aducă un overhead foarte mare sistemului de calcul.
7. Token-ul SABOTORE sa poată fi folosit fără un overhead foarte mare la primirea datelor (de exemplu, securizarea datelor introduse de la tastatura prin intermediul token-ului SABOTORE sa nu duca la o întârziere considerabilă datorită procesării datelor pe token).
8. Token-ul să aibă dimensiuni și greutate reduse (e.g., format de stick USB).
9. Utilizatorul sa învețe ușor sa folosească acest dispozitiv (de exemplu, să nu necesite dezasamblarea calculatorului sau conectarea a prea multe cabluri).
10. Dispozitivul trebuie sa afișeze nivelul de securitate oferit (de exemplu daca nu s-a putut realiza un canal de securitate, utilizatorul trebuie sa poată observa acest lucru vizual, direct pe token).
11. Dispozitivul trebuie să aibă un grad de toleranta la erori (atât din punct de vedere electronic, cât și software - să nu prezinte defecte pe timpul unei utilizări îndelungate).
12. În caz de defect permanent, dispozitivul să fie ușor înlocuibil (e..g, folosirea unui sistem de gestiune / redundanță a cheilor) pentru a evita pierderile de date.

Cerințele tehnice de securizare a datelor atunci când sunt procesate pe calculator:

Procesarea datelor trebuie realizata **doar** într-un mediu de execuție protejat. Pentru aceasta trebuie parcurs un schimb de chei între tokenul SABOTORE și o enclavă Intel SGX.

1. Interfața de comunicare intre componenta software protejată (din interior enclavei SGX) și componenta ce rulează pe sistemul de operare (considerat nesigur) sa nu ofere accesul la datele prelucrate.
2. Să nu accepte date neautentificate spre procesare (la intrare).
3. Să ofere o metoda de autentificare pe baza de chei asimetrice generate de catre token-ul SABOTORE.
4. Să ofere o metoda de autentificare folosind o semnătura digitala electronica validă.
5. Atacurile hardware sau de tip side-channel sau bug-uri de securitate ale arhitecturii de procesor (e.g., SPECTRE) nu sunt luate in considerare pentru acest prototip.

Cerințele tehnice de securizare a datelor atunci când sunt procesate pe token-ul SABOTORE:

1. Atacurile hardware sau de tip side-channel nu sunt luate in considerare pentru acest prototip.
2. Să nu fie procesate date care nu pot fi autentificate.
3. Să ofere o interfață prin care software-ul instalat pe token sa poată fi actualizat într-un mod sigur.
4. Să ofere o metoda de autentificare folosind o semnătura digitala electronica validă.
5. Overhead-ul adăugat prin procesarea datelor sa fie sub 20%.

Cerințele tehnice de securizare a datelor când sunt transferate intre calculator si token-ul SABOTORE:

1. Trebuie sa se garanteze confidențialitatea datelor de intrare/ieșire prin folosirea unui algoritm de criptare simetric. Recomandarea este folosirea AES 128 biți.
2. Trebuie sa se garanteze integritatea datelor de intrare/ieșire prin folosirea unui algoritm de tip HMAC. Algoritmul de hashing recomandat este SHA2.
3. Trebuie sa se ofere protecția împotriva unui atac de tip replay prin adăugarea unui număr de secvență fiecărui pachet transmis intre token si calculator. Important ca numărul de secvență sa fie incrementat si sa nu se poată repeta.
4. Trebuie sa se garanteze autentificarea dispozitivului SABOTORE de către calculator. Pentru acest lucru recomandam ca la instalarea software-ului pe calculator sa se salveze într-un mod protejat si cheia publica a dispozitivului. Aceasta va fi ulterior folosita in procesul de autentificare.
5. Să se garanteze “perfect forward secrecy” prin schimbarea cheii simetrice de criptare la fiecare <*x*> minute (în funcție de cerințele aplicației); se recomandă folosirea unui protocol Diffie-Hellman autentificat.

Cerințele tehnice de funcționalitate:

1. Este necesară o componenta de tip driver pentru configurarea token-ului SABOTORE.
2. Este necesară o asociere / preconfigurare cu sistemul gazdă în prealabil înainte de prima folosire (pentru schimbul de chei de autentificare).
3. Token-ul SABOTORE trebuie sa funcționeze folosind interfața USB 2.0, opțional USB 3.0.

4. Token-ul SABOTORE trebuie sa funcționeze pe sistemul de operare Linux, optional se va realiza un driver si pentru Windows.
5. Software-ul care rulează in mod protejat trebuie sa ofere o funcționalitate de debugging.
6. Atunci când este dezactivat, token-ul SABOTORE să nu intervină cu procesul normal de funcționare al dispozitivelor de intrare/ieșire (passthrough).
7. Token-ul SABOTORE trebuie sa aibă o metoda de comunicare directa cu utilizatorul, propunem utilizarea unui LED RGB și a unei codificări în culori: verde – comunicarea securizată cu aplicația este activa; roșu – comunicarea dintre token si calculator este activă dar nu este activată securizarea datelor (perifericele conectate funcționează în modul neautentificat); galben – exista o problema de comunicare intre token si aplicația software.

4 Cerințe tehnice pentru implementarea sistemului securizat de stocare si transfer de date folosind enclava SGX.

In aceasta secțiune vom specifica cerințele tehnice necesare pentru crearea token-ului SABOTORE folosit in scenariul 3 (stocarea datelor criptate pe un dispozitiv extern). De menționat ca deși unele dispozitive de stocare externe oferă protejarea datelor pe baza de parola, acest scenariul folosește capabilitățile procesoarelor moderne pentru a realiza protecția datelor folosind un sistem de chei publice private.

Similar cu cerințele tehnice dezvoltate pentru scenariile 1 si 2, din punct de vedere al procesării informațiilor, in acest scenariu datele se vor aflat atât in procesare (“data at execution”), date in tranzit (“data in transit”) cat si stocate (“data at rest”). Obiectivele de securitate care trebuie atinse vor fi tratate separat pentru fiecare dintre cele trei stări.

Cerințe tehnice necesare pentru oferirea unui grad de utilizabilitate, in plus fata de cele definite pentru scenariile 1 si 2:

1. Utilizatorul sa poată recupera datele salvate pe dispozitivul extern de stocare.
2. Utilizatorul sa poată migra ușor la un calculator nou (prin intermediul token-ului).

Cerințele tehnice de securizare a datelor atunci când sunt procesate pe calculator sunt similare cu cele definite in secțiunea “Cerințe tehnice pentru implementarea transferului securizat de date intre unitatea centrala de procesare si dispozitivele periferice”. Similar pentru datele procesate pe token-ul SABOTORE dar si pentru datele transferate intre calculator si token.

Cerințele tehnice de securizare a datelor atunci când sunt stocate pe dispozitive externe:

1. Datele stocate pe dispozitive externe sa fie criptate pentru a oferi confidențialitate. Recomandam algoritmul AES128.
2. Datele trebuie sa conțină un HMAC pentru a oferi integritate. Recomandam folosirea algoritmului SHA2.
3. Cheia de decriptare a datelor să NU fie stocată în clar pe același dispozitiv extern ca și datele.
4. Trebuie sa existe o semnătură digitala care sa autentifice utilizatorul care a criptat datele.

5. Autentificarea datelor sa poate fi realizata atât prin parola cat si prin folosirea unei semnături digitale ale token-ului.