



Project VoidWarnities

16.11.2021

Vatafu Vladut

Nr4, Str Garii
Becicherecu Mic, jud.Timis

Overview

Acest proiect are ca scop principal, realizarea unui videoclip asemeni celui prezent în link-ul anotat mai jos [0]Link-uri utile . Acesta inițiativa are ca secundar a atrage cat mai multe persoane de vârste tinere și a promova proiecte de tip STEM, orientate pe categoria securitate cibernetica , subcategoria Hardware. O problema tipică identificată este mentalitatea greșită cum ca ar fi nevoie de studii superioare precum Bsc,Msc,Phd pentru a pătrunde în tainele atacurilor de tip "Side-Channel" , prezente atât la nivel de hardware cât și la nivel de software.

Goals

1. Identificarea,procurarea și acumularea cunoștințelor necesare pentru realizarea acestui videoclip informativ
2. Procurarea echipamentului necesar.
3. Prezentarea prototipurilor specifice fiecărui atac împarte (din engl. "Demo")
4. Întocmirea unui "scenariu" (din engl. "Script") necesar realizarii scurtmetrajului online
5. Stabilirea unei perioade de timp pentru a realiza acesta proiecție online

Specifications

În aceasta pelicula se vor realiza următoarele atacuri cibernetice de tip nr. "Side-Channel":

- Vcc Glitching pentru introducerea audiența în aceste tipuri de atac. Demonstrația consta în următoarele procedee:
 - Glitch-uirea(din engl."Glitch" sin."Defectiune") computerului "Raspberry Pi 3" model b+ în timp de acesta rulează următorul cod [1](Vezi antet capitol Link-uri utile). Acesta secvența de cod are ca scop calcularea(din engl."Compute") unei variabile counter de timp de 100000000 de iterații. In momentul in care atacul se ve executa asupra computerului Raspberry Pi, sursa din care este alimentat computerului primește un sub impuls electronic care va perturba(corupe) valoarea nr de iterații .
- Vcc Glitching pentru a demonstra "crashu-ul"(oprirea fortate neautorizata) asupra întregului sistem de calcul a Raspberry pi.

- Clock Glitching pentru a recupera exponentul privat d dintr-un algoritm ce calculeaza o criptare de baza algoritmului RSA , ulterior decriptandu mesajele criptate

Milestones

I. Identificarea,procurarea și acumularea cunoștințelor necesare pentru realizarea acestui videoclip informativ

In aceasta etapa, realizatorul scurtmetrajului și anume pr.Vatafu Vladut identifica, prioritizeaza, și acumuleaza cunoștințele necesare pentru a realiza acest videoclip.

Acesta și-a luat prilejul de a realiza acest procedeu deja astfel incat a întocmit o listă cu resursele necesare de studiu:

-<https://wiki.newae.com/>

-<https://www.youtube.com/watch?v=dVkCNiM0PL8>

-<https://github.com/newaetech/chipwhisperer-jupyter/tree/master/courses>

-https://github.com/newaetech/chipwhisperer-jupyter/blob/master/archive/Fault_5-RSA_Fault_Attack.ipynb

II. Procurarea echipamentului necesar

-Placa necesara pentru a injecta volatjul necesar NAE-CW1173-2PART

-Pogo-Pin P25-0126

-CON-SMA-EDGE-SRP-RF / Coaxial Connector, SMA RP Coaxial, Straight Jack, Solder, 50 ohm, Beryllium Copper

-Panavise Mini PCB Vice

Suma totala este de **1.596,43 RON** incluzand și transportul

III. Prezentarea atacului prototip (din engl. "Demo")

După îndeplinirea sarcinilor corespunzătoare primului obiectiv , persoana în cauza și anume pr.Vatafu Vladut v-a execute prototipurile specifice atacurilor menționate în primul capitol în fața pr. Insert Name care v-a asista prin intermediul mediul de comunicare virtual acest lucru realizandu-se prin aplicația Discord pentru a confirma ca toate aranjamentele necesare au fost luate pentru a efectua atacurile menționate anterior, in paragraful de mai sus.

IV. Întocmirea unui "scenariu" (din engl. "Script") necesar realizarii scurtmetrajului online

În cazul în care toate condițiile menționate mai sus(respectiv 1,3) au fost îndeplinite și toată aparatura a fost achizitionata, subsemnatul Vatafu Vladut are a vorbii cu subsemnatul Insert name despre cum v-a decurge scurtmetrajul

V. Stabilirea unei perioade de timp pentru a realiza acesta proiectie online

După ce toate îndatoririle menționate prezentate au fost îndeplinite, se va discuta cu subsemnatul Insert Name pentru a concluziona și a stabili efectuaarea scurtmetrajului și timpului necesar pentru realizarea acestuia

Antet

Resurse folosite la întocmirea acestui document

Link-uri utile:

[0]<https://www.youtube.com/watch?v=dVkCNiM0PL8>

[1]<https://github.com/SpiralBLOCK/Project-VoidWarnities/blob/main/hack.c>