ATLAS Kobold

Platformă online pentru analiza binarelor

Telefoanele mobile moderne sunt dispozitive puternice care rulează sisteme de operare complete. Funcțiile lor sunt îmbunătățite cu aplicații bogate, localizate de obicei într-un magazin online, ușor de instalat și de utilizat.

Un set bogat de aplicații oferă o funcționalitate extinsă pentru utilizator, dar crește, în același timp, probabilitatea riscurilor de securitate, cum ar fi scurgeri de date private, pierderi de bani sau daune de reputație.

Sistemele de operare moderne mobile adaugă niveluri de securitate pentru a reduce riscurile. Kobold oferă dezvoltatorilor și furnizorilor de soluții software un mijloc de a evalua securitatea produselor lor.

Kobold

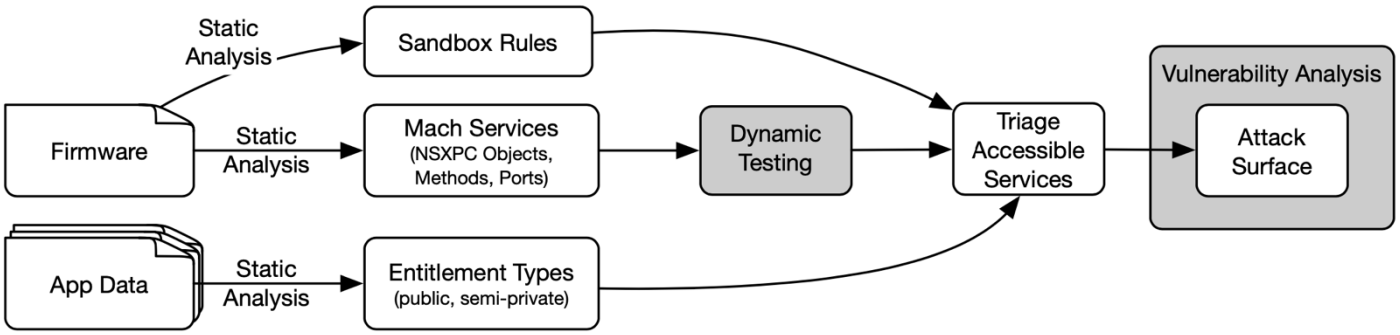
Kobold este un framework pentru studierea defectelor în serviciile din Apple iOS. Kobold este software open source într-un ecosistem de soluții pentru evaluarea securității Apple iOS. Preferința pentru Apple iOS este motivată de numărul relativ redus de cercetători implicați în iOS, de cerința de analiză și reversing (majoritatea codului este proprietar) și de caracteristicile de securitate prezentate de Apple pentru iOS.

Kobold este folosit pentru a investiga interfața de comunire inter-proces din Apple iOS: NSXPC.

Caracteristicile ATLAS Kobold

- Apple iOS
- testează IPC (NSXPC)
- tehnici de fuzzing
- analiză statică + dinamică
- identifică defecte în servicii de sistem

https://github.com/malus-security/kobold



Funcționare Kobold

Kobold folosește două informații cheie. În primul rând, interfețele IPC standardizate (de exemplu, NSXPC) conțin tipare previzibile în cod compilat, care pot fi identificate prin analiză statică. În al doilea rând, mesajele de eroare returnate prin încercări neautorizate de acces la serviciile IPC pot oferi un model al politicii de control de acces IPC iOS. Folosind aceste informații, Kobold oferă o analiză statică a programului binar, bazându-se pe un model pentru a enumera interfețele NSXPC și apoi utilizează în mod dinamic sondarea sistematică pentru a extrage o aproximație a politicii de control de acces codată de verificări condiționale în cadrul unui serviciu dat.

Kobold abordează provocările în a determina care metode NSXPC sensibile la securitate și confidențialitate sunt accesibile aplicațiilor terțe printr-o combinație de analiză statică și testare dinamică, analiza statică a lui Kobold ajută la enumerarea surplusului de atac, în timp ce analiza dinamică permite unui analist să trieze care servici NSXPC pot conține vulnerabilități.

Kobold este împărțit în trei componente. În primul rând, efectuează o anchetă a drepturilor disponibile pentru cererile terților. În al doilea rând, enumeră serviciile NSXPC accesibile aplicațiilor terțe. În al treilea rând, evaluăm sensibilitatea la securitate a serviciilor accesibile NSXPC pentru a evidenția serviciile care ar putea să permită atacuri de deputați confuzi.

Prima și a doua sarcină sunt automatizate. Am dezvoltat scripturi și instrumente integrate existente pentru extragerea drepturilor de aplicare și enumerarea serviciilor NSXPC. A treia sarcină folosește analiza fuzzing și manuală pentru a investiga metodele de servicii NSXPC care sunt accesibile și sensibile la securitate.

Kobold funcționează pe Apple iOS 9, 10 și 11. A dus la identificarea a 3 CVE-uri de către Apple.

Despre ATLAS

Proiectul "Hub inovativ pentru tehnologii avansate de securitate cibernetică (ATLAS)" își propune îmbunătățirea performanțelor de cercetare și de colaborare în domeniul securității cibernetice, adresând teme de mare interes: securitatea aplicațiilor și sistemelor de operare, securitatea IoT și cloud. Proiectul ATLAS este finanțat printr-un grant acordat de Ministerul Cercetării și Inovării din România, CCCDI - UEFISCDI, proiect nr. PN-III-P1-1.2-PCCDI-2017-0272, în cadrul PNCDI III.