BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024
http://excel.fit.vutbr.cz

Platforma pre automatizované vytváranie odtlačkov mobilných aplikácií

Kristián Kičinka

Abstrakt

Práca je zameraná na popis vývoja nástroja umožňujúceho automatizovanú tvorbu odtlačkov mobilných aplikácií, na základe odtlačkov TLS. Popisuje návrh jednotlivých modulov, na ktorých je založený proces generovania. Venuje sa problematike automatizovaného sťahovania súborov APK android aplikácií, popisuje podporované odtlačky TLS, z ktorých sú vytvárané odtlačky mobilných aplikácií. Venuje sa téme automatizácie inštalácie a spúšťania mobilných aplikácií, na virtuálnych zariadeniach, ako aj procesu analýzy sieťovej komunikácie daných aplikácií. V neposlednom rade rozoberá testovanie prípadu identifikácie mobilných aplikácií na základe vytvorených odtlačkov.

xkicin02@vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Úvod

Motiváciou vytvorenia práce bola snaha automatizovať proces vytvárania odtlačkov mobilných aplikácií a vytvoriť centrálnu databázu odtlačkov. Automatizovanie procesu by prispelo k zjednodušeniu práce správcov sietí, ako aj k zefektívneniu procesu identifikácie mobilných aplikácií. Jedným z ďalších podnetov vytvorenia práce bola možnosť analýzy malvérových aplikácií pomocou odtlačkov TLS.

Práca je zameraná na automatizovanie procesu vytvárania odtlačkov mobilných aplikácií založených na odtlačkoch spojení TLS, kombináciách týchto odtlačkov, prípadne na spojení daných odtlačkov s hodnotou SNI. V rámci procesu generovania odtlačkov je riešené získavanie súborov APK, potrebných pre zahájenie generovania, automatická inštalácia a spúšťanie aplikácií na virtuálnom zariadení, ako aj analýza sieťovej komunikácie, generovanie odtlačkov TLS a samotné vkladanie vytvorených odtlačkov do databázy.

Existujúcim riešením daného problému je vykonávanie procesu generovania odtlačkov mobilných aplikácií manuálne. V takomto prípade je potrebné manuálne vytvoriť a spustiť Android emulátor, manuálne inštalovať a spúšťať aplikácie a monitorovať ich komunikáciu. V poslednom kroku by používateľ musel analyzovať zachytenú komunikáciu, vytvoriť odtlačky TLS a spracovať ich do odtlačkov mobilných aplikácií.

Vytvorená platforma poskytuje riešenie daného problému, umožňuje automatizované vytváranie odtlačkov mobilných aplikácií na základe zadaných vstupov od používateľa. Jednou z ďalších výhod je možnosť spracovávania viacerých požiadaviek používateľov súčasne, čo urýchľuje proces generovania.

Vytvorený systém podporuje viaceré typy odtlačkov spojení TLS, medzi ktorými sú zaradené odtlačky `JA4`, `JA4S` a `JA4X`. Ide o relatívne nový typ odtlačkov vytvorený organizáciou **Floxio** v septembri roku 2023, s cieľom zlepšenia presnosti detekcie a v prípade odtlačkov JA4X s cieľom detekcie škodlivého softvéru[1].

2. Automatizované vytváranie odtlačkov

Automatizované vytváranie odtlačkov mobilných aplikácií je realizované prostredníctvom niekoľkých samostatných modulov, medzi ktoré patrí modul získavania súborov APK 2.2, modul inštalácie a spúšťania 2.3, modul analýzy komunikácie 2.4 a modulu zabezpečujúceho vytváranie odtlačkov 2.5. Na obrázku obrázok 1 je zobrazený celkový návrh vytvorenej platformy. Zobrazuje prepojenie jednotlivých modulov a spôsob ich komunikácie.

Používateľ má možnosť zadať požiadavku prostredníctvom webového alebo rozhrania API, tá je následne zaradená do fronty požiadaviek. V prípade ak je

voľné virtuálne zariadenie a požiadavka prišla na rad v obsluhe, začína sa proces generovania odtlačkov. Výsledky generovania sú ukladané do databázového systému a následne zobrazované používateľovi prostredníctvom webového rozhrania.

2.1 Odtlačky TLS

V rámci vytvorenej platformy má používateľ možnosť generovať rôzne druhy odtlačkov TLS, medzi ktoré patria odtlačky typu `JA3`, `JA3S`, `JA4`, `JA4S`, `JA4X`. Odtlačky typu `JA3` a `JA4` sú vytvorené z dát paketu `ClientHello` [2, 1], odtlačky `JA3S` a `JA4S` sú vytvárané zo `ServerHello` správ [2, 1]. Odtlačky `JA4X` sú vytvárané z dát x509 certifikátov [1].

2.2 Získavanie súborov APK

Získavanie súborov APK je rozdelené do dvoch variant, prvou je vkladanie súboru APK používateľom priamo prostredníctvom webového rozhrania platformy alebo rozhrania API. V prípade vstupu prostredníctvom názvu aplikácie alebo textového súboru je potrebné stiahnutie súboru APK. Sťahovanie je realizované prostredníctvom programu `aria2c`, ktorému je na vstup predaný priamy odkaz na stiahnutie. Aplikácie sú sťahované z portálu **ApkPure**. Odkaz je vytváraný spojením statickej časti a názvu balíčka potrebnej aplikácie. Názov balíčka je získavaný zo zadaného súboru alebo z portálu **SerpApi**.

2.3 Inštalácia a spúšťanie

Inštalácia a spúšťanie mobilných aplikácií je postavené na virtuálnom emulátore android zariadenia. Dané zariadenie je naviac vytvárané v prostredí Docker kontainera, aby bolo možné zabezpečiť škálovateľnosť a izoláciu od systému na ktorom je portál nasadený. Daný prístup taktiež umožňuje izoláciu sieťovej komunikácie prostredníctvom vytvárania bridge adaptérov. Samotná inštalácia a spúšťanie aplikácií sú zabezpečené prostredníctvom príkazov `adb`.

2.4 Analýza sieťovej komunikácie

Analýza sieťovej komunikácie je zabezpečovaná prostredníctvom nástroja `tshark`. K zachytávaniu komunikácie dochádza bezprostredne po nainštalovaní aplikácie. V rámci procesu zachytávania je aplikácia spúšťaná celkovo 4 krát. Čas analýzy jedného spustenia je stanovený na dobu 30 sekúnd. Za tento čas sú v aplikácii generované náhodné akcie.

2.5 Vytváranie odtlačkov mobilných aplikácií

Vytváranie odtlačkov mobilných aplikácií je zabezpečované prostredníctvom Python skriptu, ktorý zo zachytených dát sieťovej komunikácie vytvorí odtlačky podporované TLS, ktoré následne na základe adresy IP a portov prepojí a tým vytvorí odtlačok mobilnej aplikácie.

3. Identifikácia mobilných aplikácií

V rámci vývoja platformy bol testovaný scenár identifikácie mobilných aplikácií. Cieľom bolo zistiť, do akej miery je možné vytvorené odtlačky využiť pri identifikácii. V rámci testovania boli využívané aplikácie z datasetov popísaných v plagáte.

3.1 Testovacia topológia

Testovacia topológia je zobrazená na obrázku s označením Obrázok 3. V rámci testovanie bolo využívané zariadenie s operačným systémom debian 12, na ktorom bolo spustené zariadenie Android virtual device (AVD)[3]. Aplikácie boli postupne spúšťané a analyzované.

3.2 Výsledky testovania

Výsledky testovania je možné pozorovať v tabuľke s označením Tabuľka 1. Z výsledkov je zrejmé, že najpresnejšia detekcia aplikácií bola realizovaná prostredníctvom spojenia odtlačkov `JA3_JA3S_SNI`, `JA4_JA4S_SNI` a `JA3_JA3S_SNI_JA4_JA4S`.

4. Závery

V rámci práce bola vytvorená platforma, umožňujúca automatizované vytvárania odtlačkov mobilných aplikácií, so schopnosťou súčasného spracovávania viacerých požiadaviek používateľov. Možné scenáre využitia platformy: identifikácia aplikácií pri monitorovaní komunikácie, identifikácia nebezpečných aplikácií, detekcia malvéru.

V rámci možných rozšírení je možné spracovať filtráciu SNI serverov, ktoré nepatria priamo výrobcom aplikácie, a nie sú jedinečné pre danú aplikáciu.

Poďakovanie

Rád by som poďakoval svojmu školiteľovi bakalárskej práce doc. Ing. Petrovi Matouškovi, Ph.D., M.A. za odbornú pomoc, usmernenia a cenné rady pri vypracovávaní mojej bakalárskej práce.

Literatúra

[1] John Althouse. Ja4+ network fingerprinting. online, 2023. https://blog.foxio.io/ja4%2B-network-fingerprinting.

[2] Tls fingerprinting with ja3 and ja3s. online, 2022. https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967.

[3] Create and manage virtual devices. online, 2024. https://developer.android.com/studio/run/managing-avds.