BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023
http://excel.fit.vutbr.cz

Generátor odtlačkov mobilných aplikácií

Kristián Kičinka

Abstrakt
Hlavnou myšlienkou práce bolo vytvoriť aplikáciu, ktorá by umožnila automatizované vytváranie odtlačkov TLS z mobilných aplikácií, vytvorených na platforme Android. Vyvíjaná platforma prispeje k zlepšeniu v oblasti analýzy sieťovej prevádzky, ako aj k zvýšeniu efektivity práce sieťových administrátorov. Vyššie spomínaná platforma je dostupná vo forme webovej aplikácie, ktorá dokáže používateľovi poskytnúť natívne používateľské rozhranie. Rozhranie poskytuje používateľovi hneď niekoľko možností zadania android aplikácie, pre ktorú majú byť odtlačky generované. Pri špecifikácii typov odtlačkov, ktoré majú byť generované má používateľ na výber z niekoľkých variant, medzi ktoré patrí JA3, JA3S a NetFlow. Platforma ponúka možnosť evidovania už vygenerovaných odtlačkov mobilných aplikácií prostredníctvom databázového systému. V neposlednom rade je možné na interakciu s aplikáciou využívať vytvorené API.

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

1. Úvod

Motivácia Inšpiráciou a hlavnou motiváciou vytvorenia tejto práce bola skutočnosť, že na trhu doposiaľ absentuje obdobný systém venovaný danej problematike v takomto rozsahu, ktorý by disponoval potrebnou funkcionalitou, častokrát vyžadovanou koncovými používateľmi. Cieľovú skupinu používateľov tohto projektu predstavujú prevažne sieťoví administrátori.

Definícia problému Sieťoví administrátori sa potýkajú s problémom identifikácie mobilných aplikácií, nainštalovaných v mobilných zariadeniach, pripojených k sieti v ich správe. Tento fakt môže predstavovať isté bezpečnostné riziko. Na to, aby bolo možné predísť takejto situácii je potrebné, aby administrátori spracovali veľké množstvo dát, častokrát "ručne", čo je v dnešnej dobe časovo a zároveň finančne náročné.

Existujúce riešenia Počas skúmania existujúcich riešení boli nájdené platformy, ktoré umožňujú generovanie odtlačkov JA3 a ich ukladanie do internej databázy. Príkladom takejto platformy je portál JA3.ZONE (`https://ja3.zone`). Portál však neumožňuje vytvárať priamo odtlačky mobilných aplikácií a taktiež nepodporuje generovanie iných typov odtlačkov.

Naše riešenie Vyvíjaná aplikácia združuje funkcionalitu už existujúcich čiastkových riešení problému a poskytuje používateľovi možnosť automatizovane vytvárať odtlačky mobilných aplikácií. Používateľ má možnosť výberu typu odtlačku, ako aj možnosť dohľadania už vytvorených odtlačkov z databázy.

Výhody riešenia Navrhnuté používateľské rozhranie podporuje viacero možných vstupov pre zadanie android aplikácie. K dispozícii je taktiež API, ktoré poskytuje vygenerované odtlačky bez interakcie, s grafickým používateľským rozhraním.

2. Štruktúra práce

Projekt ako celok pozostáva z niekoľkých samostatných modulov, ktoré medzi sebou komunikujú. Každý z modulov reprezentuje jeden krok z návrhu aplikácie. Medzi základné časti aplikácie patrí:

- **automatizované získanie aplikácie**
- **analýza sieťovej komunikácie**
- **generovanie odtlačkov aplikácie**
- **poskytnutie výsledkov používateľovi**

Proces generovania odtlačkov začína získaním aplikácie, pre ktorú je potrebné vygenerovať odtlačky. Za túto časť zodpovedá modul **automatizované získanie aplikácie**. Ak bola táto časť úspešná, pristupuje sa k inštalácii aplikácie a zahájeniu analýzy sieťovej prevádzky. V ďalšom kroku je aplikácia spustená prostredníctvom android emulátora. Na pozadí dochádza k analýze sieťovej prevádzky. Ukon-

čením analýzy dochádza k spusteniu procesu generovania, vopred definovaných typov odtlačkov mobilnej aplikácie. Ako posledný prichádza na rad proces, ktorý poskytne vygenerované odtlačky používateľovi a zároveň ich zaeviduje v databázovom systéme. Jednotlivé moduly sú volané prostredníctvom jazyka PHP z backendovej časti webovej aplikácie.

2.1 Automatizované získanie aplikácií

Proces automatizovaného získavania aplikácií je rozdelený na niekoľko častí a variant. Používateľ má možnosť zadať aplikáciu prostredníctvom vloženia .apk súboru. V takomto prípade je zadaný súbor následne uložený v systéme a odovzdaný na spracovanie ďalšiemu modulu. Okrem vloženia APK súboru môže používateľ taktiež vložiť textový súbor obsahujúci názvy balíčkov aplikácií, určených na generovanie. Súbor je taktiež uložený a následne sa pristupuje k spracovaniu jednotlivých názvov a sťahovaniu APK súborov. V neposlednom rade je možné prostredníctvom vyhľadávacieho poľa zadať názov aplikácie, z ktorej je potrebné generovať odtlačky. Zadaním názvu sa zobrazí ponuka vyhovujúcich aplikácií. Ponuka aplikácií je získaná pomocou externého API. Kliknutím na konkrétnu aplikáciu sa spustí proces sťahovania .apk súboru danej aplikácie.

2.2 Analýza sieťovej komunikácie

Modul zastrešuje zachytávanie a analýzu sieťovej komunikácie sledovanej mobilnej aplikácie. Proces odchytu paketov a následného spracovania pre potreby skriptu určeného na generovanie odtlačkov mobilných aplikácií, je vykonávaný pomocou programu tshark. Zachytávaná je len komunikácia TLS. Následne dochádza k filtrovaniu zachytenej komunikácie na základe zvoleného typu odtlačku resp. odtlačkov. Napr. ak by bol požadovaný odtlačok JA3, výstupom procesu by bol súbor, ktorý by obsahoval správy typu "Client Hello".

2.3 Generovanie odtlačkov aplikácií

Generovanie odtlačkov mobilných aplikácií je zabezpečované pomocou Python skriptov. V skripte dochádza k postupnému prechádzaniu zachytených paketov, spracovaných predošlým modulom a získavaniu dát potrebných na vytvorenie zadaného typu odtlačku mobilnej aplikácie. Jednotlivé získané dáta sa ukladajú do reťazca, z ktorého je následne pomocou MD5 hešovacej funkcie vytvorený výsledný odtlačok mobilnej aplikácie. Jednotlivé, takto vytvorené odtlačky, sú vkladané do poľa a následne odovzdané ďalšiemu modulu.

2.4 Poskytnutie odtlačkov používateľovi

Tento modul zabezpečuje zobrazenie výsledných vygenerovaných odtlačkov používateľovi, ako aj ich uloženie do databázového systému. Odtlačky získané z Python skriptu predošlého modulu sú upravené do formy zoznamu a následne zobrazené používateľovi prostredníctvom webového rozhrania. Okrem samotných odtlačkov je zobrazený aj názov aplikácie, verzia a názov balíčka. Každá z týchto položiek je zároveň evidovaná v databáze, ku ktorej má používateľ prístup pomocou podstránky **Fingerprints database**.

3. Praktický príklad použitia

Praktickým príkladom využitia vytvoreného generátora môže byť potreba zamedziť, prípadne odhaliť používanie zakázanej aplikácie v spravovanej sieti. Takouto aplikáciou môže byť napr. aplikácia **TikTok**. Sieťový administrátor vyhľadá aplikáciu TikTok prostredníctvom webového rozhrania a vygeneruje odtlačky aplikácie. V tomto konkrétom prípade zvolí napr. **JA3** odtlačky. Vygenerované odtlačky uloží do textového súboru. Následne vykoná analýzu sieťovej komunikácie spravovanej siete, napr. prostredníctvom programu Wireshark. Tento program umožňuje získať JA3 odtlačky zo zachytenej komunikácie. V poslednom kroku porovná získané odtlačky s odtlačkami vygenerovanými generátorom, čím zistí, či došlo k použitiu danej aplikácie. Ak je komunikácia takejto aplikácie identifikovaná, administrátor môže získať IP adresy, prostredníctvom ktorých aplikácia komunikuje, prípadne ich zablokovať alebo inak obmedziť.

4. Zhrnutie

Vytvorená aplikácia umožňuje používateľom automatizovane generovať jednotlivé odtlačky mobilných aplikácií. Zároveň disponuje možnosťou vyhľadávania a zobrazovania už vygenerovaných odtlačkov prostredníctvom databázy. V neposlednom rade, je možné pri generovaní odtlačkov, ako aj pri vyhľadávaní v databáze využívať nie len webové rozhranie, ale aj vytvorené API.

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 tejto práce.