При використанні будь-якого з перерахованих біометричних сканерів, як правило, 100% точності недосяжна. Так як результати декількох сканів особи, відбитків пальця або райдужної оболонки ока одного користувача завжди містять відмінності.

Література:

1. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.
2. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).
3. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).
4. Hunko M.A., Tkachov V.M. Development of a module for sorting the ipaddresses of user nodes in cloud firewall protection of web resources. Дев’ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційнокомунікаційних технологій та засобів управління». 2019. С. 30.
5. Tkachov V. Architecture of overlay network with nested vpn tunneling / M. Hunko, V. Tkachov, M. Bondarenko // "Сучасні напрями розвитку інформаційно комунікаційних технологій та засобів управління" : матеріали Дев'ятої міжнар. наук.-техн. Конф., 9–10 квітня 2020 р. – Харків, 2020. – С. 36.

Воропаєва К.А., студент
Харківський національний університет радіоелектроніки, м Харків
Кафедра електронних обчислювальних машин

ВРАЗЛИВІСТЬ МОБІЛЬНИХ ПРИСТРОЇВ ПІД КЕРУВАННЯМ ОС ANDROID

Операційна система Android вважається однією з найбільш захищених операційних систем в наш час. Розробники цієї ОС на своєму офіційному сайті розповідають, що в ОС зроблено дуже багато роботи для

того щоб створення традиційних експлойтів було нерентабельно, складно, неможливо. Виникає питання, а чи є взагалі уразливості в ОС, які могли б привести до компрометації системи? Чи будуть ці уразливості відрізнятися від стандартних вразливостей програмного забезпечення? Чи можна знайти ці уразливості в CWE TOP 25? Або в Android унікальні уразливості?

Основою платформи Android є ядро Linux. Використання ядра Linux дозволяє Android використовувати ключові функції безпеки і дозволяє виробникам пристроїв розробляти апаратні драйвери для відомого ядра. Архітектура ОС Android складається з рівнів, кожен рівень архітектури відділений друг від друга і виконує функції на різних рівнях привілеїв. Всі рівні Android ввібрали в себе найкраще, що було на момент створення ОС з інших open source проектів з точки зору безпеки. Якщо об'єднати ці два факти, то виходить, що для того щоб атакувати цю операційну систему необхідно, щоб у атакуючого було в арсеналі по 1 вразливою функції на кожному з рівнів ОС. Це досить серйозно ускладнює процес створення експлойта для атаки на ОС. Однак, все одно Ресечер з усього світу знаходять способи як можна атакувати цю ОС і роблять це досить успішно.

Уразливість в операційній системі Android 10. Якщо звернутися до загальної класифікації вразливостей CWE Top 25, то вразливість можна віднести до класу CWE-502. Даний клас вразливостей може виникати як в веб, так і в десктопних додатках. Основною особливістю уразливості вважається той факт, що за допомогою неї можна абсолютно непомітно для ОС і користувача впровадити свій код в уразливе додаток. Можливо це за рахунок того, що об'єкти, які піддаються процедурі десеріалізациі або у роботі можуть описувати функцію-складальник, яка може виконувати похідні функції. Уразливість відома досить давно і при необережному використанні функцій десеріалізациі може стати критичною. В ОС Android так і сталося. При успішному використанні уразливості можна захопити контроль над прівілегірова.

Схоже, що навіть поділ привілеїв, використання найпередовіших технологій не рятує від найпоширеніших помилок програмного забезпечення. ОС можна атакувати і класичними експлойта на пошкодження пам'яті і більш сучасними аналогами, які використовують механізми ОС.

Література:

1. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical

Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.
2. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).
3. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).
4. Hunko M.A., Tkachov V.M. Dvelopment of a module for sorting the ipaddresses of user nodes in cloud firewall protection of web resources. Дев'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційнокомунікаційних технологій та засобів управління». 2019. С. 30.
5. Tkachov V. Architecture of overlay network with nested vpn tunneling / M. Hunko, V. Tkachov, M. Bondarenko // "Сучасні напрями розвитку інформаційно комунікаційних технологій та засобів управління" : матеріали Дев'ятої міжнар. наук.-техн. конф., 9–10 квітня 2020 р. – Харків, 2020. – С. 36.

Воропаєва К.А., студентка
Гунько М.А., студент
Харківський національний університет радіоелектроніки, м Харків
Кафедра електронних обчислювальних машин

РОЗРОБКА НАТИВНИХ ТА ГІБРИДНИХ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ ПЛАТФОРМ ANDROID ТА IOS

Вже на стадії проектування мобільного додатка важливо розуміти, яка мова вигідніше використовувати для конкретного проекту. Поряд з нативної розробкою (наприклад, для iOS - Swift або Objective-C, для Android - Java або Kotlin), використовуються Кросплатформені фреймворки, такі як React Native і Flutter.

При створенні мобільних додатків найчастіше потрібно випустити версії як на iOS, так і на Android. Для цього можна звернутися до нативної або кроссплатформенной («гібридної») розробці.

Нативная розробка - це класичне рішення, яке вимагає писати програми під кожну платформу окремо, використовуючи різні мови і з