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

ВИДИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ В МОБІЛЬНИХ ДОДАТКАХ ПІД КЕРУВАННЯМ ОС ANDROID

Для ідентифікації користувача в додатку можна використовувати біометрії - наприклад, сканери райдужної оболонки ока, геометрії особи або відбитка пальця. Хоча ці технології відомі і популярні, у початківців розробників через нестачу інформації до сих пір виникають ті чи інші питання.

Ідентифікація користувачів необхідна в багатьох додатках, які обробляють особисті дані. Популярні способи біометричної ідентифікації, за даними дослідження: сканер відбитків пальців (fingerprint) - 57%, сканер геометрії особи (face ID) - 14% та інші методи: сканери райдужної оболонки ока (IRIS) і геометрії руки (3-5%).

Сканер відбитка пальця (fingerprint). Для того, щоб «дізнатися» користувача за відбитком пальця і безпечно зберігати його дані. Так, на пристроях Apple зразок відбитка пальця проводиться через хеш-функцію перед збереженням в захищений обчислювальному модуль. На пристроях Android ступінь безпеки залежить від виробника, які він використовує підходів і рішень. Як правило, робота зі сканерами відбитка пальця регламентується окремими документами, в тому числі специфікаціями Google. Провідні виробники смартфонів, такі як Samsung, використовують досить надійні і точні ємнісні сенсорами і забезпечують високу ступінь безпеки даних.

Сканер геометрії особи (face ID). Якщо додаток ідентифікує користувача по обличчю, сканування здійснюють за рахунок ємнісний камери. У порівнянні з попереднім способом, тут потрібно ще більш складний алгоритм, що вимагає високої точності захоплення зображення і розподілу більш 30 тисяч контрольних точок по зображенню особи користувача. У свою чергу, це визначає більш високі вимоги до камери смартфона.

Сканер райдужної оболонки ока (IRIS). Сканер визначає ті чи інші особливості зовнішності користувача і геометричну форму райдужки, використовуючи ємнісні камери. Хоча такий спосіб біометричного захисту може здатися перспективним, у нього є свої уразливості. З одного боку, для зняття блокування недостатньо знайти і пред'явити фотографію власника, адже камера визначає обсяг зображення. Однак, такий ризик вище при одночасному використанні фотографії та контактних лінз.

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