Date: 9th January-2026

ANDROID OPERATSION TIZIMIDAGI MAVJUD TAHDIDLAR VA ZAIFLIKLAR

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi assistenti
Xayriddinov Shaxboz Shavkatovich
Oripov Asilbek Baxtiyor o'g'li
Ismoilov Fayozbek Nodirbek o'g'li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: Ushbu maqolada Android operatsion tizimidagi mobil ilovalarga xos bo'lgan asosiy tahdidlar va zaifliklar tahlil qilinadi. Statistik ma'lumotlar asosida Android va iOS platformalarida aniqlangan yuqori xavfli zaifliklar, ularning kelib chiqish sabablari hamda hujumchilar tomonidan foydalanish imkoniyatlari ko'rib chiqiladi. Mijoz va server tomonidagi zaifliklar, xavfsiz ma'lumotlarni saqlash, autentifikatsiya mexanizmlaridagi kamchiliklar va zararli dasturlar tahdidi yoritilgan. Shuningdek, Android operatsion tizimida xavfsizlikni ta'minlash usullari, jumladan shifrlash texnologiyalari, Application Sandbox, SELinux, tasdiqlangan yuklash (Verified Boot) va kriptografik mexanizmlar tahlil qilinadi. Maqola mobil ilovalar xavfsizligini oshirish bo'yicha amaliy tavsiyalar berish bilan yakunlanadi.

Kalit so'zlar: Android, mobil ilovalar xavfsizligi, zaifliklar, kiberxavfsizlik, shifrlash, Application Sandbox, SELinux, IPC, zararli dasturlar, autentifikatsiya, mobil tahdidlar.

Statistik ma'lumotlarga ko'ra, 2018-yilda mobil ilovalar foydalanuvchilarning qurilmalariga 200 milliard martadan ko'proq yuklab olingan. Marketing Land ma'lumotlariga ko'ra, raqamli makonda o'tkaziladigan vaqtning 57 foizi smartfon yoki planshetlardagi dasturlarga sarflangan vaqtdir. Mobil qurilmalar hayotimizning bir qismiga aylandi: messenjerlar, bank xizmatlari, biznes ilovalari, mobil operatorlarning shaxsiy hisoblari – hayotning zamonaviy ritmi bilan biz bu ilovalardan deyarli har kuni foydalanamiz. Juniper Research ma'lumotlariga ko'ra, mobil bank ilovasidan foydalanuvchilarning umumiy soni ikki milliardga yaqinlashmoqda, bu butun kattalar aholisining qariyb 40% ni tashkil qiladi [1].

Positive Technologies mutaxassislari muntazam ravishda mobil ilovalar xavfsizligini tahlil qiladi. Ushbu hisobotda 2018-yilda iOS va Android uchun mobil ilovalarning xavfsizlik sinovlari davomida olingan statistik ma'lumotlar keltirilgan.

Yuqori xavfli zaifliklar iOS uchun mobil ilovalarning 38 foizida va Android platformasi uchun ilovalarning 43 foizida aniqlangan.

Ko'pgina xavfsizlik muammolari ikkala platforma uchun ham umumiydir. Xavfsiz ma'lumotlarni saqlash - bu mobil ilovalarning 76 foizida aniqlangan. Parollar, moliyaviy ma'lumotlar, shaxsiy ma'lumotlar va shaxsiy yozishmalar xavf ostida.

Xakerga ma’lumotlarni o‘g‘irlash uchun kamdan-kam hollarda smartfonga jismoniy kirish kerak bo‘ladi: zaifliklarning 89 foizi zararli dasturlardan foydalanish mumkin.

Kamchiliklarning aksariyati xavfsizlik mexanizmlaridagi xatolar bilan bog‘liq (iOS va Android ilovalari uchun mos ravishda 74% va 57%, server qismlari uchun 42%). Bunday zaifliklar dizayn bosqichida kiritiladi va ularni yo‘q qilish kodga jiddiy o‘zgartirishlar kiritishni talab qiladi.

Mijoz tarafidagi zaifliklar

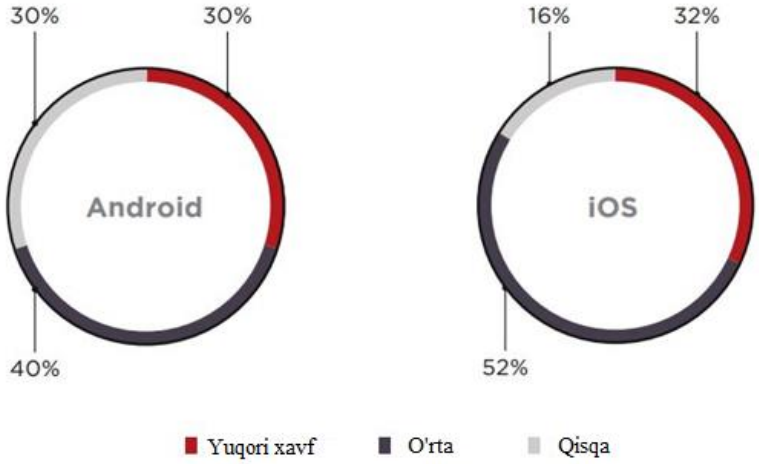
Zaifliklarning 60% mijoz tomonida jamlangan.

Zaifliklarning 89% qurilmaga jismoniy kirishsiz foydalanish mumkin.

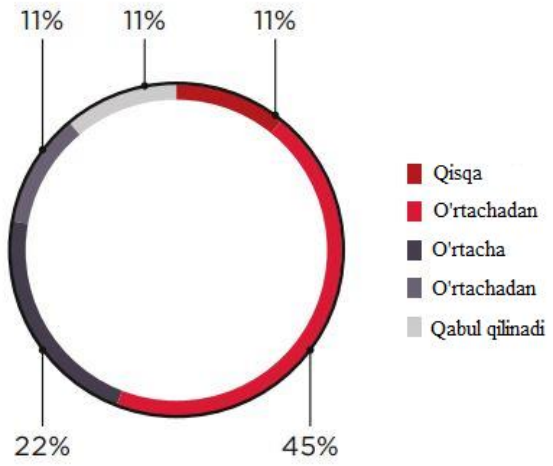
Zaifliklarning 56% dan ma’muriy huquqlarsiz (jailbreak yoki root) foydalanish mumkin.

Muhim zaifliklarga ega Android ilovalari iOS ilovalariga qaraganda bir oz ko‘proq (43% ga nisbatan 38%). Biroq, bu farq unchalik katta emas va Android va iOS uchun mobil ilovalarning mijoz qismlari xavfsizligining umumiy darajasi taxminan bir xil. Ikkala platforma uchun mobil ilovalarning mijoz qismlaridagi barcha zaifliklarning uchdan bir qismi yuqori darajadagi xavfga ega.

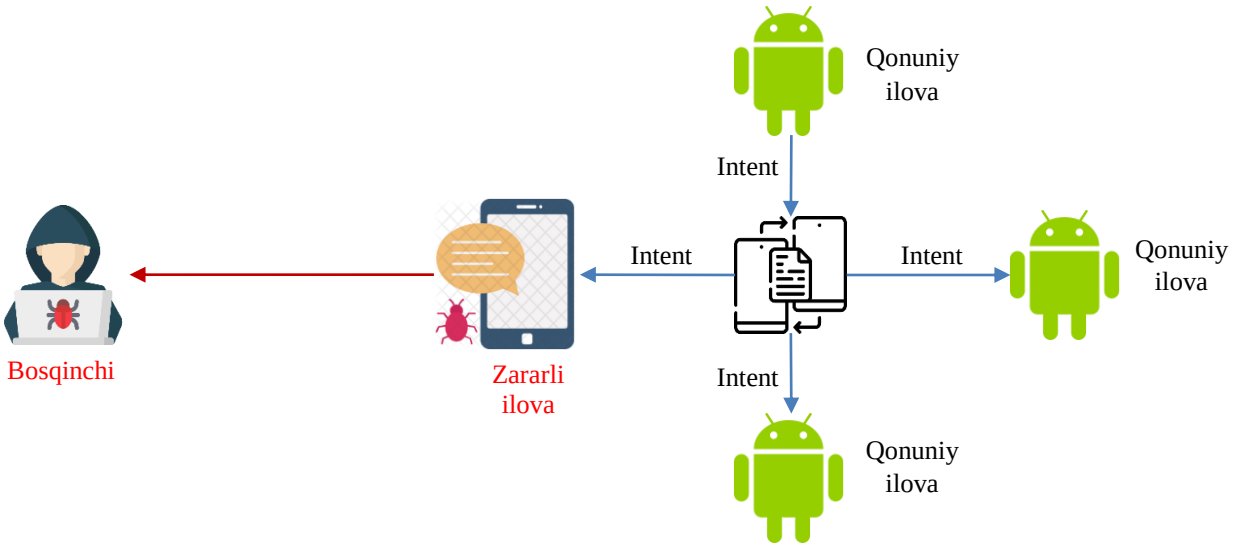
1.2-rasm. Zaiflik xavfining maksimal darajasi (mijoz qismlarining ulushi ko‘rsatilgan)



1.3-rasm. Turli darajadagi xavf darajasidagi zaifliklarning nisbati

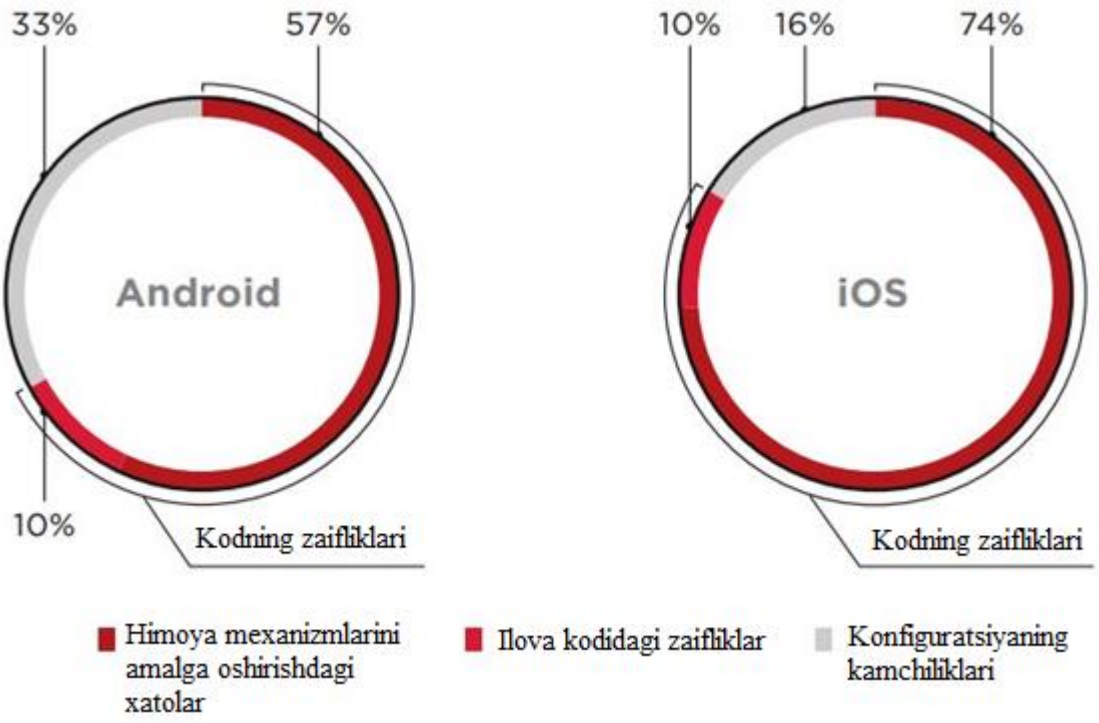


1.4-rasm. Mijoz qismlarining xavfsizlik darajasi (tizimlar ulushi)



1.5-rasm. Android operatsion tizimida xavfsiz jarayonlararo aloqa sxemasi

Xavfli jarayonlararo aloqaning zaifligi dastur komponentlari o‘rtasidagi o‘zaro ta’sir uchun interfeyslarni loyihalash bosqichida kiritiladi va xavfsizlik mexanizmlarini amalga oshirishdagi xatolarga ishora qiladi. Xavfsizlik mexanizmlaridagi xatolar iOS ilovalaridagi zaifliklarning 74 foizini va Android platformalaridagi zaifliklarning 57 foizini keltirib chiqardi.



1.6-rasm. Har xil turdagi zaifliklarning ulushi

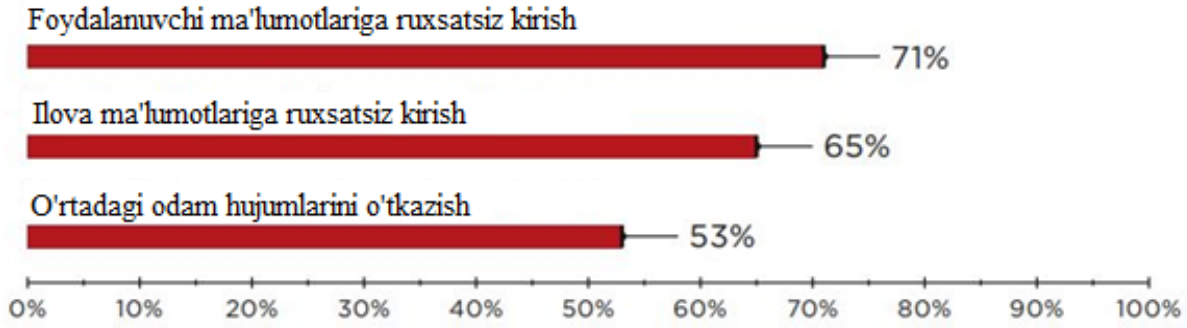
Mobil qurilmada turli xil ma’lumotlar saqlanishi mumkin, masalan, geolokatsiya ma’lumotlari, shaxsiy ma’lumotlar, shaxsiy yozishmalar, hisoblar, moliyaviy ma’lumotlar, lekin ularni mobil ilovalarda saqlash xavfsizligiga har doim ham e’tibor berilmaydi. Xavfsiz ma’lumotlarni saqlash OWASP Mobile Top 10−2016 reytingida ikkinchi o‘rinda turadi; bu zaiflik mobil ilovalarning 76 foizida topilgan.

2018-yil avgust oyida hujumchilar Air Canada mobil ilovasining 20 ming foydalanuvchisining shaxsiy ma’lumotlarini o‘g‘irlashgan. McAfee ma’lumotlariga ko‘ra, mobil qurilmalar uchun zararli dasturlar soni ortib bormoqda: har chorakda 1,5 milliondan 2 milliongacha yangi nusxalar aniqlanadi, 2018 yil oxiriga kelib esa umumiy hajm 30 million nusxadan oshdi. Mobil qurilmalar uchun zararli dasturlar soni va xilma-xilligining doimiy o‘sib borishi mijoz tomoniga hujumlar ommabopligini sezilarli darajada oshirmoqda va server tomonidagi zaifliklar mobil ilovalar xavfsizligiga asosiy tahdid bo‘lib qolmadi.

Mobil ilovalarning server qismlarida dasturning kodida ham, xavfsizlik mexanizmlarida ham zaifliklar mavjud. Ikkinchisi orasida ikki faktorli autentifikatsiyani amalga oshirishning kamchiliklarini ta’kidlash kerak. Agar siz ikkita bir xil so‘rovni bir-biridan keyin, minimal interval bilan serverga yuborsangiz, u holda bir martalik parollar qurilmadagi ilova foydalanuvchisiga push-bildirishnomalar orqali ham, bog‘langan telefon raqamiga SMS orqali yuboriladi. Natijada, tajovuzkor SMS-xabarlarni ushlab qolish qobiliyatiga ega bo‘lib, qonuniy foydalanuvchi nomidan operatsiyalarni amalga oshirishi mumkin, masalan, o‘z hisobidan pul o‘tkazishi mumkin.

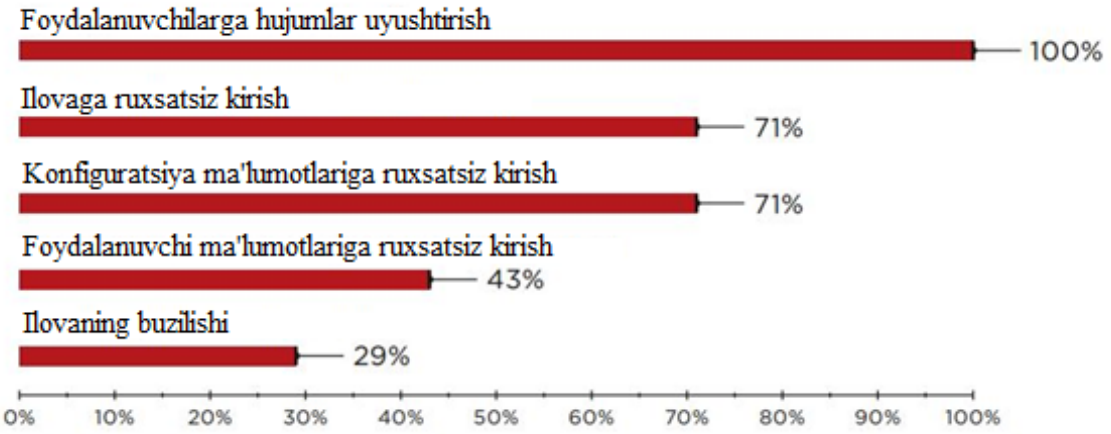
Mobil ilova tahdidlari. Ilovalarning 18 foizi autentifikatsiya ma’lumotlarini kiritishga urinishlar sonini cheklamaydi. Ba’zan mobil ilovani buzish uchun na zararli dastur, na xakerlik vositalari talab qilinmaydi. Misol uchun, ilovada PIN-kodni kirita

olmasligingiz soni bo‘yicha cheklov bo‘lmasligi mumkin. Yana bir misol: parolni kiritishga urinishlar soniga cheklovlar faqat mijoz tomonidan qo‘yiladi va dastur qayta ishga tushirilganda urinishlar hisoblagichi nolga qaytariladi. Bu ikkala kamchiliklar tajovuzkorga parolni cheksiz ko‘p marta kiritish imkonini beradi.



1.7-rasm. Mijoz qismlariga tahdidlar (tizimlar ulushi)

Server qismlaridagi zaifliklar tufayli foydalanuvchilarga hujum qilish mumkin. Cross-Site Scripting zaifligi serverlarning 86 foizida topilgan. Bu eng keng tarqalgan veb zaifligi. Uning yordami bilan tajovuzkorlar zararli skriptlardan foydalangan holda, cookie-fayllar kabi qurbonning hisob ma’lumotlarini o‘g‘irlashlari mumkin. Ammo zaiflik, agar ular HTML va JavaScript-ni qo‘llab-quvvatlaydigan komponentlardan foydalansa, mobil ilovalarga ham tahdid solishi mumkin. Masalan, WebView - bu Android ilovalariga veb-kontentni bevosita ilova ichida ko‘rsatish imkonini beruvchi tizim komponenti [5].



1.8-rasm. Server qismlari uchun eng yaxshi 5 ta tahdid (tizimlar foizi)

Xulosa

Mobil ilovalar kundalik hayotning ajralmas qismiga aylanganligi sababli ularning xavfsizligini ta’minlash dolzarb masalalardan biri hisoblanadi. Tadqiqot natijalari shuni ko‘rsatadiki, Android platformasidagi ilovalarning katta qismida yuqori va o‘rta darajadagi xavfli zaifliklar mavjud bo‘lib, ularning aksariyati mijoz tomonida joylashgan. Xavfsizlik mexanizmlaridagi xatolar, ma’lumotlarni himoyasiz saqlash va autentifikatsiya jarayonidagi kamchiliklar foydalanuvchi ma’lumotlarining o‘g‘irlanishiga olib kelishi mumkin.

Android operatsion tizimi Linux yadrosi, sandbox mexanizmi, faylga asoslangan shifrlash va kriptografik API’lar orqali yuqori darajadagi himoyani ta’minlasa-da, ishlab chiquvchilar tomonidan xavfsizlik talablariga rioya qilinmasligi umumiy xavfsizlik

darajasini pasaytiradi. Shuning uchun mobil ilovalarni loyihalash va ishlab chiqish jarayonida xavfsizlikni birlamchi omil sifatida ko‘rib chiqish, zamonaviy kriptografik usullardan foydalanish va server hamda mijoz tomonidagi himoya mexanizmlarini kuchaytirish zarur.

FOYDALANILGAN ADABIYOTLAR:

1. Juniper Research. *Mobile Banking Users Worldwide* – Statistik hisobot, 2018.
2. Positive Technologies. *Mobile Application Security Research*, 2018.
3. OWASP Foundation. *OWASP Mobile Top 10 – 2016*.
4. McAfee Labs. *Mobile Malware Threat Report*, 2018.
5. Android Developers. *Android Security Overview*.
6. Android Developers. *WebView Security Best Practices*.
7. Google. *Android Encryption and KeyStore Documentation*.
8. Linux Foundation. *Linux Kernel Security Overview*.