MOBIL ILOVALARDA AXBOROT XAVFSIZLIGI (ANDROID VA IOS)

Husenov Dilshodbek Furqat o‘g‘li
Abdumutalov Jamoliddin Tolibjon o'g'li
Eshboboyev Diyorbek Husan o‘g‘li
Imamaliyev Aybek Turapbayevich
Muhammad Al-Xorazmiy nomidagi
Toshkent Axborot Texnologiyalari Universiteti

Annotatsiya. *Ushbu maqolada mobil ilovalarda, xususan, Android va iOS operatsion tizimlarida axborot xavfsizligini ta’minlash masalalari ko‘rib chiqiladi. Mobil qurilmalar kundalik hayotda keng qo‘llanilayotgani sababli ulardagi ilovalar orqali foydalanuvchilarning shaxsiy va maxfiy ma’lumotlari xavf ostida qolmoqda. Ishda mobil ilovalarga xos bo‘lgan xavfsizlik tahdidlari, foydalanuvchi ma’lumotlarini himoyalash usullari, mobil operatsion tizimlarning xavfsizlik arxitekturasi, himoya mexanizmlari, zararli dasturlardan himoyalanish yo‘llari va ilova ishlab chiqishda xavfsizlikni inobatga olish prinsiplariga e’tibor qaratiladi. Shuningdek, Android va iOS tizimlari orasidagi xavfsizlik farqlari tahlil qilinadi va amaliy tavsiyalar beriladi.*

Kalit so‘zlar: *mobil ilovalar,, axborot xavfsizligi, android xavfsizligi, ios xavfsizligi, mobil tahdidlar, maxfiylik, ilova xavfsizligi, ma’lumotlarni himoyalash, zararli dasturlar, kriptografiya.*

Axborot texnologiyalarining jadal rivojlanishi mobil qurilmalarning hayotimizdagi o‘rnini keskin oshirdi. Bugungi kunda foydalanuvchilarning ko‘pchilik ish faoliyati, muloqoti, moliyaviy va shaxsiy axborotlari mobil ilovalar orqali amalga oshirilmoqda. Shu bilan birga, bu ma’lumotlarning xavfsizligi masalasi dolzarb muammolardan biriga aylanmoqda. Ayniqsa, Android va iOS

kabi ommabop platformalardagi ilovalarda axborot xavfsizligini ta’minlash texnik va huquqiy yondashuvlarni talab etadi.

Mobil telefon hayotimiz, faoliyatimizning ajralmas qismiga aylandi. Usiz kelajagimizni tasavvur ham qila olmaymiz. Ammo internet shiddat bilan rivojlanayotgan bir davrda global tarmoq va boshqa yo‘llar orqali xavf solishi mumkin bo‘lgan turli xurujlar mobil aloqani ham chetlab o‘tmaydiki, bugun aynan mobil telefon va undagi ma’lumotlarga yo‘naltirilgan xatarlar va ulardan himoyalanishga to‘xtalamiz.

Mobil aloqa tizimlari xizmat ko‘rsatadigan hududni qamrab oladigan yacheykalar (sotalar) ko‘rinishida yaratiladi. Har bir yacheykaning markazida o‘z yacheykasi doirasida barcha mobil stansiyalarga xizmat ko‘rsatuvchi baza stansiyasi joylashadi. Abonentning harakatlanishida tizimning yacheykalari orasida bitta baza stansiyadan boshqasiga xizmat ko‘rsatishni uzatish – estafetali uzatish (handover) amalga oshiriladi.

Barcha baza stansiyalari ajratilgan simli yoki radiorele aloqa kanallari orqali mobil aloqasining kommutatsiya markazi bilan ulangan. Mobil aloqa tizimlarining o‘lchamlari katta bo‘lgan holda ularda qo‘shimcha kommutatsiya markazlari joylashtirilishi mumkin. Kommutatsiya markazidan umumiy foydalanishdagi telefon tarmog‘iga chiqish mavjud, u orqali mobil aloqa tizimi bilan o‘zaro harakat amalga oshiriladi. Abonent boshqa mobil aloqa tizimi hududiga o‘tganida unga xizmat ko‘rsatish bitta mobil aloqa tizimidan boshqasiga o‘tkaziladi, ya’ni rouming amalga oshiriladi.

1. Mobil ilovalardagi xavfsizlik tahdidlari

Mobil ilovalar quyidagi asosiy tahdidlarga duch keladi:

Zararli dasturlar (malware): Ilovaga zararli kod kiritilishi natijasida foydalanuvchi ma’lumotlari o‘g‘irlanadi.

Ma’lumotlarni ruxsatsiz uzatish: Foydalanuvchi roziligisiz ma’lumotlar uchinchi tomon serverlariga yuborilishi.

Tarmoq hujumlari: Ochiq Wi-Fi tarmoqlarida ma’lumotlar uzatish jarayonida “Man-in-the-middle” kabi hujumlar orqali ma’lumotlar o‘g‘irlanadi.

Ruxsatlar ekspluatatsiyasi: Ilova ortiqcha ruxsatlar so‘rab, foydalanuvchi ustidan nazoratni qo‘lga kiritishi mumkin.

2. Android va iOS xavfsizlik arxitekturasi

Android ochiq manba kodiga ega bo‘lib, bu yondashuv bir tomondan keng imkoniyatlar yaratsa, boshqa tomondan esa xavfsizlik nuqtai nazaridan zaifliklarga olib keladi. Android xavfsizligini ta’minlashda quyidagilar muhim rol o‘ynaydi:

Sandboxing: Har bir ilova alohida muhitte ishlaydi.

Ruxsatlar tizimi: Ilova ishlashi uchun kerakli ruxsatlar foydalanuvchidan so‘raladi.

Play Protect: Google tomonidan zararli ilovalarga qarshi avtomatik skanerlash tizimi.

iOS yopiq tizim bo‘lib, xavfsizlikka alohida e’tibor qaratiladi. Asosiy jihatlar:

Ilova tekshiruvi: Har bir ilova App Store’da qat’iy tekshiruvdan o‘tadi.

Kod imzolash: Faqat Apple tomonidan imzolangan kodlar bajariladi.

Ma’lumotlarni shifrlash: Qurilmadagi ma’lumotlar AES algoritmlari bilan himoyalangan.

3. Himoya usullari va tavsiyalar

Ilova ishlab chiquvchilar uchun:

Minimal ruxsatlar talab qilish

Ma’lumotlarni uzatishda HTTPS protokolidan foydalanish

Foydalanuvchi ma’lumotlarini lokal bazada saqlamaslik yoki shifrlab saqlash

Doimiy xavfsizlik testlarini o‘tkazish (penetratsiya testi, kod tahlili)

Foydalanuvchilar uchun:

Faqat rasmiy do‘konlardan ilova yuklab olish

Ilovalar talab qilayotgan ruxsatlarni tekshirish

Qurilmada antivirus va xavfsizlik ilovalaridan foydalanish

Ilovani doimiy yangilab boorish

Xulosa qilib aytganda, mobil ilovalarda axborot xavfsizligini ta’minlash barcha foydalanuvchilar va ishlab chiquvchilarning mas’uliyatli yondashuvini talab etadi. Android va iOS platformalari o‘zining xavfsizlik mexanizmlari bilan bu yo‘nalishda sezilarli taraqqiyotga erishgan bo‘lsa-da, tahdidlar hamon mavjud. Shuning uchun, doimiy yangilanib boruvchi xavfsizlik strategiyalari va amaliy yondashuvlar muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. "The Complete Android Oreo Developer Course - Build 23 Apps!" by Rob Percival, Nick Walter

2. "Kotlin Programming: The Big Nerd Ranch Guide" by Josh Skeen, David

Greenhalgh

3. "Realm: Building Modern Swift Apps with Realm Database" by Tim Oliver