MOBIL ILOVALARDA MA’LUMOTLARNI O‘G‘IRLASH VA SOXTALASHTIRISHGA QARSHI HIMOYA USULLARINI TAHLIL QILISH VA BAHOLASH

Turdiyev Temur
Ro‘zmatov Nuraddin Islomboy o‘g‘li
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
Kompyuter injiniringi fakulteti, Axborot xavfsizligi yo‘nalishi, 4-kurs Urganch, O‘zbekiston

Annotatsiya

Maqsad: Ushbu tadqiqot mobil ilovalarda ma’lumotlarni o‘g‘irlash va soxtalashtirish tahdidlariga qarshi qo‘llaniladigan himoya usullarini tizimli tahlil qilish va samaradorlik mezonlari bo‘yicha baholashga qaratilgan. Metodlar: Tadqiqotda adabiyotlarni tizimli ko‘rib chiqish, taqqoslama tahlil va STRIDE tahdid modellash metodologiyasi qo‘llanildi. 2018–2024-yillar oralig‘ida chop etilgan 120 dan ortiq maqola ko‘rib chiqilib, 38 tasi tanlandi; himoya mexanizmlari to‘rtta mezon bo‘yicha 1–5 ball tizimida baholandi. Natijalar: Hujum vektorlari tahlili shuni ko‘rsatdiki, tarmoq hujumlari (28%) va zararli dasturlar (23%) eng ko‘p tarqalgan tahdidlardir. AES-256 shifrlash (4,9/5,0), TLS 1.3 (4,8/5,0) va OAuth 2.0 (4,6/5,0) eng yuqori samaradorlikka ega himoya mexanizmlari sifatida aniqlandi. Taklif etilgan uch qatlamli himoya modeli ma’lumot o‘g‘irlashni aniqlashda 94,7%, tarmoq hujumlarini oldini olishda esa 97,2% ko‘rsatkichga erishdi. Xulosa: Ko‘p qatlamli himoya yondashuvi yagona mexanizmga nisbatan 2,3–2,8 baravarga samarali ekanligi tasdiqlandi. Mobil ilova ishlab chiquvchilarga AES-256 shifrlash, qisqa muddatli JWT tokenlar va TLS 1.3 ni majburiy qo‘llash tavsiya etiladi.

Kalit so‘zlar: mobil ilovalar, ma’lumotlar xavfsizligi, kriptografiya, autentifikatsiya, JWT, OAuth 2.0, RASP, shifrlash, zaifliklar, axborot xavfsizligi

Kirish

Raqamli texnologiyalarning jadal rivojlanishi natijasida mobil ilovalar zamonaviy hayotning ajralmas qismiga aylandi. Jahon statistikasiga ko‘ra, 2024-yilga kelib dunyo bo‘ylab 6,8 milliarddan ortiq smartfon foydalanuvchisi qayd etilgan bo‘lib, kundalik moliyaviy operatsiyalar, shaxsiy muloqot, tibbiy ma’lumotlar va davlat xizmatlari aksariyat hollarda mobil ilovalar orqali amalga oshirilmoqda [1]. Bu holat, o‘z navbatida, mobil ilovalarni kiberjinoyatchilar uchun asosiy nishonga aylantirmoqda.

Mobil ilovalarda ma’lumotlarni o‘g‘irlash va soxtalashtirish muammosi axborot xavfsizligi sohasining dolzarb yo‘nalishlaridan biri hisoblanadi. OWASP (Open Web

Application Security Project) tashkilotining 2023-yildagi hisobotiga ko‘ra, mobil ilovalarning 70% dan ortiq qismida kamida bitta kritik zaiflik mavjud bo‘lib, bu zaifliklarning katta qismi ma’lumotlarni himoyasiz saqlash va uzatish bilan bog‘liq [2]. Bunday zaifliklardan foydalangan holda amalga oshirilgan hujumlar natijasida yiliga milliardlab dollar miqdorida iqtisodiy zarar yetkazilmoqda.

Mavzu bo‘yicha ilmiy adabiyotlarni o‘rganish shuni ko‘rsatadiki, tadqiqotchilar mobil ilovalar xavfsizligi muammosini turli aspektlardan tahlil qilgan. Felt va boshqalar [3] Android ilovalarida ruxsat tizimidagi zaifliklarni o‘rganib, foydalanuvchilar ma’lumotlariga ruxsatsiz kirish imkoniyatlarini aniqlagan. Enck va hamkasblari [4] TaintDroid tizimini ishlab chiqib, mobil ilovalardagi ma’lumot oqimlarini real vaqt rejimida kuzatishni amalga oshirgan. Lu va boshqalar [5] iOS va Android tizimlarida kriptografik protokollarning noto‘g‘ri qo‘llanilishi natijasida yuzaga keladigan zaifliklarni tasniflab, samarali himoya choralari taklif qilgan.

Shu bilan birga, adabiyotlarni tahlil qilish natijasida bir qator tadqiqot bo‘shliqlari aniqlandi. Birinchidan, mavjud ishlarning aksariyati alohida hujum turlarini yoki alohida himoya usullarini o‘rganadi, lekin kompleks tahdid modeliga asoslangan yaxlit baholash metodologiyasi etarlicha ishlab chiqilmagan. Ikkinchidan, turli tadqiqotchilarning natijalari o‘rtasida ziddiyatlar mavjud: masalan, ba’zi manbalar JWT tokenlarning xavfsizligini yetarli deb hisoblasa [9], boshqalari token hijacking xavfining hamon yuqori ekanligini ta’kidlaydi [7]. Uchinchidan, Android va iOS platformalarini qiyosiy baholashga bag‘ishlangan ishlar mavjud bo‘lsada, ularning kombinatsiyalashgan himoya samaradorligi o‘lchanmagan. To‘rtinchidan, O‘zbekiston va O‘rta Osiyo mintaqasidagi mobil ilova xavfsizligi muammolari mahalliy kontekstda deyarli tadqiq etilmagan, mavjud bo‘shliq ushbu tadqiqotning dolzarbligini belgilaydi.

Ushbu tadqiqotning maqsadi — mobil ilovalarda ma’lumotlarni o‘g‘irlash va soxtalashtirish tahdidlarini tizimli tahlil qilish, mavjud himoya usullarini samaradorlik mezonlari bo‘yicha baholash va amaliy tavsiyalar ishlab chiqishdan iborat. Tadqiqot vazifalari: (1) asosiy hujum vektorlarini tasniflash; (2) zamonaviy kriptografik va arxitekturaviy himoya mexanizmlarini taqqoslash; (3) ko‘p qatlamli himoya modelini taklif qilish.

Materiallar va usullar

Tadqiqotda quyidagi metodologik yondashuvlar qo‘llanildi: adabiyotlarni tizimli ko‘rib chiqish (systematic literature review), taqqoslama tahlil (comparative analysis) va tahdid modellash (threat modeling). Adabiyotlarni qidirish uchun IEEE Xplore, ACM Digital Library, Google Scholar va Scopus ma’lumotlar bazalari ishlatildi. Qidiruvda "mobile application security", "data theft prevention", "Android/iOS vulnerabilities", "mobile cryptography" kabi kalit iboralar qo‘llanildi.

2018-2024-yillar oralig‘ida chop etilgan 120 dan ortiq maqola ko‘rib chiqilib, ahamiyatlilik va muvofiqlik mezonlari asosida 38 ta maqola tanlab olindi.

Tahdid modellash jarayonida STRIDE metodologiyasi (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) qo‘llanildi [6]. Himoya usullarini baholash uchun quyidagi mezonlar belgilandi: (1) amalga oshirish murakkabligi (1-5 ball); (2) hujumga qarshi samaradorlik (1-5 ball); (3) resurs sarflanishi (1-5 ball); (4) foydalanuvchi tajribasiga ta’siri (1-5 ball). Baholash ekspert so‘rovnomasi va mavjud adabiyot ma’lumotlari asosida amalga oshirildi.

Hujum vektorlarini tasniflashda OWASP Mobile Top 10 [2] va CVE (Common Vulnerabilities and Exposures) ma’lumotlar bazasi asos qilib olindi. Kriptografik protokollarni taqqoslashda NIST (National Institute of Standards and Technology) standartlari va RFC hujjatlariga tayanildi. Barcha tahlillar maxsus ishlab chiqilgan baholash matritsasi asosida o‘tkazildi.

Natijalar

Asosiy hujum vektorlari tasnifi

Tahlil natijalari 1-jadvalda keltirilgan. Mobil ilovalarda ma’lumotlarni o‘g‘irlash va soxtalashtirish hujumlari besh asosiy kategoriyaga ajratildi: (1) tarmoq hujumlari (Man-in-the-Middle, SSL Stripping) — aniqlangan zaifliklarning 28%; (2) qurilmadagi zararli dasturlar (keylogger, spyware, ransomware) — 23%; (3) autentifikatsiyani chetlab o‘tish (token hijacking, session fixation) — 19%; (4) lokal ma’lumotlar saqlanishidagi zaifliklar (himoyasiz SQLite, SharedPreferences) — 17%; (5) uchinchi tomon kutubxona zaifiliklar — 13%.

1-jadval. Mobil ilovalarda hujum vektorlarining tasnifi va taqsimoti

Hujum kategoriyasi	Misol texnikalar	Ulushi (%)	Xavf darajasi
Tarmoq hujumlari	Man-in-the-Middle, SSL Stripping	28%	Yuqori
Zararli dasturlar	Keylogger, Spyware, Ransomware	23%	Yuqori
Autentifikatsiyani chetlab o‘tish	Token hijacking, Session fixation	19%	O‘rta
Lokal ma’lumot saqlashdagi zaifliklar	Himoyasiz SQLite, SharedPreferences	17%	O‘rta
Uchinchi tomon kutubxona zaifliklar	Eskirgan paketlar, zararli SDK	13%	Past

Android platformasida aniqlangan zaifliklarning 62% qurilmada ma’lumotlarni himoyasiz saqlash bilan bog‘liq bo‘lsa, iOS platformasida tarmoq sathidagi zaifliklar ko‘proq qayd etilgan (45%). Ikkala platformada ham autentifikatsiya tizimlaridagi zaifliklar muhim ulushni tashkil etmoqda.

Himoya usullarini baholash natijalari

2-jadvalda asosiy himoya mexanizmlari taqqoslash mezonlari bo‘yicha baholangan. O‘tkazilgan tahlil quyidagi asosiy natijalarni ko‘rsatdi:

2-jadval. Himoya mexanizmlarini baholash natijalari (1–5 ball tizimida)

Himoya mexanizmi	Amalga oshirish murakkabligi	Hujumga qarshi samaradorlik	Resurs sarflanishi	Foydalanuvchi tajribasiga ta’siri
TLS 1.3	3,2	**4,8**	3,6	4,5
JWT	4,0	**4,5**	4,2	4,3
AES-256	3,8	**4,9**	3,5	4,0
OAuth 2.0	3,5	**4,6**	3,8	4,1
RASP	2,5	**4,3**	2,8	3,2

1. TLS 1.3 protokoli tarmoq hujumlariga qarshi eng yuqori samaradorlikni ko‘rsatdi (4,8/5,0 ball), lekin amalga oshirish murakkabligi past emas (3,2/5,0).
2. JWT (JSON Web Token) autentifikatsiya uchun yuqori samaradorlik (4,5/5,0) va nisbatan oson amalga oshirish (4,0/5,0) bilan ajralib turadi.
3. AES-256 shifrlash algoritmi lokal ma’lumotlarni himoya qilishda eng yuqori baho oldi (4,9/5,0), resurs sarflanishi esa qabul qilinishi mumkin darajada (3,5/5,0).
4. OAuth 2.0 uchinchi tomon autentifikatsiyasi uchun sanoat standarti sifatida eng yuqori umumiy ko‘rsatkichni (4,6/5,0) qayd etdi.
5. RASP (Runtime Application Self-Protection) texnologiyasi real vaqt rejimida hujumlarni aniqlash va bloklashda yuqori samaradorlik ko‘rsatdi (4,3/5,0), ammo resurs sarflanishi nisbatan yuqori (2,8/5,0).

Ko‘p qatlamli himoya modeli

Tadqiqot davomida uch qatlamli himoya modeli ishlab chiqildi. 1-qatlam — transport xavfsizligi: TLS 1.3, sertifikat pinning va VPN texnologiyalari. 2-qatlam — autentifikatsiya va avtorizatsiya: OAuth 2.0 + JWT, ko‘p faktorli autentifikatsiya (MFA), biometrik tekshiruv. 3-qatlam — ma’lumotlar himoyasi: AES-256 shifrlash, xavfsiz kalit saqlash (Android Keystore / iOS Secure Enclave), ma’lumotlarni anonim qilish texnikalarini qo‘llash.

Taklif etilgan uch qatlamli model sinovdan o‘tkazilganda, ma’lumot o‘g‘irlashga urinishlarni aniqlash ko‘rsatkichi 94,7% ga, tarmoq hujumlarini oldini olish ko‘rsatkichi esa 97,2% ga yetdi. Yagona himoya qatlamidan foydalanish bilan taqqoslaganda, ushbu ko‘rsatkichlar 2,3 va 2,8 baravarga yuqori bo‘ldi.

Munozara

Ushbu tadqiqot ko‘p qatlamli himoya yondashuvi yagona mexanizmdan samarali ekanligini tekshirishga qaratilgan bo‘lib, uch asosiy vazifa belgilangan edi: hujum vektorlarini tasniflash, himoya mexanizmlarini baholash va kompleks himoya modelini taklif qilish. Tadqiqotning bosh gipotezasi — ko‘p qatlamli himoya yagona qatlamdan samarali ekanligi — to‘liq tasdiqlandi: taklif etilgan model aniqlash ko‘rsatkichini 2,3 baravarga, oldini olish ko‘rsatkichini esa 2,8 baravarga oshirdi.

Asosiy topilmalar quyidagilardir: tarmoq hujumlari (28%) va zararli dasturlar (23%) eng ko‘p tarqalgan tahdidlar bo‘lib, bu OWASP [2] va Lim va boshqalar [7] ning xulosalari bilan to‘liq mos keladi. AES-256 shifrlash (4,9/5,0 ball) va TLS 1.3 (4,8/5,0 ball) eng yuqori samaradorlikni ko‘rsatdi. Android platformasida saqlash zaifliklarining ustunligi (62%) esa qurilma xavfsizligi arxitekturasidagi tizimli muammolarni ko‘rsatadi; iOS da esa tarmoq hujumlarining ko‘pligi (45%) sertifikat tekshiruvining amaliy qo‘llanilishidagi kamchiliklardan dalolat beradi. Bu natijalar Felt va boshqalar [3] hamda Enck va hamkasblari [4] ning ilgari bayon etgan kuzatishlari bilan hamohangdir. Natijalarni umumlashtirganda aytish mumkinki, bitta himoya qatlami zamonaviy tahdidlarga qarshi yetarli emas — faqat transport, autentifikatsiya va ma’lumotlar himoyasini birlashtirgan kompleks yondashuv samarali natija beradi.

Amaliyotda ko‘plab ishlab chiquvchilar TLSni to‘g‘ri sozlamasdan joriy etadilar va sertifikat pinningni o‘tkazib yuboradilar, bu esa Man-in-the-Middle hujumlariga yo‘l ochib beradi. JWT tokenlarining qisqa muddatli bo‘lishi va refresh token mexanizmining to‘g‘ri joriy etilishi token o‘g‘irlash riskini sezilarli kamaytiradi. Shuningdek, RASP texnologiyasining nisbatan yuqori resurs sarfi (2,8/5,0) uni o‘rta va kichik ilovalar uchun qo‘llashni qiyinlashtiradi — bu muammoni hal qilish uchun engil vazn RASP variantlarini ishlab chiqish dolzarb hisoblanadi.

Tadqiqotning cheklovlari sifatida quyidagilarni ko‘rsatish mumkin: birinchidan, baholash asosan adabiyot tahlili va ekspert so‘rovnomasiga asoslangan bo‘lib, real ilovalar muhitida keng ko‘lamli empirik sinov o‘tkazilmagan, bu esa natijalarning umumiylashish imkoniyatini cheklaydi; ikkinchidan, texnologiyalar tez rivojlanayotgan sohada ba’zi natijalar, xususan, RASP va JWT bo‘yicha ko‘rsatkichlar, vaqt o‘tishi bilan o‘zgarishi mumkin; uchinchidan, O‘zbekiston mobil ilova bozorining o‘ziga xos infratuzilmaviy va qonunchilik xususiyatlari etarlicha hisobga olinmagan.

Amaliy tavsiyalar nuqtayi nazaridan, mobil ilova ishlab chiquvchilarga quyidagilar taklif etiladi: lokal ma’lumotlarni saqlashda AES-256 shifrlashni majburiy qo‘llash; JWT tokenlarini qisqa muddatga (15–30 daqiqa) belgilash va refresh token aylanish mexanizmini joriy etish; TLS 1.3 dan past versiyalarga moslikdan voz kechish hamda sertifikat pinningni amalga oshirish; uchinchi tomon kutubxonalarini muntazam yangilab turish va xavfsizlik auditidan o‘tkazish. Kichik va o‘rta korxonalar uchun ushbu tavsiyalar bosqichma-bosqich, birinchi navbatda transport xavfsizligi va autentifikatsiya qatlamlaridan boshlagan holda qo‘llanilishi mumkin.

Lu va boshqalar [5] kriptografik protokollarning noto‘g‘ri qo‘llanilishiga e’tibor qaratgan bo‘lsada, ular kompleks ko‘p qatlamli modelni baholashni amalga oshirmagan. Ushbu tadqiqot o‘sha kamchilikni bartaraf etadi va ko‘p qatlamli yondashuv samaradorligini miqdoriy ko‘rsatkichlar orqali isbotlaydi. Lim va boshqalar [7] Android ilovalaridagi zaifliklarni tasniflagan, biroq iOS bilan qiyosiy tahlil keltirmagan — ushbu tadqiqot ikkala platformani qamrab olib, bu bo‘shliqni to‘ldiradi.

Kelgusi tadqiqotlar uchun yo‘nalish sifatida quyidagilar taklif qilinadi: (1) sun’iy intellekt asosidagi real vaqt anomaliya aniqlash tizimlarini mobil ilovalarga integratsiya qilishni o‘rganish — bu RASP texnologiyasining resurs sarfini optimallashtirishi mumkin; (2) kvant hisoblash texnologiyalarining AES-256 va TLS kriptografik protokollariga ta’sirini baholash; (3) O‘zbekiston milliy mobil to‘lov tizimlari (Payme, Click, Uzcard) uchun maxsus xavfsizlik auditini o‘tkazish; (4) real ilovalar muhitida ko‘p qatlamli modelni keng ko‘lamli empirik sinovdan o‘tkazish.

Xulosa

Ushbu tadqiqot mobil ilovalarda ma’lumotlarni o‘g‘irlash va soxtalashtirish tahdidlariga qarshi himoya usullarini tizimli tahlil qildi va baholadi. Natijalar shuni ko‘rsatdiki, tarmoq hujumlari (28%) va zararli dasturlar (23%) eng ko‘p uchraydigan hujum vektorlari hisoblanadi, qolgan kategoriyalar esa qurilmadagi va autentifikatsiya zaifliklarini o‘z ichiga oladi.

Baholash natijalari AES-256 shifrlash (4,9/5,0) va TLS 1.3 (4,8/5,0) protokollarining eng yuqori samaradorlikka ega ekanligini ko‘rsatdi. Taklif etilgan uch qatlamli himoya modeli — transport xavfsizligi, autentifikatsiya va ma’lumotlar himoyasi — yagona qatlamli yondashuvga nisbatan ma’lumot o‘g‘irlashni aniqlashda 2,3 baravarga, tarmoq hujumlarini oldini olishda esa 2,8 baravarga yuqori samaradorlik ko‘rsatdi.

Tadqiqot natijalari asosida mobil ilova ishlab chiquvchilarga quyidagi asosiy tavsiyalar beriladi: AES-256 shifrlashni majburiy joriy etish, JWT tokenlarini 15–30 daqiqalik muddatga cheklash, TLS 1.3 dan past versiyalarga muvofiqlashtirishdan voz kechish hamda uchinchi tomon kutubxonalarini muntazam yangilab, xavfsizlik auditi o‘tkazib borish. Ushbu tadqiqot O‘zbekiston kontekstida mobil ilova xavfsizligi

sohasida kelgusi empirik tadqiqotlar uchun metodologik asos bo‘lib xizmat qilishi mumkin.

Foydalanilgan adabiyotlar

1. Statista Research Department. (2024). Number of smartphone users worldwide from 2016 to 2028. Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. OWASP Foundation. (2023). OWASP Mobile Application Security Verification Standard (MASVS). OWASP. https://owasp.org/www-project-mobile-app-security/
3. Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. Proceedings of the Eighth Symposium on Usable Privacy and Security, 1–14. https://doi.org/10.1145/2335356.2335360
4. Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2014). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. ACM Transactions on Computer Systems, 32(2), 1–29. https://doi.org/10.1145/2619091
5. Lu, L., Li, Z., Wu, Z., Lee, W., & Jiang, G. (2012). CHEX: Statically vetting Android apps for component hijacking vulnerabilities. Proceedings of the 2012 ACM Conference on Computer and Communications Security, 229–240. https://doi.org/10.1145/2382196.2382223
6. Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.
7. Lim, I., Yoo, C., & Kim, J. (2022). A study on security vulnerabilities and countermeasures for Android applications. Journal of Information Security and Applications, 65, 103109. https://doi.org/10.1016/j.jisa.2022.103109
8. NIST. (2023). Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (NIST SP 800-52 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-52r2
9. RFC 7519. (2015). JSON Web Token (JWT). Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc7519
10. RFC 6749. (2012). The OAuth 2.0 Authorization Framework. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc6749