ISSN 2181-3187

BIOMETRIK AUTENTIFIKATSIYANING XAVFSIZLIK TAHDIDLARI VA HIMOYA USULLARI TAHLILI

Jabbarov Nuriddin Akbarovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, assistent
nuriddinjabbarov2606@gmail.com

Annotatsiya. Ushbu maqolada biometrik autentifikatsiya tizimlariga tahdid soluvchi xavfsizlik muammolari tahlil qilinadi hamda ularni bartaraf etish uchun mavjud texnik va tashkiliy himoya usullari ko‘rib chiqiladi. Avvalo, autentifikatsiya protokollariga nisbatan amalga oshiriladigan hujumlar — masqarad, takroriy uzatish, soxtalashtirish, kechiktirish va tanlangan matn asosidagi hujumlar turlari bayon qilinadi. Asosiy e’tibor biometrik autentifikatsiya vositalariga, xususan, foydalanuvchining barmoq izi, yuz tasviri yoki boshqa jismoniy-biologik belgilariga asoslangan tizimlarga qaratilgan. Har bir tahdid turi yuzaga kelish ssenariysi bilan birga tahlil qilinadi va unga nisbatan taklif etiladigan samarali himoya choralari — tiriklikni aniqlash texnologiyalari, kriptografik shifrlash, ko‘p faktorli autentifikatsiya, vaqt belgilari, sessiya nazorati kabi yondashuvlar bilan tavsiflanadi. Maqolada keltirilgan jadval biometrik autentifikatsiya tahdidlarini tizimli ko‘rinishda taqdim etib, ularni baholash va solishtirish imkonini beradi. Tadqiqot natijalari biometrik xavfsizlik tizimlarining samaradorligini oshirishga xizmat qiluvchi texnologik yechimlarni ishlab chiqishda muhim ahamiyat kasb etadi.

Kalit so‘zlar: biometrik autentifikatsiya, axborot xavfsizligi, tahdidlar, himoya usullari, spoofing, ko‘p faktorli autentifikatsiya, kriptografik himoya, tiriklikni aniqlash, autentifikatsiya protokoli, sessiya xavfsizligi.

Abstrakt. This paper analyzes the security threats to biometric authentication systems and reviews the existing technical and organizational protection methods to mitigate them. It first outlines common attacks on authentication protocols—such as masquerade, replay, spoofing, delay, and chosen-text attacks. Special attention is given

ISSN 2181-3187

to biometric authentication tools that rely on physical and biological characteristics of users, such as fingerprints, facial features, and others. Each type of threat is examined through possible attack scenarios, and corresponding countermeasures—such as liveness detection technologies, cryptographic encryption, multi-factor authentication, timestamps, and session control—are described in detail. A structured table presents a comparative analysis of biometric authentication threats, providing a clear framework for their evaluation. The results of this study are of practical significance for the development of effective technological solutions aimed at enhancing the reliability of biometric security systems.

Keywords: biometric authentication, information security, threats, protection methods, spoofing, multi-factor authentication, cryptographic protection, liveness detection, authentication protocol, session security.

KIRISH

Zamonaviy raqamli axborot muhitida foydalanuvchilarni aniqlash va ularga ruxsat berish mexanizmlari — autentifikatsiya tizimlari — axborot xavfsizligining ajralmas bo‘lagi hisoblanadi. An’anaviy parol, token yoki kartalarga asoslangan autentifikatsiya usullari qulay bo‘lishiga qaramay, ularning xavfsizlik darajasi tobora ortib borayotgan kiberhujumlar qarshisida yetarli darajada emasligi isbotlangan. Shu bois, oxirgi yillarda tabiiy va noyob fiziologik xususiyatlarga asoslangan biometrik autentifikatsiya tizimlariga e’tibor keskin oshdi.

Biometrik autentifikatsiya foydalanuvchining barmoq izi, yuz tasviri, ovoz ohangi, qadam tashlashi kabi belgilarini aniqlab, ularni identifikatsiya qilish orqali tizimga kirish imkonini beradi. Bu yondashuv, boshqa usullarga nisbatan qulayroq va xavfsizroq bo‘lib ko‘rinsa-da, o‘ziga xos tahdidlar va zaifliklarga ega. Biometrik ma’lumotlarning o‘zgartirib bo‘lmasligi, soxtalashtirish usullarining rivojlanishi, shuningdek, hujumchilarning turli texnik vositalardan foydalangan holda tizimlarni

ISSN 2181-3187

aldashga bo‘lgan urinishi, bu autentifikatsiya usulini yanada chuqurroq o‘rganishni talab qiladi [1].

Ushbu maqolada biometrik autentifikatsiyaga nisbatan mavjud xavfsizlik tahdidlari tahlil qilinadi, hujum turlari klassifikatsiya qilinadi va har bir hujumga qarshi samarali himoya choralarining texnik asoslari bayon etiladi. Maqolaning asosiy maqsadi — autentifikatsiya tizimlarining ishonchliligini oshirishga qaratilgan amaliy tavsiyalarni shakllantirishdan iborat.

NATIJALAR

Autentifikatsiya protokollariga bo‘ladigan asosiy hujumlar quyidagilar:

- maskarad (imitation) hujumi. Foydalanuvchi o‘zini boshqa shaxs sifatida ko‘rsatishga urinadi va shu orqali o‘sha shaxsga berilgan imkoniyatlar va imtiyozlardan foydalanishni maqsad qiladi;

- autentifikatsiya almashinuvida tarafni almashtirish (interleaving attack). Bu hujumda hujumchi ikki tomon orasidagi autentifikatsiya almashinuvi jarayonidagi trafikni o‘zgartirishga harakat qiladi. Bu almashtirishning turlari quyidagicha bo‘lishi mumkin: ikki foydalanuvchi o‘rtasida autentifikatsiya muvaffaqiyatli o‘tadi va ulanish o‘rnatiladi, ammo hujumchi ulardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

- takroriy uzatish (replay attack). Bu hujumda foydalanuvchilardan biri tomonidan yuborilgan autentifikatsiya ma’lumotlari qayta-qayta uzatiladi, shu bilan tizimni aldashga harakat qilinadi;

- uzatishni qaytarish (reflection attack). Takroriy uzatish hujumining bir turi bo‘lib, hujumchi ushlab qolgan sessiya ma’lumotlarini protokolga orqaga qaytaradi va shu yo‘l bilan autentifikatsiyani buzishga urinadi;

ISSN 2181-3187

- majburiy kechikish (forced delay). Hujumchi ma’lumotni ushlab qolib, uni ma’lum vaqt o‘tgach yuboradi, tizimning ish faoliyatini sekinlashtirish yoki xatolik yuzaga keltirish maqsadida amalga oshiriladi;

- matn tanlashli hujum (chosen text attack). Hujumchi autentifikatsiya trafigini ushlab qolib, uni maxsus tanlangan matnlar bilan almashtirib, uzoq muddatli kriptografik kalitlar haqida ma’lumot olishga urinadi [2].

Autentifikatsiya usullariga qaratilgan hujumlar:

1. Siz bilgan biror narsa usuli bilan autentifikatsiyani buzishga qaratilgan hujum turlari:

a. Parollar lug‘at hujumi (dictionary attack). Eng ko‘p ishlatiladigan parollar ro‘yxatidan foydalanib, tizimga kirishga harakat qilinadi;

b. Parol variantlarini sinash (Brute force hujumi). Parolning barcha mumkin bo‘lgan kombinatsiyalari ketma-ket sinab ko‘riladi;

c. “Yelka orqali qarash” (shoulder surfing). Foydalanuvchi parolni kiritayotgan paytda uning yonida turib, ko‘z bilan ko‘rib olish orqali parolni o‘g‘irlash;

d. Zararli dasturlar orqali hujum (keylogger va boshqa). Maxsus zararli dastur foydalanuvchi kompyuteriga o‘rnatilib, klaviaturadan kiritilgan barcha ma’lumotlarni, jumladan parollarni ham, hujumchining serveriga yuboradi.

2. Sizda mavjud biror narsa usuli bilan autentifikatsiyani buzishga qaratilgan hujum turlari:

a. Fizik o‘g‘irlash. Bu hujumda hujumchi foydalanuvchining tokeni yoki smart kartasini o‘g‘irlab, tizimga kirishga urinadi. Bu ushbu autentifikatsiya turidagi eng xavfli hujum hisoblanadi;

b. Dasturiy tokenlarning zaifligi. Ayrim tokenlar dasturiy shaklda (masalan, ilova tarzida) bo‘lib, zararli dasturlarga qarshi zaif bo‘lishi mumkin;

ISSN 2181-3187

c. Mobil qurilmalardagi tokenlar. Dasturiy ko‘rinishdagi tokenlar mobil qurilmalarda ishlaydi va bu qurilmalarga zararli dastur o‘rnatilgan bo‘lsa, token boshqarib olinishi mumkin.

3. Sizning biror narsangiz — biometrik autentifikatsiyani buzishga qaratilgan hujum turlari:

a. Qalbakilashtirish (spoofing). Bu turdagi hujumda biometrik parametrni soxtalashtirish orqali tizimni aldashga urinish amalga oshiriladi. Misol uchun, yuz tuzilishi o‘xshash bo‘lgan shaxs (masalan, Xasan o‘rniga Xusan) autentifikatsiyadan o‘tishga urinadi yoki sifatli foydalanuvchi yuz surati orqali tizimni chalg‘itishga harakat qiladi;

b. Biometrik ma’lumotlar bazasini buzish. Ushbu hujumda tizimda saqlanayotgan biometrik ma’lumotlar (barmoq izi, yuz tasviri va boshqalar) o‘zgartiriladi. Ya’ni, haqiqiy foydalanuvchining biometrik parametrlari hujumchining ma’lumotlari bilan almashtiriladi, natijada tizimga hujumchi o‘zini haqiqiy foydalanuvchi sifatida tanitib kira oladi [3].

Autentifikatsiya usullariga qaratilgan hujumlarni oldini olish choralari. Har bir autentifikatsiya usuli uchun unga xos himoya mexanizmlari mavjud. Shu bilan birga, umumiy xavfsizlikni ta'minlash va hujumlarni oldini olish maqsadida quyidagi choralar tavsiya etiladi:

- murakkab parollardan foydalanish. Bu usul lug‘at asosidagi hujumlar va barcha mumkin bo‘lgan parol variantlarini sinab ko‘rish (brute-force) hujumlarini samarali tarzda bartaraf etishga yordam beradi;
- ko‘p faktorli autentifikatsiya (MFA) qo‘llash. Bu usul autentifikatsiyaning bir nechta omiliga (masalan, parol + barmoq izi yoki token) asoslanadi va yuqorida tilga olingan deyarli barcha hujumlarga qarshi yuqori darajadagi himoya ta’minlaydi;

ISSN 2181-3187

- token va qurilmalarni xavfsiz saqlash. Jismoniy autentifikatsiya vositalarining o‘g‘irlanishi yoki zararli dasturlar ta’siriga tushib qolishining oldini olish uchun tokenlarni xavfsiz muhitda saqlash tavsiya etiladi;

- tiriklikni aniqlash texnologiyalaridan foydalanish. Biometrik autentifikatsiyada statik tasvir yoki qalbaki biometrik namunalar orqali amalga oshiriladigan hujumlarga qarshi tiriklikni aniqlash (liveness detection) samarali himoya chorasi hisoblanadi.

Yuqorida ko‘rib chiqilgan autentifikatsiya protokollariga qaratilgan hujumlarning oldini olish va ularning xavfsizligini ta’minlash uchun quyidagi texnik yechimlar qo‘llaniladi:

- so‘rov–javob mexanizmlari, vaqt belgilari, tasodifiy sonlar, identifikatorlar va raqamli imzolar kabi himoya vositalaridan foydalanish. Bu elementlar orqali ma’lumotlarning haqiqiyligini tekshirish va takroriy hujumlarning (replay attack) oldini olish mumkin;

- autentifikatsiya natijasini foydalanuvchining tizimdagi keyingi faoliyatiga bog‘lash. Bunday yondashuvda foydalanuvchi autentifikatsiyadan o‘tgach, uning keyingi muloqoti uchun maxfiy seans kalitlari shakllantiriladi. Bu esa autentifikatsiyadan keyingi uzatiladigan axborotning butligini va maxfiyligini ta’minlaydi;

- tizim bilan o‘rnatilgan seans davomida vaqti-vaqti bilan autentifikatsiyani qayta bajarish. Bu usul foydalanuvchining seansidan noto‘g‘ri foydalanish yoki sessiya o‘g‘irlanishining oldini olishga yordam beradi.

“So‘rov–javob” mexanizmi autentifikatsiyada foydalanuvchini aniqlashning samarali usullaridan biridir. Agar A foydalanuvchi V foydalanuvchi yuborgan xabar haqiqiyligiga shubha qilsa, u holda V ga tasodifiy tarzda tanlangan, oldindan ma’lum bo‘lmagan X qiymatini yuboradi. Keyin, V foydalanuvchi ushbu X qiymatiga maxsus amal – masalan, f(X) funksiyasini bajaradi va natijani A ga qaytaradi. Chunki X

ISSN 2181-3187

tasodifiy tanlanadi, V bu amalni faqatgina so‘rov kelgandan keyin bajara oladi. Shundan so‘ng, A foydalanuvchi natijani tekshiradi va shu orqali V foydalanuvchi aslida kimligini tasdiqlaydi. Kamchiligi shundaki, agar hujumchi yetarlicha so‘rov-javob namunalarini qo‘lga kiritsa, u funksiyadagi andozani aniqlashi va keyingi autentifikatsiya jarayonlarini aldashi mumkin [4].

Vaqtni belgilash usuli har bir yuborilgan xabarga maxsus vaqt ko‘rsatkichini qo‘shishni nazarda tutadi. Bu orqali tarmoqdagi foydalanuvchi har bir xabarning yangilik darajasini baholay oladi va agar u juda eski deb topilsa, uni rad etish huquqiga ega bo‘ladi, chunki bu xabar soxtalashtirilgan bo‘lishi ehtimoli bor.

Biroq, vaqt belgilashga asoslangan autentifikatsiyada qabul qilinadigan kechikish vaqtini aniqlash muammosi yuzaga keladi. Chunki vaqt belgisi qo‘shilgan xabar bir zumda manzildan manzilga yetib bora olmaydi. Bundan tashqari, xabar jo‘natuvchi va qabul qiluvchining tizimlaridagi soatlar ham har doim bir xil aniqlikda ishlamaydi, ya’ni ular orasida muvofiqlik (sinxronlik) bo‘lmasligi mumkin.

Autentifikatsiya protokollarini solishtirish va tanlashda quyidagi muhim omillar e’tiborga olinadi [5]:

- o‘zaro autentifikatsiya imkoniyati. Bu xususiyat autentifikatsiya jarayonida ikki tomon bir-birining haqiqiyligini tekshirishi zarur bo‘lgan holatlarni bildiradi;
- hisoblashda samaradorlik. Autentifikatsiya protokolini bajarish uchun kerak bo‘ladigan hisoblash amallari soni bilan bog‘liq bo‘lgan mezon;
- aloqadagi samaradorlik. Bu parametr autentifikatsiya uchun uzatiladigan xabarlar soni va ularning hajmini bildiradi;
- uchinchi tomon ishtiroki. Ba’zi protokollar qo‘shimcha ishonchli tomonlarga (masalan, simmetrik kalitlarni tarqatadigan server yoki sertifikatlarni boshqaruvchi markaz) tayanadi;

ISSN 2181-3187

 xavfsizlik asoslari. Protokolning xavfsizligi qanday asoslar bilan ta’minlanganligini ko‘rsatadi. Misol uchun, nollik bilim asosidagi isbot mexanizmlari keltirilishi mumkin;

maxfiylikni ta’minlash. Protokolda maxfiy kalit yoki boshqa muhim ma’lumotlarni saqlash va himoyalash mexanizmlarining mavjudligi nazarda tutiladi.

1-jadval

Biometrik autentifikatsiyaga qarshi tahdidlar va ularning himoya usullarining tahliliy jadvali

Hujum turi Hujum ta'rifi Ta'sir doirasi Himoya usullari Izoh

Maskarad (Imitation) Foydalanuvchi o‘zini boshqa shaxs sifatida ko‘rsatishga urinadi Autentifikatsiya tizimlariKo‘p faktorli autentifikatsiya, tiriklikni aniqlash texnologiyalari Foydalanuvchi o‘rniga kirish uchun eng ko‘p uchraydigan hujum turi bo‘lib, uni aniqlash qiyin bo‘lishi mumkin.

Autentifikatsiya almashinuvida tarafni almashtirish (Interleaving attack) Hujumchi ikki tomon o‘rtasidagi autentifikatsiya ma'lumotlarini almashtiradi Protokol darajasi So‘rov–javob mexanizmlari, vaqt belgilari, raqamli imzolar Ushbu hujumda hujumchi sessiya davomida boshqaruvni qo‘lga olishga harakat qiladi, bu seans xavfsizligini buzadi.

Takroriy uzatish (Replay attack) Avvalgi autentifikatsiya ma’lumotlarini qayta-qayta yuboradi Tarmoq va autentifikatsiya Vaqt belgilaridan foydalanish, seans identifikatorlari Ko‘p hollarda real vaqt belgilash tizimi yo‘qligida yuzaga keladi, tizimni aldashga qaratilgan oddiy va samarali hujum.

Uzatishni qaytarish (Reflection attack) Hujumchi ushlab qolgan ma'lumotlarni orqaga qaytaradi Tarmoq va protokol Maxsus autentifikatsiya mexanizmlari,

ISSN 2181-3187

qo‘shimcha tekshiruvlar Replay hujumining o‘ziga xos shakli bo‘lib, tizimdan o‘zini himoya qilish uchun qo‘shimcha protokol talab qiladi.

Majburiy kechikish (Forced delay) Ma’lumotni ushlab, keyin yuborish orqali tizim ish faoliyatini buzadi Tizim ish faoliyati Monitoring, vaqt cheklovlari Ushbu hujum tizimning xizmat ko‘rsatish vaqtini pasaytirishga yoki DoS hujumlariga yo‘l ochadi.

Matn tanlashli hujum (Chosen text attack) Maxsus tanlangan autentifikatsiya trafigi orqali kalitlarni aniqlashga urinish Kriptografik tizimlar Kriptografik protokollar, kalitlarni muntazam yangilash Juda murakkab va xavfli hujum turi bo‘lib, kalitlar xavfsizligini sinovdan o‘tkazadi.

1-jadvaldagi ma’lumotlar asosida ko‘rishimiz mumkinki, biometrik autentifikatsiya tizimlaridagi turli hujum turlari o‘zaro xavf darajasi va qo‘llaniladigan himoya usullari bo‘yicha farq qiladi. Masalan, maskarad (imitation) hujumi biometrik tizimlarda foydalanuvchi shaxsini soxtalashtirish orqali tizimga noqonuniy kirishga urinishni anglatadi va bu eng jiddiy tahdidlar sirasiga kiradi. Shu bilan birga, autentifikatsiya almashinuvida tarafni almashtirish (interleaving attack) kabi hujumlar tizim va foydalanuvchi o‘rtasidagi trafikni manipulyatsiya qilishni o‘z ichiga oladi, bu esa sezilarli xavfsizlik zaifliklarini keltirib chiqaradi.

Takroriy uzatish (replay attack) va uzatishni qaytarish (reflection attack) hujumlari autentifikatsiya ma’lumotlarining qayta ishlatilishi yoki orqaga yuborilishi orqali amalga oshiriladi, bu esa tizimning soxtalashtirilgan sessiyalarni qabul qilishiga sabab bo‘ladi. Majburiy kechikish (forced delay) va matn tanlashli (chosen text) hujumlar esa tizim ish faoliyatiga ta’sir ko‘rsatib, uni sekinlashtirish yoki kriptografik kalitlar haqidagi ma’lumotlarni oshkor qilishga urinadi.

ISSN 2181-3187

Shuningdek, autentifikatsiyaning turli usullariga qarshi hujumlar ham o‘zaro farqlanadi. Masalan, parol asosidagi hujumlarda lug‘at hujumi va kuchli sinovlar keng tarqalgan bo‘lsa, “yelka orqali qarash” va zararli dasturiy ta’minot yordamida ma’lumot o‘g‘irlash ham katta xavf tug‘diradi. Fizik tokenlarning o‘g‘irlanishi yoki mobil qurilmalardagi tokenlarning boshqaruvini yo‘qotishi kabi holatlar esa aynan “sizda mavjud narsangiz” turidagi autentifikatsiyaga xavf soladi.

Biometrik autentifikatsiyada esa qalbakilashtirish (spoofing) va biometrik ma’lumotlar bazasini buzish kabi hujumlar eng ko‘zga ko‘ringan tahdidlar hisoblanadi, chunki ular foydalanuvchi shaxsini aldashga to‘g‘ridan-to‘g‘ri ta’sir qiladi.

Jadvaldan ko‘rinib turibdiki, har bir hujum turiga qarshi o‘ziga xos himoya choralarini qo‘llash zarur. Masalan, murakkab parollar va ko‘p faktorli autentifikatsiya tizimlari hujumlarning aksariyat turini oldini olishda samarali bo‘ladi. Tokenlarni va qurilmalarni xavfsiz saqlash, shuningdek tiriklikni aniqlash texnologiyalaridan foydalanish biometrik autentifikatsiya tizimlarining xavfsizligini oshiradi.

Umuman olganda, jadval xavfsizlik tahdidlarining har bir turi va ularning oldini olish usullarini tizimli ko‘rinishda taqdim etib, autentifikatsiya protokollarining kuchli va zaif tomonlarini yaxshiroq tushunishga yordam beradi.

XULOSA

Biometrik autentifikatsiya tizimlari zamonaviy axborot xavfsizligi infratuzilmasining ajralmas qismi sifatida tobora keng qo‘llanilmoqda. Ularning asosiy afzalliklari — foydalanuvchi qulayligi, yuqori darajadagi aniqlik va parol kabi unutiluvchi omillarga bog‘liqlikning yo‘qligi — bu texnologiyani an’anaviy autentifikatsiya usullariga kuchli muqobil sifatida ko‘rsatmoqda. Biroq, tahlillar shuni ko‘rsatadiki, bu tizimlar ham turli ko‘rinishdagi kiberhujumlar — xususan, spoofing, qayta uzatish, baza ma’lumotlarini buzish kabi xavflarga duch keladi.

Ushbu maqolada biometrik autentifikatsiyaga nisbatan mavjud tahdidlar chuqur tahlil qilinib, har bir hujumga qarshi samarali texnik va tashkiliy himoya choralarining

ISSN 2181-3187

dolzarbligi asoslab berildi. Ayniqsa, tiriklikni aniqlash (liveness detection), ko‘p faktorli autentifikatsiya (MFA), kriptografik himoya mexanizmlari, vaqt belgilaridan foydalanish, seanslarni boshqarish kabi yondashuvlar xavfsizlik darajasini sezilarli oshirishga xizmat qiladi.

Biometrik autentifikatsiya tizimlarining ishonchliligini yanada mustahkamlash uchun ularning arxitekturasida xavfsizlikning "by design" tamoyiliga amal qilish, hujum modellari asosida muntazam xavf tahlilini o‘tkazish, shuningdek, foydalanuvchilarni xabardor qilish va maxfiylik masalalariga jiddiy yondashish zarur. Maqolada taqdim etilgan tahlil natijalari, ilmiy hamda amaliy jihatdan biometrik autentifikatsiyaning xavfsizlik darajasini baholash va yanada takomillashtirishga xizmat qiluvchi muhim asos bo‘lib xizmat qiladi.

ADABIYOTLAR RO‘YXATI

1. Чистов Д.А., Серов Д.В. Методы обеспечения информационной безопасности биометрических систем. // Информационные технологии и безопасность. — 2021. — №4. — С. 22–30.

2. Jain, A. K., Ross, A., & Nandakumar, K. Introduction to Biometrics. — Springer Science & Business Media, 2011. — 312 p.

3. Zhuang, Y., & Gavrilova, M. L. Multimodal Biometrics and Intelligent Image Processing for Security Systems. — IGI Global, 2013.

4. International Organization for Standardization. ISO/IEC 24745:2011 — Information technology — Security techniques — Biometric information protection. — Geneva: ISO, 2011.

5. Stallings, W. Cryptography and Network Security: Principles and Practice. 8th ed. — Pearson, 2023. — 752 p.