ISSN 3060-4567

AXBOROT XAVFSIZLIGINI TA'MINLASHDA IDENTIFIKATSIYA VA AUTENTIFIKATSIYA TIZIMLARINING AHAMIYATI

Shukurov Orziqul Pardayevich

Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,

e-mail: norkuvvatchunaev@gmail.com

***Annotatsiya**: Bugungi kunda axborot xavfsizligini ta'minlash juda dolzarb muammolardan biriga aylanib bormoqda. Mazkur maqolada identifikatsiya va autentifikatsiya jarayonlaring axborot xavfsizligini ta'minlashdagi ahamiyati qaratilgan bo'lib, identifikatsiya va autentifikatsiya tizimlari turlari haqida ma'lumot keltirilgan.*

***Kalit so'zlar**: identifikatsiya, autentifikatsiya, avtorizatsiya, kiberxavfsizlik, biometrika, bir faktorli va ko'p faktorli autentifikatsiya .*

Axborot xavfsizligi tizimlarining asosiy elementlaridan biri bu identifikatsiya (foydalanuvchini tanish) va autentifikatsiya (uning haqiqatda kimligini tekshirish) jarayonlaridir. Ular foydalanuvchilarga tizimlarga kirish ruxsatini berish va resurslarga huquqli kirishni cheklash imkonini yaratadi. Ammo zamonaviy kiberjinoyatlar fonida bu jarayonlar tobora murakkablashib bormoqda.

Bugungi kunda kiberjinoyatchilar an'anaviy login-parol tizimlaridan tortib, ikki omilli autentifikatsiyalarga, hatto biometrik autentifikatsiya tizimlariga qarshi ham murakkab hujumlar uyushtirmoqda.

Kompyuter tizimida ro'yxatga olingan har bir sub'ekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma'noda indentifikatsiyalovchi axborot bog'liq. Bu ushbu sub'ektga nom beruvchi son yoki simvollar satri bo'lishi mumkin. Bu axborot sub'ekt indentifikatori deb yuritiladi. Agar foydalanuvchi tarmoqda ro'yxatga olingan indentifikatorga ega bo'lsa u legal (qonuniy), aks holda legal bo'lmagan (noqonuniy) foydalanuvchi hisoblanadi.

ISSN 3060-4567

Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o‘tishi lozim.

Identifikatsiya (Identification) - foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funktsiyadir. Foydalanuvchi tizimga uning so‘rovi bo‘yicha o‘zining identifikatorini bildiradi, tizim esa o‘zining ma’lumotlar bazasida uning borligini tekshiradi.

Autentifikatsiya (Authentication) - ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o‘zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o‘tqazishda tekshiruvchi taraf tekshiriluvchi tarafning xaqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi. Odatda foydalanuvchi tizimga o‘z xususidagi noyob, boshqalarga ma’lum bo‘lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya sub’ektlarning (foydalanuvchilarning) haqiqiy ekanligini aniqlash va tekshirishning o‘zaro bog‘langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog‘liq. Sub’ektni identifikatsiyalash va autentifikatsiyalashdan so‘ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (Authorization) - subektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya sub’ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning konfidentsialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog‘langan.

Autentifikatsiya qilish omillari tizim har kimga biron bir narsaga kirish huquqini berishdan oldin shaxsini tasdiqlash uchun foydalanadigan ko‘plab turli elementlarni aniqlaydi. Shaxsning identifikatori shaxs nimani bilishi mumkinligini aniqlaishi mumkin va xavfsizlik to‘g‘risida gap ketganda, tizimda kimgadir ruxsat

ISSN 3060-4567

berish uchun kamida ikkita yoki uchta autentifikatsiya qilish omillarini tekshirish kerak. Xavfsizlik darajasiga qarab, autentifikatsiya qilish omillari quyidagilarda bir biridan farq qilishi mumkin.

Bir faktorli autentifikatsiya - bu autentifikatsiya jarayonining eng oddiy shakli bo‘lib, foydalanuvchiga veb-sayt yoki tarmoqda muayyan tizimga kirish huquqini berish uchun parolni talab qiladi. Shaxs identifikatorini tekshirish uchun faqat bitta ma’lumotlardan foydalanib tizimga kirishni amalga oshirishi mumkin. Masalan, foydalanuvchi nomiga tegishli parolnigina talab qilish orqali faqat bitta faktorli autentifikatsiya yordamida login ma’lumotlarini tekshirishi mumkin.

Bir faktorli autentifikatsiya: Ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma’lumotni ham talab qiladi. Foydalanuvchi nomi va parolni maxfiy ma’lumotlar bilan birgalikda ishlatish xakerlarga muhim va shaxsiy ma’lumotlarni o‘g‘irlashni ancha qiyinlashtiradi.

Ko‘p faktorli autentifikatsiya: Bu autentifikatsiyaning eng ilg‘or usuli bo‘lib, foydalanuvchilarga tizimga kirish huquqini berish uchun mustaqil autentifikatsiya kategoriyalaridan ikki yoki undan ko‘p darajadagi xavfsizlikni talab qiladi. Autentifikatsiya qilishning ushbu shakli har qanday ma’lumotlarga ta’sir qilishni bartaraf etish uchun bir-biridan mustaqil bo‘lgan omillardan foydalanadi. Moliyaviy tashkilotlar, banklar va huquqni muhofaza qilish idoralarida ko‘p faktorli autentifikatsiyadan foydalanish odatiy holdir.

Avtorizatsiya sizning shaxsingiz tizim tomonidan muvaffaqiyatli tasdiqlanganidan so‘ng amalga oshiriladi. Shuning uchun sizga ma’lumot, fayllar, ma’lumotlar bazalari, fondlar va boshqa manbalarga to‘liq kirish huquqini beradi. Ammo avtorizatsiya sizning kirish huquqingizni aniqlagandan keyingina manbalarga kirish huquqini tasdiqlaydi. Boshqacha qilib aytganda, avtorizatsiya - bu autentifikatsiya qilingan foydalanuvchining muayyan manbalardan foydalana olishini aniqlatuvchi jarayon hisoblanadi. Autentifikatsiya orqali xodimning identifikatori va parollarini tekshirilib, tasdiqlanganidan so‘ng, keyingi qadam qaysi xodimning qaysi

ISSN 3060-4567

qavatga kirish huquqiga ega ekanligi va bu avtorizatsiya orqali nimalarni amalga oshirilishini aniqlash imkonini beradi.

Tizimga kirish autentifikatsiya va avtorizatsiya bilan himoyalangan va ular ko‘pincha bir-biri bilan birgalikda ishlatiladi. Garchi ikkalasi ham bundan keyin turli xil tushunchalarga ega bo‘lsa ham, ular veb-servis infratuzilmasi uchun, ayniqsa tizimga kirish huquqi haqida gap ketganda juda muhimdir. Har bir atamani tushunish juda muhim va xavfsizlikning muhim jihati hisoblanadi.

Identifikatsiya va autentifikatsiya tizimlari kiberxavfsizlikning birinchi mudofaa chizig‘i hisoblanadi. Ularning zaifligi barcha axborot resurslari xavfsizligiga tahdid soladi. Bugungi tahdidlar tobora murakkablashib borayotganligi sababli, parolga asoslangan yondashuvlar o‘z ahamiyatini yo‘qotmoqda. Shuning uchun ham kombinatsiyalangan, foydalanuvchi xatti-harakatlariga asoslangan va AI yordami bilan ishlovchi tizimlar kelajakda keng joriy etilishi kutilmoqda.

Biometrik identifikatsiya — bu foydalanuvchini tanib olish usuli bo‘lib, u insonning noyob jismoniy yoki xulq-atvorga oid xususiyatlariga asoslanadi. Ushbu usulda foydalanuvchining barmoq izi, yuz tuzilishi, ko‘z to‘r pardasi, ovozi yoki hatto yurish uslubi kabi biometrik belgilar aniqlanadi va ular orqali autentifikatsiya amalga oshiriladi.

Bunday tizimlar foydalanuvchi haqida oldindan yozib olingan biometrik ma’lumotlarni saqlaydi. Kirish vaqtida foydalanuvchi o‘z biometrik belgilarini taqdim etadi va tizim ushbu ma’lumotlarni oldingi yozuvlar bilan solishtirib, shaxsni aniqlaydi.

Biometrik identifikatsiya an’anaviy usullarga nisbatan xavfsizroq hisoblanadi, chunki biometrik belgilarni unutib bo‘lmaydi, ularni boshqa birovga topshirib bo‘lmaydi va ularni qalbakilashtirish anchayin mushkul. Shu boisdan, bu usul ko‘plab zamonaviy xavfsizlik tizimlarida keng qo‘llanilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. Xabibullayev J.D., DDoS-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili // Лучшие интеллектуальные

исследования, 2025-yil 26-fevral. Vol. 39, №-3. –b 121-131.

2. Chunayev N.E., Xabibullayev J.D., Application of blockchain technology to ensuring reliability and data security in the internet of things, “Moliya-kredit tizimini strategik rivojlantirishning muammolari va ustuvor yo‘nalishlari” mavzusida xalqaro ilmiy-amaliy konferensiya 2024-yil 25-aprel. –b. 27-29.

3. https://uzbekdevs.uz/maqolalar/axborot-xavfsizligida-identifikatsiya-va-autentifikatsiya