Emro Science and Education
International open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · "Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnol... DOI: 10.5281/zenodo.24319020

materiallar to'plami

MOBIL ALOQA AVLODLARIDA MOBIL STANSIYA VA BAZA STANSIYALARINING IDENTIFIKATSIYA VA AUTENTIFIKATSIYA MASALALARINI TADQIQ QILISH.

Karimov Sodiq – TATU Nurafshon filiali assistenti

Annotatsiya. 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 konfidensialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma'murlash muolajasi uzviy bog'langan.

Kalit.zo'zlar: Avtorizatsiya (Authorization), Autentifikatsiya va avtorizatsiya

Mobil aloqa tizimlarining tuzilishi va ishlashi.

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].

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. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi komp'yuter tizimining identifikatsiya va autentifikatsiya jarayonidan o'tishi lozim [2].

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

Published: 10.11.2023

Cite this article: Karimov Sodiq (2023). Mobil aloqa avlodlarida mobil stansiya va baza stansiyalarining identifikatsiya va autentifikatsiya masalalarini tadqiq qilish. Emro Science and Education, 1(1). https://doi.org/10.5281/zenodo.24319020

© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

materiallar to‘plami



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 (foydalanuvchi-larning) 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 konfidensialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog‘langan.

Ma’murlash (Accounting) – foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, taxlillash va ularga mos reaksiya ko‘rsatish uchun juda muhimdir. Autentifikatsiya protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarni hisobga olish zarur:

- o‘zaro autentifikatsiyaning mavjudligi. Ushbu xususiyat autentifikatsion almashinuv taraflari o‘rtasida ikkiyoqlama autentifikatsiyaning zarurligini aks ettiradi;
- hisoblash samaradorligi. Protokolni bajarishda zarur bo‘lgan amallar soni;
- kommunikatsion samaradorlik. Ushbu xususiyat autentifikatsiyani bajarish uchun zarur bo‘lgan xabar soni va uzunligini aks ettiradi;
- uchinchi tarafning mavjudligi. Uchinchi tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko‘rsatish mumkin;

- xavfsizlik kafolati asosi. Misol sifatida nullik bilim bilan isbotlash xususiyatiga ega bo‘lgan protokollarni ko‘rsatish mumkin;
- sirni saqlash. Jiddiy kalitli axborotni saqlash usuli ko‘zda tutiladi.

Bir martalik yostiqlar

Yostiqchining bir martalik autentifikatsiyasi har ikki tomonli raqamlar, so'zlar yoki belgilar juftlarining bir xil ro'yxatiga ega bo'lishini talab qiladi. Eng xavfsiz ro'yxatlar tasodifiy ravishda tuziladi. Bir tomoni (Elis) boshqasi (Bob) bilan almashtirishni talab qilganda, Bob Elisga ro'yxatdan tanlangan narsalardan biri shaklida da'vo yuboradi. Elis mos keladigan moslashtirilgan element bilan javob berishi kerak (1-1-rasm). Qiyinchilik ishlatilgandan so'ng, u ro'yxatdan chiqib ketadi va boshqa ishlatilmaydi.



1-1-rasm **Bir martalik yostiqlar yordamida autentifikatsiya qilish**

Bir martalik yostiqni autentifikatsiya qilishning bir martalik xususiyati shafqatsiz kuch hujumi bilan biron bir muayyan chaqiriqqa tegishli javobni taxmin qilishni imkonsiz qiladi, ya'ni to'g'ri javobni urmaguncha turli xil javoblar bilan takroran javob berish orqali. Xuddi shunday, keyingi qiyinchilik qanday bo'lishi kerakligini taxmin qilishning iloji yo'q. Ro'yxatlar haqiqatan ham tasodifiy ravishda yaratilgan deb taxmin qilsak, bunday tizimni buzishning yagona yo'li bu juftliklar ro'yxati tarkibining ba'zi bir qismlarini bilishdir. Shu sababli, bir martalik maydonchani xavfsiz ulashgandan so'ng, uni xavfli aloqa kanallari orqali ishlatish mumkin. Agar kimdir aloqani yashirsa, ular ushbu javob-javob juftligini olishlari mumkin. Biroq, bu ma'lumot ularga hech qanday foyda keltirmaydi, chunki bu muammo endi hech qachon takrorlanmaydi.

Chaqiriqlarga javob beradigan juftliklar bilan bog'liq birinchi muammo shundaki, kompyuterlarda chindan ham tasodifiy ro'yxatlarni yaratish qiyin. Pseudorandom ro'yxatlarini olish ancha osonroq va to'g'ri algoritm va urug 'qiymati bo'yicha taxminni hisobga olgan holda (hech bo'lmaganda) takrorlanishi mumkin. Ikkinchi muammo shundaki, bu usul har bir muxbir juftligi o'ziga xos ro'yxatlar to'plamiga ega bo'lgan taqdirdagina foydalidir. Aks holda, ro'yxatning qaysi egasi autentifikatsiya qilinishini

aniqlash mumkin emas. Va nihoyat, har qanday umumiy maxfiy usulda bo'lgani kabi, ro'yxatlar ham baham ko'rilganda va ularni xavfsiz saqlashda sir tutilishi kerak. Agar ro'yxatlardan biri uchinchi tomon tomonidan olingan bo'lsa, usul buzilgan va xavfsizlik buzilishi aniqlanmasligi mumkin.

Vaqt va voqealarga asoslangan autentifikatsiya

Vaqtga asoslangan autentifikatsiya - bu sirni faqat ishtirok etgan ikki tomonga ma'lum bo'lgan tarzda vaqti-vaqti bilan o'zgartiradigan umumiy maxfiy usul.

Masalan, bitta variantda ikkala tomon ham urug 'raqamlarining bir xil kichik to'plamidan boshlanadi (ikkitasi yoki uchtasi) va ulardan yangi sonni hisoblaydigan matematik funktsiyadan foydalanadi. Har bir vaqt oralig'i (masalan, daqiqada bir marta), avvalgi ikki yoki uchta raqamdan yangi raqam hisoblanadi va eng qadimgi raqam bekor qilinadi. Ikkala tomon ham o'z vaqtlarini sinxronlashtirgan va bir xil urug 'raqamlaridan boshlagan ekan, ular joriy autentifikatsiya raqamini hisoblashlari mumkin. Uchinchi tomon ketma-ketlikni hisoblash uchun etarli raqamlarni ushlab qolishidan yoki raqam tugashidan oldin o'zlarini tasdiqlashidan saqlanish uchun raqamlar xavfsiz aloqa kanali orqali uzatilishi kerak. Xavfsizlikni yanada oshirish uchun (masalan, raqam yaratadigan ID karta yo'qolgan yoki o'g'irlangan bo'lsa), ishlab chiqarilgan raqam faqat ikki tomonga ma'lum bo'lgan parol yoki PIN kod bilan birlashtiriladi.

Boshqa umumiy maxfiy usullarda bo'lgani kabi, vaqtga asoslangan autentifikatsiya qilish umumiy sirning jismoniy xavfsizligiga bog'liq va har bir alohida foydalanuvchi noyob yaratilgan raqam va PIN-kodga ega bo'lishi kerak.
Hodisalarga asoslangan autentifikatsiya vaqtga *asoslangan autentifikatsiyaga* juda o'xshaydi, faqat yangi qiymatni yaratish taymer o'rniga aniq foydalanuvchi harakati tomonidan qo'zg'atiladi. Ushbu sxemaning umumiy o'zgarishlaridan birida foydalanuvchi yangi qiymat hosil qilish uchun apparat belgilaridagi tugmachani bosadi (oldingi bir necha qiymatlar asosida hisoblab chiqilgan) [3].

Foydalanilgan adabiyotlar

9. Каримов Ш.С. Программа для обнаружения ошибок при приеми и передачи информации // Агенство по интеллектуальной собственности РУз. №DGU 05939, 08.01.2019.

10. Каримов Ш.С., Атажонов М.О., Шербобоева Г.Б. Автоматизированная система сбора и формирования данных в информационно-телекомуникационных сетях // Агенство по интеллектуальной собственности РУз. №DGU 05940, 08.01.2019

11. Каримов Ш.С., Бахриева Х.А., Нигматов З.З. Разработка интегрированной информационной среды технологического процесса // ТАТУ УФ “Муҳаммад ал-хоразмий издошлари” мавзусидаги Республика илмий-техникавий анжумани материаллари. –С.321-323