YAGONA IDIFIKATSIYA TIZIMIDAN O`TISH VA MILLIY TARMOQ RESURSLARIDAN FOYDALANISH.

ANDIJON QISHLOQ XO‘JALIGI VA AGROTEXNOLOGIYALAR INSTITUTI
IPAKCHILIK VA TUTCHILIK YO‘NALISHI
1-BOSQICH 86-GURUH TALABASI
XUSANOV DIYORBEK SHAVKATBEK O`G`LI
e-mail: diyorbek_xusanov@gmail.com

Kalit so‘zlar:login, parol idenifikatsiya autenfikatsiya avtorizatsiya ro`yxatdan o`tish.

Annotatsiya:Yagona idenifikatsiya tizimi, OneID, milliy tarmoq axbarot tizimini idenifikatsiya qilish, autentifikator kerak.One Id idenifikatsiyasi tizimi xaqida: Yagona identifikatsiya tizimi (YAIT) OneID davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlari va tijorat tashkilotlarining turli veb-saytlari va portallariga barcha foydalanuvchilar uchun qulay foydalanish uchun mo‘ljallangan.OneID veb-saytlarga bir qator xizmatlarni taqdim etish uchun foydalanuvchilarni aniqlash imkonini beradi. Buning uchun foydalanuvchilar o‘zlarining shaxsiy ma’lumotlarini YAIT OneID-da, jumladan login, parol, to‘liq ism, JSHSHIR va hokazolarni oldindan ro‘yxatdan o‘tkazishlari kerak.veb-saytga kirish uchun foydalanuvchi OneID-da o‘z shaxsiy kabinetidan foydalanuvchi nomi va parolni kiritishi kerak.Shundan so‘ng, tizim kiritilgan ma’lumotlarning muvofiqligini tekshiradi va autentifikatsiya natijasini foydalanuvchi identifikatori bilan birga qaytaradi.

OneID shuningdek, veb-saytlarga bir martalik parol va elektron raqamli imzo yordamida foydalanuvchilarning qo‘shimcha autentifikatsiyasini amalga oshirish imkoniyatini beradi. Buning uchun so‘rov parametrlarida qulay autentifikatsiya turini ko‘rsatishingiz kerak. Birinchi orinda idenifikatsiya nimaligini bilib olsak. Idenifikatsiya so`zini ma`nosi krimi-nalistikada ob’yekt yoki shaxsning umumiy va xususiy belgilari majmuiga qarab ay-nanligini aniqlash.
Har kuni biz turli tizimlarda identifikatsiya, autentifikatsiya va avtorizatsiyadan o'tamiz, lekin aslida ushbu atamalar nima anglatishini bilamizmi?

Identifikatsiya - uni bajarish natijasida identifikatsiya subyekti uchun uni bu tizimda aniqlaydigan identifikator belgilanadigan amaliyot.

Autentifikatsiya - haqiqatga muvofiqlikni tekshirish amaliyoti. Masalan, foydalanuvchi kiritgan parolni ma'lumotlar bazasiga kiritilgan parolga muvofiqligini tekshirish.

Avtorizatsiya - ma'lum shaxsga muayyan amaliyotlarni bajarish huqiqini berish.

Quyigadi misolga batafsil ko'ramiz: siz ijtimoiy tarmoqdagi akkauntingizga kirmoqchisiz

1. Ijtimoiy tarmoq login kiritishni so'rayapti, siz uni kirityapsiz, tizim uni mavjud deb beradi — bu identifikatsiya.
2. Endi parolni kiritish kerak, siz uni kirityapsiz, parollar muvofiqligi tufayli tizim sizni haqiqiy foydalanuvchi deb topyapti — bu autentifikatsiya.
3. Tizim sizga xabarlar lentasini ko'rish va foto yuklash huquqini berdi — bu avtorizatsiya.

Axbarot tizimlarida idenifikatsiya qilish-bu idenifikatsiya qilish ob`ekti uchun uning idenifikatorini aniqlanadigon axborot tizimida ushbu sub`yektini yagona idenifikatsiya qilishi jarayonidir Axborot tizimida idenifikatsiya qilish tartib – tamoilini amalga oshirish uchun avvalo sub`yektga tegishliy idefikatorini berilishi kerek (yani sub`yekt axbarot tizimida ro`yxatdan otish lozim) Identifikatsiya qilish jarayoni autentifikatsiya bilan bevosita bog‘liq: sub’ekt autentifikatsiya jarayonidan o‘tadi va agar autentifikatsiya muvaffaqiyatli o‘tgan bo‘lsa, u holda axborot tizimi autentifikatsiya omillari asosida sub’ekt identifikatorini aniqlaydi. Bunday holda, identifikatsiyaning ishonchliligi to‘liq amalga oshirilgan autentifikatsiya jarayonnig ishonchlilik darajasi bilan belgilanadi. raqamli autentifikatsiya — avval identifikatsiya qilingan mijozdan real vaqt rejimida olingan fotosurat yoki videotasvirni dastlabki identifikatsiya ma’lumotlari bilan avtomatlashtirilgan holda (inson omilisiz) solishtirish orqali mijozning shaxsini tekshirish va tasdiqlash jarayonidir.

Idenifikatsiya qilish ro`yxatdan o`tish nimaga kerek?

Ro‘yxat o`tishda — terrorizmga, ommaviy qirg‘in qurolini tarqatishga qarshi kurashishni amalga oshiruvchi davlat organlari va O‘zbekiston Respublikasining boshqa vakolatli organlaridan taqdim etilayotgan ma’lumotlar, shuningdek chet davlatlarning vakolatli organlari va xalqaro tashkilotlaridan rasmiy kanallar orqali taqdim etilayotgan ma’lumotlar asosida O‘zbekiston Respublikasi Bosh prokuraturasi huzuridagi Iqtisodiy jinoyatlarga qarshi kurashish departamenti tomonidan tuzilgan terrorchilik faoliyatida yoki ommaviy qirg‘in qurolini tarqatishda ishtirok etayotgan yoki ishtirok etishda gumon qilinayotgan shaxslar ro‘yxati aniqlashdan iboratdir. Tarmoq tizimida ishlash biroz qiyinchiliklar keltitib chiqarishi mumkin, shuni etiborga olgan holda tarmoq resurslaridan foydalanish usullarini keltirib o’tamiz. Mijoz S, tarmoq resursidan foydalanish maqsadida autentifikatsiya serveri AS ga so’rov yo’llaydi. Server AS foydalanuvchini uning ismi va paroli yordamida identifikatsiyalaydi va mijozga ruhsat ajratish xizmati serveri TGSdan (Ticket Grating Service) foydalanishga ruhsat yuboradi.

Axborot resurslarining muayyan maqsadli serveri RS dan foydalanish uchun mijoz S TGS dan maqsadli server RS ga murojaat qilishga ruhsat so'raydi. Xamma narsa tartibda bo'lsa TGS kerakli tarmoq resurslaridan foydalanishga ruxsat berib, mijoz S ga mos ruhsatni yuboradi.

1. C -> AS - mijoz S ning TGS xizmatiga murojaat qilishga ruxsat so'rab so'ngra server AS dan so'rovni amalga oshiradi. xarqanday boshqarish axboroti uzatilganida maxfiy kalitlar kompleksini (mijozning maxfiy kaliti, serverning maxfiy kaliti, mijoz-server juftining maxfiy seans kalitlari) ko'p marta shifrlashni ishlatadi. Kerberos shifrlashning turli algoritmlaridan va xesh-funktsiyalardan foydalanishi mumkin, ammo qo'llab-quvvqtlsh uchun Triple DES va MD5 algoritmlari o'rnatilgan bo'ladi. Kerberos tizimida ishonch xujjatlarining ikki turidan foydalaniladi: ruhsat (tricket) va autentifikator (authentifacator). Ruhsat serverga ruhsat berilgan mijozning identifikatsion ma'lumotlarini xavfsiz uzatish uchun ishlatiladi. Uning tarkibida axborot xam bo'lib, undan server ruhsatdan foydalanayotgan mijozning xaqiqiy ekanligini tekshirishda foydalanishi mumkin.

Autentifikator - ruhsat bilan birga ko'rsatiluvchi qo'shimcha atribut yoki alomat deb yuritiladi. Endi Kerberos xujjatlarida ishlatiluvchi belgilashlar tizimi keltirib o'tamiz. C – mijoz S - server a - mijozning tarmoq manzili v - ruhsat ta'siri vaqtining boshlanishi va oxiri T - vaqt belgisi K_X - maxfiy kalit x K_{XY} - x va y uchun seans kaliti {m}K_X - sub'ekt x ning maxfiy kaliti K_X bilan shifrlangan xabar m $T_{X,Y}$ - y dan foydalanishga ruhsat x $A_{X,Y}$ - x va y uchun autentifikator. Kerberos ruhsati qo'yidagi shaklga ega:$T_{K,S}$ = S ,{C, a, v, $K_{C,S}$; }K_S.

Ruhsat bitta mijozga qat'iy belgilangan serverdan foydalanish uchun qat'iy belgilangan vaqtga beriladi. Uning tarkibida mijoz ismi, uning tarmoq adresi, mijoz xarakatining boshlanish va tugash vaqti va serverning maxfiy kaliti KS shifrlangan seans kaliti $K_{C,S}$; bo'ladi. Mijoz ruhsatni rasshifrovka qilaolmaydi u serverning maxfiy kalitini bilmaydi, ammo u ruhsatni shifrlangan shaklda serverga ko'rsatishi mumkin. Ruhsat tarmoq orqali uzatilayotganda tarmoqdagi yashirincha eshitib turuvchilarning birortasi xam uni o'qiy olmaydi va o'zgartira olmaydi. Kerberos autentifikatori qo'yidagi shaklga ega: $A_{K,S}$ ={C, t, kalit}$K_{C,S}$ Mijoz maqsadli serverdan foydalanishni xoxlaganida autentifikatorni yaratadi. Uning tarkibida mijoz ismi, vaqt belgisi, mijoz va server uchun umumiy bo'lgan seans kaliti $K_{C,S}$ shifrlangan seans kaliti bo'ladi. Ruhsatdan farqli xolda autentifikator bir marta ishlatiladi.

Autentifikatorning ishlatilishi ikkita maksadni ko'zlaydi. Birinchidan, autentifikatorda seans kalitida shifrlangan qandaydir matn bo'ladi.

Bu kalitning mijozga ma'lumligidan dalolat beradi. Ikkinchidan, shifrlangan ochiq matnda vaqt belgisi mavjud. Bu vaqt belgisi autentifikator va ruhsatni ushlab qolgan niyati buzuq odamga ulardan biror vaqt

o’tganidan so’ng autentfikatsiyalash muoljasini o’tishda ishlatishiga imkon bermaydi. Kerberosning autentifikatsiyalash serveri o’zining ma'lumotlar bazasida mijoz xususidagi ma'lumotlarni qidiradi. Agar mijoz xususidagi axborot ma'lumotlar bazasida bo’lsa, Kerberos mijoz va TGS orasida ma'lumot almashish uchun ishlatiladigan seans kalitini generatsiyalaydi. Kerberos bu seans kalitini mijozning maxfiy kaliti bilan shifrlaydi. So’ngra u TGS xizmatiga mijozning xaqiqiyligini isbotlovchi TGT (Ticket Granting Ticket) ruhsatining ajratilishi uchun mijozga ruhsat yaratuvchidir.

Xulosa qilib aytganda idenifikatsiya biz uchun kelajakdagi jinoyatchilikni xuquq buzarlik jabirlanish moddiy va manaviy zarar ko`rishni oldini oladigon kiber yordamchidir.

Foydalanilgan adabiyotlar

1. O.Abduraxmonov "Development of a structure for implementation of parallel algorithmes based on cubic splines in a multiple nuclear processor” International Journal of Engineering and Information Systems //Vol. 5,Issue 5.,Pages: 63-66,2021 y.
2. O.Abduraxmonov “Ko‘p yadroli protsessorda kubik bazisli splaynlar asosida parallel algoritmlarni amalga oshirish tuzilmasini ishlab chiqish” Academic Research In Edicational Sciences Scientific Journal // Vol.2,Issue3.,Pages: 628-633,2021 y.
3. O.Abduraxmonov “Some methods of signals digital operation” International journal for advanced research in science & technology // Vol.10,Issue 06.,Pages: 1-4, 2020 y.
4. Usmonova Mavludahon Soyibjon qizi “"Library of Programming Languages Python"Easy Delivery Methods Using Modern Information Communication Tools” European Journal of Pedagogical Initiatives and Educational Practices ISSN (E): 2938-3625 Volume 1, Issue 1, April, 2023
5. Usmonova Mavludakhon “Operating Principles and Applications of Blockchain Technology” European Journal of Pedagogical Initiatives and Educational Practices ISSN (E): 2938-3625 Volume 1, Issue 9, December, 2023
6. M.S. Usmonova.”Multimedia texnologiyalaridan oliy ta'limda foydalanish” “ҚИШЛОҚ ХЎЖАЛИГИДА РЕСУРС ТЕЖОВЧИ ИННОВАЦИОН ТЕХНОЛОГИЯЛАРДАН САМАРАЛИ ФОЙДАЛАНИШНИНИГ ИЛМИЙ-АМАЛИЙ АСОСЛАРИ” МАВЗУСИДАГИ ХАЛҚАРО ИЛМИЙ ВА ИЛМИЙ-ТЕХНИК АНЖУМАН АНДИЖОН 2023