IDENTIFIKATSIYA VA AUTETIFIKATSIYA

Sattorov Islomjon
O‘zMU magistranti

Annotatsiya: *Ushbu maqolada Identifikatsiya va autetifikatsiya haqida umumiy tushunchalar berilgan. Ularning foydali jihatlari va structural arxitektonikasi misollar yordamida izohlangan.*

Kalit so’zlar: *Identifikatsiya, autetifikatsiya, server, himoya, parol.*

Identifikatsiya va autetifikatsiyani axborot xavfsizligining texnik-dasturiy vositalarining asosi deyish mumkin, chunki boshqa servislar shaxsi aniqlangan (yoki shunday deb faraz qilingan) iste’molchilar ishlaydilar, bu servis esa murojaat etuvchining shaxsini (yoki identifikatori, yoki manzili, yoki qaysi jarayonligi) aniqlaydi. Uni mudofaaning oldingi chizig‘i yoki ixtiyoriy axborot fazosining «kirish eshigi» deb atash mumkin. Identifikatsiya jarayonida muloqotga kirgan sub’ekt (u iste’molchi yoki biror iste’molchi nomidan ishlayotgan jarayon yoki boshqa tizimning texnik-dasturiy komponenti) o‘zini tanishtiradi, servis esa buni tekshirib ko‘radi. Odatda shaxsning haqiqatan aytilgan odam ekanligini autentifikatsiya aniqlaydi, bu xizmatni boshqacha atamasi nusxaning (shaxs) aslligini tekshirishdir. Bu atama hamdo‘stlik mamlakatlarida autentifikatsiya ko‘rinishida qo‘llanilsa ham, uning ingliz tilidagi asl nusxasi authentication dir. Autentifikatsiya bir yoqlama – klient serverga o‘zini rasmiy, ya’ni, qonuniy iste’molchi ekanini isbotlayotganda (masalan, iste’molchining biror tizimga kirishi jarayonida) va ikki yoqlama (masalan, bevosita muloqot qilish jarayonida) muloqotga kirayotganlarning ikkisi ham o‘zining rasmiy taraf ekanligini isbotlayotganda bo‘lishi mumkin. Tarmoqda har bir tizim o‘z xududi va kirishchiqish joyiga ega bo‘lishi mumkin. Shu kirish–chiqishlarni nazorat etish jarayonida ikki omilga ahamiyat berish lozim: - autentifikatsiya qilish (ya’ni, sub’ektning asl nusxa ekanligini tekshirib, tasdiqlash) uchun qanday vositadan foydalaniladi? - identifikatsiya/autentifikatsiya qilish jarayonida ma’lumotlar almashinuvi qanday tashkil etilgan va himoyalangan? Odatda sub’ekt o‘zining rasmiy taraf ekanligini isbotlash uchun quyidagilardan hech bo‘lmaganda bittasini taqdim etadi: - biror kelishilgan shartli so‘z (parol, shaxsiy identifikatsiya nomeri, kriptografik kalit va hokazolar); - unga aynan shu maqsadda berilgan texnik vosita (shaxsiy magnit kartasi, uni tanituvchi shaxsiy axborot saqlanuvchi disketa, disk yoki flesh hotira qurilmasi va hokazo); - uning jismoniy belgilarini aks ettiruvchi biror tana a’zosi yoki xususiyati (yuz tasviri,

tovushi, ko‘z to‘r yoki mo‘g‘iz pardasi tasviri, til yuzasi tasviri, barmoq izi tasviri va hokazo, ya’ni biometrik parametrlari - qisqacha bioparametrlari). Ochiq tarmoq muhitida identifikatsiya/autentifikatsiya taraflari o‘rtasida ishonch marshruti, ya’ni, axborot almashinuvi uchun foydala-niladigan xavfxatarlardan xoli ishonchli aloqa liniyasi bo‘lishi juda mushkul muammo. Shu sababli, bir sub’ekt tomonidan ikkinchisiga o‘zini tanitish va rasmiy taraf ekanligini isbotlash uchun uzatilgan axborot ikkinchi taraf tomonidan qabul qilingan axborot bilan bir xil bo‘lishi kafolatlanmagan, ya’ni olingan belgilar ishonchli ekanligi shubha ostida bo‘ladi. Shu sababli aloqa liniyasida passiv (ya’ni, uzatilayotgan axborotga ta’sir ko‘rsatmasdan, uni faqat o‘qib/eshitib olish) va faol, ya’ni aktiv axborot tutib olib uning ustida biror amal bajarish usullarda yashirin eshitish/o‘qish imkoniyatlaridan himoyalash zarur. Buning uchun, birinchi navbatda, parollarni tarmoq orqali ochiq yoki shifrlangan (shifrlansa ham undan foydalanish imkoni bor) ko‘rinishlarda uzatmaslik, matnlarni esa avvalo himoyalangan liniyalarda, qolaversa ishonchliroq shifrlab hamda to‘liqligini tekshirish imkonini beradigan vositalar bilan birga uzatish maqsadga muvofiq. Bundan tashqari, autentifikatsiya qaydnomalarini ham murakkablashtirish ziyon qilmaydi. Axir tarmoqda o‘tirgan odam sizdan yuzlab-minglab kilometr masofada bo‘lishi mumkin, uni o‘z ko‘zingiz bilan ko‘rib turmaganligingizdan keyin shaxsining haqiqiyligiga aniq ishonch hosil qilish qiyin, chunki zamonaviy vositalar kerakli shaxs yuz tasvirini videotasvirga yozib olib undan foydalanish, animatsiya vositalaridan foydalanilganda esa o‘z yuz tasviringizni to‘g‘ridanto‘g‘ri videokameradan kiritib, so‘ng uni uzatish jarayonida kerakli tasvirga aylantirish orqali xattoki yuz ifodasi, mimika va og‘iz harakatlari ham suxbat mavzuiga to‘liq mos kelishi mumkin, tovushni ham xuddi shunday yo‘l bilan kerakli odamnikiga o‘xshatish, til yuzasi, barmoq izi, ko‘zning to‘r va mo‘g‘iz pardalarining «yumshoq» - ya’ni, hotira qurilmalariga yozib olingan nusxasi, «qattiq» - ya’ni, biror shaffof materialdagi (tsellofan plenka) tasviri, kontakt linzalar, mulyajlardan (ya’ni, yasama nusxa, masalan, barmoq nusxasi) foydalanish va hokazo imkoniyatlar borki, bulardan qutulish uchun yangi, ishonchli vosita va usullar ishlab chiqishdan o‘zga iloj yo‘q. Ishonchli identifikatsiya/autentifikatsiya qilish yana shu sabablarga ko‘ra mushkulki, bulardan biri iste’molchi qulayligi va administratorning xavfsizlik maqsadida qiladigan xatti-harakatlarining o‘zaro ziddiyatidir. Administrator imkon boricha yaxshiroq tekshirishga harakat qilsa, iste’molchi tezroq maqsadiga erishishi uchun kamroq tekshiruvni hoxlaydi. To‘g‘rida, bitta axborot olish uchun 5-10 minut savol-javob qilish kimga yoqadi. Faraz qiling, avtobusga chiqish uchun yozma ravishda ariza, mahalla qo‘mitasidan ma’lumotnoma, pasportda viza, qon va boshqa analizlar topshirish, natijasini kutib keyin chiqadigan bo‘lsangiz tillodan bo‘lsa ham

bu avtobusga chiqmasdingiz. Tarmoq servislarini himoyalashda ham shunga o‘xshash muammolar tug‘dirmaslik uchun tekshiruvni qisqartirsangiz yuqorida aytib o‘tganimizday hech bir tekshiruv yuz foiz ishonchli natija bermasligi mumkin – shartli so‘zlarni bilib olish, texnik vositalarni o‘g‘irlab olish, bioparametrlarni qalbakilashtirish mumkin

FOYDALANILGAN ADABIYOTLAR:

1. Kim David. Fundamentals of Information Systems Security. -USA, 2014. -p.544.

2. Mark Stump. Information Security: principles and practice. -2 nd ed. -USA, 2011. -p.608.

3. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. -Т.: Ўзбекистон маркаси, 2009. -432 б.

4. Пардаев А.Х. ва бошқалар. Ахборот хавфсизлиги: муаммо ва ечимлар. -Т.:Ёзувчи, 2004.

5. Мамаев М., Петренко С.. Технологии защиты информации в интернете. -С/П:Питер, 2002. -844