Sanayev M.E.
assistant
Samarqand Iqtisodiyot va Servis Instituti

IDENTIFIKASIYA VA AUTENTIFIKATSIYA

Annotatsiya. Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo‘lib, u an’anaviy ko‘p martali parollarni ishlatishiga asoslangan. Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o‘zining identifikatori va parolini teradi. Bu ma’lumotlar autentifikatsiya serveriga ishlanish uchun tushadi.

Kalit so’z: Tarmoq, DES algoritm, Autentifikatsiya, Vaqt sinxronizatsiyasi, Bir martali parollarga asoslangan autentifikatsiyalash, Xavfsizlik.

Sanayev M.E.
assistant
Samarkand Institute of Economics and Service

IDENTIFICATION AND AUTHENTICATION

Abstract. One of the most common authentication schemes is simple authentication, which is based on the use of traditional multiple-use passwords. A simple authentication process for a user on a network can be imagined as follows. A user trying to access the

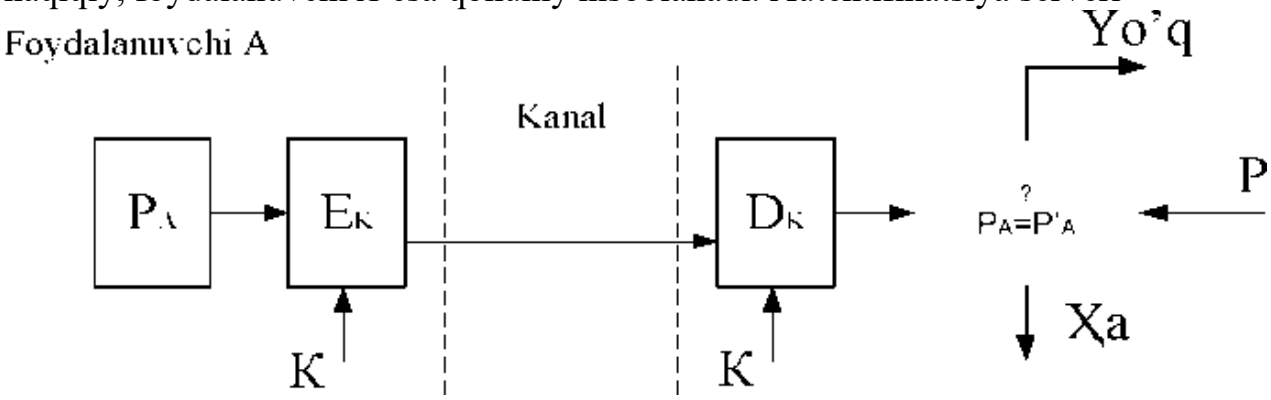
Key word: Network, DES algorithm, Authentication, Time synchronization, Authentication based on one-time passwords, Security.

Kirish: Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifikatori bo‘yicha ma’lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o‘tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizasiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi 6.1-rasmda keltirilgan.

Ravshanki, foydalanuvchining parolini shifrlamasdan uzatish orqali autentifikatsiyalash varianti xavfsizlikning xatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash Ek va rasshifrovka qilish D_k vositalari kiritilgan. Bu vositalar bo‘linuvchi maxfiy kalit K orqali boshqariladi. Foydalanuvchining haqiqiyligini tekshirish foydalanuvchi yuborgan parol P_A bilan autentifikatsiya serverida saqlanuvchi dastlabki qiymat

^{P}A ni taqqoslashga asoslangan. Agar P_A va ^{P}A qiymatlar mos kelsa, parol P_A haqiqiy, foydalanuvchi A esa qonuniy hisoblanadi. Autentifikatsiya serveri



6.1-rasm. Paroldan foydalangan holda oddiy autentifikatsiyalash.

Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operasion tizimdan foydalanishni nazoratlash ro‘yxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuqning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funksiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli o‘rniga uning bir tomonlama funksiya h(.) dan foydalanib olingan tasvirini yuborishi shart. Bu o‘zgartirish g‘anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g‘anim echilmaydigan sonli masalaga duch keladi.

Ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash tizimining bardoshligi past, chunki ularda autentifikatsiyalovchi axborot ma’noli so‘zlarning nisbatan katta bo‘lmagan to‘plamidan jamlanadi. Ko‘p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug‘atda bo‘lmasin va ularni topish qiyin bo‘lsin.

Bir martali parollarga asoslangan autentifikatsiyalashda foydalanishga har bir so‘rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan bir marta foydalanishga yaroqli. Agar, hatto kimdir uni ushlab qolsa ham parol foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikasiyalash tizimi masofadagi foydalanuvchilarni tekshirishda qo‘llaniladi.

Bir martali parollarni generatsiyalash apparat yoki dasturiy usul oqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to‘lov plastik kartochkalariga o‘xshash mikroprotsessor

o‘rnatilgan miniatyur qurilmalar ko‘rinishda amalga oshiradi. Odatda kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo‘lmagan displey darchasiga ega.

Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo‘llashning quyidagi usullari ma’lum:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.

2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro‘yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.

3. Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentikasiyalash texnologiyasini ko‘rsatish mumkin. Bu texnologiya SecurityDynamics kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan CiscoSystems kompaniyasining serverlarida amalga oshirilgan.

Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oralig‘idan so‘ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi:

• har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit;

• joriy vaqt qiymati.

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikasiya nomeri PINni kiritish taklif etiladi. PIN to‘rtta o‘nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma’lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generatsiyalash algoritmini bajaradi. So‘ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat’iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

• apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me’yoridan chetlashishi aniq o‘lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;

• server muayyan apparat kalit generatsiyalagan kodlarni kuzatadi va zaruriyat tug‘ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog‘liq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralig‘i mobaynida

haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizasiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

Bir martali paroldan foydalanib autentifikatsiyalashni amalga oshiruvchi yana bir variant - «so‘rov-javob»sxemasi bo‘yicha autentifikatsiyalash. Foydalanuvchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko‘rinishidagi so‘rovni uzatadi. Foydalanuvchining apparat kaliti bu tasodifiy sonni, masalan DES algoritmi va foydalanuvchining apparat kaliti xotirasida va serverning ma’lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida rasshifrovka qiladi. Tasodifiy son - so‘rov shifrlangan ko‘rinishda serverga qaytariladi. Server ham o‘z navbatida o‘sha DES algoritmi va serverning ma’lumotlar bazasidan olingan foydalanuvchining maxfiy kaliti yordamida o‘zi generatsiyalagan tasodifiy sonni shifrlaydi. So‘ngra server shifrlash natijasini apparat kalitidan kelgan son bilan taqqoslaydi. Bu sonlar mos kelganida foydalanuvchi tarmoqdan foydalanishga ruxsat oladi. Ta’kidlash lozimki, «so‘rov-javob»autentifikatsiyalash sxemasi ishlatishda vaqt sinxronizasiyasidan foydalanuvchi autentifikatsiya sxemasiga qaraganda murakkabroq.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro‘yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo‘linuvchi ro‘yxati maxfiy parollar ketma-ketligi yoki nabori bo‘lib, har bir parol faqat bir marta ishlatiladi. Ushbu ro‘yxat autentifikasion almashinuv taraflar o‘rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so‘rov-javob jadvali ishlatiladi. Bu jadvalda autentifikasilash uchun taraflar tomonidan ishlatiluvchi so‘rovlar va javoblar mavjud bo‘lib, har bir juft faqat bir marta

ishlatilishi shart.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

• o‘zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;

• bir tomonlama funksiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o‘zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

Keng tarqalgan bir martali paroldan foydalanishga asoslangan autentifikatsiyalash protokollaridan biri Internet da standartlashtirilgan S/Key (RFC1760) protokolidir. Ushbu protokol masofadagi foydalanuvchilarning

haqiqiyligini tekshirishni talab etuvchi ko‘pgina tizimlarda, xususan, Cisco kompaniyasining TACACS+tizimida amalga oshirilgan.

Sertifikatlar asosida autentifikatsiyalash

Tarmoqdan foydalanuvchilar soni millionlab o‘lchanganida parollarning tayinlanishi va saqlanishi bilan bog‘liq foydalanuvchilarni dastlabki ro‘yxatga olish muolajasi juda katta va amalga oshirilishi qiyin bo‘ladi. Bunday sharoitda

raqamli sertifikatlar asosidagi autentifikatsiyalash parollar qo‘llanishiga ratsional alternativa hisoblanadi.

Raqamli sertifikatlar ishlatilganida kompyuter tarmog‘i foydalanuvchilar xususidagi hech qanday axborotni saqlamaydi. Bunday axborotni foydalanuvchilarning o‘zi so‘rov-sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o‘ziga yuklanadi.

Foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar foydalanuvchilar so‘rovi bo‘yicha maxsus vakolatli tashkilot-sertifikasiya markazi CA (Certificate Authority) tomonidan, ma’lum shartlar bajarilganida beriladi. Ta’kidlash lozimki, sertifikat olish muolajasining o‘zi ham foydalanuvchining haqiqiyligini tekshirish (ya’ni, autentifikatsiyalash) bosqichini o‘z ichiga oladi. Bunda tekshiruvchi taraf sertifikasiyalovchi tashkilot (sertifikasiya markazi SA) bo‘ladi.

Sertifikat olish uchun mijoz sertifikasiya markaziga shaxsini tasdiqlovchi ma’lumotni va ochiq kalitini taqdim etishi lozim. Zaruriy ma’lumotlar ro‘yxati olinadigan sertifikat turiga bog‘liq. Sertifikasiyalovchi tashkilot foydalanuvchining haqiqiyligi tasdiG‘ini tekshirganidan so‘ng o‘zining raqamli imzosini ochiq kalit va foydalanuvchi xususidagi ma’lumot bo‘lgan faylga joylashtiradi hamda ushbu ochiq kalitning muayyan shaxsga tegishli ekanligini tasdiqlagan holda foydalanuvchiga sertifikat beradi.

Sertifikat elektron shakl bo‘lib, tarkibida qo‘yidagi axborot bo‘ladi:

- ushbu sertifikat egasining ochiq kaliti;
- sertifikat egasi xususidagi ma’lumot, masalan, ismi, elektron pochta adresi, ishlaydigan tashkilot nomi va h.;
- ushbu sertifikatni bergan tashkilot nomi;
- sertifikasiyalovchi tashkilotning elektron imzosi - ushbu tashkilotning maxfiy kaliti yordamida shifrlangan sertifikasiyadagi ma’lumotlar.

Sertifikat foydalanuvchini tarmoq resurslariga murojaat etganida autentifikatsiyalovchi vosita hisoblanadi. Bunda tekshiruvchi taraf vazifasini korporativ tarmoqning autentifikatsiya serveri bajaradi. Sertifikatlar nafaqat autentifikatsiyalashda, balki foydalanishning ma’lum xuquqlarini taqdim etishda ishlatilishi mumkin. Buning uchun sertifikatga qo‘shimcha hoshiyalar kiritilib ularda sertifikasiya egasining foydalanuvchilarning u yoki bu kategoriyasiga mansubligi ko‘rsatiladi.

Ochiq kalitlarning sertifikatlar bilan uzviy bog‘liqligini alohida ta’kidlash lozim. Sertifikat nafaqat shaxsni, balki ochiq kalit mansubligini tasdiqlovchi xujjatdir. Raqamli sertifikat ochiq kalit va uning egasi o‘rtasidagi moslikni

o‘rnatadi va kafolatlaydi. Bu ochiq kalitni almashtirish xavfini bartaraf etadi.

Agar abonent axborot almashinuvi bo‘yicha sherigidan sertifikat tarkibidagi ochiq kalitni olsa, u bu sertifikatdagi sertifikasiya markazining raqamli imzosini ushbu sertifikasiya markazining ochiq kaliti yordamida tekshirish va ochiq kalit adresi va boshqa ma’lumotlari sertifikatda ko‘rsatilgan foydalanuvchiga tegishli ekanligiga ishonch hosil qilishi mumkin. Sertifikatlardan foydalanilganda foydalanuvchilar ro‘yxatini ularning parollari bilan korporasiya serverlarida saqlash zaruriyati yo‘qoladi. Serverda sertifikasiyalovchi tashkilotlarning nomlari va ochiq kalitlarining bo‘lishi yetarli.

Sertifikatlarning ishlatilishi sertifikasiyalovchi tashkilotlarning nisbatan kamligiga va ularning ochiq kalitlaridan qiziqqan barcha shaxslar va tashkilotlar foydalana olishi (masalan, jurnallardagi nashrlar yordamida) taxminiga asoslangan.

Sertifikatlar asosida autentifikatsiyalash jarayonini amalga oshirishda sertifikasiyalovchi tashkilot vazifasini kim bajarishi xususidagi masalani echish muhim hisoblanadi. Xodimlarni sertifikat bilan ta’minlash masalasini korxonaning o‘zi echishi juda tabiiy hisoblanadi. Korxona o‘zining xodimlarini yaxshi biladi va ular shaxsini tasdiqlash vazifasini o‘ziga olishi mumkin. Bu sertifikat berilishidagi dastlabki autentifikatsiyalash muolajasini osonlashtiradi. Korxonalar sertifikatlarni generatsiyalash, berish va ularga xizmat ko‘rsatish jarayonlarini avtomatlashtirishni ta’minlovchi mavjud dasturiy maxsulotlardan foydalanishlari mumkin. Masalan, NetscapeCommunications kompaniyasi serverlarini korxonalarga shaxsiy sertifikatlarini chiqarish uchun taklif etadi.

Foydalanilgan adabiyotlar:

1. Eshquvvat o’g’li M.S, Zafar qizi Z.B AREAS OF APPLICATION OF ARTIFICIAL INTELLIGENCE ISSN: 2181-4027_SJIF: 4.995 Volume-27, Issue-2, February-2023. 61-64.
2. Eshquvvat o’g’li M.S, Naim o‘g‘li M. D, Xamrobek o’g’li N.N, DATA MININGDA CRISP-DM METODOLIGIYASI TASNIFI Часть-11_ Том-1_ Декабрь-2023 43-46.
3. Файзиев Б.М., Бегматов Т.И., Санаев М.Э. ОБРАТНАЯ ЗАДАЧА ПО ОПРЕДЕЛЕНИЮ КИНЕТИЧЕСКОГО КОЭФФИЦИЕНТА В МОДЕЛИ ФИЛЬТРАЦ II TOM TATU SF MA’RUZALAR TO‘PLAMI 9 aprel 2022-yil 11-13.
4. Файзиев Б.М., Бегматов Т.И., Санаев М.Э ИДЕНТИФИКАЦИЯ КОЭФФИЦИЕНТА КИНЕТИКИ В МОДЕЛИ ФИЛЬТРАЦИИ СУСПЕНЗИИ В ПОРИСТОЙ СРЕДЕ 144-145.
5. Файзиев Б.М., Бегматов Т.И., Санаев М.Э. ИДЕНТИФИКАЦИЯ КОЭФФИЦИЕНТА КИНЕТИКИ В МОДЕЛИ ФИЛЬТРАЦИИ СУСПЕНЗИИ В ПОРИСТОЙ СРЕДЕ ХАЛҚАРО ИЛМИЙ-АМАЛИЙ АНЖУМАН МАТЕРИАЛЛАРИ 2022 йил, 11-12 май 360-361.

6. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, MA'LUMOTLARNI SINFLASHTIRISHDA BIRCH ALGORITMI AHAMIYATI Часть-11_ Том-1_ Декабрь -2023 39-42.
7. Eshquvvat o'g'li.M.S, Elmurza o'g'li.Z.B, Anvar o'g'li.B.A DATA MININGDA SEMMA METODOLIGIYASI TASNIFI Часть-11_ Том-1_ Декабрь -2023 35-38.
8. Naim o‘g‘li M. D., Abdishukur o'g'li S. A. THE NUMPY LIBRARY OF THE PYTHON PROGRAMMING LANGUAGE IS AN OPTIMAL SOLUTION FOR WORKING WITH ARRAYS //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 195-197.
9. Naim o’g’li M. D., Baxtiyor o‘g’li E. S. DATA SCIENCE METHODOLOGY IN LEARNING PROGRAMMING //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 207-210.
10. Amanbayevna A. S., Naim o’g’li M. D. GEOMETRIC MODELING AND VISUALIZATION OF SELF-SIMILAR STRUCTURES BASED ON FRACTAL THEORY //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 187-188.
11. Ernazarov, A. E. Features of defining goals and objectives in training. Society and innovations-Obshchestvo i innovatsii-Society and innovations.
12. Ergashevich, E. A. AJMR. AJMR.
13. Artikovich, A. S., Arulmoly, C., Kiruthika, A., Mody, P., Elopra, P., Kamsi, R., & Ergashevich, E. A. AJMR. AJMR.