ISSN: 2181-4341, IMPACT FACTOR (RESEARCH BIB) – 7,245, SJIF – 5,431

Imamaliyev Aybek Turapbayevich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti katta o‘qituvchisi
Pochta oimamaliyev1987@gmail.com

“SAVOL-JAVOB” MEXANIZMIGA ASOSLANGAN HMAC ALGORITMI YORDAMIDA FOYDALANUVCHILARNI AUTENTIFIKATSIYALASH USULI

Annotatsiya: Ushbu maqolada “Savol-javob” mexanizmiga asoslangan autentifikatsiya usullarining tahlili o‘rganib chiqildi. “Savol-javob” asosidagi autentifikatsiya usuli keng qo‘llanilsa-da, so‘nggi paytlarda uni amalga oshirish va samaradorligiga qaratilgan keng qamrovli tadqiqotlar etishmasligini keltirish mumkin. Shunga ko‘ra, takomillashtirilgan autentifikatsiya usuli, “Savol-javob” asosidagi autentifikatsiyani amalga oshirish va samaradorligi bilan bog‘liq bo‘lgan tadqiqotlar hamda ushbu mexanizmni amalga oshirishda foydalaniladigan kriptografik usullar va xavfsizlik protokollari tahlil etilgan. Shuningdek, “Savol-javob” mexanizmiga asoslangan HMAC algoritmi yordamida foydalanuvchilarni autentifikatsiyalash usuli taklif etilgan.

Kalit so‘zlar: identifikatsiya, autentifikatsiya, parol, maxfiylik, konfidensiallik, xavfsizlik, PFS, PKI, HMAC, raqamli imzo, kriptografiya, shifrlash, kalitlarni boshqarish.

Аннотация: В данной статье рассматривается анализ методов аутентификации на основе механизма «Вопрос-Ответ». Хотя аутентификация на основе «Вопрос-Ответ» широко используется, в последнее время отсутствует комплексное исследование ее реализации и эффективности. Соответственно, анализируются исследования, связанные с реализацией и эффективностью усовершенствованного метода аутентификации, аутентификации на основе «Вопрос-ответ», а также криптографических методов и протоколов безопасности, используемых при реализации этого механизма. Также предложен метод аутентификации пользователя с использованием алгоритма HMAC на основе механизма «Вопрос-Ответ».

Ключевые слова: идентификация, аутентификация, пароль, секретность, конфиденциальность, безопасность, PFS, PKI, HMAC, цифровая подпись, криптография, шифрование, управление ключами.

Annotation: In this paper, examines the analysis of authentication methods based on the “Challenge-response” mechanism. Although “Challenge-response”-based authentication is widely used, recently there has been a lack of comprehensive research on its implementation and effectiveness. Accordingly, studies related to the implementation and effectiveness of the improved authentication method, “Challenge-response” based authentication, as well as the cryptographic methods and security protocols used in the implementation of this mechanism are analyzed. Also, a user authentication method using the HMAC algorithm based on the “Challenge-response” mechanism is proposed.

Keywords: identification, authentication, password, privacy, confidentiality, security, PFS, PKI, HMAC, digital signature, cryptography, encryption, key management.

Kirish

Bugungi kunda raqamli tizimlarda autentifikatsiya masalasi onlayn tizimlar, tarmoqlar va xizmatlar xavfsizligini ta’minlashda muhim hisoblanadi. Foydalanuvchilarni autentifikatsiyalashning an’anaviy vositasi bo‘lgan foydalanuvchining nomi va paroli kombinatsiyasi turli xil hujumlar, jumladan, fishing, qo‘pol kuch va lug‘at hujumlariga nisbatan zaif ekanligi ma’lum bo‘ldi. So‘nggi yillarda xavfsizlik borasida qo‘shimcha darajani ta’minlaydigan va ruxsatsiz kirish xavfini kamaytiradigan yanada ilg'or va murakkab autentifikatsiya usullariga e’tibor qaratilmoqda[12]. Bunday usullardan biri “Savol-javob” mexanizmi bo'lib, u foydalanuvchilarning shaxsini tekshirish uchun bir qator savollar berish bilan bog‘liq kontseptsiyasiga asoslangan. Ushbu yondashuv turli ilovalarda, jumladan, onlayn-banking, elektron tijorat va ijtimoiy media platformalarida qo‘llanilmoqda. “Savol-javob” mexanizmi an'anaviy autentifikatsiya usullariga nisbatan bir qator afzalliklarga ega, jumladan foydalanuvchi tajribasini yaxshilash, xavfsizlikni oshirish va firibgarlik xavfini kamaytirish[13]. Biroq, bir qator afzalliklarga qaramay, “Savol-javob” mexanizmi kamchiliklardan holi emas. Ushbu yondashuvning muvaffaqiyati so'ralgan savollarning sifati va dolzarbligiga, shuningdek, foydalanuvchining aniq va izchil javob berish qobiliyatiga bog'liq. Bundan tashqari, “Savol-javob” mexanizmi turli xil hujumlarga, jumladan, faraz qilish hujumlariga nisbatan zaif bo‘lishi mumkin, bunda buzg‘unchi turli kombinatsiyalarni sinab ko‘rish orqali to‘g‘ri javoblarni taxmin qilishga harakat qiladi.

Ushbu tahlilda “Savol-javob” mexanizmiga asoslangan turli xil autentifikatsiya usullarini, jumladan ularning kuchli va zaif tomonlarini ko‘rib chiqiladi. Shuningdek, ushbu usullarning samaradorligiga ta‘sir qiluvchi asosiy omillarni muhokama qilish va ularning xavfsizligi va qulayligini oshirish uchun ularni takomillashtirish bo‘yicha ma’lumotlar beriladi.

Mavjud ishlar tahlili

Conklin va boshqalar tomonidan parolarga asoslanga autentifikatsiya usullari tahlil etilgan. Bu usul tizim tomonidan berilgan savolga javoban foydalanuvchi parolini kiritishini o'z ichiga oladi. So‘ngra parol tizim tomonidan saqlangan va xeshlangan parol bilan tekshiriladi [1]. Khan va boshqalar tomonidan bir martalik parolga asoslangan autentifikatsiya usullari tadqiq etilgan. Ushbu usul foydalanuvchiga SMS yoki elektron pochta orqali bir martalik parolni olish va autentifikatsiyadan o‘tish imkoniyatini o'z ichiga oladi, Bunda autentifikatsiyadan o‘tish uchun bir martalik parol tizimga kiritiladi [2]. Sharma va boshqalar tadqiqotchilar Ochiq kalitlar infratuzilmasi (PKI) asosidagi autentifikatsiya usullarini tahlil etishdi. Bu usul foydalanuvchilarni autentifikatsiyalash uchun raqamli sertifikatlar va ochiq kalit kriptografiyasidan foydalanishni o‘z ichiga oladi [3]. Kim va boshqalar tomonidan Challenge-Response Authentication Protocol (CRAP) protokoli asosida foydalanuvchiarni autentifikatsiyalash bo‘yicha tadqiqotlar o‘tkazgan [4]. Bu usul ochiq tarmoq orqali foydalanuvchilarni autentifikatsiyalash uchun “Savol-javob” protokolidan foydalanishni o'z ichiga oladi.

Asosiy qism

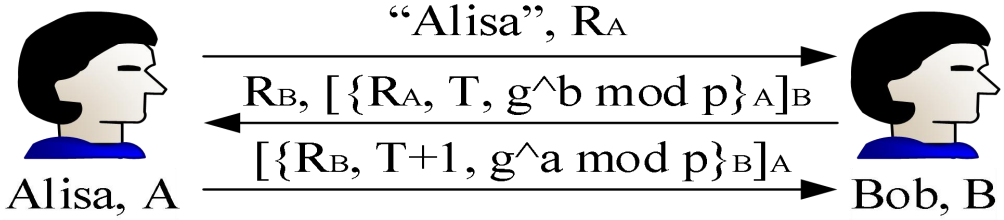
Ushbu maqolada maxfiy kalitli kriptotizimdan foydalanib “Savol-javob” mexanizmiga asoslangan ikki tomonlama autentifikatsiyalash usullarini ishlab chiqish masalasi ko‘rib chiqiladi. Umumiy holda maxfiy kalitli kriptotizimlarga asoslangan autentifikatsiya usullarida umumiy kalitni almashinish boshqa ishonchli usul, masalan SSL/TLS va h.k. orqali amalga oshiriladi. Quyida ularga muqobil bo‘lgan maxfiy kalitni taqsimlashni yuqori xavfsizlik darajasini ta’minlagan holatda amalga oshirish imkonini beruvchi usul taqdim etiladi. Ushbu usul ikki tomonlama autentifikatsiyani va sessiya kalitini taqsimlashni amalga oshiradi. Bundan tashqari, bu turdagi protokollar mukammal ilg‘or xavfsizlik (Perfect Forward Secrecy, PFS) talabini ham bajarishi shart hisoblanadi [5].

Perfect Forward Secrecy - bu xavfsizlik xususiyati bo‘lib, buzg‘unchi autentifikatsiya protokolida ishlatiladigan uzoq muddatli kalitlar yoki sertifikatlarga ega bo‘lsa ham, ular avvalroq yozib olingan aloqalarning shifr matinni ocha olmasligini ta’minlaydi [6]. Boshqacha qilib aytganda, PFS buzg‘unchi autentifikatsiya protokolida ishlatiladigan shaxsiy kalitlar yoki sertifikatlarni buzsa ham, ular ilgari shifrlangan ma'lumotlarni ocha olmasligini ta'minlaydi[7].

PFS ikkita kalit birikmasidan foydalangan holda ishlaydi: uzoq muddatli kalit va qisqa muddatli kalit. Uzoq muddatli kalit dastlabki ulanishni o‘rnatish va foydalanuvchini autentifikatsiyalash uchun, qisqa muddatli kalit esa, aloqani shifrlash uchun ishlatiladi [8]. Qisqa muddatli kalit tasodifiy tarzda yaratiladi va faqat bitta seans uchun ishlatiladi[11]. Bu shuni anglatadiki, agar buzg‘unchi uzoq muddatli kalitga ega bo‘lsa ham, qisqa muddatli kalitga ega bo‘lmagani uchun ilgari yozib olingan hech qanday aloqani paroliga ega bo‘la olmaydi[9].

Faraz qilaylik Alisa va Bob uzoq vaqt foydalaniluvchi taqsimlangan kalit KAB ga ega. Shundan so‘ng, agar PFSni ular istasa, KAB kalitdan shifrlash kaliti sifatida foydalanmasliklari zarur. Uning o‘rniga ular sessiya kaliti KS ni kelishishlari zarur bo‘ladi va zarur bo‘lmagan vaqtdan so‘ng, ya’ni, sessiya tugagandan so‘ng, ushbu kalitni unutishlari zarur bo‘ladi. Shunday qilib, oldingi protokollar kabi, uzoq vaqt foydalaniluvchi kalit KAB yordamida sessiya kaliti KS ni hosil qilishlari zarur bo‘ladi. Shunday qilib, PFS uchun ma’lum vaqtdan keyin KAB kalit topilgan taqdirda ham KS kalitni aniqlash imkoniyati yo‘q bo‘lishini shart qilib olish zarur [10].

Ikki tomonlama autentifikatsiyalash, sessiya kaliti va PFSni ta’minlovchi protokol 1-rasmda keltirilgan.



1-rasm. Ikki tomonlama autentifikatsiya, sessiya kalit va PFSni ta’minlovchi protokol

bu yerda, [] – amali ochiq kalitni kriptotizimlardan foydalanib imzolashni, {} – amali esa ochiq kalitli kriptotizimlardan foydalanib shifrlashni, T – joriy vaqt metkasini bildiradi. Mazkur holda sessiya kaliti KS=gab mod p tenglik orqali hisoblab topiladi.

Bir martalik qiymatlar asosida ochiq kalitli kriptotizimlarga asoslangan ushbu usul quyidagi afzalliklarga ega:

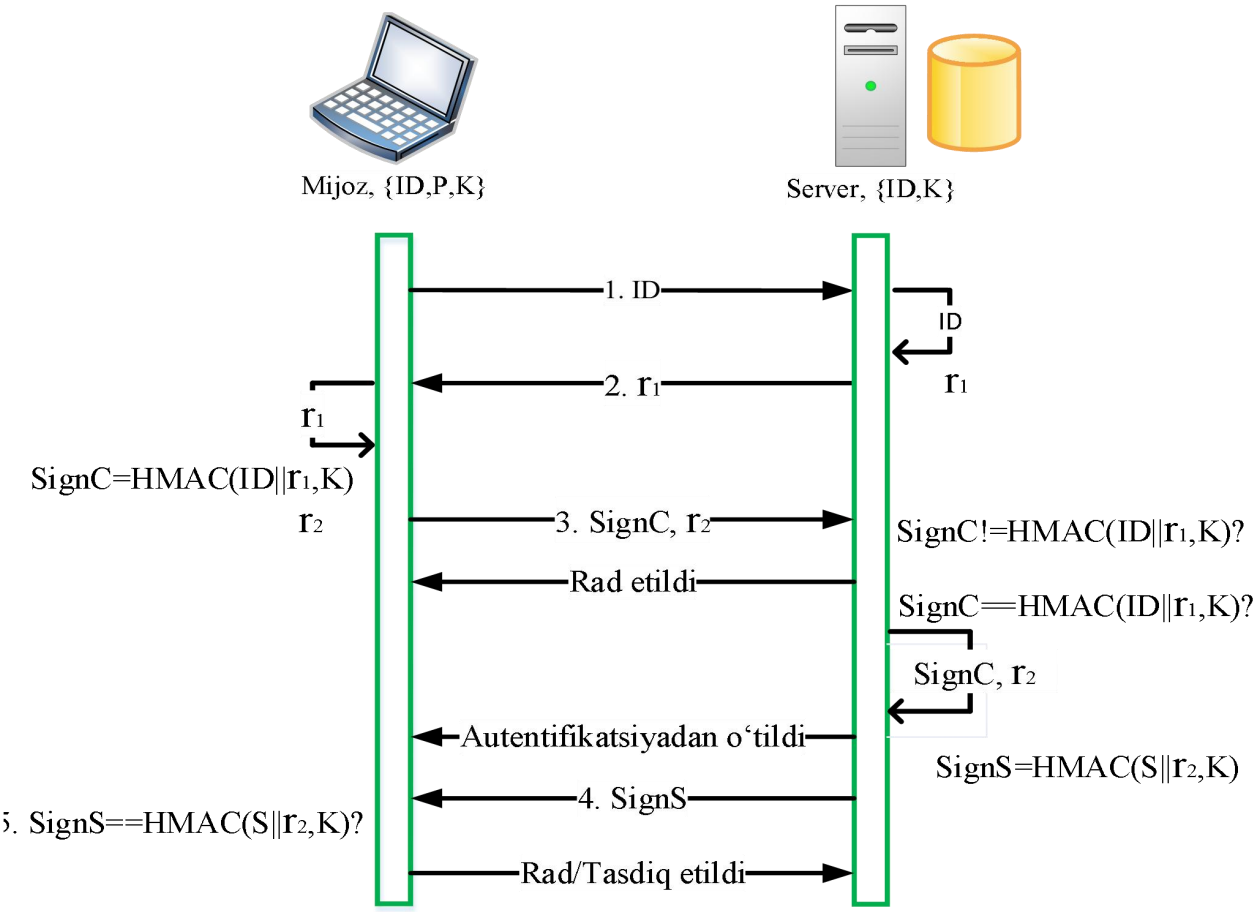
- imzolashga asoslangan ikki tomonlama autentifikatsiyalash;

- tasodifiy son va vaqt metkasiga asoslangan xabarni takrorlash hujumidan himoyalash va xabarni “yangiligi (freshness)”ni ta’minlash;

- Diffi-Hellman protokoliga asoslangan sessiya kalitini PFSni ta’minlagan holda hosil qilish.

Ushbu usul maxfiy kalitli tizimlar ishlashi uchun talab etiladigan umumiy kalitni taqsimlashga xizmat qiladi. Ushbu usul asosida A va B tomonlarni umumiy kalitga ega deb hisoblab, “Savol-javob” mexanizmiga asoslangan quyidagi usul taklif etildi.

“Savol-javob” mexanizmiga asoslangan HMAC algoritmi yordamida foydalanuvchilarni autentifikatsiyalash usuli. Ushbu usul ishlashi uchun mijoz (C) va server (S) o‘rtasida umumiy kalit talab etiladi. Ushbu kalit yuqorida keltirilgan protokol asosida amalga oshirilganini faraz qilgan holda, quyida HMAC asosida ikki tomonlama autentifikatsiyalashni amalga oshiruvchi usulning kirish protsedurasi bilan tanishib chiqiladi.



2-rasm. HMAC asosida ikki tomonlama autentifikatsiyalash usuli

Usulining **kirish** protsedurasi quyidagi bosqichlardan iborat (2-rasm):

1-bosqich. $C \rightarrow S: ID$. Dastlabki bosqichda mijoz o‘zini serverga tanitish uchun identifikatorini, ID yuboradi.

2-bosqich. $S \rightarrow C: r_1$. Ikkinchi bosqichda server foydalanuvchini o‘zining bazasida mavjudligini tekshirgandan so‘ng, unda tasodifiy kattalik r_1 ni yuboradi.

3-bosqich. $C \rightarrow S: SignC, r_2$. Shundan so‘ng, mijoz tomon o‘zida ma’lum umumiy maxfiy kalit K bilan tasodifiy kattalik r_1 ga imzo qo‘yadi. Imzolash simmetrik kriptotizim, HMAC asosida

amalga oshiriladi: $\mathrm{SignC} = \mathrm{HMAC}(\mathrm{ID}||\mathrm{r}_1, \mathrm{K})$. Agar mijoz ham serverni autentifikatsiyalamoqchi bo‘lsa, tasodifiy kattalik r_2 ni hosil qiladi va uni SignC imzoga qo‘shib yuboradi.

4-bosqich. $\mathrm{S} \rightarrow \mathrm{C}: \mathrm{SignS}$. Server qabul qilingan SignC qiymatni o‘zida mavjud K kalit va r_1 tasodifiy qiymat yordamida hosil qilingan qiymat bilan taqqoslash orqali foydalanuvchini autentifikatsiyadan o‘tkazadi. Mijoz tomoni serverni haqiqiyligini ta’lab etganda, $\mathrm{SignS} = \mathrm{HMAC}(\mathrm{S}||\mathrm{r}_2, \mathrm{K})$ qiymatni hisoblab, uni mijozga yuboradi. Agar talab etilmasa, foydalanuvchiga muvaffaqiyatli autentifikatsiyadan o‘tilganligi haqida xabar yuboriladi.

5-bosqich. Server tomonidan yuborilgan SignS imzoni tekshirish uchun foydalanuvchi o‘zida mavjud umumiy kalit K va tasodifiy qiymat r_2 dan foydalanadi: $\mathrm{HMAC}(\mathrm{S}||\mathrm{r}_2, \mathrm{K})$. Agar ushbu ikki qiymat o‘zaro teng bo‘lsa, foydalanuvchi serverni autentifikatsiyadan o‘tkazadi.

Yuqorida keltirilgan usulda HMAC algoritmidan foydalanilgan bo‘lib, xesh funksiya sifatida ixtiyoriy bardoshli algoritmlardan biri tanlanishi mumkin. Bundan tashqari, yuqoridagi usulni simmetrik blokli shifrlash algoritmi bilan ham almashtirish mumkin. Buni uchun mos ravishda $\mathrm{HMAC}(\mathrm{ID}||\mathrm{r}_\mathrm{i}, \mathrm{K})$ ifodani $\mathrm{E}(\mathrm{ID}||\mathrm{r}_\mathrm{i}, \mathrm{K})$ ifoda bilan almashtirishning o‘zi yetarli hisoblanadi.

Xulosa

Xulosa qilib aytganda, PFS xavfsizlikning muhim xususiyati bo‘lib, buzg‘unchi autentifikatsiya protokolida ishlatiladigan uzoq muddatli kalitlar yoki sertifikatlarga ega bo‘lsa ham, ular ilgari yozib olingan shifrlangan ma’lumotlarni ochuvchi kalitga ega bo‘la olmasligini ta’minlaydi. PFS xavfsizlikni yaxshilash, hujumlardan himoyalash va uzoq muddatli kalitlarni buzish bo‘yicha bir qator muammolarni oldini olish kabi afzalliklarni beradi. Shunga ko‘ra, taklif etilgan HMAC algoritmi yordamida foydalanuvchilarni autentifikatsiyalash usuli foydalanuvchilarni xavfsiz autentifikatsiyalashga yordam beradi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Conklin A., Dietrich G., Walz D. Password-based authentication: a system perspective //37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the. – IEEE, 2004. – C. 10 pp.
2. Khan R. H., Miah J. Performance Evaluation of a new one-time password (OTP) scheme using stochastic petri net (SPN) //2022 IEEE World AI IoT Congress (AIIoT). – IEEE, 2022. – C. 407-412.
3. Sharma K., Shrivastava G. Public key infrastructure and trust of web based knowledge discovery //Int. J. Eng., Sci. Manage. – 2014. – T. 4. – №. 1. – C. 56-60.
4. Kim S. et al. Dynamic key update strategy in physical-layer challenge-response authentication //2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS). – IEEE, 2019. – C. 1-6.
5. Turapbayevich I. A., Karimovich G. S., Usmanov S. Algorithm of Generating One-Time Passwords for Two-Factor Authentication of Users //World Conference Intelligent System for Industrial Automation. – Cham : Springer Nature Switzerland, 2022. – C. 132-139.
6. Verlan A. F. et al. Methods of Formation of a Security Policy in Access Differentiation Processes //Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE). – International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE), 2014. – C. 204.

7. Naidu D. Two-factor authentication for effective information security //International Research Journal of Modernization in Engineering Technology and Science. – 2022. – T. 4. – №. 6. – C. 4307-4312.
8. Shemshi V. et al. Verification of electronic identity in federated systems using multi-factor authentication //Journal of Applied Sciences-SUT (JAS-SUT). – 2022. – T. 8.
9. Cremers C., Feltz M. Beyond eCK: Perfect forward secrecy under actor compromise and ephemeral-key reveal //Computer Security–ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings 17. – Springer Berlin Heidelberg, 2012. – C. 734-751.
10. Avoine G., Canard S., Ferreira L. Symmetric-key authenticated key exchange (SAKE) with perfect forward secrecy //Topics in Cryptology–CT-RSA 2020: The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24–28, 2020, Proceedings. – Springer International Publishing, 2020. – C. 199-224.
11. Cremers C., Feltz M. Beyond eCK: perfect forward secrecy under actor compromise and ephemeral-key reveal //Designs, Codes and Cryptography. – 2015. – T. 74. – №. 1. – C. 183-218.
12. Mandal S., Mohanty S. Multi-party key-exchange with perfect forward secrecy //2014 International Conference on Information Technology. – IEEE, 2014. – C. 362-367.
13. Xu S. et al. An improved mutual authentication protocol based on perfect forward secrecy for satellite communications //International Journal of Satellite Communications and Networking. – 2020. – T. 38. – №. 1. – C. 62-73.