ISSN 2181-3187

AUTENTIFIKATSIYA USULLARIGA QARATILGAN HUJUMLAR

Shodimurodov Ulug'bek Akmalovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali, talabasi
Jo'rayev Asom Qo'liboy o'g'li
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali, talabasi

ANNOTATSIYA

Maqolada autentifikatsiya usullariga qaratilgan hujumlar va ularga qarshi choralar to'g'risida tahlil qilinadi. Autentifikatsiya usullari, shaxsiy ma'lumotlarni himoya qilish uchun keng qo'llaniladigan tizimlar hisoblanadi. Maqolada autentifikatsiya usullari (parol, biometrik ma'lumotlar, xavfsizlik sorovlari, kod kiritish va boshqalar) ta'riflanadi va ularni hujumlariga qarshi xavfsizlik chora-tadbirlari keltiriladi. Hujumlar (parol uchun hujumlar, men-in-the-middle hujumlar, brute force hujumlar, biometrik ma'lumotlarga hujumlar va boshqalar) tavsiflanadi va ularni oldini olish uchun tavsiyalar beriladi.

Kalit so'zlar: *Autentifikatsiya, hujum, xavfsizlik, parol, biometrika, men-in-the-middle, brute force, kod, hujumlar, himoya, autentifikatsiya usullari.*

KIRISH

Autentifikatsiya, yoki shaxsiy ma'lumotlarni tasdiqlash, onlayn xizmatlar va tizimlarda ahamiyatga ega bo'lgan muhim jarayonlardan biridir. Foydalanuvchining xizmatga kirish jarayonida o'zini aniqlash uchun turli autentifikatsiya usullari qo'llaniladi. Bu autentifikatsiya usullari, foydalanuvchini tanish, uning identifikatorini va so'zi tasdiqlashda yordam beradi. Asosiy autentifikatsiya usullari quyidagilardir: parol, biometrik ma'lumotlar, xavfsizlik sorovlari, kod kiritish va boshqalar. Shuningdek, autentifikatsiya usullariga qaratilgan hujumlar foydalanuvchining shaxsiy ma'lumotlariga zarar yetkazishi mumkin.

Autentifikatsiya jarayonining muhim ahamiyati tufayli, ushbu maqolada autentifikatsiya usullari va ularga qarshi hujumlar tahlil qilinadi. Har bir autentifikatsiya usuli (parol, biometrik ma'lumotlar, xavfsizlik sorovlari, kod kiritish va boshqalar) ko'rib chiqiladi va ularning xususiyatlari, afzalliklari va kamchiliklari ta'riflanadi. Shuningdek, autentifikatsiya usullari bilan bog'liq hujumlar (parol uchun hujumlar, men-in-the-middle hujumlar, brute force hujumlar, biometrik ma'lumotlarga hujumlar va boshqalar) tavsiflanadi va ularni oldini olish uchun tavsiyalar beriladi.

ISSN 2181-3187

Autentifikatsiya usullari va ularga qarshi hujumlar tahlili, foydalanuvchilarga xavfsiz autentifikatsiya usullarini qo'llashga rag'batlantirish va xavfsizlikni oshirishga yordam berishi maqsadida amalga oshirilgan.

Autentifikatsiya usullari: Autentifikatsiya, onlayn xizmatlarga kirish jarayonida foydalanuvchini aniqlash uchun turli usullarni o'z ichiga oladi. Eng keng tarqalgan autentifikatsiya usullari quyidagilardir:

Parol: Eng oddiy va ko'p ishlatiladigan autentifikatsiya usuli. Foydalanuvchi o'ziga xos parolni kiritadi va tizim uni tasdiqlaydi. Ammo, parollar odatda ko'p marta ishlatiladi, o'zi saqlanadi yoki yomon ko'rinishda tanlanganligi sababli hujumga oson bo'lishi mumkin.

Biometrik ma'lumotlar: Bu usulda foydalanuvchi o'zning unikal fizikaviy xususiyatlari yoki o'zga xos matnlarni (biometrik ma'lumotlar) qo'llab-quvvatlaydi, masalan, qo'llar izi, qulupnay, yuz shakli yoki ko'z qopqog'i. Bu usul eng yuqori darajada xavfsizlikni ta'minlaydi, lekin unikal ma'lumotlarni yaratish va saqlash oson emas.

Xavfsizlik sorovlari: Foydalanuvchiga shaxsiy savollarni javoblash uchun ishlatiladi. Bu usul oddiy savollardan unikal bo'lishi mumkin va foydalanuvchining xavfsizlik darajasini oshiradi. Ammo, unikal savollar ham yaxshi saqlanishi kerak.

Kod kiritish: Bu usulda foydalanuvchiga tizim tomonidan yuborilgan kodni kiritish talab etiladi. Bu usul darhol tizimga kirishni ta'minlaydi, lekin kodlar uchun xavfsizlik ta'minlash muhimdir.

Autentifikatsiya usullariga qaratilgan hujumlar: Autentifikatsiya usullari hujumlariga qaramay, foydalanuvchining shaxsiy ma'lumotlarini himoya qilish uchun xavfsizlik choralariga ega bo'lishi zarur. Quyidagi hujumlar autentifikatsiya usullariga ta'sir ko'rsatishi mumkin:

Parol uchun hujumlar: Hujumchilar parollarni qo'lda tutish, brute force serlarini sinash, yoki tizimlar yordamida parollarni hisoblash orqali foydalanuvchining hisobiga kirishga urinishadi.

Men-in-the-middle hujumlar: Hujumchilar foydalanuvchilar va tizimlar orasida o'zaro bog'lanishni to'liq bilmasdan ma'lumotlarni o'zgartirishi, ochirishi yoki o'qishi mumkin.

Brute force hujumlar: Bu usulda hujumchilar barcha ehtimol parollar to'plamini sinab ko'radilar. Bu odatda katta miqdordagi kompyuter kuchini talab qiladi, ammo eng oddiy autentifikatsiya usullari uchun ham samarali bo'lishi mumkin.

Biometrik ma'lumotlarga hujumlar: Hujumchilar biometrik ma'lumotlarni o'zgartirish yoki ko'chirish orqali autentifikatsiyani buzishga urinishishi mumkin.

Qo'llash to'g'risida maslahatlar: Autentifikatsiya usullariga qaratilgan hujumlarni oldini olish uchun quyidagi maslahatlar berilishi mumkin:

ISSN 2181-3187

Kuchli va o'zaro takrorlanmas parollar: Foydalanuvchilarga kuchli va o'zaro takrorlanmas parollar ishlatish, ularni vaqt-vaqtda o'zgartirish.

Biometrik ma'lumotlarni qo'llash: Biometrik autentifikatsiya usullarini qo'llab-quvvatlash, shuningdek, biometrik ma'lumotlarni saqlash uchun yaxshi xavfsizlik choralarini ta'minlash.

Xavfsizlik sorovlarining unikal bo'lishi: Xavfsizlik sorovlari yaxshi ko'zdan kechirilishi va foydalanuvchining xavfsizlik darajasini oshirish uchun unikal bo'lishi kerak.

Kod kiritishning qat'iylik darajasi: Kod kiritishni taqozo etish orqali foydalanuvchining hisobiga kirishni qat'iyroq qilish.

XULOSA

Autentifikatsiya usullari onlayn xizmatlarga kirishni himoya qilishda muhim rollarni o'ynaydi. Biroq, ular hamkorlikchi dasturlar uchun boy bo'lishi mumkin. Hujumlar autentifikatsiya usullariga ta'sir ko'rsatishi mumkin, shuning uchun xavfsizlik choralariga e'tibor berilishi kerak. Parol uchun hujumlar, men-in-the-middle hujumlar, brute force hujumlar va biometrik ma'lumotlarga hujumlar keng qo'llaniladigan autentifikatsiya usullariga qaratilgan hujumlardan ba'zi misollar hisoblanadi. Hujumlarga qarshi qo'l to'g'risida xavfsizlik choralariga ega bo'lish, foydalanuvchilarni xavfsiz autentifikatsiya usullarini qo'llashga rag'batlantirish, va foydalanuvchilarga kuchli va o'zaro takrorlanmas parollar ishlatish maslahatlari berilishi muhimdir.

ADABIYOTLAR RO'YXATI

1. Stallings, W. (2013). Network Security Essentials: Applications and Standards. Pearson.
2. Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.
3. Gollmann, D. (2010). Computer Security. John Wiley & Sons.
4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.