INTERNET OF THINGSDA XAVFSIZLIK

Umarov Bekzod Azizovich
Farg‘ona davlat universiteti amaliy matematika va informatika Kafedrasi o‘qituvchisi, ubaumarov@mail.ru
Turg‘unova Gulsanam Murodil qizi
Farg‘ona davlat unversiteti 3-kurs talabasi,
turgunova.a2103@gmail.com

Annotatsiya: *IoT (Internet of Things) xavfsizligi — bu IoT qurilmalarining, tarmoqlarining va ularning ma'lumotlarini himoya qilish bilan bog'liq bo'lgan xavfsizlik tadbirlarining majmui. IoT qurilmalari kundalik hayotimizda ko'plab joylarda, masalan, uylarimizda (aqlli uy qurilmalari), sog'liqni saqlash tizimlarida, sanoat ishlab chiqarishida va transportda foydalaniladi. Biroq, bu qurilmalar tarmoqqa ulanish orqali yangi xavf-xatarlarni keltirib chiqaradi.*

Kalit so’zlar: *Ma’lumotlar shifrlash, kriptografiya, autentifikatsiya, avtorizatsiya, kiberhujumlar, IOT xavfsizlik protokollari.*

Abstract: *IoT (Internet of Things) security is a set of security measures related to the protection of IoT devices, networks and their data. IoT devices are used in many places in our daily lives, such as in our homes (smart home devices), health systems, industrial production and transportation. However, these devices pose new risks by connecting to the network.*

Keywords: *data encryption, cryptography, authentication, authorization, cyberattacks, IoT security protocols.*

Абстрактный: *Безопасность IoT (Internet of Things) — это комплекс мер безопасности, связанных с защитой устройств IoT, сетей и их данных. Устройства интернета вещей используются во многих местах нашей повседневной жизни, таких как наши дома (устройства умного дома), системы здравоохранения, промышленное производство и транспорт. Однако эти устройства создают новые риски, подключаясь к сети.*

Ключевые слова: *шифрование данных, криптография, аутентификация, авторизация, кибератаки, протоколы безопасности Интернета вещей.*

Kirish:

IoT xavfsizligi (IoT Security) — bu Internet of Things (IoT) qurilmalarini, tarmoqlarini, va ularga ulanish orqali olingan ma'lumotlarni himoya qilishga qaratilgan bir qator texnologik, strategik va operatsion choralardan iborat bo'lgan xavfsizlik sohasidir. IoT qurilmalari har xil sohalarda, masalan, uy-joy tizimlaridan (aqlli uylar), sog'liqni saqlash,

transport va sanoat avtomatizatsiyasidan tortib, shaxsiy va biznes hayotiga qadar keng qo'llaniladi. Biroq, IoT qurilmalari va tizimlari kiberhujumlarga va boshqa xavf-xatarlarga nisbatan juda zaif bo'lishi mumkin, chunki ular ko'plab tarmoqlarga ulanadi va ularda zaif xavfsizlik choralari bo'lishi mumkin.

IOT hujum maydoni: tahdidlar va xavfsizlik yechimlari. IoT bugungi kunda mavjud bo‘lgan eng ko‘p qirrali texnologiyalardan biridir. Internetning keng tarqalganligi, tarmoq ulanishining o‘sib borayotgan sig'imi va ulangan qurilmalarning xilma-xilligi IoT-ni kengaytiriladigan va moslashuvchan qiladi. Oziq-ovqat ishlab chiqarish, korxonalar, moliya, sog'liqni saqlash va energetika kabilar IoT inqilob qilgan sohalarning bir nechtasi, xususan uning kengayishi, sanoat buyumlar interneti bilan bog’liq. Shu bilan birga, u aqlli uylar, binolar va hatto shaharlarni ham yaratishga oshirishga olib keldi.

Biroq, IoTning tobora ortib borayotganligi uning mumkin bo‘lgan oqibatlarini tan olishni ham anglatadi. Masalan korxona sharoitida, IoT ko‘pincha ofisni avtomatlashtirish (OA) va operatsion texnologiyalar (OT) sohalarida uchraydi. Bu tashkilot ichida joylashtirilgan bir nechta IoT va IIoT qurilmalariga aylanadi. Bunday o‘rnatish hech qachon kiberxavfsizlik xavfini tug'dirmagan bo‘shliqlarda tahdidlar ehtimolini oshiradi. Ushbu umumiy maydonlardagi IoT qurilmalari IoT tizimlarining ma'lumotlarni yig'ish va monitoring qilish imkoniyatlari orqali intranet va ma'lumotlar bazasi serverlari kabi muhim tizimlarga ta'sir ko‘rsatishi mumkin. Natijada, hatto aqlli xonalar va aqlli qahva mashinalari kabi zararsiz ko‘rinadigan IoT qurilmalarini o‘z ichiga olgan tahdidlar ham ular o‘rnatilgan muhitga qarab katta ta'sir ko‘rsatishi mumkin.

IoT bugungi kunning voqeligi, yashash tarzining bir qismi, shuning uchun texnologiya u qo‘llaniladigan muhitga - IoT tizimlari va qurilmalari nuqtai nazaridan muvaffaqiyatli hujumlarga olib kelishi mumkin bo‘lgan xavfsizlik muammolarini batafsil o‘rganib chiqish alohida masala hisoblanadi.

IOT xavfsizlikka ta'sir qilish jihatlari. IoT tizimlari va qurilmalariga tahdidlar, asosiy texnologiyaga ega bo‘lgan ba'zi xususiyatlar tufayli kattaroq xavfsizlik xatarlariga aylanadi. Ushbu xususiyatlar IoT muhitlarini funktsional va samarali qiladi, ammo ular tahdid qiluvchilar tomonidan suiste'mol qilinishi mumkin. Bu xususiyatlarga quyidagilar kiradi:

- Katta hajmdagi ma’lumotlarni to‘plash. IoT sensorlari va qurilmalari o‘zlarining muhitlari va foydalanuvchilaridan juda batafsil ma'lumotlarni to‘playdi. Bu ma’lumotlar IoT muhitlarining to‘g‘ri ishlashi uchun zarur. Biroq, bu ma'lumotlar himoyalanmagan yoki o‘g'irlangan yoki boshqa tarzda buzilgan bo‘lsa, bir nechta kaskadli salbiy ta'sirlarni anglatishi mumkin.
- Virtual va jismoniy muhitlarning ulanishi. Ko‘pgina IoT qurilmalari o‘z muhitlaridan olgan ma'lumotlar bilan ishlashga qodir. Bu qobiliyat virtual va jismoniy tizimlar orasidagi masofani qisqartiradi. Ammo foydalanuvchilar uchun qulay bo‘lsa-da, u kibertahdidlarning jismoniy oqibatlarga tezroq aylanishiga imkon beradi va shu bilan xavfsizlikka ta'sir ko‘rsatadi.

- Arxitekturani markazlashtirish. IoT tizimlariga an’anaviy markazlashtirilgan arxitekturani qo‘llash xavfsizlikka salbiy ta’sir ko‘rsatishi mumkin. Markazlashtirilgan arxitektura shuni anglatadiki, har bir qurilma va sensor tomonidan to‘plangan ma'lumotlar bazaviy stansiyaga uzatiladi. Korxonada katta hajmdagi ma'lumotlarni to‘playdigan minglab qurilmalar tomonidan ishlatiladigan asosiy ma'lumotlar bazasi bir xil bo‘lishi mumkin. Bu alohida ma'lumotlar bazalariga qaraganda kam xarj bo‘lishi mumkin, ammo u bitta tugunga murakkab tarzda bog'langan hujum maydoni xavfini yanada oshiradi.

IoT ning hujum maydoni ta’rifi. IoT loyihasining bir qismi sifatida, Ochiq veb-ilovalar xavfsizligi loyihasi (OWASP) IoT hujumlari maydoni (yuzasi) yoki IoT tizimlari va ilovalaridagi tahdidlar va zaifliklar mavjud bo‘lgan sohalar ro‘yxatini e'lon qildi . Quyida IoT hujumi maydonlarining qisqacha mazmuni keltirilgan:

- Qurilmalar. Qurilmalar hujumlarni boshlashning asosiy vositasi bo‘lishi mumkin. Zaifliklar kelib chiqishi mumkin bo‘lgan qurilma qismlari uning xotirasi, proshivka, jismoniy interfeys, veb-interfeys va tarmoq xizmatlaridir. Buzg'unchilar, shuningdek, boshqa xavfsiz bo‘lmagan standart sozlamalar, eskirgan komponentlar va xavfsiz yangilanish mexanizmlaridan foydalanishlari mumkin.
- Aloqa kanallari. Hujumlar IoT komponentlarini bir-biri bilan bog'laydigan kanallardan kelib chiqishi mumkin. IoT tizimlarida ishlatiladigan protokollar butun tizimlarga ta'sir qilishi mumkin bo‘lgan xavfsizlik muammolariga ega bo‘lishi mumkin. IoT tizimlari xizmatni rad etish (Denial of Service, DoS) va firibgarlik kabi ma'lum tarmoq hujumlariga ham sezgir.
- Ilovalar va dasturlar. IoT qurilmalari uchun veb-ilovalar va tegishli dasturiy ta'minotdagi zaifliklar buzilgan tizimlarga olib kelishi mumkin. Masalan, veb-ilovalar foydalanuvchi hisob ma'lumotlarini o‘g'irlash yoki zararli dasturiy ta'minot yangilanishlarini surish uchun ishlatilishi mumkin. IoT tahdidlarining kengayishi va tarqashi. IoT internetga ulangan jismoniy qurilmalar, transport vositalari va maishiy texnikalarning o‘sib borayotgan tarmog'ini anglatadi. Ushbu qurilmalar ma'lumotlarni to‘playdi va almashadi, bu esa biznes va iste'molchilar uchun yangi imkoniyatlar yaratadi. IoT, shuningdek, chekka hisoblash tarmoqlarini quvvatlantiradi va ma'lumotlarni kerakli joyga yaqinroq yetkazib berishga imkon beradi. Bu o‘z-o‘zidan boshqariladigan avtomobillardan tortib operatsion texnologiyalarni masofadan nazorat qilishgacha bo‘lgan hamma narsaga ta'sir qiladi.

IoT xavfsizligi nima uchun muhim?

Kiberhujumlar va zararli dasturlar: IoT qurilmalari tarmoqqa ulanishda foydalanilsa, ular kiberhujumlar va zararli dasturlarning maqsadi bo'lishi mumkin. Bu qurilmalar xakerlar tomonidan botnetlarga aylantirilishi yoki ma'lumotlar o'g'irlanishi uchun ishlatilishi mumkin.

Maxfiylik: IoT qurilmalari shaxsiy va nozik ma'lumotlarni (masalan, sog'liqni saqlash, uyda yashovchi insonlar haqida) yig'ishi va uzatishi mumkin, bu esa maxfiylik muammolarini keltirib chiqaradi.

Integratsiya va ko'p qurilma ishlashi: IoT tizimlari bir nechta qurilma va platformalarning integratsiyasi orqali ishlaydi, shuning uchun xavfsizlikni ta'minlashda murakkabliklar paydo bo'lishi mumkin.

IoT xavfsizligining asosiy sohalari:

1. **Qurilma xavfsizligi**:

IoT qurilmalarining o'zlari himoyasiz bo'lishi mumkin. Ular zaif parollar, kam shifrlash yoki nosoz xavfsizlik protokollari bilan jihozlangan bo'lishi mumkin. Qurilmalarga kirishni nazorat qilish uchun kuchli autentifikatsiya va shifrlash usullari kerak.

2. **Ma'lumotlar xavfsizligi**:

IoT qurilmalaridan olingan ma'lumotlar tarmoq orqali uzatiladi va ko'plab qurilmalar tomonidan ishlanadi. Ma'lumotlar shifrlanishi va integriteti (butunligi) ta'minlanishi kerak. Agar ma'lumotlar zararlansa yoki o'g'irlanadigan bo'lsa, bu katta xavf tug'dirishi mumkin.

3. **Tarmoq xavfsizligi**:

IoT qurilmalari tarmoqqa ulanadi va ular orqali ma'lumotlar almashiladi. Tarmoqni himoya qilish uchun xavfsizlik devorlari, tarmoqni shifrlash, va xavfsiz ulanish protokollari (masalan, VPN) ishlatiladi. IoT tarmoqlarini maxsus xavfsizlik devorlari va monitoring vositalari orqali himoya qilish zarur.

4. **Qurilma autentifikatsiyasi va avtorizatsiyasi**:

IoT qurilmalariga kirish uchun kuchli autentifikatsiya va avtorizatsiya mexanizmlari joriy etilishi zarur. Bu foydalanuvchi yoki qurilmaning huquqini tasdiqlash va ruxsat etilgan faoliyatni amalga oshirish uchun ishlatiladi.

5. **Zararli dasturlar va botnetlar**:

IoT qurilmalari zararli dasturlar va botnetlar uchun nishon bo'lishi mumkin. Bu dasturlar qurilmalarda ishlash orqali tarmoqni bostirish yoki hujumlar amalga oshirishga yordam beradi. IoT qurilmalarini doimiy ravishda yangilab borish va zararlardan himoya qilish zarur.

6. **Xavfsizlik yangilanishlari (patches)**:

IoT qurilmalari va tizimlarining doimiy yangilanishi xavfsizlikni ta'minlashda muhim rol o'ynaydi. Yangilanishlar xavfsizlikdagi zaifliklarni tuzatadi va yangi tahdidlarga qarshi kurashishga yordam beradi.

7. **Zero Trust Model (ZTM)**:

Zero Trust modeliga ko'ra, har bir IoT qurilmasiga kirish yoki tarmoqga ulanayotganda doimiy tekshiruv va tasdiqlash talab qilinadi. Bu model tarmoqdagi har bir qurilmani potentsial xavf sifatida ko'radi va uni tekshiradi.

IoT xavfsizligini ta'minlash uchun strategiyalar:

1. **Tarmoqni shifrlash**:

IoT qurilmalaridan uzatilayotgan ma'lumotlarni shifrlash, xususan, internet orqali uzatilayotgan ma'lumotlarni himoya qilish uchun SSL/TLS kabi xavfsiz protokollarni qo'llash zarur.

2. **Kuchli parollar va autentifikatsiya**:

IoT qurilmalarining parollari murakkab bo'lishi kerak va avtomatik ravishda o'zgartirilishi kerak. Foydalanuvchilarga ikki faktorli autentifikatsiya (2FA) va biometrik autentifikatsiya kabi xavfsizlik choralari taklif etilishi kerak.

3. **Qurilmalarning tez-tez yangilanishi**:

IoT qurilmalari uchun ishlab chiqaruvchilar xavfsizlik yangilanishlarini tez-tez chiqarishlari kerak. Bu yangilanishlar xavfsizlik zaifliklarini tuzatadi va qurilmalarning xavfsiz ishlashini ta'minlaydi.

4. **Xavfsiz tarmoq arxitekturasi**:

IoT qurilmalarini tarmoqqa ulashda xavfsiz tarmoq arxitekturasi yaratish, masalan, qurilmalarni alohida subnetlarda joylashtirish, ma'lumotlarni segmentatsiya qilish va xavfsizlik devorlarini qo'llash kerak.

5. **IoT xavfsizlik protokollarini joriy etish**:

IoT qurilmalari uchun xavfsizlik protokollari va standartlarini qo'llash, masalan, HTTPS, MQTT, CoAP, va boshqa xavfsiz tarmoq protokollarini qo'llash kerak.

Xulosa: Yuqorida aytib o‘tilgan IoT hujumi maydonlaridan xulosa qilish mumkinki, IoT tizimlarining barcha asosiy tarkibiy qismlaridan foydalanish mumkin. Shuning uchun IoT tizimlarini yaratish va saqlashda xavfsizlik ustuvor bo‘lishi kerak. IoT tizimi qanday miqyosda va qanday muhitda o‘rnatilgan bo‘lishidan qat'iy nazar, xavfsizlikni tizimning har bir jihatiga yaxshiroq integratsiya qilish uchun dizayn bosqichidan boshlab ko‘rib chiqish kerak. Shu tarzda, IoT tizimi individual qurilmalaridan tortib umumiy konfiguratsiyasigacha ham funktsional, ham xavfsiz bo‘lishi uchun moslashtirilishi mumkin. IoT xavfsizligi, IoT tizimlarining samarali va xavfsiz ishlashini ta'minlash uchun doimiy ehtiyotkorlik, zamonaviy texnologiyalarni joriy etish va xavfsizlik choralari bilan mustahkamlanishi kerak. Qurilmalarning tarmoqqa ulanishi va ma'lumotlar almashinuvi ortib borishi bilan, IoT xavfsizligini ta'minlash har bir qurilma, tarmoq va foydalanuvchi uchun yuqori darajada e'tiborli bo'lishi zarur. IoT xavfsizligini ta'minlash uchun ham texnik, ham strategik choralar doimiy ravishda yangilanishi va kuchaytirilishi kerak.

FOYDALANILGAN ADABIYOTLAR:

1.Neubert, H. K. P., Instrument Transducers, 2d ed., Clarendon Press, Oxford, 1975.

2.Ogata, K., Modern Control Engineering, 2d ed., Prentice-Hall, Englewood Cliffs, N.J., 1990.

3.Rock, I., Lightness Constancy, Perception, W. H. Freeman, New York, 1984.

4.Seippel, R. G., Optoelectronics, Reston Publishing Co., Reston, Va., 1981. 5.Shortley, G., and D. Williams, Quantum Property of Radiation, Prentice-Hall, Englewood Cliffs, N.J., 1971.

6.Chappel, A. (ed.), Optoelectronics: Theory and Practice, McGraw-Hill, New York, 1978.

7.Doebelin, E. O., Measurement Systems: Application and Design, 4th ed., McGraw-Hill, New York, 1990.

8.https://cyberleninka.ru/article/n/iot-muhiti-xavfsizligining-zaif-tomonlari-va-oldini-olish-yechimlari

9.Holliday, D., and R. Resnick, Physics, Wiley, New York, 1975.