

O'RNATILGAN TIZIMLARDA XAVFSIZLIK MUAMMOLARI VA HIMOYA USULLARI

Xolmatov Murodil Zoxid o'g'li*Fargona davlat texnika universiteti talabasi***Azizbek Abdulxamidov Abdullayevich***Ilmiy raxbar: t.f.f.d PhD*

Annotatsiya: Ushbu maqolada o'rnatilgan tizimlarda uchraydigan asosiy xavfsizlik muammolari, ularning kelib chiqish sabablari hamda himoya usullari tahlil qilinadi. Zamonaviy aqlli qurilmalar, IoT texnologiyalari va mikrokontroller asosidagi tizimlarning keng tarqalishi bilan kiberxavfsizlik masalalari dolzarb bo'lib bormoqda. Maqolada autentifikatsiya, shifrlash, xavfsiz dasturlash va apparat himoyasi kabi usullar ko'rib chiqilgan.

Kalit so'zlar: o'rnatilgan tizimlar, IoT, kiberxavfsizlik, mikrokontroller, autentifikatsiya, shifrlash, himoya.

Abstract: This article discusses the main security problems of embedded systems, their causes, and protection methods. With the rapid development of smart devices, IoT technologies, and microcontroller-based systems, cybersecurity issues are becoming increasingly important. The paper examines authentication, encryption, secure programming, and hardware protection methods.

Keywords: embedded systems, IoT, cybersecurity, microcontroller, authentication, encryption, protection.

Аннотация: В данной статье рассматриваются основные проблемы безопасности встроенных систем, причины их возникновения и методы защиты. С распространением интеллектуальных устройств, IoT-технологий и систем на базе микроконтроллеров вопросы кибербезопасности становятся особенно актуальными. В статье анализируются методы аутентификации, шифрования, безопасного программирования и аппаратной защиты.

Ключевые слова: встроенные системы, IoT, кибербезопасность, микроконтроллер, аутентификация, шифрование, защита.

Kirish. O'rnatilgan tizimlar zamonaviy texnologiyalarning ajralmas qismiga aylangan. Ular avtomobillar, tibbiy qurilmalar, sanoat avtomatikasi, aqlli uy tizimlari va mobil qurilmalarda keng qo'llaniladi. Internet of Things (IoT) texnologiyalarining rivojlanishi bilan ushbu tizimlar internetga ulanib,

ma'lumot almashish imkoniyatiga ega bo'ldi. Biroq bu holat xavfsizlik bilan bog'liq muammolarni ham yuzaga keltirdi. Ko'plab o'rnatilgan tizimlar resurslari cheklanganligi sababli murakkab xavfsizlik mexanizmlarini qo'llash imkoniga ega emas. Natijada ular kiberhujumlar uchun oson nishonga aylanishi mumkin. Shu sababli o'rnatilgan tizimlarda xavfsizlikni ta'minlash dolzarb masalalardan biri hisoblanadi.

Methods. Maqolada o'rnatilgan tizimlar xavfsizligi bo'yicha ilmiy manbalar, texnik adabiyotlar va zamonaviy IoT qurilmalarining ishlash tamoyillari tahlil qilindi. Tadqiqot davomida tizimlarda uchraydigan asosiy xavfsizlik muammolari o'rganilib, ularni bartaraf etishning dasturiy va apparat usullari ko'rib chiqildi. Shuningdek, dasturiy ta'minotni muntazam yangilab borish, xavfsizlik monitoringini tashkil etish va foydalanuvchi ma'lumotlarini himoyalash ham zamonaviy o'rnatilgan tizimlar uchun muhim talab hisoblanadi. Biroq amaliyotda bu jarayonlarda bir qator muammolar yuzaga keladi, jumladan: qurilmalarning resurslari cheklanganligi sababli murakkab xavfsizlik algoritmlarini qo'llash qiyinligi, yangilanishlarni barcha qurilmalarga bir vaqtda yetkazishdagi texnik muammolar, hamda kiberhujumlarning tobora murakkablashib borishi. Bundan tashqari, ko'plab o'rnatilgan tizimlarda standartlashtirish yetarli darajada emasligi ham xavfsizlikni ta'minlashda qo'shimcha qiyinchiliklar tug'diradi.

Kelajakda sun'iy intellekt va bulutli texnologiyalar bilan integratsiyalashgan o'rnatilgan tizimlar yanada keng qo'llanilishi kutilmoqda. Biroq bu integratsiya yangi xavf-xatarlarni ham yuzaga keltiradi, masalan ma'lumotlar uzatishdagi maxfiylik buzilishi va tarmoq orqali hujumlar sonining ortishi. Shu sababli, xavfsizlikni loyihalash bosqichidan boshlab joriy etish, xavf-xatarlarni oldindan aniqlash va xalqaro xavfsizlik standartlariga amal qilish dolzarb vazifa bo'lib qoladi.

Natijada, o'rnatilgan tizimlarda ishonchli xavfsizlik mexanizmlarini qo'llash nafaqat qurilmalar barqarorligini ta'minlaydi, balki foydalanuvchilarning shaxsiy ma'lumotlari va tarmoq infratuzilmasini himoya qilishda ham muhim rol o'ynaydi. Shu bilan birga, xavfsizlikka oid ilmiy tadqiqotlarni rivojlantirish va malakali mutaxassislarni tayyorlash ushbu sohaning kelajakdagi taraqqiyotida katta ahamiyat kasb etadi.

Natijalar. O'rnatilgan tizimlarda xavfsizlik muammolari

1. Ruxsatsiz kirish Ko'plab qurilmalarda oddiy yoki standart parollar ishlatiladi. Bu esa hujumchilarga tizimga oson kirish imkonini beradi.

2. Dasturiy zaifliklar Noto'g'ri yozilgan dastur kodi xotira toshib ketishi (buffer overflow), zararli kod ishlashi yoki tizimning ishdan chiqishiga olib kelishi mumkin.

3. Ma'lumotlarni ushlab qolish Tarmoq orqali yuborilgan ma'lumotlar shifrlanmagan bo'lsa, ular uchinchi tomon tomonidan o'qilishi mumkin.

4. Fizik hujumlar Qurilmaning apparat qismiga to'g'ridan-to'g'ri kirish orqali mikrokontroller xotirasidagi ma'lumotlarni olish mumkin.

5. IoT qurilmalaridagi zaifliklar IoT qurilmalarining internetga doimiy ulanishi ularni viruslar va botnet hujumlariga duchor qiladi.

Himoya usullari

1. Kuchli autentifikatsiya

Murakkab parollar va ikki bosqichli autentifikatsiya tizim xavfsizligini oshiradi.

2. Ma'lumotlarni shifrlash

AES va RSA kabi shifrlash algoritmlaridan foydalanish ma'lumotlarni himoya qiladi.

3. Xavfsiz dasturlash

Dastur yozishda xavfsizlik standartlariga amal qilish tizimdagi zaifliklarni kamaytiradi.

4. Firmware yangilanishlari

Qurilma dasturini muntazam yangilab borish xavfsizlik xatolarini tuzatishga yordam beradi.

5. Apparatura himoyasi

Mikrokontrollerlarda himoya bitlari va maxsus xavfsizlik modullaridan foydalanish fizik hujumlardan himoya qiladi.

Real vaqt OT arxitekturası

1.Yadro (kernel)

Real vaqt OTning asosiy qismi, resurslarni boshqarish, vazifalarni rejalashtirish va boshqa muhim funksiyalarni amalga oshiradi

2. Vazifalarni rejalashtirish

Vazifalarni belgilangan tartibda va vaqt chegaralarida bajarishni ta'minlaydigan algoritmlar.

Xulosa: O'rnatilgan tizimlar zamonaviy texnologiyalarning asosiy qismlaridan biri bo'lib, ularning xavfsizligini ta'minlash juda muhim hisoblanadi. IoT va aqlli qurilmalar sonining ortishi bilan kiberxavfsizlik muammolari ham ko'paymoqda. Ushbu maqolada o'rnatilgan tizimlarda uchraydigan asosiy xavfsizlik muammolari va ularni bartaraf etish usullari ko'rib chiqildi. Kuchli autentifikatsiya, shifrlash, xavfsiz dasturlash va apparat

himoyasi tizim xavfsizligini sezilarli darajada oshirishi mumkin. Shuningdek, dasturiy ta'minotni muntazam yangilab borish, xavfsizlik monitoringini tashkil etish va foydalanuvchi ma'lumotlarini himoyalash ham zamonaviy o'rnatilgan tizimlar uchun muhim talab hisoblanadi. Kelajakda sun'iy intellekt va bulutli texnologiyalar bilan integratsiyalashgan o'rnatilgan tizimlar yanada keng qo'llanilishi kutilmoqda. Shu sababli, xavfsizlikni loyihalash bosqichidan boshlab joriy etish, xavf-xatarlarni oldindan aniqlash va xalqaro xavfsizlik standartlariga amal qilish dolzarb vazifa bo'lib qoladi.

Natijada, o'rnatilgan tizimlarda ishonchli xavfsizlik mexanizmlarini qo'llash nafaqat qurilmalar barqarorligini ta'minlaydi, balki foydalanuvchilarning shaxsiy ma'lumotlari va tarmoq infratuzilmasini himoya qilishda ham muhim rol o'ynaydi. Shu bilan birga, xavfsizlikka oid ilmiy tadqiqotlarni rivojlantirish va malakali mutaxassislarni tayyorlash ushbu sohaning kelajakdagi taraqqiyotida katta ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR:

1. Karimov Q.X. O'rnatilgan tizimlar asoslari. – Toshkent, 2022.
2. Stallings W. Cryptography and Network Security. – Pearson Education, 2019.
3. David Simon. An Embedded Software Primer. – Addison-Wesley, 2018.
4. IoT Security Foundation. Embedded System Security Guide, 2023.
5. Barr M. Programming Embedded Systems in C and C++. – O'Reilly Media, 2020.
6. Microcontroller-Based Embedded Systems / Muhammad Ali Mazidi, Janice Gillispie Mazidi. – Pearson, 2021.
7. Embedded Systems Architecture / Daniele Lacamera. – Packt Publishing, 2021.
8. IEEE. Embedded Systems and IoT Security Standards, 2022.
9. The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors / Joseph Yiu. – Newnes, 2019.
10. NIST. Guidelines for IoT Device Cybersecurity, 2023.
11. Real-Time Concepts for Embedded Systems / Qing Li, Caroline Yao. – CMP Books, 2017.
12. Embedded Systems Design / Frank Vahid, Tony Givargis. – Wiley, 2019.

13. Practical Electronics for Inventors / Paul Scherz, Simon Monk. – McGraw-Hill Education, 2016.

14. Internet of Things / Rajkumar Buyya, Amir Vahid Dastjerdi. – Morgan Kaufmann, 2016.

15. Secure Coding in C and C++ / Robert C. Seacord. – Addison-Wesley, 2013.