DASTURIY-HIMOYALANGAN (FIRMWARE-BASED) XAVFSIZLIK: TIZIMLI DASTURLASH ORQALI QURILMALARNI MUHOFAZA QILISH

Umarov Begzodbek Azizovich
Farg‘ona davlat universiteti amaliy matematika va informatika kafedrasi o’qituvchisi ubaumarov@mail.ru
Ro‘ziyev Abdulloxon Yorqinbek o’g’li
Farg’ona davlat unversiteti, talaba
roziyevabdulloxon8@gmail.com

Annotatsiya: *Ushbu maqolada dasturiy-himoyalangan (firmware-based) xavfsizlik konsepsiyasi, uning tizimli dasturlash orqali amalga oshirilishi va zamonaviy qurilmalarni muhofaza qilishdagi ahamiyati tahlil qilinadi. Firmware xavfsizligi atrofida yuzaga keladigan tahdidlar va ularni bartaraf etish uchun qo‘llaniladigan tizimli dasturlash usullari, xotira boshqaruvi va xavfsiz yangilanish texnologiyalari batafsil ko‘rib chiqiladi.*

Kalitso‘zlar: *firmware, xavfsizlik, dasturiy-himoya, tizimli dasturlash, raqamli imzolash, ishonchli yuklash, xotira boshqaruvi, yangilanish, rootkit, bootkit, IoT, kriptografiya, xavfsizlik protokollari, tahdidlarni aniqlash, firmware tahdidlari*

Abstract: *This article analyzes the concept of firmware-based security, its implementation through systematic programming, and its significance in protecting modern devices. The threats surrounding firmware security and the systematic programming methods used to mitigate them, including memory management and secure update technologies, are examined in detail.*

Keywords: *firmware, security, software-based protection, systematic programming, digital signature, secure boot, memory management, update, rootkit, bootkit, IoT, cryptography, security protocols, threat detection, firmware threats*

Аннотация: *В данной статье анализируется концепция программно-защищенной (на основе прошивки) безопасности, её реализация посредством системного программирования и значение в защите современных устройств. Рассматриваются угрозы, связанные с безопасностью прошивки, а также методы системного программирования, применяемые для их устранения, включая управление памятью и технологии безопасного обновления.*

Ключевыеслова: *прошивка, безопасность, программная защита, системное программирование, цифровая подпись, безопасная загрузка, управление памятью, обновление, руткит, буткит, IoT, криптография, протоколы безопасности, обнаружение угроз, угрозы прошивки*

Kirish

Zamonaviy raqamli texnologiyalar hayotimizning deyarli barcha jabhalariga chuqur kirib borgan bir paytda, qurilmalar xavfsizligi tobora muhim va dolzarb masalaga aylanmoqda. Ayniqsa, Internetga ulangan aqlli qurilmalar sonining keskin ortib borayotgani fonida, bu qurilmalarni himoya qilishning ishonchli va chuqur darajali mexanizmlari zaruratga aylangan. Bu yerda so‘z aynan qurilmalarning past darajadagi dasturiy ta’minoti - ya’ni firmware haqida bormoqda. Firmware — bu qurilma ishga tushganda bevosita apparat bilan ishlovchi va ularning asosiy funktsiyalarini boshqaruvchi doimiy (va ko‘pincha o‘zgartirilishi cheklangan) dasturiy qatlamdir. U mikrokontrollerlar, BIOS/UEFI, printerlar, marshrutizatorlar, sanoat uskunalari va IoT qurilmalar kabi ko‘plab platformalarda muhim rol o‘ynaydi. So‘nggi yillarda ko‘plab kiberhujumlar aynan firmware qatlamiga qaratilgan bo‘lib, bu tahdidlar odatdagi operatsion tizim xavfsizlik choralari bilan aniqlanmasligi yoki to‘liq bartaraf etilmasligi bilan xavflidir. Masalan, “MoonBounce” deb nomlangan rootkit 2022 yilda aniqlangan bo‘lib, u UEFI firmware darajasida yashiringan va doimiy, sezilmas tarzda ishlagan. Bunday holatlar, firmware xavfsizligini mustahkamlashda tizimli dasturlash yondashuvlarining naqadar muhim ekanini ko‘rsatadi. Tizimli dasturlash orqali apparat resurslarini to‘g‘ridan-to‘g‘ri boshqarish, past darajadagi xavfsizlik protokollarini amalga oshirish va tahdidlarga real vaqtda javob berish imkoniyati yaratiladi.

Ushbu maqolada firmware darajasidagi xavfsizlik muammolari, ular bilan bog‘liq tahdidlar, va tizimli dasturlash asosida ishlab chiqilayotgan himoya usullari chuqur tahlil qilinadi. Shuningdek, real hayotdagi misollar yordamida zamonaviy qurilmalarni qanday qilib dasturiy-himoyalangan tarzda xavfsiz qilish mumkinligi ko‘rib chiqiladi. Bu mavzu nafaqat ilmiy-tadqiqot, balki amaliy sohalarda — ayniqsa sanoat, tibbiyot, mudofaa va mobil qurilmalar xavfsizligi uchun muhim ahamiyat kasb etadi.

Firmware - bu kompyuterlar, mikrokontrollerlar, tarmoqli qurilmalar, IoT tizimlari va boshqa ko‘plab elektron uskuna va tizimlarda ishlatiladigan past darajadagi dasturiy ta’minot bo‘lib, u qurilmaning asosiy funktsiyalarini nazorat qilish, uni ishga tushirish va boshqarish uchun xizmat qiladi. Firmware apparat va yuqori darajadagi dasturiy ta’minot o‘rtasida vositachi bo‘lib xizmat qiladi. U odatda qurilmaning o‘ziga o‘rnatilgan (yoki “ichki”) xotirada joylashgan bo‘ladi va ko‘pchilik hollarda foydalanuvchi tomonidan o‘zgartirilmaydi yoki faqat maxsus vositalar yordamida yangilanadi. Bu xususiyatlari uni odatiy dasturlar va operatsion tizimlardan ajratib turadi. Bugungi kunda firmware ko‘plab zamonaviy qurilmalar faoliyatida muhim rol o‘ynaydi. Masalan, kompyuter ishga tushayotganda birinchi bo‘lib ishga tushadigan BIOS yoki UEFI tizimlari aynan firmware hisoblanadi. Ular qurilmaning barcha asosiy apparat komponentlarini ishga tayyorlaydi, operatsion tizimni yuklaydi va undan keyin ham qurilmaning doimiy ishlashida ishtirok

etadi. Xuddi shunday, marshrutizatorlar, printerlar, aqlli maishiy texnika vositalari, avtomobil elektron tizimlari, mobil telefonlar va tibbiyot qurilmalari kabi juda ko‘p turdagi qurilmalar o‘z ichida firmware dasturiga ega. Bu shuni anglatadiki, firmware’ning har qanday zaifligi yoki noto‘g‘ri ishlashi, butun qurilmaning funksional ishlashiga va hattoki foydalanuvchi xavfsizligiga ham tahdid soladi.

Tizim xavfsizligi nuqtai nazaridan firmware ayniqsa xavfli qatlamlardan biridir. Chunki u foydalanuvchi darajasidagi dasturiy ta’minotdan pastroqda ishlaydi, odatda maxfiy va ko‘zga ko‘rinmas bo‘ladi, va shu sababli u orqali amalga oshiriladigan hujumlar ko‘pincha ancha kech aniqlanadi yoki umuman sezilmasdan qoladi. Shuningdek, firmware’ning o‘zi doimiy xotirada joylashgani uchun, unga kiritilgan zararli kod foydalanuvchi operatsion tizimini qayta o‘rnatish yoki diskni tozalash orqali ham bartaraf etilmasligi mumkin. Shu sababli, zamonaviy kiberxavfsizlikda firmware darajasidagi tahdidlar eng xavfli va murakkab muammolardan biri hisoblanadi. So‘nggi yillarda firmware bilan bog‘liq ko‘plab real hujumlar qayd etilgan. Masalan, “LoJax” va “MoonBounce” kabi rootkitlar UEFI firmware darajasida ishlaydi va kompyuter operatsion tizimi yuklanmasidan oldin ishga tushadi. Bu esa foydalanuvchi antiviruslari yoki himoya dasturlariga bu tahdidni aniqlashni imkonsiz qilishi mumkin. Bundan tashqari, ko‘plab IoT qurilmalarining firmware’lari juda soddalashtirilgan, zaif autentifikatsiya tizimlariga ega va yangilanish mexanizmlari mavjud emas. Bu esa ular orqali botnetlar yaratish, tarmoqqa hujum uyushtirish va ma’lumotlarni o‘g‘irlash kabi harakatlarni amalga oshirish imkonini beradi.

Firmware’ning xavfsizlikdagi o‘rni nafaqat tahdidlar, balki himoya vositasi sifatida ham ahamiyatlidir. Aynan tizimli dasturlash orqali ishlab chiqilgan barqaror va xavfsiz firmware komponentlari, qurilma darajasida ishonchli ishga tushirish (trusted boot), kodni imzolash (code signing), apparatni identifikatsiyalash va kriptografik tekshiruvlar kabi xavfsizlik mexanizmlarini ta’minlashi mumkin. Masalan, zamonaviy mikrokontrollerlarda firmware tasdiqlangan raqamli imzo asosida ishga tushiriladi, agar imzo mos kelmasa, qurilma bloklanadi yoki xavfsiz rejimga o‘tadi. Bu kabi yondashuvlar nafaqat viruslardan himoyalanish, balki ma’lumotlar maxfiyligini ta’minlash va qurilmalarni ruxsatsiz o‘zgartirishdan himoya qilish uchun ham xizmat qiladi. Tizimli dasturlash tamoyillaridan foydalanilgan holda yaratilgan firmware’lar apparat bilan bevosita ishlaydi, ya’ni protsessor registrlarini boshqarish, tarmoq interfeyslarini sozlash, xotira bo‘limlarini muhofaza qilish va tashqi qurilmalar bilan aloqani nazorat qilish kabi funktsiyalarni bajara oladi. Bu darajadagi boshqaruv firmware’ni nafaqat zaruriy texnik komponent, balki tizim xavfsizligini ta’minlashda muhim strategik vosita sifatida qarashga undaydi. Aynan shuning uchun bugungi kunda ko‘plab ishlab chiqaruvchilar firmware xavfsizligiga alohida e’tibor qaratmoqda va uni rivojlantirish uchun tizimli dasturchilarni jalb qilmoqda.

Birinchi navbatda, firmware kodining yaxlitligini ta’minlash muhimdir. Bu maqsadda raqamli imzolash va kriptografik autentifikatsiya keng qo‘llaniladi. Firmware fayli ishlab chiqaruvchi tomonidan raqamli imzo bilan tasdiqlanadi va qurilma ishga tushganda tizimli dastur ushbu imzoni tekshiradi. Agar imzo mos kelmasa, firmware ishga tushmaydi yoki qurilma xavfsiz rejimga o‘tadi. Bu usul zararli kodning firmware’ga qo‘shilishining oldini oladi va ruxsatsiz yangilanishlarga to‘sqinlik qiladi. Raqamli imzolash mexanizmlari, odatda, public-key kriptografiyasi asosida ishlaydi, bu esa xavfsizlikni yuqori darajaga ko‘taradi va firmware manbasining ishonchliligini kafolatlaydi.

Ikkinchi muhim usul - ishonchli yuklash mexanizmi (trusted boot) bo‘lib, u tizimning dastlabki bosqichlarida firmware va operatsion tizim yuklanishini xavfsiz tarzda nazorat qiladi. Ushbu mexanizm qurilma yoqilganda, birinchi navbatda firmware kodining yaxlitligini tekshiradi, keyin esa operatsion tizimni boshlaydi. Agar biror komponent buzilgan yoki o‘zgartirilgan bo‘lsa, tizim yuklanmaydi yoki muqobil, himoyalangan rejimga o‘tadi. Bu yondashuv yordamida zararli dasturlar tizim ishga tushishidan oldin bloklanadi va qurilmaning to‘liq ish faoliyatiga aralashishi oldi olinadi. Tizimli dasturlash bu jarayonda past darajadagi apparat resurslarini boshqarish orqali ishonchli boot jarayonini ta’minlaydi.

Uchinchidan, xotira boshqaruvi va ajratish tizimlari firmware xavfsizligining asosiy elementlaridan biridir. Tizimli dasturlash yordamida firmware’ning bajariladigan kodlari va ma’lumotlar qismi alohida xotira segmentlarida saqlanadi va bir-biridan mustaqil himoyalanadi. Bu usul orqali biror zararli dastur yoki xatolik natijasida xotira buzilishi, ma’lumotlar yoki kodning noto‘g‘ri o‘zgartirilishi ehtimoli kamayadi. Bundan tashqari, ba’zi ilg‘or tizimli dasturlash yondashuvlarida xotira himoyasi va cheklovlari apparat tomonidan ham qo‘llab-quvvatlanadi, masalan, Memory Protection Unit (MPU) yoki Memory Management Unit (MMU) orqali, bu esa xavfsizlikni yanada mustahkamlaydi.

To‘rtinchidan, firmware yangilanishining xavfsizligini ta’minlash muhim ahamiyatga ega. Ko‘plab qurilmalarda firmware yangilanishi zarur bo‘lib, noto‘g‘ri yoki ruxsatsiz yangilanish qurilmani zaiflashtirishi mumkin. Shu sababli, tizimli dasturlash usullari firmware yangilanish paketlarini raqamli imzo bilan tasdiqlash, yangilanish jarayonini shifrlash va ishonchli tranzaktsion mexanizmlar orqali amalga oshirishni ta’minlaydi. Bunday mexanizmlar yangilanish jarayonida xatolik yuz bersa, qurilmani avvalgi xavfsiz holatga qaytarishga imkon beradi, bu esa qurilmaning doimiy ishlashini kafolatlaydi.

Firmware tahdidlarining turlari juda xilma-xildir va ular zamonaviy raqamli qurilmalar xavfsizligiga jiddiy tahdid solmoqda. Eng ko‘p uchraydigan firmware tahdidlari orasida rootkitlar, bootkitlar, manipulyatsiya va zaifliklardan foydalanish, zararli yangilanishlar, shuningdek, fizik va tarmoqli hujumlar bor. Rootkitlar — bu zararli dasturlar bo‘lib, ular firmware darajasida yashirincha ishlaydi va qurilmaning pastki qatlamlarini nazorat qilib,

odatiy xavfsizlik vositalaridan yashirinadi. Masalan, MoonBounce rootkiti 2022 yilda aniqlangan bo‘lib, u UEFI firmware’ga o‘rnatilgan va tizim ishga tushishidan oldin ishga tushib, yuqori darajadagi nazoratni qo‘lga kiritgan. Bu rootkit ko‘plab antivirus dasturlari va xavfsizlik tizimlari tomonidan aniqlanmasligi bilan xavflidir.

Bootkitlar esa BIOS yoki UEFI tizimiga zarar yetkazadigan, shu bilan butun operatsion tizimning ishga tushishini nazorat qiluvchi zararli dasturlar hisoblanadi. Ular qurilma yoqilganda ishga tushib, tizimni nazorat qiladi va foydalanuvchining xavfsizlik choralarini chetlab o‘tadi. Bootkitlar eng xavfli tahdidlardan biri bo‘lib, ularni bartaraf etish juda qiyin. Masalan, LoJax bootkiti, 2018 yilda kashf etilgan, foydalanuvchi BIOS yoki UEFI firmware’ga zarar yetkazib, qurilmaning butun xavfsizlik tizimini buzgan.

Firmware’ga zararli yangilanishlar ham keng tarqalgan muammo hisoblanadi. Agar firmware yangilanish jarayoni yetarlicha himoyalanmagan bo‘lsa, hujumchi zararli kodni yangilanish sifatida o‘rnatishi mumkin. Bu esa qurilmaning uzoq muddat davomida nazorat ostida qolishiga olib keladi. Misol uchun, 2017 yilda tarmoqlar orqali IoT qurilmalarga zarar yetkazish uchun firmware yangilanish orqali kirib borilgan bir nechta hujum holatlari qayd etilgan. Bu qurilmalar zararli botnet tarmoqlariga aylantirilgan va ulardan katta hajmdagi tarmoq hujumlari uyushtirilgan. Bundan tashqari, firmware zaifliklaridan foydalanish orqali hujumchilar qurilma funksiyalarini manipulyatsiya qilishi mumkin. Masalan, ma’lum bir qurilmaning firmware’dagi zaiflik yordamida hujumchi o‘zining kodini ishga tushirishi yoki ma’lumotlarni o‘g‘irlashi mumkin. Ushbu turdagi tahdidlar ko‘pincha tahlil qilish uchun qiyin bo‘lib, ko‘plab qurilmalarda uzoq vaqt davomida aniqlanmay qoladi. Misol tariqasida, 2020 yilda aniqlangan turli sanoat uskunalaridagi firmware zaifliklari keltirilishi mumkin, ular xavfsizlikka jiddiy zarar yetkazgan. Fizik hujumlar ham firmware tahdidlariga kiradi. Bu turdagi hujumlarda hujumchi qurilmaga bevosita jismoniy kirish imkoniga ega bo‘lib, firmware kodini o‘zgartirish yoki manipulyatsiya qilish imkoniyatiga ega bo‘ladi. Masalan, mikrokontrollerlar yoki aqlli kartalardagi firmware’ga bevosita kirish usullari orqali ma’lumotlarni o‘g‘irlash yoki qurilmani buzish holatlari mavjud.

Tarmoqli hujumlar ham firmware darajasida amalga oshirilishi mumkin. Masalan, tarmoqga ulangan printer, marshrutizator yoki boshqa qurilmaning zaif firmware’lari orqali hujumchilar tarmoqqa kirib, ma’lumotlarni o‘g‘irlash, qurilmani nazorat qilish yoki tarmoqning boshqa qurilmalariga zarar yetkazishlari mumkin. Bu kabi holatlar 2016 yilda Mirai botneti orqali yuzaga kelgan, u IoT qurilmalarining zaif firmware’laridan foydalanib, dunyodagi ko‘plab tarmoqlarga zarar yetkazgan. Umuman olganda, firmware tahdidlarining turi va ularning murakkabligi qurilmalarning o‘ziga xosligiga, ularning ishlash sohasiga va ularni himoya qilish darajasiga bog‘liq. Zamonaviy qurilmalarda firmware himoyasi yuqori

darajada bo‘lishi kerak, chunki bu qatlamsiz xavfsizlikni ta’minlashning asosiy kalitidir. Real hayotdagi misollar ko‘rsatadiki, firmware tahdidlarini e’tiborsiz qoldirish katta xavflarga olib keladi va tizimli dasturlash orqali ularni bartaraf etish uchun kompleks yechimlar ishlab chiqilishi shart.

Xulosa

Firmware darajasidagi tahdidlar zamonaviy raqamli qurilmalar xavfsizligiga bevosita ta’sir qiluvchi eng murakkab va xavfli muammolardan biri hisoblanadi. Rootkitlar, bootkitlar, zararli yangilanishlar, zaifliklardan foydalanish va fizik hamda tarmoqli hujumlar kabi turli tahdid turlari firmware himoyasining zaif tomonlarini fosh qiladi va qurilmalarning ishonchliligini, shuningdek, ma’lumotlarning maxfiyligi va yaxlitligini buzadi. Real hayotdagi misollar ushbu tahdidlarning nafaqat nazariy, balki amaliy jihatdan jiddiy oqibatlarga olib kelishini ko‘rsatadi. Shu bois, firmware xavfsizligini ta’minlash uchun tizimli dasturlash usullari va zamonaviy kriptografik texnologiyalarni keng joriy etish zarur.

Kelajakda firmware tahdidlariga qarshi kurashish samaradorligini oshirish uchun yangi yondashuvlar va texnologiyalar ishlab chiqilishi muhimdir. Jumladan, sun’iy intellekt va mashinani o‘rganish texnologiyalarini firmware monitoring va tahdidlarni aniqlash jarayonlariga integratsiya qilish, ishonchli yuklash tizimlarini yanada takomillashtirish, hamda apparat va dasturiy ta’minotning yanada chuqurroq integratsiyasini ta’minlash istiqboldagi asosiy yo‘nalishlardir. Shuningdek, firmware uchun standartlashtirilgan xavfsizlik protokollarini yaratish va ularni keng joriy etish, qurilmalarning turli turlari va ishlab chiqaruvchilari o‘rtasida xavfsizlikni bir xilda ta’minlash imkonini beradi.

Xulosa qilib aytganda, firmware xavfsizligi zamonaviy texnologik infratuzilmaning mustahkam poydevori hisoblanadi. Tizimli dasturlash asosida yaratilgan himoya choralari va ilg‘or texnologiyalar yordamida firmware tahdidlaridan himoyalanish imkoniyati sezilarli darajada oshadi. Shu bois, kiberxavfsizlik sohasi mutaxassislari, ishlab chiqaruvchilar va tadqiqotchilar firmware himoyasini rivojlantirishga katta e’tibor qaratishi lozim. Bu nafaqat individual qurilmalarning ishonchliligini, balki butun raqamli ekotizimning xavfsizligini ta’minlash uchun zarurdir.

Foydalanilgan adabiyotlar:

1. Stallings, W. *Operating Systems: Internals and Design Principles*. Pearson, 2018.
2. Tanenbaum, A. S., Bos, H. *Modern Operating Systems*. Pearson, 2015.
3. S. Checkoway et al., “Return-Oriented Programming Without Returns,” *ACM CCS*, 2010.
4. Costin, A., Zarras, A., “A Large-Scale Analysis of the Security of Embedded Firmwares,” *NDSS*, 2014.
5. Chen, S., et al., “Understanding and Securing the Firmware Update Mechanism,” *IEEE Security & Privacy*, 2017
6. Yunis, M. va Yassir, A. (2020). Aqlli shaharlarda IoT: IoT aloqa texnologiyalarini har tomonlama ko'rib chiqish. Kelajak avlod kompyuter tizimlari, 108, 202-213.
7. Gubbi, J., Buyya, R., Marusic, S. va Palaniswami, M. (2013). Narsalar Interneti (IoT): Vizyon, arxitektura elementlari va kelajak yo'nalishlari. Kelajakdagi avlod kompyuter tizimlari, 29(7), 1645-1660.
8. Raza, S., Wallgren, L. va Voigt, T. (2017). Kam quvvatli keng tarmoqli tarmoqlar: IoT ilovalari uchun keyingi chegara. Kompyuter bilan aloqa, 89-90, 11-20.
9. Umarov, B., G'ulomjonova, S. (2024). BULUT TEXNOLOGIYASI VA ULARDAN FOYDALANISH. Zamonaviy ta'limda innovatsion tadqiqotlar,
10. Azizovich UB. INNOVATSION TEXNOLOGIYALAR ORQALI O'QITUVCHILAR KOMETANSIYATINI SHAKLLANTIRISH TASOSIYLARI. Finlyandiya xalqaro ta'lim ilmiy jurnali. Ijtimoiy va gumanitar fanlar. 2023
11. B.Umarov., M.Umarova. THE PROBLEM OF APPROXIMATING SIGNALS BASED ON MODELING OF WAVELET - HAAR TRANSFORMATION. - 2020.