MULTIINTERFEYSLI USB QURILMALARNI AVTOMATIK IDENTIFIKATSIYALASHDA METAMA'LUMOTLARNING AHAMIYATI

PhD, dotsent **Nishanov I.I., Mamajonov J.M.**

Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

ANNOTATSIYA

Bugungi kunda dunyoda ishlab chiqilayotgan multiinterfeysli USB qurilmalar bur vaqtni o'zida bir nechtagacha interfeyslarni qo'llab quvvatlash imkoniyatiga ega. Biroq bunday multiinterfeysli USB qurilmalarga HID interfeyslarni yashirish yo'li orqali kiberhujumlarni amalga oshirish imkoniyatlari paydo bo'lmoqda. HID klassidagi USB qurilmalarning funksionalligi va murakkabligining ortib borishi orqali ularni avtomatik identifikatsiya qilish murakkablashib bormoqda. Maqolada yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiya qilishda metama'lumotlardan foydalanilanishning ahamiyati haqida gap boradi. Tadqiqot davomida yashirin HID interfeyslarning xususiyatlarini aniqlash imkoniyatlari o'rganiladi va samarali identifikatsiya qilishda metama'lumotlardan foydalanish usuli batafsil ko'rib chiqiladi.

Kalit so'zlar: USB, interfeys, qurilma, deskriptor jadvallari, klass, HID, identifikator, sozlanma, identifikatsiya, metama'lumot, vendor, ma'lumotlar bazasi.

АННОТАЦИЯ

Разрабатываемые сегодня мултиинтерфейсные USB-устройства способны поддерживать несколько интерфейсов одновременно. Однако существуют возможности для кибератак скрыть HID-интерфейсы на таких мултиинтерфейсных USB-устройствах. По мере увеличения функциональности и сложности USB-устройств класса HID их автоматическая идентификация становится все сложнее. В статье рассматривается важность использования метаданных при автоматической идентификации USB-устройств со скрытым HID-интерфейсом. В исследовании изучаются возможности идентификации характеристик скрытых HID-интерфейсов и подробно рассматривается метод использования метаданных для эффективной идентификации.

Ключевые слова: USB, интерфейс, устройство, таблицы дескрипторов, класс, HID, идентификатор, конфигурация, идентичность, метаданные, вендор, база данных.

ABSTRACT

Multi-interface USB devices being developed today are capable of supporting multiple interfaces simultaneously. However, there are opportunities for cyber-attacks to hide the HID interfaces on such multi-interface USB devices. As USB HID devices increase in functionality and complexity, automatic identification becomes increasingly difficult. The article discusses the importance of using metadata in automatically identifying USB devices with a hidden HID interface. The study explores the ability to identify the characteristics of hidden HID interfaces and details the method of using metadata for effective identification.

Keywords: USB, interface, device, descriptor tables, class, HID, identifier, configuration, identity, metadata, vendor, database.

Har qanday tizimning boshqaruvini samarali amalga oshirish uchun undagi boshqaruv obyektlari haqida o‘z vaqtida ishonchli ma’lumotlarga ega bo‘lish lozim. Boshqaruv obyektlarini tezkor identifikatsiya qilish, ular haqida ma’lumotlarni to‘plash va qayta ishlashda AIDC (Automatic Identification and Data Capture) usulidan foydalaniladi. Avtomatik identifikatsiya va ma’lumotlarni to‘plash (AIDC) - obyektlarni avtomatik ravishda tanib olish usullarini, ular haqida ma’lumotlar to‘plashni va ma’lum qoidalar asosida inson aralashuvisiz ularni kompyuter tizimlariga kiritishni anglatadi[1]. Avtomatik identifikatsiya va ma’lumotlarni to‘plash (AIDC) ko‘p manbalarda “avtomatik identifikatsiya”, “avtoidentifikatsiya”, “avtomatik ma’lumotlarni yig‘ish” deb ataladi[2] va bugungi kunda shbu usuldan inson shaxsni tasdiqlashda foydalaniladi. Avtomatik identifikatsiya biror bir shaxs yoki obyektga tegishli tasvir, tovush yoki videolarni tahlil qilish jarayoni bo‘lib, ularning cheklangan hudud yoki tizimga kirishiga ruxsat berish uchun ma’lumotlari maxsus bazadagi ma’lumotlar bilan solishtirib chiqiladi. Odatda Avtomatik identifikatsiya va ma’lumotlarni to‘plashda (AIDC) QR kodlar, shtrix-kodlar, radiochastotalarni identifikatsiyalash (RFID), biometrika (ko‘z qorachig‘i va yuzni aniqlash kabi), magnit chiziqlar, belgilarni optik aniqlash (OCR), smart-kartalar va ovozni aniqlash texnologiyalaridan foydalaniladi.

Bugungi kunda dunyoda avtomatik identifikatsiya uchun quyidagi usullardan foydalaniladi[3]:

• *Akustik-magnit ma’lumotni o‘qish* magnitlangan elementga (magnit karta) ega plastinkadan foydalanishga asoslangan bo‘lib, unda magnit lentadagi kabi kerakli ma’lumotlar qayd etiladi hamda bu usuldan ma’lum xizmatlarga debet kartalar, kirish kartalari orqali ruxsat berish uchun foydalaniladi;

• *Radiochastotali identifikatsiyalash* (RFID texnologiyasi) identifikatsiya qilinayotgan ob’yektga kam quvvatli radiouzatkich (transponder) joylashtirish va u

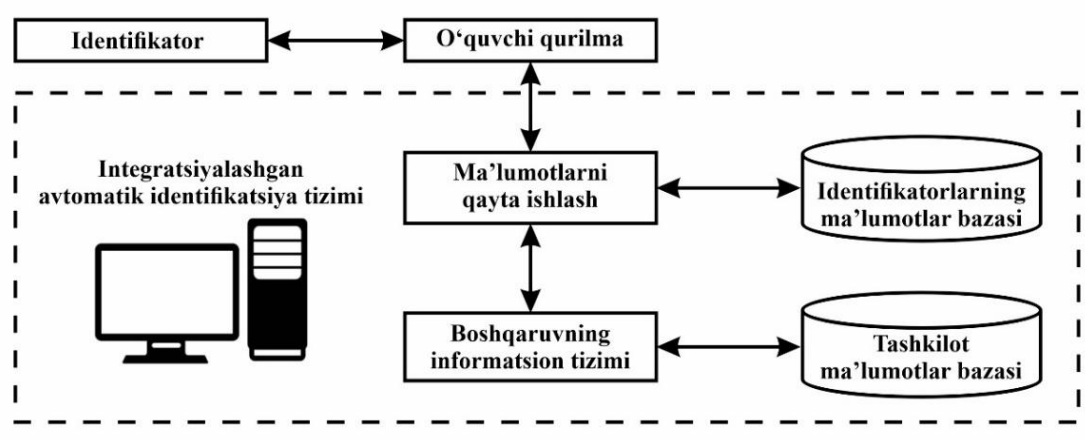
orqali hotiradagi shaxsga doir uzatilayotgan ma’lumotlar ikkinchi tomondan o‘qish qurilmasi (rider) yordamida qabul qilish orqali amalga oshiriladi;

• *Optik tanib olish usulida* shtrix-kod ko‘rinishidagi etiketka obyektga birkitiladi va undagi belgilar maxsus qurilma orqali tanib olinadi. Ushbu usul oziq ovqat, kiyim kechak maxsulotlarini identifkatsiya qilishda keng qo‘llaniladi.

• *Biometrik identifikatsiya* tizim subyektlarining o‘ziga xos jismoniy xususiyatlarini o‘lchashga asoslanadi hamda yuqori darajadagi identifikatsiyaning ishonchliligi, biometrik xususiyatlarning ob’yektdan ajralmasligi va ularni qalbakilashtirishning yuqori murakkabligi bilan tavsiflanadi. Shaxsni identikatsiya qilishda aynan shu usuldan keng foydalaniladi.

Avtomatik identifikatsiya tizimida (1-rasm) ob’yektiga o‘rnatilgan identifikator ma’lumotlari o‘qib oluvchi qurilma tomonidan tanib olinib, qayta ishlash uchun uzatilgandan so‘ng identifikatorlar bazasidagi ma’lumotlardan foydalangan holda autentifikatsiya va avtorizatsiya ishlari amalga oshiriladi. Bunda obyektni avtomatik identifikatsiya qilishda o‘sha obyekt bilan tizim o‘rtasida obyektni tanib oluvchi maxsus vosita uning identifikatsiya ma’lumotlarini tizimga uzatish uchun xizmat qilmoqda.

So‘nggi paytlarda avtomatik identifikatsiyalash usullaridan foydalanishning keskin o‘sishi, ularni standartlashtirish tufayli ularni boshqaruv hamda kompyuter tizimlariga keng integratsiya qilinishi ortidan shaxslarni, tovar, kiyim kechak va oziq ovqat mahsulotlarini avtomatik identifikatsiyalash imkoniyatlarini bermoqda.

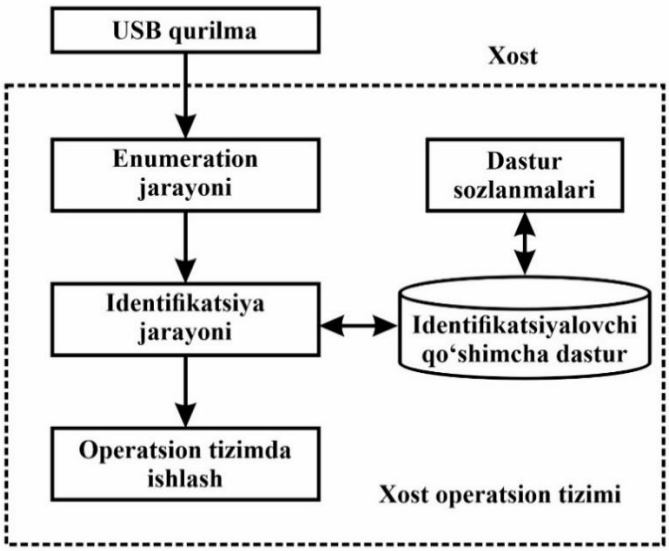


1-rasm. Avtomatik identifikatsiya tizimining ishlash chizmasi.

Bugungi kunda USB standarti asosida ishlovchi qurilmalarning xususiyatlari, imkoniyatlari, har tomonlama qulayliklaridan kelib chiqib ular butun dunyoda ommalashib borayotganligi USB tizimining quyi pog‘onasidagi zaifliklardan foydalanuvchi yashirin HID interfeysli USB qurilmalar bilan kompyuter va axborot

tizimlariga kiberhujumlarni amalga oshirish imkoniyatini ham oshirib bormoqda. Yashirin HID interfeysli USB qurilmalaridan kiberhimoyani ta’minlash uchun ularni identifikatsiyalash va tizimga kirishini cheklash zarur bo‘ladi. USB qurilmalarini identifikatsiyalash va tizmga kirishini cheklash xostda enumeration jarayonidan so‘ng operatsion tizimdagi maxsus dasturiy vosita yordamida amalga oshiriladi (2-rasm).

Bunda tizimga ulanishga ruxsat beriladigan USB qurilmalar ro‘yxatini tuzish va har safar tizimga ulanishda qurilmani ushbu ro‘yxatga muvofiqligini tekshirish orqali ushbu muammoni hal qilish mumkin. Qurilmani identifikatsiya qilishda uning turi, ishlab chiqaruvchisi, seriya raqami kabi parametrlardan foydalanuvchi maxsus dasturiy ta’minot tekshiruvi natijasiga qarab tizimga bog‘lanishga harakat qilayotgan USB qurilma bloklanishi yoki tizimga kirishga ruxsat berilishi mumkin[4].

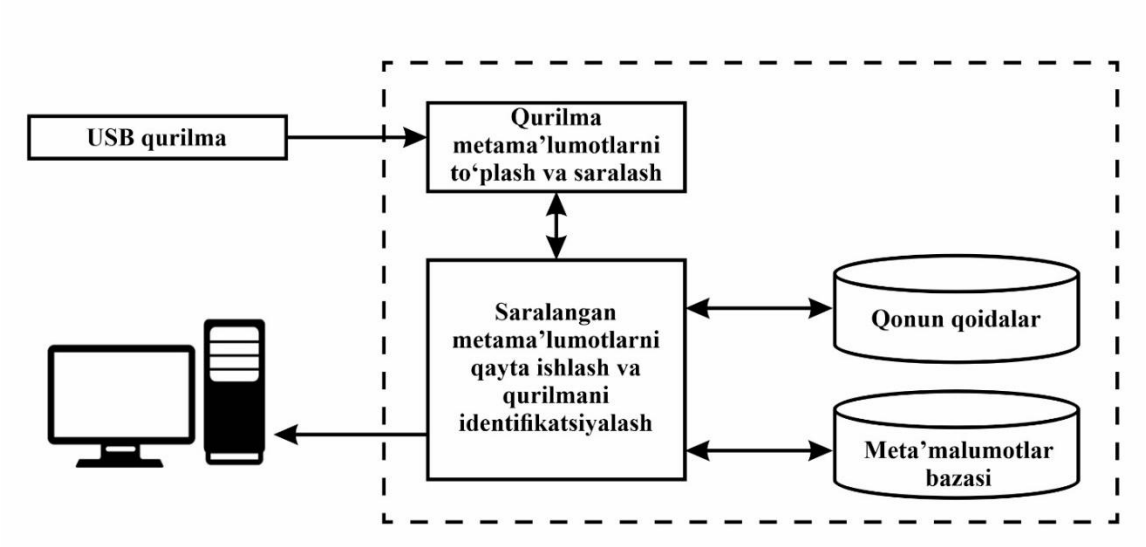


2-rasm. USB qurilmani dasturiy vosita yordamida identifikatsiyalash chizmasi.

USB qurilmalarini ro‘yhat bo‘yicha tekshiruvchi maxsus dasturiy ta’minot turlariga NetWrix USB Blocker[5], MyUSBOnly[6], USBGuard[7], USB Disabler Pro[8] kabi dasturiy ta’minotlarni misol keltirish mumkin. Biroq USB qurilmalarining imkoniyatlaridan foydalanib amalga oshirilayotgan kiberhujum usullari va turlari tahlili natijasida quyi pog‘onalardagi ya’ni mantiqiy va interfeys pog‘onalaridagi zaifliklardan amalga oshiriladigan hujumlarda ushbu dasturlar yordam berma olmaydi. Yuqorida ko‘rib chiqilgan avtomatik identifikatsiya usullari va USB qurilmalarini identifikatsiyalovchi dasturiy vositalar yashirin HID interfeysli yoki kontrafakt qurilmalarni aniqlay olmasligi ularni takomillashtirish zaruriyatini taqozo etadi.

Taklif qilinayotgan usulda USB qurilma xostga bog‘lanmasdan oldin uning metama’lumotlari asosida avtomatik identifikatsiya qilinadi va yuqoridagi usulning takomillashishiga erishiladi (3-rasm). Usul mohiyatiga ko‘ra yashirin HID interfeysli

USB qurilmalarni avtomatik identifikatsiya qilishda qurilmaning metama'lumotlaridan[1] foydalaniladi. Dastlab, USB qurilma metama'lumotlarini to'plash va ular ichidan yashirin interfeyslarni, kontrafakt qurilmani aniqlashga kerak bo'ladigan ma'lumotlarni saralab olish zarur bo'ladi.



3-rasm. USB qurilmalarini avtomatik identifikatsiyalash usulining chizmasi.

USB qurilmasi metama'lumotlarini to'plash va taqdim qilishga yordam beradigan *Thesycon USB Descriptor Dumper*, *USBDeview*, *USB Forensics and Tracking Tools (USBFT)*, *USBlyzer* kabi maxsus dasturiy ta'minotlar va *Write Blockers, USB Write-Blocker Hardware, USB Duplicators, USB Protocol Analyzers* kabi apparat qurilmalari bugungi kunda mavjud. Biroq bu dasturiy va apparat vositalar tizimga ulangan USB qurilmalarining metama'lumotlarni bir qisminigina taqdim eta oladi va qurilmalarni boshqarish yoki tizimda cheklash vazifasini bajarmaydi.

USB qurilma metama'lumotlari - qurilma bilan bog'liq bo'lgan axborotlar yoki ma'lumotlar to'plami bo'lib, uning turli atributlari hamda xususiyatlarini tavsiflaydi va ushbu ma'lumotlar kiberxavfsizlikni ta'minlashda USB qurilmalarini boshqarish va tahlil qilish uchun juda muhim hisoblanadi. USB qurilma metama'lumotlari sirasiga quyidagi ma'lumotlar kiradi:

- qurilma identifikatorlari haqidagi ma'lumotlar;
- qurilma klassi haqidagi ma'lumotlar;
- qurilmaning sozlanmalari haqidagi ma'lumotlar;
- qurilma ulanish tarixi haqidagi ma'lumotlar;
- qurilma bilan o'zaro almashingan ma'lumotlar hajmi;
- foydalanuvchi haqidagi ma'lumotlar.

[1] Metama'lumotlar - identifikatsiyalash, tashkillashtirish, taqdim etish, joylashtirish va boshqarishga yordamlashuvchi ma'lumotlarga oid axborotlar majmui [9]

USB qurilma metama’lumotlarining asosiy qismi qurilmaning deskriptor jadvallarida aks etsa, qolgan qismi xostning operatsion tizimidagi drayverlarda namoyon bo‘ladi.

Qurilma identifikatorlari. USB qurilmalari unikal identifikatorlarga ega bo‘lib, ular operatsion tizimga qurilmani tanib olish va boshqarish uchun kerak bo‘ladigan ma’lumotlardir[10]. Identifikatorlar haqida USB qurilmasidagi deskriptorlar jadvallaridan hamda draverlardagi ma’lumotlardan bilib olish mumkin va ular quyidagi ma’lumotlarni o‘zida aks etadi:

Vendor ID (VID): Qurilma ishlab chiqaruvchiga berilgan unikal kod.

Product ID (PID): Aniq bir qurilma turiga berilgan unikal kod.

***Qurilma klassi*.** Har bir qurilma o‘ziga tegishli klass bo‘yicha turli xil vazifalarni bajaradi va o‘zining maxsus ma’lumotlariga ega bo‘ladi [11]. Ular quyidagi ma’lumotlarni o‘zida aks etadi:

Device Class Code: qurilma klassini aniqlaydigan 2 honali 16 lik sanoq sistemasidagi sonlardan tashkil topgan kod. Ushbu kodlar ma’lum bir qurilmani qaysi toifaga tegishliligini belgilab beradi.

Subclass Code [95, 142-b]: Qurilmaning maqsadini yoki funksional xususiyatlarini aniqroq ko‘rsatib berishga yordam beruvchi va uning klassini yanada batafsilroq belgilovchi qo‘shimcha kod. Subklass kodi qurilma identifikatsiyasini aniqroq amalga oshirishga, operatsion tizimda drayverlar belgilashga yordam beradi va Device Class kodi bilan birgalikda ishlaydi.

Protocol Code [95, 142-b]: xost yoki boshqa qurilmalar bilan aloqa qilish uchun USB qurilmasi tomonidan ishlatiladigan maxsus aloqa protokolini aniqlaydigan kod. Ushbu kod qurilma xostning operatsion tizim bilan bog‘lanish va ma’lumotlarni uzatish uchun qanday buyruq va protokollardan foydalanishini ko‘rsatib beradi.

***Qurilma sozlanmalari haqidagi ma’lumotlar*.** Ushbu ma’lumotlar qurilmadagi interfeyslar soni, quvvat manbalari haqidagi aniq ma’lumotlarni o‘z ichiga oladi[12]. Ular quyidagi asosiy ma’lumotlarni o‘zida aks ettiradi:

NumConfigurations: Qurilma tomonidan qo‘llab quvvatlanadigan sozlanmalar soni.

NumInterfaces: Sozlanma tomonidan qo‘llab-quvvatlanadigan interfeyslar sonini belgilovchi ma’lumotlar.

Attributes: Zaxiralangan, shina orqali yoki avtonom quvvatlanishi hamda, masofadan turib uyg‘otishni belgilovchi ma’lumotlar.

MaxPower: Qurilma to‘liq ishga tushganda USB qurilmasiga beriladigan maksimum quvvatni belgilovchi ma’lumotlar.

***Qurilma ulanish tarixi haqidagi ma’lumotlar*.** Ushbu ma’lumotlar USB qurilmani xostga ulangani va uzilgani haqidagi ma’lumotlarni yig‘uvchi jurnal bo‘lib,

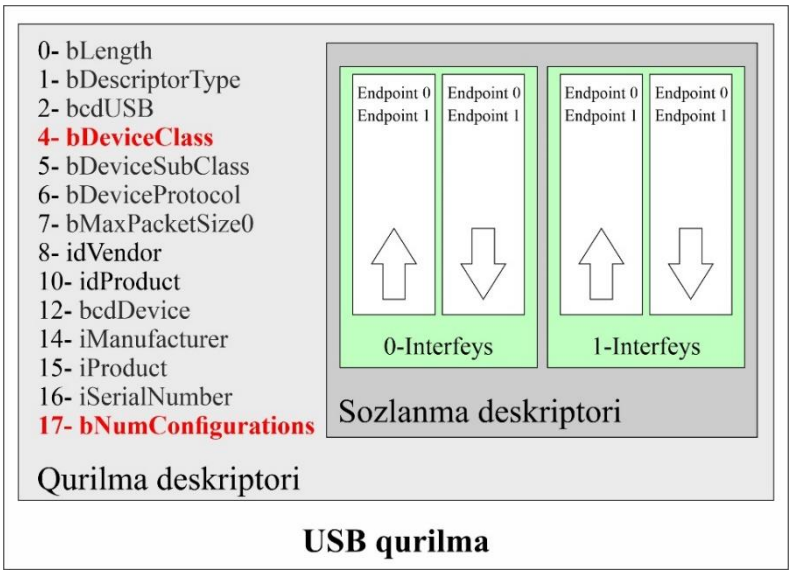
xostning maxsus xotirasida saqlanadi va qurilmadan qachon foydalanilganligini kuzatish hamda potensial xavfsizlik insidentlarini aniqlashga yordam beradi [13].

Qurilma bilan o‘zaro almashingan ma’lumotlar hajmi. Bu ma’lumotlar xost va qurilma o‘rtasida o‘zaro almashilgan va qurilmadan xostga yoki xostdan qurilmaga ko‘chirilgan ma’lumotlar hajmi haqidagi axborotlarni o‘z ichiga oladi. USB qurilmasi bilan almashingan ma’lumotlar monitoringi va auditining muhim jihati bo‘lib, ma’lumotlar xavfsizligini ta’minlashga va USB qurilmalaridan foydalanish ustidan nazoratni olib borishga yordam beradi.

Foydalanuvchi haqida ma’lumotlar. Metama’lumotlar tarkibiga USB qurilmani ulayotgan vaqtdagi xostdan foydalanishni amalga oshirayotgandagi foydalanuvchi haqidagi ma’lumotlar ham kiradi. Ushbu ma’lumotlar kim tomonidan qurilma ulanganligini aniqlashga yordam beradi.

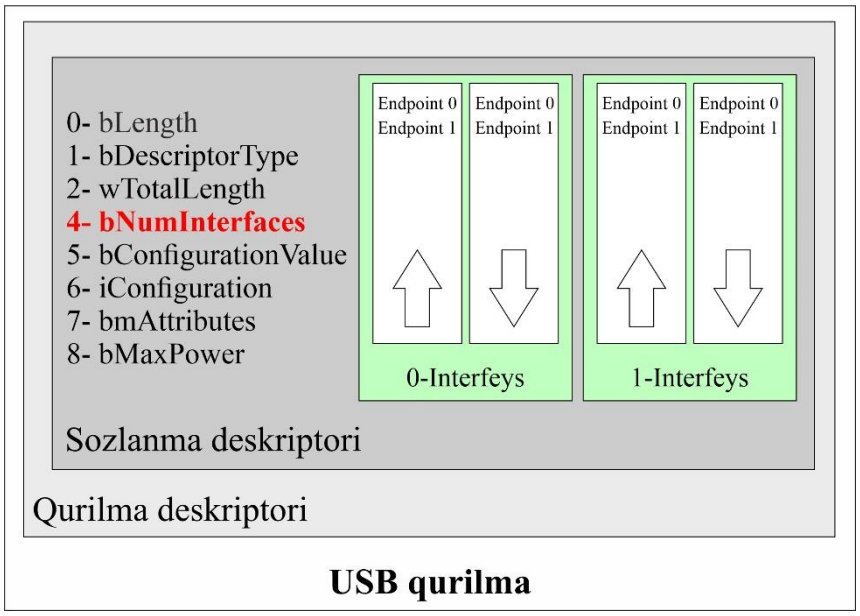
Yashirin interfeysga ega yoki kontrafakt USB qurilmalarini identifikatsiya qilishda yuqorida sanab o‘tilgan hamda to‘plangan metama’lumotlar ichidan yashirin interfeysni va qurilmani ishlab chiqaruvchilarini aniqlashga zarur bo‘ladigan qurilmaning sozlanmalari, klassi va identifikatorlari haqidagi axborotlarni aks ettiruvchi metama’lumotlar saralab olinadi.

Saralab olingan metama’lumotlar ichidan USB qurilmasining deskriptor jadvalining 4-bayti ya’ni *bDeviceClass* kodi yordamida qurilmaning klassi aniqlanadi. Agarda qurilma deskriptorida *bDeviceClass* kodi kiritlmagan bo‘lsa qurilmaning klassi u qo‘llab quvvatlaydigan interfey klassi bilan aniqlanadi. Deskriptor jadvalining 17-baytidagi *bNumConfigurations* kodi yordamidan qurilma qo‘llab quvvatlaydigan sozlanmalar soni aniqlanadi (4-rasm).



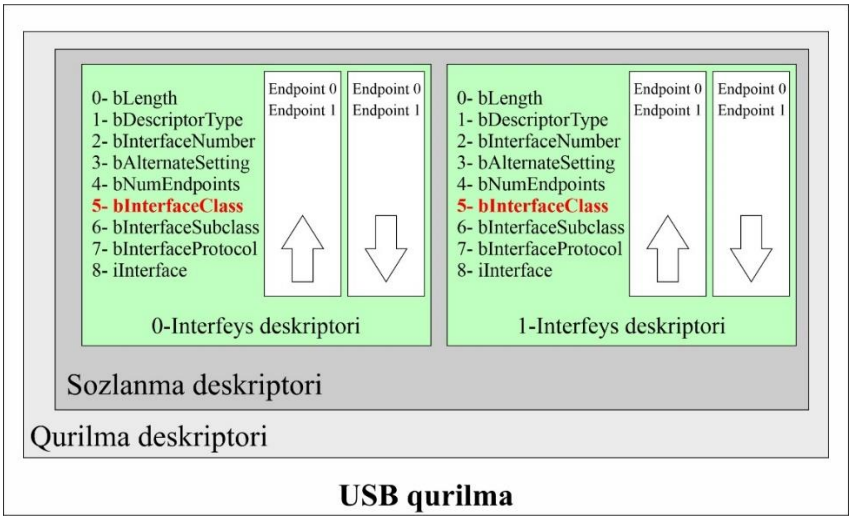
4-rasm. USB qurilmasining qurilma deskriptor jadvali.

Keyingi qadamda saralab olingan metama'lumotlar ichidan USB qurilma qo'llab quvvatlaydigan har bir sozlanma deksriptorlari jadvalining 4-baytidagi *bNumInterfaces* qiymati tekshiriladi va qurilma sozlanmasidagi interfeyslar soni aniqlanadi (5-rasm).



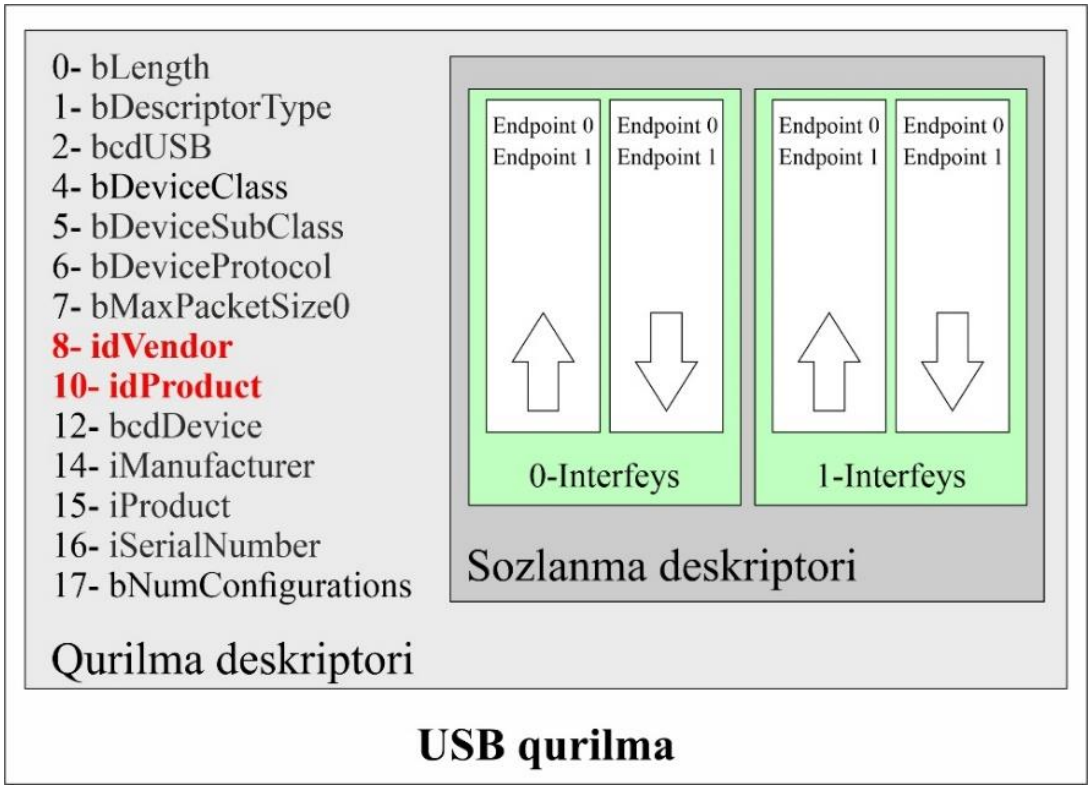
5-rasm. USB qurilmasining sozlanma deskriptor jadvali.

Keyingi qadamda ko'p interfeysli qurilmaning har bir interfeysi ketma ket ravishda har bir interfeys deskriptor jadvalining 5-baytidagi *bInterfaceClass* kodi HID klass (03) kodiga tekshiriladi. Agarda qaysidir interfeysning *bInterfaceClass* kodi HID klassga mos kelsa ushbu qurilmaga yashirin HID intefeys joylashtirilgan bo'ladi va ushbu qurilma yashirib HID interfeysli qurilma deb hisoblanadi (6-rasm).



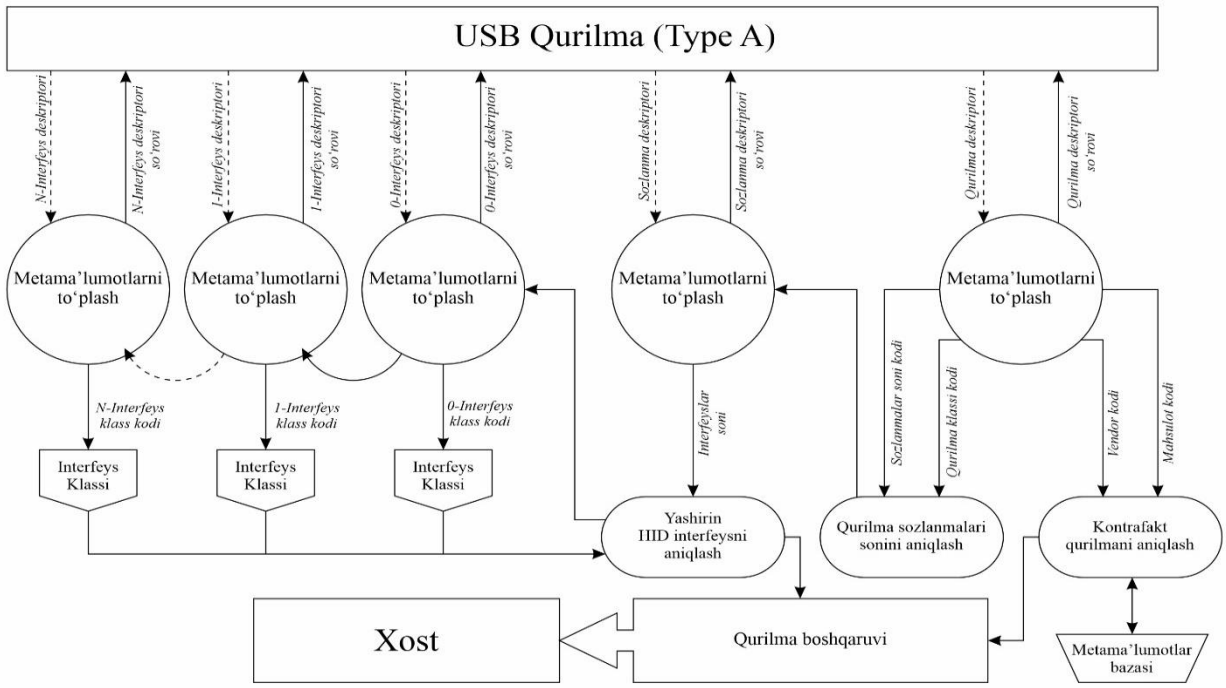
6-rasm. Ko'p interfeysli USB qurilmasidagi interfeyslar deskriptor jadvallari.

Keyingi qadamda qurilmaning kontrafakt emasligini aniqlash uchun qurilma deskriptori jadvalining 8-baytidagi *idVendor* kodi va 10-baytidagi *idProduct* kodi saralab olinadi (7-rasm). Saralab olingan kodlar USB-IF tashkilotidan rasmiy ro‘yhatdan o‘tgan vendorlar va mahsulotlarning ID ma’lumotlaridan tashkil topgan metama’lumotlar bazasiga solishtirib chiqiladi.



7-rasm. Ko‘p interfeysli USB qurilmasidagi qurilma deskriptor jadvali.

USB-IF tashkilotidan rasmiy ro‘yhatdan o‘tgan vendorlar va mahsulotlarning identifikator ma’lumotlari Stephen J. Gowdy tomonidan ishlab chiqilgan, muntazam ravishda yangilab boriladigan “Linux-USB Project”[14] va “The SZ development”[15] kompaniyasining web sahifasidagi ma’lumotlardan foydalanib metama’lumotlar bazasi yaratiladi. Yaratilgan metama’lumotlar bazasida qurilmaning vendori va mahsuloti kodi bo‘lmasa yoki tafovutlar aniqlansa bunday qurilma rasmiy maqomga emas va kontrafakt qurilma deb hisoblanadi.



8-rasm. USB qurilmani metama'lumotlar asosida identifikatsiyalash usuli.

USB qurilmalarni identifikatsiyalash usuliga quyida ko'rsatilgan jarayonlarni joriy qilish orqali avtomatik identifikatsiya tizimi va USB qurilmalarni identifikatsiyalash takomillashtirildi:

USB qurilmalarning metama'lumotlarini to'plash va saralash;

saralangan metama'lumotlar yordamida USB qurilma sozlanmasi va interfeyslari soni shuningdek, qurilmani ishlab chiqaruvchi vendor va mahsulot kodini aniqlash;

ko'p interfeysli qurilmaning har bir interfeysini HID klassga tekshirish va yashirin HID interfeysni aniqlash;

qurilmani ishlab chiqaruvchi vendori va mahsulot kodini metama'lumotlar bazasidan solishtirish orqali kontrafakt qurilmalarni aniqlash;

yashirin HID interfeysli va kontrafakt qurilmalarni aniqlashtirish natijalariga ko'ra USB qurilmalarning boshqaruvini amalga oshirish.

USB qurilmalarining kompyuter va axborot tizimlariga kirish nazoratini USB qurilmani metama'lumotlar asosida identifikatsiyalash usuli (8-rasm) yordamida amalga oshirish orqali USB tizimining mantiqiy, interfeys pog'onalaridagi zaifliklardan foydalanib amalga oshiriladigan kiberhujumlardan himoyalanishga erishiladi. USB qurilmani metama'lumotlar asosida identifikatsiyalash usuli bo'yicha aniq natijalariga erishish uchun ushbu usul bilan ishlovchi apparat-dasturiy vositani modellashtirish va algoritmlarini ishlab chiqish zarur bo'ladi.

FOYDALANILGAN ADABIYOTLAR

[1] Automatic identification and data capture in mobile via RFID by K.R. Reddy, P.V. Krishna, B. Sravya. January 2018 International Journal of Pure and Applied Mathematics 118(9): 593-601 pages.

[2] Automatic identification and data capture Elektron resurs: https://en.wikipedia.org/wiki/Automatic identification and data capture (19.12.2023)

[3] А. Э. Горев, Информационные технологии на транспорте. Электронная идентификация автотранспортных средств и транспортного оборудования. ISBN 978-5-9227-0190-7. Санкт-Петербургский государственный архитектурно-строительный университет, 2010. 6-стр.

[4] Липницкий Л.А., Шалькевич П.К., Бутько А.А. Ограничение доступа к внешним интерфейсам рабочего места оператора АСУ. VII Международная научно-техническая интернет-конференция "Информационные технологии в образовании, науке и производстве" Минск, 16-17 ноября 2019 г. Страницы: 337-338

[5] NetWrix USB Blocker https://progsoft.net/ru/software/netwrix-usb-blocker#about 11.01.2024.

[6] MyUSBOnly https://www.myusbonly.com/usb-security-device-control/ 11.01.2024

[7] USBGuard https://usbguard.github.io/ 11.01.2024

[8] USB Disabler Pro https://www.intelliadmin.com/index.php/usb-disabler-pro/ 11.01.2024

[9] Mikhail Kogalovsky. Metadata, their Properties, Functions and Classifications. 14th All-Russian Scientific Conference "Digital libraries: Advanced Methods and Technologies, Digital Collections" Pereslavl-Zalessky, Russia, October 15-18, 2012. (3-14 pages)

[10] Standard USB identifiers. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/standard-usb-identifiers 24.10.2023

[11] USB Complete: The Developer’s Guide, Fifth Edition by Jan Axelson. ISBN13 978-1-931448-29-1. Copyright 1999-2015 by Janet L. Axelson. (165-page)

[12] System Architecture (USB 2.0) by Don Anderson. ISBN: 0-201-46137-4. Copyright ©2001 by MindShare, Inc. (361-page)

[13] Cybercrime Investigation Case Studies: An Excerpt from Placing the Suspect Behind the Keyboard 1st Edition. by Brett Shavers. Copyright r 2013 Elsevier Inc. ISBN: 978-0-12-409505-2 (23-p)

[14] Linux USB. http://www.linux-usb.org/ 12.01.2024 yil.

[15] The SZ Devolopment. https://www.the-sz.com/ 12.01.2024 yil