YASHIRIN INTERFEYSLI USB QURILMALARNI AVTOMATIK IDENTIFIKATSIYA QILISHNI MODELLASHTIRISH

PhD, dotsent **Nishanov I.I., Mamajonov J.M.**
Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya: *Maqolada USB qurilmani metama'lumotlar asosida identifikatsiyalash usulini modellashtirish haqida gap boradi. Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modelidagi meta'malumotlarni to'plash, saralash, saralangan metama'lumotlardan foydalanib USB qurilmadagi yashirin HID inyterfeyslarni aniqlash va USB-IF tashkilotidan ro'yhatdan o'tganligini tekshirish jarayonlari ishlash tartibi bosqichma bosqich batafsil ko'rib chiqiladi. Ushbu model USB qurilmalarini avtomatik identifikatsiyalash usullarini yanada takomillashtirishga va yashirin HID interfeysli USB qurilmalar orqali amalga oshiriladigan kiberhujumlardan himoyalanishga xizmat qiladi.*

Kalit so'zlar: *USB, USB-IF, HID, interfeys, deskriptor, klass, sozlanma, identifikatsiya, metama'lumot, vendor.*

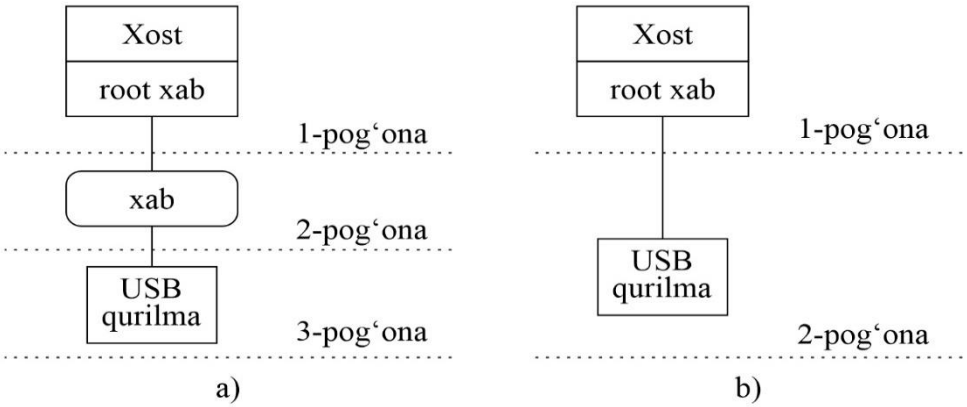
Аннотация: *Статья посвящена моделированию метода идентификации USB-устройства на основе метаданных. В ней подробно рассматривается процесс сбора метаданных в модели автоматической идентификации USB-устройств с скрытыми HID-интерфейсами. Также описаны этапы сортировки метаданных, идентификации скрытых HID-интерфейсов на USB-устройствах с использованием отсортированных метаданных и проверки их регистрации в организации USB-IF. Эта модель предназначена для дальнейшего усовершенствования методов автоматической идентификации USB-устройств и обеспечения защиты от кибератак, осуществляемых USB-устройствами со скрытым HID-интерфейсом.*

Ключевые слова: *USB, USB-IF, HID, интерфейс, дескриптор, класс, конфигурация, идентификатор, метаданные, вендор.*

Abstract: *The article focuses on modeling a method for identifying a USB device based on metadata. It provides a detailed walkthrough of the metadata collection process in the automatic identification model for USB devices with hidden HID interfaces. Additionally, the article outlines the steps for sorting metadata, identifying hidden HIDs on USB devices using the sorted metadata, and verifying their registration with the USB-IF organizations database. This model aims to enhance methods for automatically identifying USB devices and to bolster protection against cyber-attacks executed by USB devices with hidden HID interfaces.*

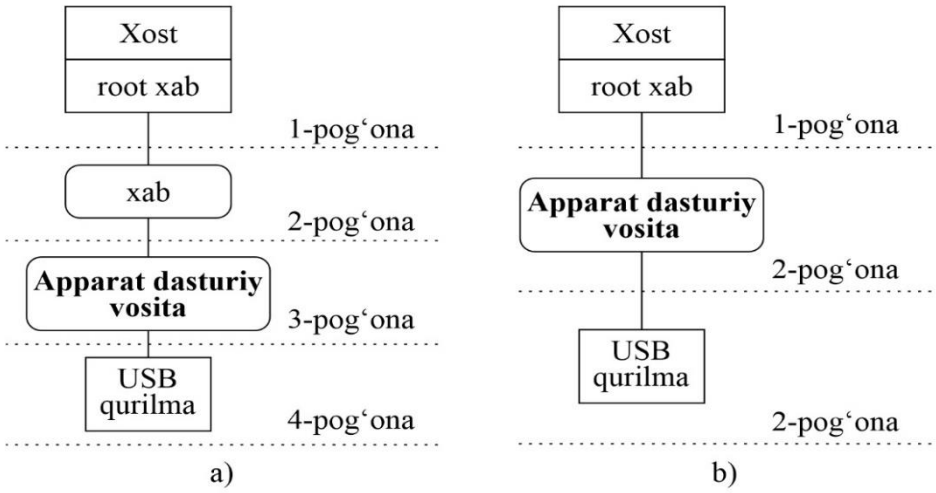
Keywords*: USB, USB-IF, HID, interface, descriptor, class, configuration, identity, metadata, vendor.*

USB protokoli zaifliklaridan foydalanib amalga oshiriladigan zamonaviy kiberhujum usullarining tahlil natijalari zararli USB-HID qurilmalaridan kiberhimoyani ta’minlashda dasturiy vositalarga qaraganda apparat dasturiy vositaning samaradorligi yuqoriroq hisoblanadi. USB qurilmalarni uning metama’lumotlari asosida identifikatsiyalash usulini apparat-dasturiy vositaga joriy qilish orqali yashirin HID interfeysli USB qurilmalaridan kiberhimoyani ta’minlashni xostga bog‘lanmasdan oldin amalga oshirish mumkin bo‘ladi. Ushbu apparat dasturiy vosita xostni imitatsiya qilish ya’ni Host-Emulating Honeypots [1] vazifasini ham bajaradi. Odatda USB qurilma xostga to‘g‘ridan to‘g‘ri ulanganda u USB tizimining ikkinchi yoki uchinchi pog‘onasiga tegishli bo‘ladi va birinchi pog‘onadagi xostda identifikatsiya qilinadi (1-rasm).



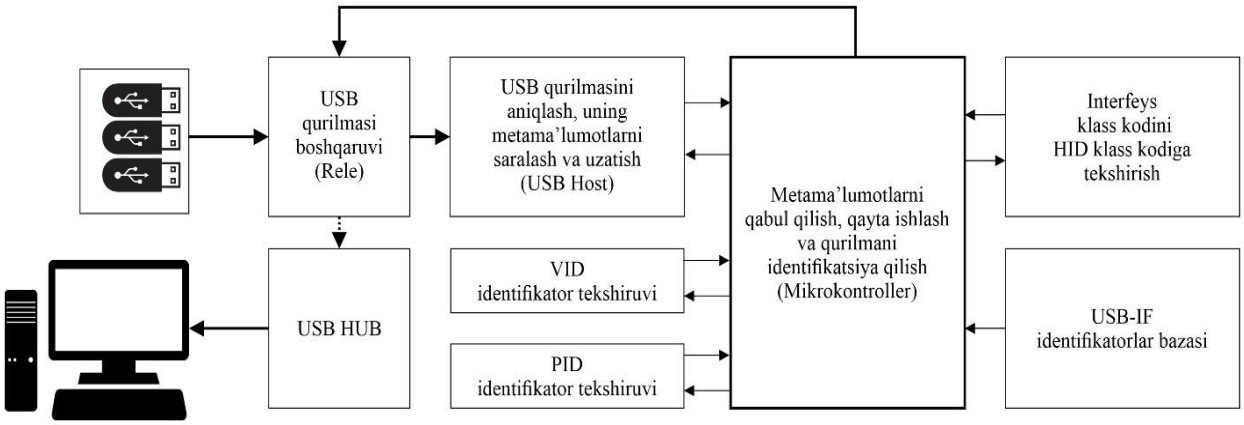
1-rasm. Xostga bog‘lanishdagi qurilmaning USB tizimidagi ishlash pog‘onasi. a) chipsetli USB xabga ega xost b) USB xabga ega bo‘lmagan xost

Xost va USB qurilma o‘rtasidagi apparat-dasturiy vositani joylashtirish orqali zararli USB qurilmalari xostgacha avtomatik identifikatsiya qilinadi va u USB tizimining ikkinchi yoki uchinchi pog‘onasida ishlaydi (2-rasm).



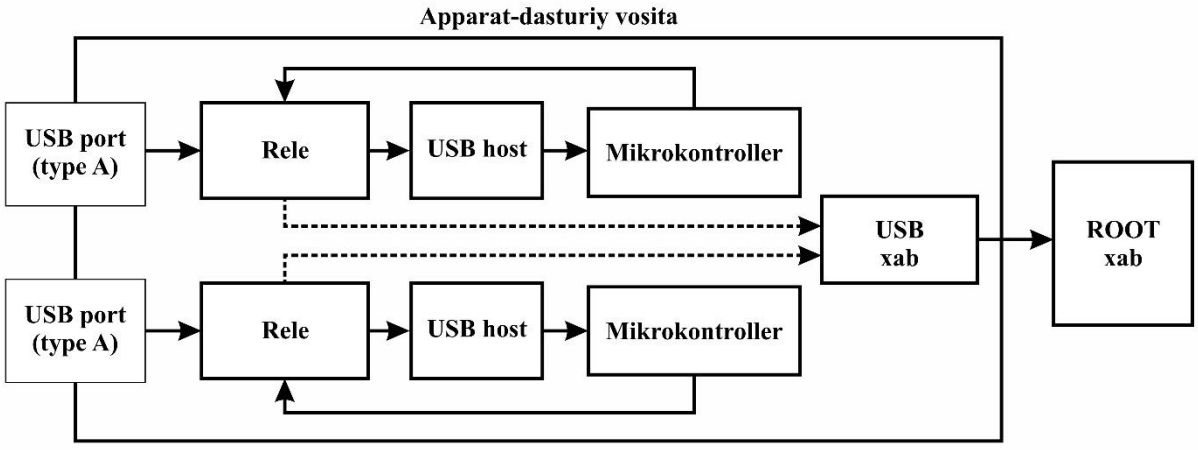
2-rasm. Xostga ulanadigan apparat dasturiy vositaning USB tizimidagi ishlash pog‘onasi. a) chipsetli USB xabga ega xost b) USB xabga ega bo‘lmagan xost

Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modeli asosida ishlovchi apparat-dasturiy vosita huddi xostdagi operatsion tizim kabi unga ulangan USB qurilmasini tanib olish uchun o‘zida enumeration jarayonini ishga tushiradi va qurilmadagi metama’lumotlarni to‘playdi. Keyinchalik metama’lumotlar qayta ishlash uchun saralab olinadi, qayta ishlanadi va kelgusida USB tizimining yuqori ish pog‘onasiga bog‘lanishiga ruxsat beriladi yoki taqiqlanadi (3-rasm).



3-rasm. Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modeli.

Apparat dasturiy vositaga ulangan qurilma rele bilan boshqariladi. Rele boshqaruvi USB qurilmani metama’lumotlar asosida identifikatsiyalash usuli yordamida amalga oshiriladi. Dasturiy apparat vositaning har bir kiruvchi porti USB Type A ko‘rinishida bo‘lib, ular uchun alohida USB host, mikrokontroller joylashtiriladi (4-rasm).



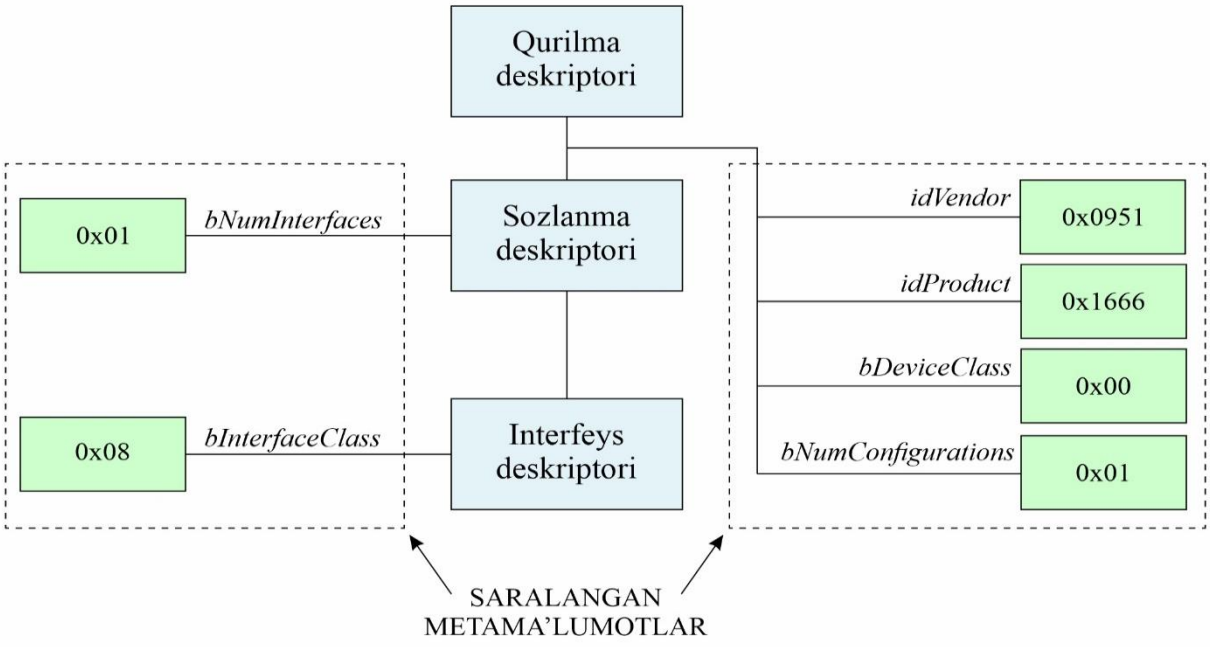
4-rasm. USB qurilmalarini rele orqali boshqaruvi chizmasi.

Apparat-dasturiy vosita bir vaqtning o‘zida bir nechtagacha USB qurilmasini qo‘llab quvvatlashi uchun releden so‘ng 6 tagacha USB qurilmaga xizmat ko‘rsatuvchi USB Xab qurilmasi qo‘shimcha qilinadi va identifikatsiyadan o‘tgan qurilmalar u orqali xostga bog‘lanadi. Dastlabki holatda relega bog‘langan USB qurilma to‘g‘ridan to‘g‘ri USB hostga yo‘naltiriladi va uning metama’lumotlari to‘planadi.

Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modeli asosida USB hostga bog‘langan qurilmadan to‘plangan metama’lumotlar orasidan quyidagi kodlar saralab olinadi:

- qurilma identifikatorlari haqidagi ma’lumotlardan:
  - -idVendor;
  - -idProduct;
  - -bNumConfigurations;
  - -bDeviceClass;
- qurilma sozlanmalaridagi ma’lumotlardan:
  - - bNumInterfaces;
- interfeys klassi haqidagi ma’lumotlardan:
  - - bInterfaceClass;

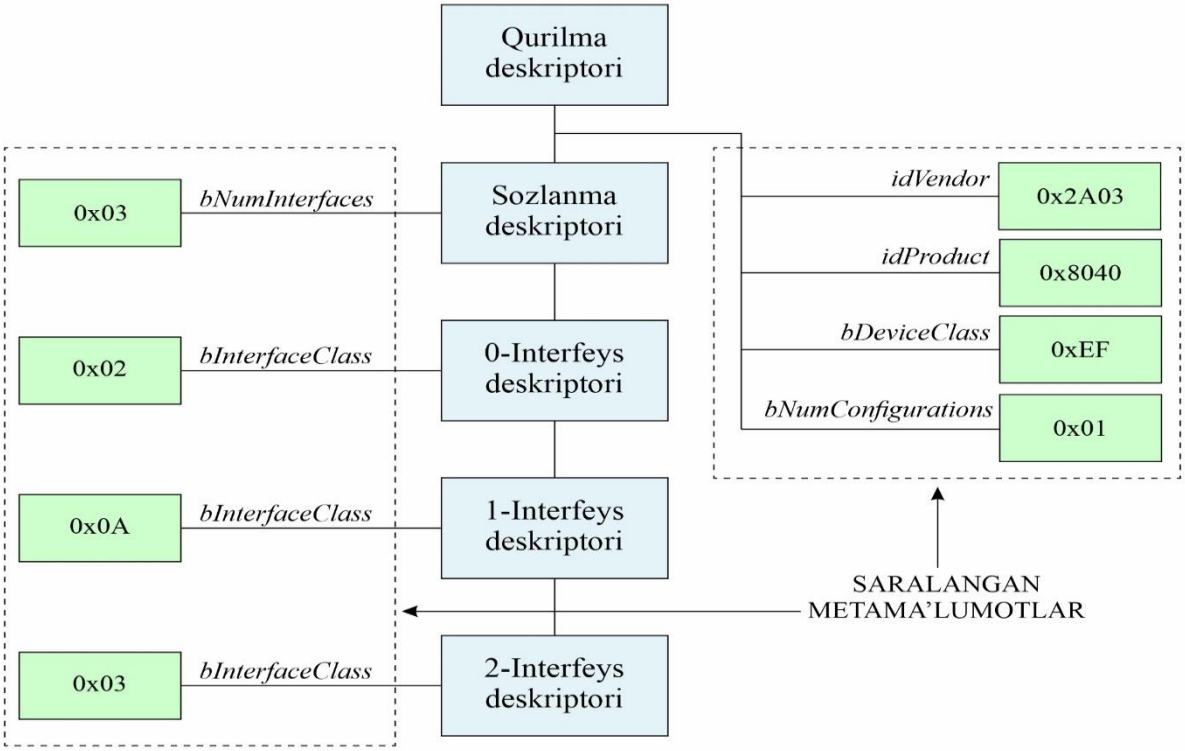
Misol uchun yakka interfeysli USB hotira qurilmasining saralangan metama’lumotlari ko‘rib chiqilsa, qurilma deskriptor jadavalidagi *idVendor* va *idProduct* kodlari uni ishlab chiqargan vendori va mahsuloti identifikatorlarini bildiradi. Qurilmaning *bDeviceClass* kodining qiymati 0 ga teng bo‘lsa va uning klass kodi interfeys deskriptor jadavlidagi ma’lumotlardan aniqalanadi. 9-jadvalga ko‘ra 00, 02, DC, EF, FF klasslariga tegishli USB qurilmalarining klassi haqidagi ma’lumotlar ularning qurilma deskriptor jadvalida aks etsa qolgan klassdagi qurilmalarning klassi haqidagi ma’lumotlari ularning interfeys deskriptor jadvallarida aks etadi (5-rasm).



5-rasm. USB hotira qurilmasining saralangan metama’lumotlari.

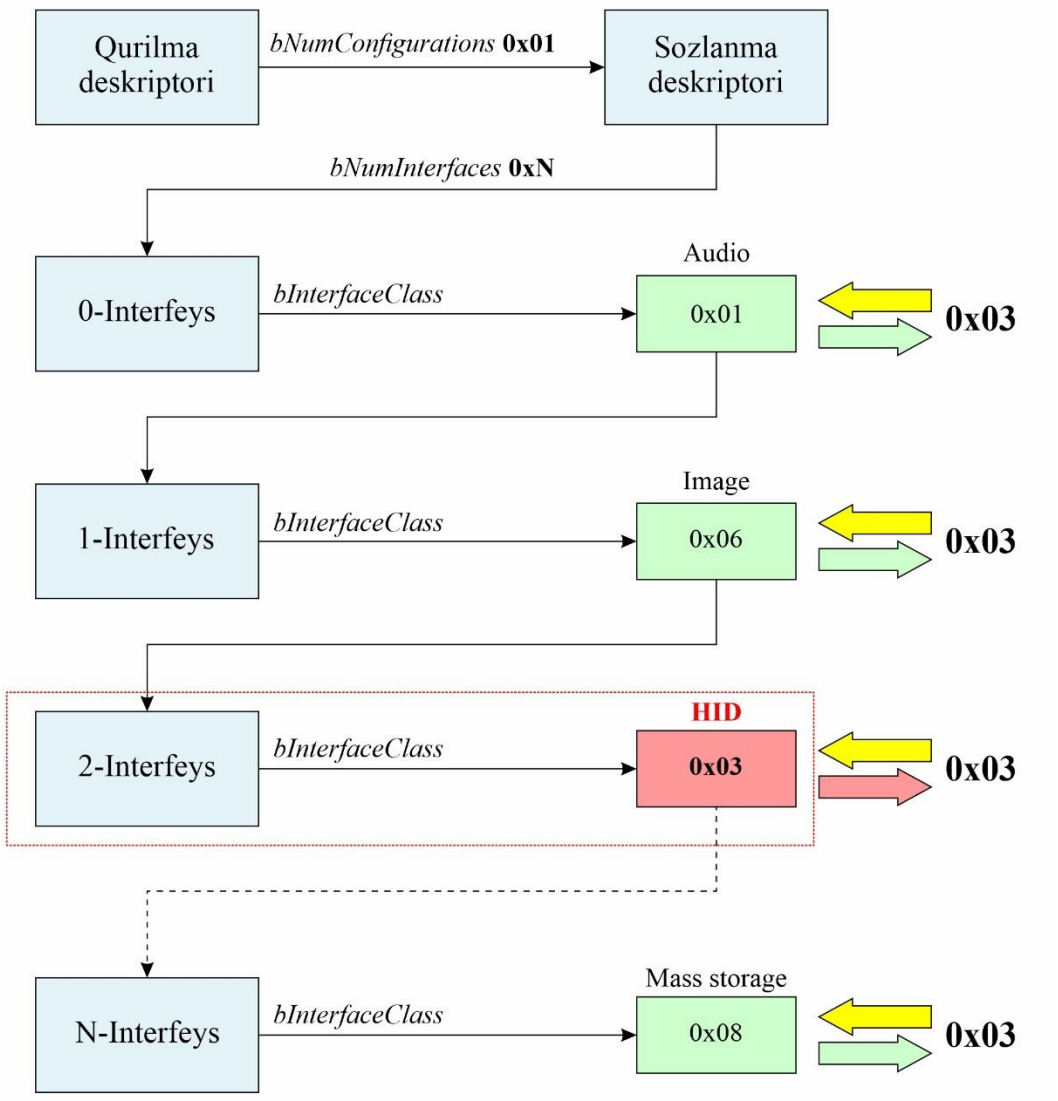
Qurilma sozlanmalaridagi ma’lumotlar sozlanmalar deskriptori jadvalida aks etadi va bu jadvalda *bNumIntrefaces* qiymati 1 ga tengligi USB qurilma yakka interfeysli ekanligini bildiradi. USB qurilmadagi interfeysning klassi haqidagi ma’lumotlar interfeys deskriptori jadvalida aks etadi va *bInterfaceClass kodi* 08 ga tengligi ushbu qurilma Mass Storage klassiga tegishli USB hotira qurilmasi ekanligini anglatadi (5-rasm).

Turli xildagi USB qurilmalarining funksiyalaridan kelib chiqib ularning sozlanmalari, interfeyslari soni bir nechtagacha bo‘lishi mumkin va ularning deskriptor jadvallari ham shunga monand bo‘ladi. Misol uchun, yakka sozlanmali ammo ko‘p interfeysli USB qurilmasida sozlanma deskriptori 1 ta bo‘lsa interfeys deskriptorlari interfeyslar soniga teng bo‘ladi (6-rasm).



6-rasm. Ko‘p interfeysli USB qurilmasining saralangan metama’lumotlari.

Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modelida USB qurilmadagi yashirin interfeyslarni aniqlash USB qurilmasining saralab olingan metama’lumotlari ichidan *bNumInterfaces* kodi asosida amalga oshiriladi va keyinchalik har bir interfeys deskriptoridagi *bInterfaceClass* kodi HID klass (03) kodiga solishtirib chiqiladi. Solishtirib chiqish natijasida qaysidir interfeysning klass kodi HID klass kodi bilan mos kelsa, qurilma yashirin HID interfeysli USB qurilma sifatida ko‘riladi aks holda u yashirin HID interfeysga ega bo‘lmagan qurilma deb hisoblanadi (7-rasm).



7-rasm. Qurilmadagi interfeyslarni HID klassga tekshirish.

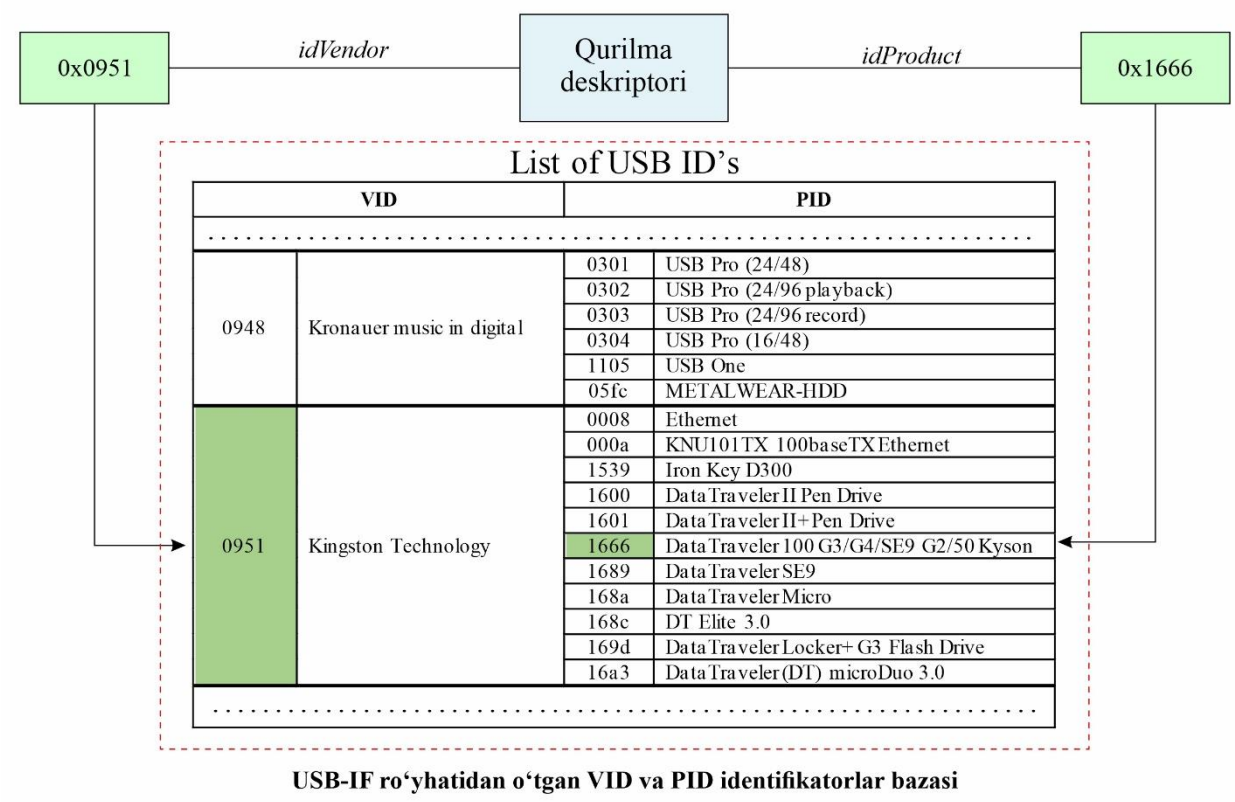
Yashirin HID interfeys tekshiruvidan so‘ng USB qurilmasini ishlab chiqaruvchi vendori va ro‘yhatdan o‘tganligini aniqlash uchun qurilma deskriptor jadavalidagi *idVendor* va *idProduct* kodlari USB-IF tashkilotining metama’lumotlar bazasida borligi va bir biriga mosligi tekshirib chiqiladi. Odatda rasmiy ro‘yhatdan o‘tmagan yoki reverse engineering usuli yordamida qayta dasturlangan USB qurilmalaridagi *idVendor* va *idProduct* kodlari metama’lumotlar bazasidagi kodlardan farq qiladi yoki umuman bir biriga mos kelmaydi.

Linux operatsion tizimida ishlovchi xostlar uchun ularga ulanayotgan USB qurilmalarini aniqlash uchun “Linux USB Project”[2] doirasida USB-IF tashkilotidan ro‘yhatdan o‘tgan USB qurilmalarining VID va PID indetifikatorlarining bazasi ishlab chiqilgan va muntazam yangilanib boriladi. Linuxning barcha destibyutivlari ushbu baza orqali unga ulanayotgan USB qurilmalarni identifikatsiya

qiladi[3]. Internet tarmog‘iga ulanmagan xostlarda baza faylini rasmiy saytdan olib xost xotirasidagi eski baza faylning ustiga yozish orqali yangilash imkoniyati ham bor.

Windows operatsion tizimida ishlovchi xostlarda Linux kabi identifikatorlar bazasi yo‘q va unga ulangan har qanday USB qurilma uning vendori rasmiy ro‘yhatdan o‘tgan yoki o‘tmaganligidan qatiy nazar tizimda avtomatik ishga tushaveradi [4]. Qurilma deskriptor jadavalidagi soxta yoki o‘zgartirilgan *idVendor* va *idProduct* kodlar USB qurilma tomonidan xostga to‘g‘ridan to‘g‘ri taqdim etiladi va bu soxta ma’lumotlar asosida Windows operatsion tizimi qurilmaga mos kelishi mumkin bo‘lgan eng yaqin standart drayver tayinlaydi va qurilma avtomatik ishga tushadi.

Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modeli asosida ishlovchi apparat-dasturiy vositada USB-IF tashkilotdan ro‘yhatidan o‘tgan identifikatorlar bazasi mavjud bo‘ladi va u orqali USB qurilma metama’lumotlari sirasiga kiruvchi *idVendor, idProduct* kodlari yordamida USB qurilmani vendori bilan mahsuloti aniqlanadi (8-rasm). Metama’lumotlar qayta ishlash jarayonida qurilmaning *idVendor, idProduct* kodlari bazadagi ma’lumotlarga mos kelmasa u kontrafakt qurilma deb hisoblanadi va USB qurilma rasmiy maqomga ega emasligi xostga ulanmasdan oldin aniqlanadi.



VID		PID	
0948	Kronauer music in digital	0301	USB Pro (24/48)
		0302	USB Pro (24/96 playback)
		0303	USB Pro (24/96 record)
		0304	USB Pro (16/48)
		1105	USB One
		05fc	METALWEAR-HDD
0951	Kingston Technology	0008	Ethernet
		000a	KNU101TX 100baseTX Ethernet
		1539	Iron Key D300
		1600	DataTraveler II Pen Drive
		1601	DataTraveler II+ Pen Drive
		1666	DataTraveler 100 G3/G4/SE9 G2/50 Kyson
		1689	DataTraveler SE9
		168a	DataTraveler Micro
		168c	DT Elite 3.0
		169d	DataTraveler Locker+ G3 Flash Drive
		16a3	DataTraveler (DT) microDuo 3.0

8-rasm. Qurilma identikatorlarini tekshirish chizmasi.

Ishlab chiqilgan yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalashning modeli yuqorida keltirib o‘tilgan meta’malumotlarni to‘plash, saralash, saralangan metama’lumotlardan foydalanib USB qurilmadagi yashirin HID inyterfeyslarni aniqlash va USB-IF tashkilotidan ro‘yhatdan o‘tganligini tekshirish jarayonlarini o‘z ichiga oladi. Yashirin HID interfeysli USB qurilmalarni avtomatik identifikatsiyalash modelining ishlash tartibi bosqichma bosqich batafsil ko‘rib chiqildi. Ushbu model USB qurilmalarini avtomatik identifikatsiyalashga xizmat qiladi va apparat-dasturiy vosita sifatida ishlab chiqiladi hamda uning ishlash algoritmini tuzib chiqish zarur bo‘ladi.

FOYDALANILGAN ADABIYOTLAR

[1] Jing Tian; Nolen Scaife; Deepak Kumar; Michael Bailey; Adam Bates; Kevin Butler. SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 Through C. IEEE Symposium on Security and Privacy (SP) 2018, Page(s):1032 – 1047.

[2] List of USB ID’s. Elektron resurs: http://www.linux-usb.org/usb.ids Tashrif buyurilgan kun: 09.01.2024 y.

[3] Recognize more devices on Linux with this USB ID Repository. Elektron resurs: https://opensource.com/article/20/8/usb-id-repository Tashrif buyurilgan kun: 09.01.2024 y.

[4] USB device class drivers included in Windows. Elektron resurs: https://learn.microsoft.com/en-us/windows-hardware/drivers/usbcon/supported-usb-classes Tashrif buyurilgan kun: 09.01.2024 y.