2-KURS KI-AT servis

8 - Mavzu

Qurilma xavfsizligi bo’yicha ishlarni olib borish

“Kompyuterni tashkil etish” fanidan Mustaqil ish

Mavzu bo’yicha bo’limlar

01

Kirish

Apparat xavfsizligi haqida umumiy tushuncha

02

Tahlil

Apparat xavfsizligi zaifliklarini tahlil qilish

03

Aniqlash

Apparat xavfsizliklarini aniqlash usullari

04

Choralar

Zaifliklar uchun qarshi choralarni ishlab chiqish

Kirish!

Apparat xavfsizligi va uning ahamiyati bo‘yicha tushuncha olishingiz mumkin

Apparat xavfsizligi (hardware security)

Bu kompyuter tizimlari va qurilmalarining fizik darajadagi himoyasi, ya'ni, ular qanday ishlab chiqariladi, saqlanadi va ishlatiladi, shularning barchasida xavfsizlikni ta’minlashga qaratilgan chora-tadbirlar majmuasi.

Apparat xavfsizligi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga yordam beradi, bu esa dasturiy xavfsizlik qatlami bilan birgalikda ishlaydi

Apparat xavfsizligining asosiy ahamiyati

Ma’lumotni o‘g‘irlashdan himoya

Apparat xavfsizligi qurilmadagi sezgir ma’lumotlarga uchinchi shaxslar kirishining oldini oladi. Ayniqsa, maxfiy yoki shaxsiy ma’lumotlar saqlanadigan qurilmalar uchun muhimdir.

Dasturiy ta’minot xavfsizligini kuchaytirish

Dasturiy xavfsizlik faqat apparat xavfsizligi ishonchli bo‘lgandagina samarali ishlaydi. Agar apparatning o‘zi zaif bo‘lsa, dasturiy himoya choralarini osonlik bilan chetlab o‘tish mumkin.

Kiberhujumlarga qarshi samarali himoya

Zamonaviy xakerlik texnikalari apparat darajasidagi zaifliklardan foydalanishni o‘z ichiga oladi, masalan, *side-channel attacks* (yo‘ldosh kanallar orqali hujumlar). Apparat xavfsizligi bu hujumlarga qarshi chora ko‘rishga yordam beradi.

02

Zaifliklarni Tahlil Qilish

Odatiy zaifliklarni ko’rib chiqamiz

Asosiy apparat xavfsizligi zaifliklari:

Side-Channel Attacks

Bu hujumlar qurilmaning energiya iste’moli, elektromagnit radiatsiyasi yoki ishlash vaqtidagi o‘zgarishlar orqali ma’lumotni o‘g‘irlash uchun amalga oshiriladi.

Firmware zaifliklari

Agar firmware o‘z vaqtida yangilanmasa yoki noto‘g‘ri himoyalansa, unga zararli dasturlar o‘rnatilishi yoki boshqa himoya choralari chetlab o‘tilishi mumkin.

Asosiy apparat xavfsizligi zaifliklari:

Supply Chain Vulnerabilities

Yetkazib beruvchilar yoki uchinchi tomon ishlab chiqaruvchilari tomonidan uskunaga maxfiy ma'lumotlarni yig'uvchi kodlarni joylashtirish.

Physical Tampering

Bankomatlarga o'rnatilgan kartalarni nusxalovchi skimmerlar yoki fizik tuzilishlarni o'zgartirib ma'lumot olish.

Hardware Backdoors

Dastlab o'rnatilgan backdoors (orqa eshiklar) orqali maxfiy tashkilotlarning himoyalangan tarmoqlariga kirish.

Zaifliklarni Aniqlash

03

Zaifliklarni aniqlash usullarini ko’ramiz

Apparat xavfsizligi zaifliklarini aniqlash

uchun turli usullar mavjud bo‘lib, ular xavfsizlik mutaxassislari tomonidan hujum ehtimolini oldindan ko‘rish, tahlil qilish va zaif nuqtalarni aniqlash uchun ishlatiladi.

Pentesting

Fuzzing

Threat Modeling

Code Review

Reverse Engineering

Pentesting

Bu usul orqali xavfsizlik mutaxassislari tizimni xakerlar uslubi bilan sinovdan o‘tkazadi. Tizimning zaif tomonlari topilib, ulardan qanday foydalanish mumkinligi o‘rganiladi.

Qo‘llanilishi: Pentesting tizimdagi orqa eshiklar, himoyasiz ma'lumotlar, va boshqa zaifliklarni aniqlash uchun ishlatiladi.

Pentesting bo’yicha video darslik

FUZZING

Fuzzing usuli tizimga kutilmagan yoki noto‘g‘ri ma'lumotlar kiritib, qanday ishlashini tekshirishni o‘z ichiga oladi. Bu orqali dasturning noto‘g‘ri ma’lumotlarga qanday reaksiya berishini va zaifliklar qayerda ekanligini aniqlash mumkin.

Qo‘llanilishi: Firmware, drayverlar va boshqa apparat dasturlarini sinovdan o‘tkazishda.

Threat Modeling

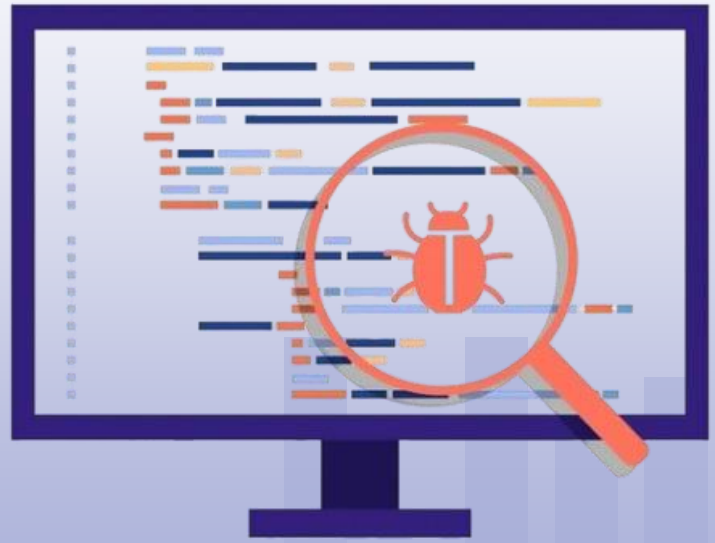
Threat modellashtirish orqali tizimga hujum qilish ehtimoli yuqori bo‘lgan nuqtalar aniqlanadi. Bu usul xavfsizlik xatarlarini tahlil qilishga yordam beradi va ular qanday himoya qilinishi kerakligini aniqlaydi.

Qo‘llanilishi: Tizim ichidagi potensial zaifliklarni aniqlash va ularning ekspluatatsiya qilish imkoniyatlarini o‘rganishda qo‘llaniladi.

Code Review

Code Review (Kod tekshiruvi) - Bu usulda apparat bilan bog‘liq dasturiy ta'minot koderlari sinchkovlik bilan tahlil qilinadi. Kod tekshiruvi paytida xavfsizlik nuqtai nazaridan xatoliklar yoki zaifliklar izlanadi.

Qo‘llanilishi: Firmware va boshqa apparat dasturlaridagi zaifliklarni aniqlash.



Reverse Engineering

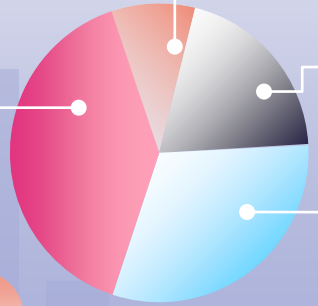
Bu usul orqali apparat ichidagi komponentlarni tahlil qilib, orqa eshik yoki boshqa zararli komponentlarni aniqlash mumkin. Ushbu usul apparatning ichki qismlarini sinchkovlik bilan o‘rganishni o‘z ichiga oladi.

Qo‘llanilishi: Zararli kodlar, maxsus o‘rnatilgan mikrosxemalar yoki backdoor’larni aniqlash.

Reverse Engineering

Diagrammada

Reverse Engineering jarayonida sarflanadigan resurslar yoki e’tiborning qaysi qismlarga qaratilishini aks ettirish mumkin:



Boshqa 10%

Asbob uskunalar 40%

20% Kadr Malakasi

30% Dasturiy ta’minot tahlili

Vaqt va boshqa resurslar

Ko’proq Uchraydi

- Firmware zaifliklari 30%
- Kriptografik zaifliklar 25%
- Tarmoq zaifliklar 20%
- Backdoor zaifliklar 10%
- Boshqa zaifliklar 15%

04

Zaiflik uchun Qarshi choralar

Ishlab chiqish bo‘yicha takliflar

Fizik xavfsizlik choralarini kuchaytirish

Muhr va korpus himoyasi

Qurilmaning ichki qismlariga ruxsatsiz kirishni oldini olish uchun muhrlar yoki yopiq korpuslardan foydalanish.

Tamper Detection mexanizmlari

Qurilmaga jismoniy aralashuv yoki buzilish sodir bo‘lganda bu haqda ogohlantiruvchi signal yuboradigan sensorlardan foydalanish.

Kriptografik xavfsizlikni kuchaytirish

Secure Boot

Qurilma yuklanayotganda, firmware yoki operatsion tizimni yuklashdan oldin uning imzosi maxsus apparat darajasidagi kalit bilan tekshiriladi

Hardware-based Encryption

Apparat darajasidagi shifrlash maxsus qurilma yoki chip yordamida ma’lumotlarni shifrlashni amalga oshiradi. Bu dasturiy shifrlashga nisbatan tezroq va ishonchliroq. Qurilmadagi barcha ma’lumotlar saqlanishidan oldin avtomatik ravishda shifrlanadi.

Tahlil va Diagnostikani qiyinlashtirish

Anti-Tamper mikrochiplar

Qurilma ichidagi ma’lumotlar yoki kodni noto‘g‘ri tahlil qilish va himoyani chetlab o‘tishni murakkablashtiruvchi maxsus chiplar o‘rnatish. Bu orqali Hackerlar apparatni tahlil qilishlarini qiyinlashtirish mumkin.

Obfuscation va Masking

Qurilmaning ichki ma’lumotlarining haqiqiy shaklini yashirish yoki kodlar tuzilishini murakkablashtirish usuli. Bu orqali Reverse Engineering jarayonini qiyinlashtirish mumkin.

Bizning jamoa bilan tanishing

Azimova Zamiraxon

Dastur dizayni bilan ishlash

Mo’ydinov No’monjon

Ma’lumotlarni topish va tahlil qilish

Azimjonov Azizbek

Dasturiy taminot bo’yicha ishlarni olib borish

Etiboringiz uchun rahmat!