XAVFSIZ MA'LUMOTLARNI ALMASHISHDA OPERATSION TIZIMNING ISHONCHLI YUKLANISHINI TA'MINLASH

Saparova G.A

Nukus davlat texnika universiteti, Sun'iy intellekt va kiberxavfsizlik kafedrasi assistenti.

Axborot-kommunikatsiya tizimlarida xavfsiz ma'lumotlarni almashish uchun belgilangan talablarga muvofiq zarur bo'lgan asosiy axborot xavfsizligi mexanizmlarini bosqichma-bosqich amalga oshirishni o'z ichiga olgan usulni ishlab chiqish kerak. Bunday mexanizmlar ishonchli tarmoq yuklanishini ta'minlashni, shu jumladan yuklangan operatsion tizim tasvirining yaxlitligini kuzatishni va OTni masofadan kompyuterga yuklashda ma'lumotlarning o'zaro ta'sirining barcha ishtirokchilarining ishonchli autentifikatsiyasini o'z ichiga oladi [1]. Bundan tashqari, tizimlarda hisoblash muhitining xavfsizligiga ishonch darajasini aniqlash uchun foydalaniladigan axborot xavfsizligi tizimining samaradorligini baholash usuli ishlab chiqilishi kerak. Ishlab chiqilgan algoritm va usullarning tavsifi quyida keltirilgan.

Me'yoriy hujjatlariga ko'ra, ishonchli yuklanish – bu dasturiy ta'minotni butunliligini nazoratini hamda ishlash muhitini nazoratlash amalga oshirish doirasida OT shtat rejimida yuklanishi va yuklanuvchi OT hamda foydalanuvchi haqiqiylik tekshiruvi muvaffaqiyatli yakunida axborot resurslariga ruxsatni taqdim etish jarayoni hisoblanadi. Agar buzg'unchi o'z operatsion tizimini tashqi muhitdan ruxsatsiz yuklab olishga muvaffaq bo'lsa, u foydalanuvchining fayl tizimiga to'liq kirish huquqiga ega bo'ladi. Bundan tashqari, qo'shimcha tahdid sifatida foydalanuvchi sodir bo'lgan voqea haqida bilmasligi olinishi mumkin - bunda, tizim ishga tushirilgan mashinada hech qanday iz qoldirmaydi.

Hozirgi vaqtda axborot xavfsizligi bozori asosan operatsion tizimning qattiq diskdan yuklanishini boshqaruvchi va ish stoli kompyuterlarida foydalanish uchun mo'ljallangan axborotni himoya qilish vositalari (AHV) bilan ifodalanadi. Bunday vositalarni disksiz mijozlarda qo'llash mumkin emas, chunki ularda amalga oshirilgan OT boshqaruv mexanizmlari, qoida tariqasida, tarmoqni yuklash uchun mo'ljallamagan va taqsimlangan terminal tizimlarining o'ziga xos xususiyatlarini hisobga olmaydi.

O'z navbatida, xavfsiz OT yuklash mexanizmi so'nggi bir necha yil ichida "bootkit" va "rootkit" kabi zararli dasturlardan himoya qilish uchun o'rnatilgan dasturiy ta'minot (DT) ishlab chiquvchilari e'tiborini tobora ko'proq jalb qilmoqda. Bunday dasturlarning maqsadi OT va tizim drayverlarining dastur kodini o'zgartirishga imkon beruvchi erta boshlashni amalga oshirishdir (masalan, backdoor o'rnatish)[2]. Xavfsiz yuklashni amalga oshiradigan eng mashhur texnologiyalardan biri Secure Boot bo'lib, u 2.2 versiyasidan boshlab BIOS o'rnini bosgan UEFI (Unified Extensible Firmware Interface) moduliga kiritilgan [3]. Ma'lumki, Microsoft o'zining Windows 8 uchun sertifikatlash dasturiga UEFI xavfsiz yuklash mexanizmini amalga oshirish uchun apparat ishlab chiqaruvchilari uchun talablarni ham kiritgan. Ushbu mexanizm yuklashdan oldin xavfsiz muhitni ta'minlashi va yuklangan modullarning (drayverlar, OT yuklagichlari va ilovalari) elektron imzosini tekshirish orqali potensial zaif nuqtalardan ruxsatsiz zararli kodlarni ishga tushirishdan himoya qilishi kerak [4].

Shuni ta'kidlash kerakki, bunday amalga oshirishda xavfsiz yuklash rejimi OTni xavfsiz yuklash uchun faqat buzg'unchi himoyalangan kompyuterga fizik kirish imkoniga ega bo'lmasa kifoya qiladi, chunki ko'p hollarda ruxsatsiz kirish (RK), kriptografik kalitlarni almashtirish mumkin. Shuningdek, UEFI(Unified Extensible Firmware Interface) spesifikatsiyalariga muvofiq xavfsiz yuklash rejimi kalitlar uchun ishonchli tarmoq yaratish mexanizmlarini ta'minlamaydi. Shunday qilib, ushbu rejim to'g'ridan-to'g'ri kompyuterlar ishlatiladigan joyda faollashtirilishi kerak.

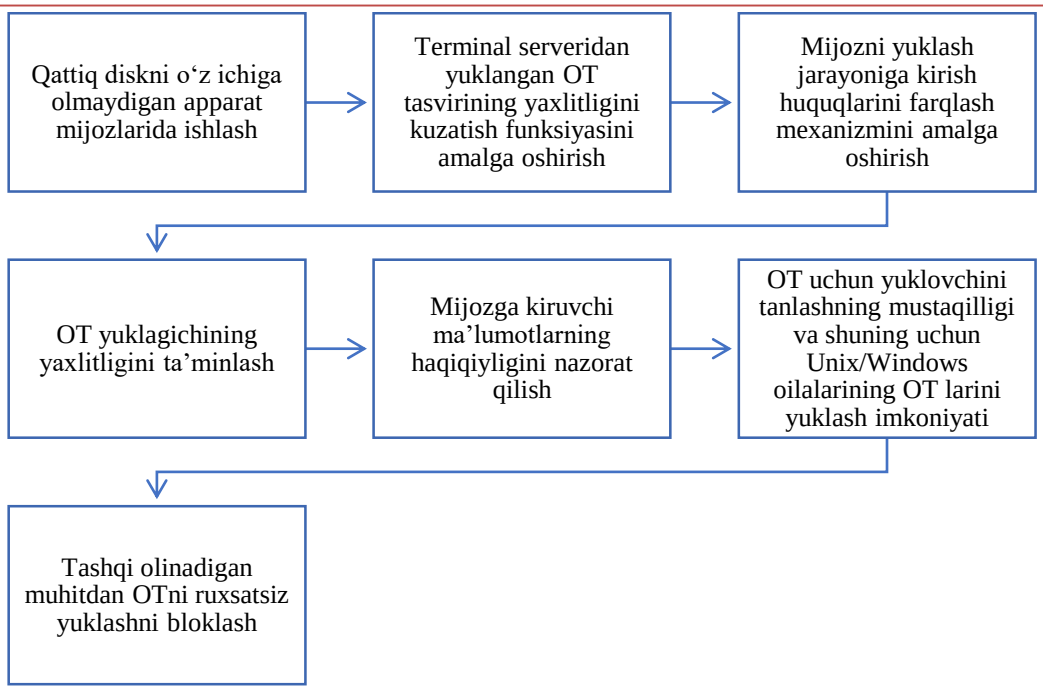
Ushbu ishda hal qilinayotgan yuklanadigan OTning yaxlitligini nazorat qilish vazifasining muhim xususiyati shundaki, tasvirning o'zi serverda saqlanadi va yuklash PXE (Preboot eXecution EnviroMent) protokoli yordamida tarmoq orqali amalga oshiriladi. Yuqorida tavsiflangan UEFI standarti PXE protokoli yordamida tarmoqni yuklash mexanizmini ham o'z ichiga oladi. Ammo protokolning an'anaviy tarzda amalga oshirilishida, yuklab olish so'rovini yuborayotganda, mijoz so'rov haqiqiy transport protokoli tomonidan amalga oshirilayotganiga ishonch hosil qila olmaydi. Shunga ko'ra, mijoz operatsion tizimni qayerdan olganini yoki uzatish jarayonida tasvirning yaxlitligi buzilganligini ishonchli bila olmaydi. Misol uchun, tarmoq protokoliga "Man-in-the-middle" hujumidan foydalanish natijasida tarmoq protokoli yuklanadigan OT obrazi bilan birga zararli kodni olishi mumkin [5]. Garchi bepul dasturiy ta'minot ishlab chiquvchilari tarmoq yuklab olish paytida tasvirlangan tahdidlarni zararsizlantirish uchun turli mexanizmlarni taklif qilishsa ham, axborot xavfsizligi bozorida hali tayyor vositalar taqdim etilmagan.

Shunday qilib, disksiz ish stantsiyalari uchun ishonchli muhitni ta'minlashning butun jarayonining muhim qismi bo'lgan xavfsiz OT yuklash kabi asosiy mexanizmni ta'minlash vazifasi hal qiliMagan.

Ishonchli yuklab olishni ta'minlash uchun tarmoq orqali yuklab olingan OT tasvirining yaxlitligini nazorat qilish va barcha ishtirokchi tomonlarni autentifikatsiya qilish uchun apparat darajasida mexanizmlarni amalga oshirish imkonini beruvchi yechim ishlab chiqildi [6].

Ishlab chiqilgan ishonchli tarmoq yuklash modulining tavsifi. Ishlab chiqilayotgan yechim maxsus disksiz shaxsiy kompyuterlarda ishlash uchun mo'ljallangan apparat-dasturiy ta'minotli ishonchli tarmoq yuklash modulini (ATITYM) yaratishni o'z ichiga oladi. Ushbu modul xavfsiz yuklash mexanizmini va kriptografik kalitlarni amalga oshiradigan proshivkani ajratish imkonini beradi. Bundan tashqari, ushbu usul OT yuklashni muayyan foydalanuvchilar uchun kerakli dasturiy ta'minot va sozlamalarga muvofiq shaxsiylashtiradi.

3.1-rasmda Operatsion tizimni xavfsiz yuklashga qo'yiladigan talabalar keltirib o'tilgan.



3.1-rasm. Operatsion tizimni xavfsiz yuklashga qo‘yiladigan talabalar

Ishlab chiqilgan ishonchli yuklash modulini amalga oshirish uchun PXE protokolini qo‘llab-quvvatlovchi tarmoq kartasi ishlatiladi va yuklash usulini amalga oshiradigan algoritm uning o‘rnatilgan dasturiy ta’minotiga kiritilgan. Ruxsatsiz ommaviy axborot vositalaridan operatsion tizimni yuklashni bloklash funksiyasi ma’muriy kirish huquqlarini olmasdan BIOS/UEFI konfiguratsiyasiga o‘zgartirishlarni taqiqlash orqali amalga oshiriladi.

Yuklab olingan tasvirning yaxlitligini nazorat qilish uchun ikkita asosiy obyekt mavjud bo‘lib, ularning o‘zgarmasligini nazorat qilish kerak:

- dastlabki bosqichda RAM xotirasiga yuklangan va keyingi yuklash jarayonini amalga oshiradigan 2-3 Kb hajmdagi OT yuklash moslamasi;
- OT obrazining o‘zi serverdan uzatiladi.

Yuklash jarayonining o‘zi boshqa barcha qadamlar asoslanadigan ishonchning asosiy nuqtasini o‘rnatadi. Bunday nuqta sifatida himoyalangan tashqi vosita (bundan buyon matnda token deb yuritiladi) tanlanadi, uning xotirasida OT yuklash moslamasi saqlanadi. Bunday tashqi axborot vositalarida o‘zining mikrokontrolleri - apparat va dasturiy ta’minot darajasida maxsus sertifikatlangan himoyaga ega bo‘lgan himoyalangan chip joylashgan bo‘lib, u ommaviy axborot vositalarining o‘zi xavfsizligiga ma’lum bo‘lgan barcha tahdidlarga, buzg‘unchilik va klonlash usullariga muvaffaqiyatli qarshilik ko‘rsatishga imkon beradi. Ushbu qurilma xotirasiga kirish faqat muvaffaqiyatli foydalanuvchi autentifikatsiyasidan so‘ng ta’minlanadi - parol kiritiladi. Yuklanuvchini bunday tokenda saqlash natijasida uning yaxlitligi kafolatlanadi. Ushbu yechim mijozga qaysi OT oilasi yuklanishiga hech qanday cheklovlar qo‘ymaydi.

Bundan tashqari, alohida himoyalangan vositadan foydalanish kirishni boshqarish muammosini hal qilish imkonini beradi: OT ni mijozga yuklash faqat tokenga ega va parolni biladigan foydalanuvchilar uchun mumkin. Token va mijozning o‘zaro autentifikatsiyasini ta’minlash uchun jarayonda ishtirok etuvchi har bir komponentni (foydalanuvchi, token, mijoz, server) almashtirish tahdidlaridan himoya qilishni ta’minlaydigan algoritmni amalga oshirish nazarda tutiladi.

Yuqoridagilarni hisobga olgan holda, ushbu yechimdan foydalanish, Secure Boot mexanizmidan farqli o‘laroq, buzg‘unchining mijozga to‘g‘ridan-to‘g‘ri kirish xavfini ahamiyatsiz qiladi, chunki u o‘z xotira qurilmasidan yuklash yoki tarmoq kartasini almashtirish imkoniyatiga ega bo‘lmaydi (autentifikatsiya algoritmi almashtirishni aniqlaydi). Bundan tashqari, ishlab chiqilayotgan modul juda moslashuvchan yechim bo‘lib, u na qo‘llaniladigan uskunaga, na OT turiga cheklovlar qo‘ymaydi. Bunday mijozlar bilan tizim boshqaruvi soddalashtirilgan, chunki administrator faqat himoyalangan foydalanuvchi ommaviy axborot vositalari bilan ishlashi kerak.

Shunday qilib, taklif etilayotgan yechimdagi asosiy vazifa server obrazining yaxlitligi va haqiqiyligini nazorat qilishni va har bir yuklab olish bosqichining xavfsiz bajarilishini ta’minlaydigan yuklab olish usulini ishlab chiqishdan iborat bo‘lib, xavfsizlik tahdidlarini amalga oshirishni istisno qiladi[6].

Axborot yaxlitligini monitoring qilishning mavjud usullarini tahlil qilish. Butunlikni buzish tahdidi deganda obyektning to‘g‘riligi va to‘liqligini saqlash xususiyatlarining har qanday buzilishi tushuniladi. Hujumchilar ma’lumotni ataylab o‘zgartirganda, ma’lumotlarning yaxlitligi buzilgan deb aytiladi. Butunlilikni nazoratlashni asosiy usullari siklik ortiqcha kod, kalitsiz va kalitli xesh-funksiyani hisoblash asosiga quriladi [7].

Amalga oshirishning soddaligi va birinchi usulning yuqori samaradorligiga qaramay, uning asosiy kamchiligini ta’kidlash kerak: hisoblash murakkabligi nuqtai nazaridan, olingan funksiya qiymatining dastlabki prototipini topish oson, buning natijasida tekshirish bosqichida olingan qiymatlarning tengligi uzatilgan ma’lumotlarning o‘zgarmasligini kafolatlamaydi [8]. Bu xususiyat yuqori xavfsizlik talablari bo‘lgan tizimlarda ushbu usuldan foydalanishni imkonsiz qiladi.

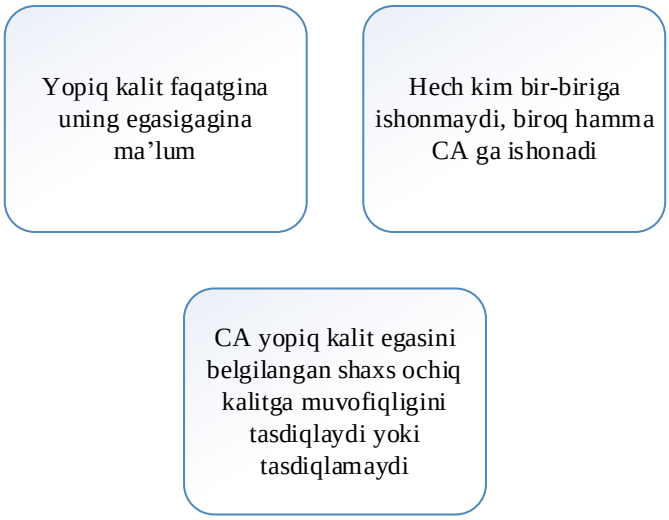
Bundan farqli o‘laroq, bir tomonlama xesh funksiyalaridan foydalanish ishlatiladigan usulning teskari transformatsiyaga chidamliligini ta’minlaydi. To‘qnashuvlarni qidirish vazifasi (chiqish sifatida bitta xesh qiymatini ishlab chiqaradigan funksiyaning bir nechta prototiplarining mavjudligi) juda ko‘p resurslarni talab qiladi va ishlashni talab qiladi.

Ammo bu afzallik bilan bir qatorda, bir tomonlama xesh-funktsiya usuli muhim xususiyatga ega: ishonchli saqlanishi yoki nazorat qiymatining ishonchli tomon tomonidan uzatilishini ta’minlash zarurati. Ishlab chiqilayotgan yechimga kelsak, serverda shakllanish vaqtida operatsion tizim tasviri uchun hisoblangan xesh qiymati almashtirish tahdidini bartaraf etadigan tarzda saqlanishi juda muhimdir. Mijoz apparat konfiguratsiyasi nuqtai nazaridan, qattiq disk yo‘qligi sababli paritet qiymatini saqlash uchun yagona ishonchli joy xavfsiz token xotirasi hisoblanadi.

Ammo yaxlitlikni boshqarish usulini amalga oshirishning ushbu varianti bir qator qiyinchiliklarni keltirib chiqaradi: tarmoq orqali mijozga yuklab olingan operatsion tizim tasviri vaqti-vaqti bilan qonuniy ravishda o‘zgarishi mumkin, masalan, yangilanishlar administrator tomonidan o‘rnatilganda. Bunday holda, token xotirasidagi nazorat qiymati qayta yozilishi kerak, chunki xesh qiymati ham o‘zgaradi. Ammo bir necha o‘nlab mijozlar mavjudligini o‘z ichiga olgan yetarlicha rivojlangan tashkilot tuzilmasi bilan bunday senariydan foydalanish ma’murning ishini juda qiyinlashtiradi.

Ochiq kalitlar infratuzilmasi tavsifi. O‘tkazilgan tasvirning yaxlitligini nazorat qilishning muqobil varianti elektron imzoni hisoblash uchun PKI dan foydalanishdir. PKI

ning asosiy xususiyati shundaki, unda amalga oshirilgan barcha xizmatlar ochiq kalit texnologiyasidan foydalangan holda taqdim etiladi. Ya'ni, PKI kriptotizim bo'lib, unda to'g'ridan-to'g'ri va teskari konvertatsiya qilish uchun ikki xil kalit ishlatiladi: ochiq (OK) va yopiq (YK)[9]. PKI ning majburiy komponenti ishonchli shaxs - sertifikatlashtirish markazi (keyingi o'rinlarda CA deb yuritiladi) bo'lib, u ochiq kalit yopiq kalitga mos kelishini va ularning egasiga tegishli ekanligini tasdiqlaydi, shu bilan birga sertifikat berish va uni EI bilan tasdiqlaydi. PKI ning asosiy tamoyillari 3.2-rasmda keltirilgan:



3.2-rasm. PKI asosiy tamoyili

Shunday qilib, elektron raqamli imzoni tekshirishi kerak bo'lgan tomon uni imzolagan tomonning ochiq kalitni olishi kerak. Bunday holda, ishonchli tomon (ya'ni, mijoz) ochiq kalitning haqiqiyligini (shu jumladan uning egaligini) tekshirishi kerak. Bunday holda, imzoni yaratuvchi terminal serverida obrazni imzolash uchun juftlik (ochiq va yopiq kalitlar) bo'lishi kerak.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Гатчан, Ю.А., Теплоухова, О.А. Способы контроля целостности образа операционной системы при удаленной загрузке на тонкие клиенты в системах терминального доступа. Электронный сборник тезисов докладов II Всероссийского конгресса молодых ученых, СПбНИУ ИТМО (Санкт-Петербург, апрель 2013). - 2013. - С. 52-53.

2 Левоневский Д.К., Ватаманюк И.В, Малов Д.А. Обеспечение доступности сер висов корпоративного интеллектуального пространства посредством управле ния потоком входных данных. Программная инженерия, т. 10, № 1, 2019. С. 20 29. DOI: 10.17587/prin.10.20-29

3 Осипов В.Ю., Воробьев В.И., Левоневский Д.К. Проблемы защиты от ложной информации в компьютерных сетях. Труды СПИИРАН. 2017. № 53. С. 97-117. DOI: 10.15622/sp.53.5

4 . Levonevskiy, D., Vatamaniuk, I., Saveliev, A. Processing models for conflicting user requests in ubiquitous corporate smart spaces. MATEC Web of Conferences, 161, 3006, 2019. DOI: 10.1051/matecconf/201816103006

5 Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar "Secure framework against cyber-attacks on cyber-physical robotic systems" Journal of Electronic Imaging, 2022

6 K. Millar, A. Cheng, H.G. Chew, C.C. Lim "Operating system classification: a minimalist approach" 2020 International Conference on Machine Learning and Cybernetics (ICMLC) (2020), pp. 143-150

7 S. Peng, A. Zhou, S. Liao, L. Liu "A threat actions extraction method based on the conditional co-occurrence degree" 7th International Conference on Information Science and Control Engineering (ICISCE) (2020), pp. 1633-1637

8 Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A. & Zheng, K., (2022). Protecting information and system integrity in industrial control system environments.

9 Murthy, S., Bakar, A. A., Rahim, F. A., & Ramli, R. (2019, May). A comparative study of data anonymization techniques. In 2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 306–309). IEEE.