6 – TOM 6 – SON / 2023 - YIL / 15 - IYUN

ANDROID XAVFSIZLIGI, XAVSLIK TIZIMLARINI YAXSHILASH.

Tojidinov Azizbek Ilhomjon o'g'li
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali talabasi
Abduraximov Ozodbek Azimjon o'g'li
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali talabasi

Annotatsiya: *Texnologiyaning paydo bo'lishi odamlarning ishlash usullarini soddalashtirgan ko'plab ishlanmalarni keltirib chiqardi. Aloqa va axborot sohasida birinchi o'rinda bo'lishga bo'lgan ehtiyoj ortib borayotganligi sababli, odamlar Android-ga asoslangan tizimlarni afzal ko'rgan katta foizli mobil telefonlardan foydalanishga murojaat qilishdi. Shunga o'xshab, tizimlar texnologiyadan kelib chiqadigan turli tahdidlarga sezgir bo'lib, tegishli xulosalar xavfsizlik kamchiliklari va maxfiy ma'lumotlarga ruxsatsiz kirish Android tizimlarining umumiy samaradorligiga katta xavf tug'dirishi mumkin. Ilovalardan foydalanish yoki o‘rnatishda Android xavfsizlik tizmlaridan qanday yaxshilash mumkinligiga e’tibor qaratdi.*

Kalit so’zlar: *Android Security , Sandbox, Linux, UID, GID, IPC*

KIRISH

So'nggi o'n yarim yil ichida Android dasturiy ta'minotining mobil telefonlarga qo'shilishi zamonaviy bozorni egallab oldi. Ko'p sonli tadqiqotlar natijasida olingan umumiy raqamlar shuni ko'rsatadiki, smartfon foydalanuvchilarining kamida 133 milliondan ziyod foydalanuvchilar Android qurilmasiga ega bo'lib, ularning soni kun sayin ortib bormoqda. Bu beixtiyor raqamlarning ko'payishi bilan operatsion tizimlarga hujumlar va tahdidlarning ko'payishini anglatadi. Android tizimlari duch keladigan turli muammolarni ta'kidlashdan oldin, ularning himoya darajalariga va tizim arxitekturasiga dasturiy qo'shimchaning o'ziga xos tuzilishini tushunish kerak.

Android ishlab chiquvchilari tizimlarning xavfsizlik arxitekturasi Linux asosidagi yadrolarga bog'liq bo'lishini ta'minlashga e'tibor qaratdilar, bu esa birlashishni ta'minlash uchun ilovalarni bir-biridan izolyatsiya qilishni ta'minlaydi. Izolyatsiya texnikasi dizayn jihatidan murakkab bo'lgan xavfsizlik modeli bilan mos ravishda ishlashi uchun imzo va turli ruxsatlarni talab qiladi. Murakkabliklar shunday ishlab chiqilganki, bu orqali foydalanuvchi o'zlari mos deb hisoblagan afzalliklarni qayta ko'rib chiqishi va o'zgartirishi mumkin. O'rnatilgan xavfsizlik sozlamalarini ko'rib chiqish orqali misol keltirish mumkin, shunda foydalanuvchi o'ziga mos keladigan afzalliklarni o'zgartiradi. Ko'pincha, Android operatsion tizimi sozlamalarni qanday o'zgartirish mumkinligi haqida tavsiflar bilan ta'minlangan bo'lsa-da, vazifalar qo'rqinchli bo'lib tuyulishi mumkin.

Xavfsiz android tizimlarining xavfsizlik modeli va foydalanuvchining xavfsizlik rollari tavsifini berish orqali davom etadi. Ochiq platforma bo'lgan Android o'zining

oddiy va bilimli foydalanuvchilariga har bir qurilmada ko'p qatlamli xavfsizlik funksiyalarini joylashtirish imkoniyatini beradi, bu esa ularning tajribasini oshirishga yordam beradi. Android operatsion tizimi tomonidan qo'llaniladigan ichki tizimda har bir qatlam tizim xavfsizligini ta'minlash uchun boshqa qatlamlar bilan birgalikda ishlaydi. Qatlamlarning barchasi birlashishni ta'minlash uchun ularni izolyatsiya qilish Linux xavfsizlik komponentidan o'z g'oyalariga asoslanadigan asosiy qatlamga birlashtirilgan .

Linux yadrosi bo'lgan birinchi qatlam qurilmaga o'rnatilgan bo'lib, ko'plab apparat ilovalari va dasturiy ta'minotini ta'minlaydi. Tadqiqotlar natijalari shuni ko'rsatadiki, yadro tomonidan ishlatiladigan apparat drayverlari displey ma'lumotlari, kamera va Bluetooth qurilmalarini o'z ichiga oladi. Bu uni sinash va qayta ko'rib chiqishni qiyinlashtiradi, chunki har qanday xato qurilma tuzilishining buzilishiga olib kelishi mumkin. Android ishlab chiquvchilari tizimli tamoyillarga ruxsat olish imkoniyatini minimallashtirish orqali bunday vaziyatlarning yuzaga kelishini yumshatishdi.

Qurilma dasturiy ta'minoti va apparat o'rtasida bog'lanishni yaratadigan apparat abstraktsiya qatlami. Foydalanuvchilar ushbu qatlamni mustaqil ravishda sozlashlari mumkin emas, chunki tizimlar ma'lumotlarni tahlil qilish va tizim samaradorligiga bog'liq. Android qurilmasi Linux yadrosidan foydalanish orqali tuzilganligi sababli, ishlab chiqish jarayoni uchun C va C++ kutubxonalarining yaxshi qismi talab qilinadi. Android ish vaqti xususiyati tizimning samarali ishlashiga imkon beruvchi muhitni o'z ichiga oladi. Ilgari Dalvik nomi bilan ma'lum bo'lgan ish vaqti xususiyati mobil qurilmaga o'rnatishda tizim kodlarini kompilyatsiya qilishda yordam beradi.

Android tizimining ushbu komponentida android tizimlarini yaratishda yordam beradigan Java tizimlari tomonidan qo'llaniladigan zarur API mavjud. Ilova qatlami qurilmalarning ma'lumotlar va grafik foydalanuvchi interfeysi talablarini ta'minlashda muhim ahamiyatga ega. Boshqa tomondan, dastur qatlami foydalanuvchi o'rnatgan ilovalardan ajratilgan tizim ilovalari bilan uzviy holda keladi. Ilovalar tizimning pastki qismidan boshlab taqdim etgan resurslarga juda bog'liq.

Yadroga asoslangan dastur sinov maydoni har bir ilovaga alohida UID (foydalanuvchi identifikatorlari) va GID (guruh identifikatorlari) beradi. Bu ilovalarning boshqa ilovalar ma'lumotlariga kirishini oldini oladi. Shunday qilib, yuklab olingan ilova tizimga kira olmaydi.

Ba'zi ilovalar boshqa ilovalarga kirishga muhtoj ekan, xavfsiz IPC bir-biri bilan muloqot qilish uchun muhim ilovalarga kirish imkonini beradi. Bu boshqa ilovalar bilan xavfsiz aloqa qilish uchun mahalliy rozetkalardan foydalanadigan ko'pgina ilovalar bilan mahalliy rozetkalar, bog'lovchilar va maqsadlar orqali amalga oshiriladi. Bog'lovchilar, shuningdek, kodni Android muhitiga tatbiq etishda muhim ahamiyatga ega va ular faqat dastur ishlayotgan vaqtda faollashadi. Tadqiqotlar shuni

ko'rsatadiki, niyatlar oldingi voqealarga qo'shimcha ravishda bajarilishi kerak bo'lgan operatsiyalar to'g'risida ma'lumot to'plashda yordam beradi.

Yuqorida ta'kidlab o'tilganidek, Android tizimlarining dastur doirasidagi ko'plab mahalliy kodlar mavjud. Bu Android ishlab chiquvchilari tizim resurslaridan zararli foydalanishning oldini olishga yordam berish maqsadida kamroq imtiyozlardan foydalangan holda tizim xizmatlarining aksariyat qismini ishga tushirishga majbur bo'lishiga olib keladi. Mahalliy kodlarga keyingi bo'limda ko'rsatilganidek, sertifikat organlariga o'xshash turli xil imzolar beriladi.

IOS tizimlari bilan taqqoslaganda, Android tizimlarida imzolash jarayonida foydalanuvchidan avtorizatsiya talab qilinmaydigan turli xil kod belgilari mavjud. Biroq, standart jarayon, keyinchalik xavfsizlik modelida qo'llaniladigan ilovalarning kodini imzolashni talab qiladi. Imzolar X.509 sertifikatlariga kriptografik jarayon qo'shimchasi uchun ochiq kalitlardan ham foydalanadi. Kod imzolari Java JAR imzolash sxemasiga qarab farqlanadi. Kod imzolari quyida ko'rsatilgan kod imzosining namunasi bilan ushbu ilovaning haqiqiyligini ta'minlaydi:

< ruxsatlar >

...

<buyum nomi =

“com.google.android.googleapps.permission.ACCESS_GOOGLE_PASSWORD”

paket = “com.google.android.gsf.login” himoyasi = “2”/>

...

Kod imzolarining nima uchun muhimligining bir qancha sabablari bor, birinchi navbatda, ilova uchun yangilanishlar ilovalar o'rtasida ishonchli munosabatlarni o'rnatish uchun bir xil muallif (bir xil kelib chiqish siyosati) qo'shimchasidan kelganligiga ishonch hosil qilish. Yuqorida aytib o'tilgan rollar ikkalasi ham yangilanish sertifikati bilan o'rnatilgan maqsadli ilovada imzolangan sertifikatlar o'rtasidagi taqqoslash orqali amalga oshiriladi. Havodan (OTA) yangilanishlar, shuningdek, dastur yamoqlari haqiqiylik va identifikatsiyani ta'minlash uchun kod imzolariga bog'liq.

Nihoyat, foydalanuvchiga ma'lum ilovalarning muhim tizim resurslariga kirishiga yo'l qo'ymaslikda yordam berish uchun Android ilovalari ruxsatnomalari amalga oshirildi. Android tizimi foydalanuvchiga o'rnatish yoki o'rnatishni tanlash imkonini beradi.m Linux yadrosi imtiyozlarga muvofiqlik jarayonini tartiblaydi va tizim fayllari va boshqa ilovalarga kirish imkonini beradi.

Android ilovalari va dasturlarini himoya qilishda va ikki xil nuqtai nazardan bir nechta yondashuvlar mavjud. Ishlab chiquvchi sifatida foydalanuvchilarning xavfsizligini yaxshiroq ta'minlash uchun qilish mumkin bo'lgan muayyan harakatlar mavjud. Bunday misollardan biri penetratsion test orqali bo'lishi mumkin, unda ishlab chiquvchi foydalanuvchi sezgir bo'lgan har qanday xavflarni aniqlaydi va kamaytiradi. Penetratsiyani tekshirish jarayoni bir qator jarayonlarni hisobga oladi, ular orasida hujumlar yuzaga kelishi, ilovalarning fayllar bilan o'zaro ta'sirini tahlil

qilish, tizimning saqlash qobiliyati va ob'ektlar o'rtasidagi aloqa kiradi. Ikkinchi nuqtai nazar, unumdorligini oshirish uchun o'rtacha foydalanuvchi tomonidan ilovaning xavfsizligini ta'minlashdan kelib chiqadi.

Tizimdan tashqaridagi aloqalar boshqa xavf omili bo'lishi mumkin. Odatda, eng mashhur ilovalar asossiz kirishni cheklash uchun kriptografiyaning qandaydir shakllaridan foydalanadi. Ilovani ishlab chiqishda foydalanuvchi hech qachon kripto-kalitni qattiq kodlamasligi juda zarur, chunki Android-dagi ilovalar ochiq kodli bo'lib, kirib kelishi muqarrar.

Nozik ma'lumotlarni baholaydigan dasturni sinovdan o'tkazish ko'rinadigan barcha bo'shliqlarni tuzatish uchun juda muhimdir. Tizim fayllari bilan bog'liq bo'lgan maksimal cheklovlar bilan to'g'ri o'qish/yozish ruxsatlarini ta'minlash foydalanuvchi ma'lumotlariga kirish huquqiga ega bo'lgan ilovalar sonini ham cheklashi mumkin. Keraksiz ma'lumotlar to'planishiga ishonch hosil qilish uchun dasturchi ma'lumotlarning kirib borishini sinovdan o'tkazishda qanday ma'lumotlar saqlanganligini baholashi kerak.

Foydalanuvchining ixtiyoriy xavfsizlik holatlari

Ruxsatlarni boshqarish—Avval aytib o‘tilganidek, foydalanuvchi o‘zi o‘rnatayotgan ilovalar befoyda emasligiga ishonch hosil qilishi va unga kerakli ruxsatnomalar berilishi kerak. Android’ning Marshmallow mikrodasturi yordamida foydalanuvchi endi ilovaga ruxsatdan foydalanishni taqiqlashi mumkin. Bu avval aytib o'tilganlarga zid bo'lishi mumkin, ammo dastur buni hisobga olgan holda to'g'ri ishlamaydi va foydalanuvchidan ishlash uchun berilgan ruxsatlarni aniq so'rashiga olib keladi. Biroq, bu, agar tashvish hissi paydo bo'lsa, ba'zi uchinchi tomon ilovalari muayyan apparat yoki fayllar bilan ishlamasligini ta'minlashi mumkin. Masofadan o‘chirish va kuzatish—Android taqdim etadigan yana bir xususiyat bu o‘g‘ri telefoningizni tortib olgan taqdirda masofadan o‘chirish va kuzatishdir. Fayllarni zaxiralash—Foydalanuvchilar o‘zlarining ilovalari va fayllarini qattiq disk yoki bulutga zaxiralashlari mumkin.

Ma'lumotlarni saqlash—Sukut bo'yicha, ko'pchilik ma'lumotlar tezkor kirish imkonini beruvchi Android qurilmasining ichki xotirasiga tushadi. Shuningdek, faylni parol yordamida himoya qiluvchi KeyStore yordamida fayllarni kalit bilan shifrlashingiz mumkin. Ilovalar yoki ma'lumotlarni tashqi saqlash eng xavfsiz usul bo'lib, masalan, telefonga o'rnatilgan SD-kartani sukut bo'yicha global o'qish/yozish mumkin; ammo, Androidning yangi versiyalari bilan tashqi SD-kartalarni shifrlash mumkin. Eng xavfsiz saqlash uchun kriptografiya sxemalaridan foydalaning, chunki aksariyat ilovalar Java Kriptografiya Architect bilan ishlaydi, ularda odatda 256-bitli AES, 256-bitli ochiq kalitlar, CBC, CTR yoki GCM rejimlaridan foydalanadi, HMAC-SHA1/256/ bilan yaxlitlikni ta’minlaydi. 512 yoki GCM. To'liq yoki fayl diskini shifrlash

ma'lumotni shifrlash uchun AES (128), CBC va SHA256 dan foydalanadigan Android qurilmasi uchun maxfiylikni ta'minlashning namunali usuli hisoblanadi.

Zararli dasturlarning oldini olish—Zararli dasturlarning oldini olishning yaxshi usuli bu haqiqat bo'lish uchun juda yaxshi ko'rinadigan narsalarni bosmaslikdir. Boshqacha qilib aytadigan bo'lsak, qaysi veb-saytlarga tashrif buyurganingizga, bosish kerak bo'lib tuyulishi mumkin bo'lgan qalqib chiquvchi reklamalarga va siz yuklab olgan ilovalar ishonchli ekanligini bilishga ehtiyot bo'ling.

Ekran qulfi—Klaviatura qulfi, ìrísí skaneri, barmoq izi skaneri, PIN-kod bloki yoki yuzni tanish dasturidan bo'ladimi, bu istalmagan o'tkinchining qurilmangizdagi ma'lumotlarga kirishini oldini olishning eng yaxshi usullaridan biridir.

Ilova blokirovkasidan foydalaning—Google Play do‘konida foydalanuvchilarning Galereya yoki Kamera kabi ba’zi ilovalarga kirishini oldini olishda foydalanish mumkin bo‘lgan minglab ilovalar mavjud. Biroq, ma'lumotlaringiz xavfsizligini ta'minlash uchun sharhlar va ushbu ilovaning mashhurligini tekshirish yaxshidir. Play do'konidagi barcha ilovalar haqiqiy emas.

Operatsion tizimni yangilab turing—Bu, albatta, aytish kerak, lekin ko'p foydalanuvchilar o'z telefonlari uchun yangilanishlarini e'tiborsiz qoldiradilar.

FOYDALANILGAN ADABIYOTLAR:

1. Dadakhon, T. (2022). Factors that Review Students' Imagination in the Educational Process. Spanish Journal of Innovation and Integrity, 5, 551-557.
2. Davi, L., Dmitrienko, A., Sadeghi, A.R. and Winandy, M. (2010) Privilege Escalation Attacks on Android. International Conference on Information Security, Chengdu, 17-19 December 2010, 346-360.
3. Sun, S.T., Cuadros, A. and Beznosov, K. (2015) Android Rooting: Methods, Detection, and Evasion. 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, Denver, 12-16 October 2015, 3-14.
4. Blasing, T., Batyuk, L., Schmidt, A.D., Camtepe, S.A. and Albayrak, S. (2010) An Android Application Sandbox System for Suspicious Software Detection. 5th International Conference on Malicious and Unwanted Software, Nancy, 19-20 October 2010, 55-62.
5. Gunasekera, S. (2012) Android Security Architecture. In: Gunasekera, S., Ed., Android Apps Security, Apress, Berkeley, 31-45.