14-LABORATORIYA ISHI

MOBIL ILOVALARNI ISHLAB CHIQISHDA RUXSATLAR, MA’LUMOTLARNI SHIFRLASH

Ishdan maqsad: Mobil ilovalarni ishlab chiqishda ruxsatlar, ma’lumotlarni shifrlashni o’rganish.

NAZARIY QISM

So'nggi yillarda mobil qurilmalardan foydalanish veb-ga katta qiziqish uyg'otdi, operatsion tizimlar rivojlanmoqda, biroq zararli kod va aniqlangan zaifliklar soni yildan-yilga deyarli chidamli ravishda o'sib bormoqda. Shu munosabat bilan axborotni ochiq aloqa kanallari orqali saqlash va uzatish jarayonida ruxsatsiz kirishdan himoya qilish uchun mo'ljallangan dasturiy vositalarni ishlab chiqish zarur. Bu muammoni hal qilish uchun turli usullar mavjud, masalan, steganografiya usullaridan foydalanish va ma'lum bir konteynerda himoyalangan ma'lumotlarni yashirish mumkin, ammo bu usul muayyan cheklovlarga ega, shuning uchun eng maqbul usul-maqbul himoya darajasini ta'minlash uchun kriptografik transformatsiyani qo'llashdir. Ishda axborotni nosimmetrik va assimetrik metodologiyadan foydalangan holda aylantirishning kriptografik usullari o'rganildi. Nosimmetrik metodologiya usullari orasida nosimmetrik kriptosistemalarning ikkita asosiy guruhi - blok va oqim shifrlari ko'rib chiqiladi. Kalitlardan foydalangan holda metodologiya usullarining qiyosiy tahlillari o'tkazildi, ushbu usullarni amalga oshirishda apparat resurslarini iste'mol qilish bo'yicha tadqiqotlar o'tkazildi. Olingan natijalar asosida amalga oshirish uchun kriptografik usullar tanlangan.

Dastur Android mobil operatsion tizimi bilan ishlaydigan Java tilida amalga oshiriladi. Ilovaning arxitekturasi muhim vaqt sarflamasdan yangi kriptografik algoritmlarni qo'shish imkonini beruvchi tarzda ishlab chiqilgan. Dastur sizga kalitlarni ishlab chiqarish, foydalanuvchi ma'lumotlarini shifrlash va parolini ochish, shuningdek olingan natijalarni Google Drive bulutli saqlashga imkon beradi.

Turli xil kirish ma'lumotlarini ishlatganda amalga oshirilgan dasturiy ta'minot sinovdan o'tkazildi. 4096 bitgacha kalitlarni ishlatganda dasturiy ta'minotni tekshirish amalga oshirildi. Tekshiruv natijasida dasturiy ta'minot belgilangan vaqt ichida barcha funktsiyalarni muntazam ravishda amalga oshirishi aniqlandi.

Android fayl va konteyner darajasida shifrlashni qo'llab-quvvatlaydi (to'liq diskli shifrlash). Ilovalar uchun platforma sifatida u uchinchi tomon shifrlash usullarini, masalan, xavfsiz papkalarni yoki messenjerlarda va pochta orqali shifrlangan yozishmalarni qo'llab-quvvatlashi mumkin. Bu shuni anglatadiki, qurilma chipseti tezda ma'lumotlarni shifrlash va parolini hal qilish uchun o'rnatilgan komponentni o'z ichiga oladi. Faylni dekodlash uchun tegishli kalit qurilmada saqlanadi va har bir foydalanuvchi harakati parol, barmoq izi, ishonchli qurilma va boshqalar. - shifrlangan ma'lumotlarga kirish uchun ishlatiladigan, xavfsiz elementga (plastik kartalarda ishlatiladiganlar kabi alohida mikroprotsessorga) murojaat qiladi. Android 6.0 Marshmallow-dan boshlab, barcha shifrlash funktsiyalari ushbu xavfsiz Element va ma'lumotlarni shifrlash va parolini hal qilish uchun qo'llaniladigan maxsus kalit, belgilar (bir martalik yoki qayta ishlatiladigan elektron kalitlar) yordamida amalga oshirilishi mumkin. Bu shuni anglatadiki, protsessorni joriy Tokenni taqdim etmasdan, ma'lumotlar shifrlangan bo'lib qoladi.

Android sozlamalarda parol kiritilmaguncha, tizim telefonni har safar yuklab olishda shifrlangan bo'lib qolishi mumkin. Telefondagi ma'lumotlar shifrlangan bo'lsa, u allaqachon xavfsizlikni ta'minlaydi, lekin parol kiritilgunga qadar yuklash jarayonini to'xtatib turish fayllarga kirishni oldini oladi va qo'shimcha himoya qatlami sifatida xizmat qiladi. Har qanday holatda, parol (yoki PIN kodi yoki grafik kaliti yoki barmoq izi) Secure Element orqali ma'lumotlarga murojaat qiladi va maxsus shifrlash kalitini olish imkoniyati yo'q – ma'lumotlar bilan nima qilinganligini va ularni qanday qilib eski ko'rinishga qaytarish kerakligini bilish uchun kerak bo'lgan yagona narsa.

Brauzeringizdagi yozishmalar va harakatlar ham shifrlanishi mumkin. Ehtimol, brauzerda ko'plab saytlar http o'rniga HTTPS bilan boshlangan manzilga ega ekanligiga e'tibor qaratilgandir. HTTP Hypertext Transfer Protocol (matn uzatish protokoli) degan ma'noni anglatadi va bu protokol internetda ma'lumotlarni yuborish va qabul qilish uchun ishlatiladi. O'z navbatida, HTTPS "SSL orqali HTTP" degan ma'noni anglatadi (Secure Sockets Layer, xavfsiz soket darajasi), protokolga shifrlash standartini qo'shadi. Brauzerda kiritgan barcha ma'lumotlar saytdan yuklab olgan ochiq kalit yordamida o'zgartiriladi, unga kiradi va veb-serverda mavjud bo'lgan maxsus kalit ularni parolini hal qilishi mumkin.

Qaytib keladigan ma'lumotlar o'zgartiriladi, shuning uchun ularni faqat noyob davlat kalit yordamida tushunish mumkin. Https bilan boshlangan xavfsiz saytlarga tashrif buyurishdan boshqa hech narsa qilish shart emas. Smartfon server aslida sertifikat bilan ko'rinadigan narsa ekanligini tekshiradi va brauzer ilovasi orqali ma'lumotlarni mustaqil ravishda shifrlaydi.

Shifrlangan yozishmalarni saqlash uchun odatda Google Play-dan ilovani yuklab olish lozim bo’ladi. Signal yoki WhatsApp kabi ilovalar uchidan uchigacha bo'lgan shifrlashni taklif qiladi, ya'ni ilova kalitlarni alohida kontaktlarga yoki guruhlarga tayinlaydi va xabar faqat unga yuborilgan shaxsni o'qishi mumkin. Ko'pchilik BlackBerry Messenger-ni xavfsiz deb hisoblaydi, ammo barcha BlackBerry qurilmalarida mavjud bo'lgan bitta umumiy kalit mavjud bo'lgani uchun, bu xavfsizlik biroz tortishuvlarga sabab bo'ladi. BBM Protected yuqori darajadagi shifrlash yoki uchidan uchgacha shifrlashni talab qiluvchi guruhlar uchun mavjud. Apple iMessage ham uchidan uchgacha shifrlashga ega, ammo faqatgina barcha yozishmalar iPhone egalari uchundir.

Foydalanadigan ushbu ilovalar, boshqa har qanday messenjerdan foydalanganidek: kontakt qo'shiladi va u bilan xabar almashiladi. Faqatgina farq shundaki, bu xabarlar shifrlangan bo'lishi mumkin, shuning uchun faqat ikki tomon – yozishmalar ishtirokchilari – ularni o'qishlari mumkin.

LABORATORIYA ISHINI TOPSHIRISH TARTIBI:

1.Ushbu mavzu bo'yicha ma'ruza darsida, laboratoriya ishining nazariy ko'rsatmalar qismida, shuningdek tavsiya etilgan adabiyotlarda ko'rilgan mavzu ma'lumotlarini yaqindan o'rganib, o'zlashtirib, nazorat savollariga javob berishga tayyor bo'ling.

2.Topshiriq sifatida har bir talaba Mobil ilovalarni ishlab chiqishda ruxsatlar, ma’lumotlarni shifrlash haqida ma’lumot beradilar va hisobot shaklida shakllantiradilar.