O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami

(2024-yil 17-18-may)

(1-qism)

JIZZAX-2024

“Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2024-yil 17-18-may. 410-bet.

Respublika miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., PhD. O‘ralov A.I.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., b.f.f.d. (PhD) O‘ralov A.I., t.f.f.d.(PhD), dotsent Abdumalikov A.A., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), dots. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dotsent Alibayev S.X., p.f.f.d. (PhD) Halimov O‘.H., p.f.f.d.(PhD), dotsent Karshiyev A.A., f.f.f.d.(PhD), dotsent Sindorov L.K., t.f.f.d.(PhD), dotsent Nasirov B.U., b.f.f.d. (PhD), dotsent Mustafaqulov M.A., f.f.f.d. (PhD) Alibekov D.A.., f-m.f.f.d. (PhD) Sharipov X.F., ps.f.f.d.(PhD) Norbekova B.Sh., i.f.n., dots. Tsoy M.P., Qayumov O.A., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

tozaligi ortib borib, eritmada bo‘yovchi modda konsentratsiyasi mato massasiga nisbatan 3% bo‘lganida egri chiziqning *Y* o'q bilan bir nuqtada kesishishi va sistemada muvozanat vujudga kelganligini ko‘rishimiz mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

1. Khusniddin Ismoilov, Sachin Chauhan, Mingxing Yang, Islamova Zulaykho, Quan Heng. Preparation and Application of Anionic and Cationic Waterborne Polyurethanes and Graphene-Cellulose Nanocrystal as an Antistatic Agent for Cashmere // Scientific Research Publishing «Graphene» New York-2019, Oct. 8. – 19-31 p.p.

2. https://dormeuil.com/blogs/news/dyeing-wool-the-art-of-colouring-cloth-for-suits

3. Инструксия по ползованию. Kompyuter kolor matching system operation and maintenanse manual. Korea industrial technology ODA. 2012. P.79.

ANDROID ILOVALARINI XAVFSIZLIK XUSUSIYATLARI TAHLILI: SSO PROTOKOLI MISOLIDA

Jabbarov Nuriddin Akbarovich
Toshkent axborot texnologiyalari universiteti
nuriddinjabbarov2696@gmail.com

Annotatsiya. Uyali telefonlar odamlarning internetga kirishlari uchun asosiy yondashuvga aylanib borayotganligi sababli, odamlar o‘z mobil telefonlaridan foydalanayotganda xavfsizlik asosiy muammo hisoblanadi. Foydalanuvchilarning cookie-fayllari va hisobga olish ma’lumotlari kabi axborotlarni himoya qilish uchun samarali izolyatsiya mexanizmlariga ega bo‘lgan veb-brauzerdan farqli o‘laroq, Yagona kelib chiqish siyosati (SOP) Android ilovalarini ishlab chiquvchilar izolyatsiya mexanizmini o‘zlari amalga oshirishlari kerak. Ushbu maqolada Facebook SDK yordamida Yagona tizimga kirish (SSO) xizmatini taqdim etuvchi ilova tahlil qilingan. Ilovadan olingan tarmoq trafigi rasmiy modellarni yaratadi va rasmiy modellarning belgilangan xususiyatlarini tekshirish uchun Proverif tekshirgichidan foydalaniladi. Tahlildan so‘ng SOPni buzadigan bitta zaiflik aniqlanadi.

Kalit so‘zlar: Yagona kelib chiqish siyosati (SOP), Yagona tizimga kirish (SSO), Android operatsion tizimi, identifikatsiya provayderida (IdP), xizmat ko‘rsatuvchi provayder (SP), Facebook SDK, Droidsafe, Proverif tajovuzkor modellar.

Hozirgi kunda axborot xavfsizligi tobora muhim ahamiyat kasb etmoqda. Kompaniyalar, hukumatlar va harbiylar turli sabablarga ko‘ra internetga ulanadi, masalan, jamoatchilikka ma’lum xizmatlarni taqdim etish, sheriklar bilan hamkorlik qilish va o‘z xodimlariga masofadan ishlashga ruxsat berish va hokazo. Biroq, ular internetga ulanganda, dushmanlar o‘zlarining ichki tarmoqlariga kirishlari va zaifliklar mavjud bo‘lsa, shaxsiy ma’lumotlariga kirishlari mumkin bo‘lgan kirish yo‘llarini ham ochib berishadi. Mobil qurilmalar orqali internetga ulangan shaxs haqida gap ketganda

ham xuddi shunday holat. Shaxsiy ma’lumotlarning sizib chiqishi jiddiy muammolarga hattoki moliyaviy yo‘qotishlarga olib kelishi mumkin [1], [2].

Android operatsion tizimi eng ommabop mobil operatsion tizimga aylandi, ammo Android ilovalari o‘ylaganchalik xavfsiz emas. Zaifliklar va tahdidlar o‘rnatilgan Android ilovasi protokolidagi nuqsonlardan [3], ilovalarda protokollarni qo‘llashdagi xatoliklar va tushunmovchiliklar [4], ma’lum SDK lardan foydalanishdagi tajribaga ega bo‘lmaslik [5] va hatto Android operatsion tizimining o‘zidan kelib chiqishi mumkin [6], [7].

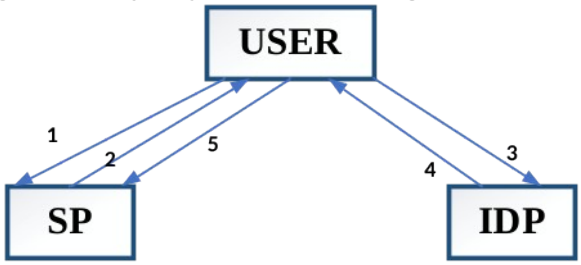
Ko‘pgina zaifliklar aslida dasturga muvofiqdir. Shuning uchun, Android ilovalarining xavfsizlik darajasini oshirish uchun ularni aniq amalga oshirishning xavfsizlik xususiyatlarini o‘rganish juda muhimdir.

Ushbu maqolada o‘zimizning davom etayotgan tadqiqot loyihamizning dastlabki natijalarini asosan ikkita tahliliy usul bilan taqdim etamiz: Yagona tizimga kirish (SSO) xizmatini taqdim etuvchi Android ilovalarining rasmiy tahlili va Android ilovalarida axborot oqimining sizib chiqishining dastlabki tahlili.

Axborot texnologiyalarining rivojlanishi bilan tobora ko‘proq veb-saytlar paydo bo‘ladi va ular foydalanuvchilarning ma’lumotlarini yozib olishni talab qiladi. Foydalanuvchilar ushbu veb-saytlarning xizmatlaridan foydalanishdan oldin ro‘yxatdan o‘tishlari kerak. Biroq, foydalanuvchi qanchalik ko‘p akkauntga ega bo‘lsa, foydalanuvchi yangi hisoblarni ro‘yxatdan o‘tkazishni shunchalik istamaydi, chunki bu turli veb-saytlarda turli hisoblarni boshqarish xarajatlarini oshiradi. Shu sababli, foydalanuvchi o‘zining turli hisoblari uchun bir xil paroldan foydalanishi mumkin. Shunga qaramay, bu muqarrar ravishda bitta parolning buzilganligi uning boshqa veb-saytlardagi identifikatorlarini xavf ostiga qo‘yadi. Buzg‘unchi hujum yordamida foydalanuvchining boshqa hisoblarini buzishga urinishi mumkin. Agar foydalanuvchi oddiy paroldan foydalansa, bu vaziyatni yanada kuchaytiradi.

SSO va Facebook-ning Androidda amalga oshirilishi

Oddiy SSO tizimga kirish jarayoni 1-rasmdagi kabi ishlaydi.



1-rasm. SSO tizimga kirish jarayoni

Bu SSO tizimiga muvaffaqiyatli kirishning umumiy jarayoni. Biroq, turli SSO dasturlarida tafsilotlar boshqacha bo‘lishi mumkin.

1) Birinchidan, foydalanuvchi IdPda o‘z identifikatori bilan SPga kirish uchun so‘rov yuboradi.

2) SP foydalanuvchi o‘zini da’vo qilgan shaxs ekanligini isbotlash uchun IdP dan kirish tokenini taqdim etishini talab qiladi. SP foydalanuvchini IdP ga yo‘naltiradi.

3) Foydalanuvchi IdP-ga kiradi va IdP-dan unga kirish tokenini yaratishni so‘raydi.

4) IdP foydalanuvchini yaratilgan kirish tokeni bilan SP ga qayta yo‘naltiradi.

5) Foydalanuvchi SP ga kirish tokenini taqdim etadi. SP kirish tokenini IdP bilan tekshiradi va foydalanuvchini tizimga kiritadi.

2-rasmda Android tizimida Facebook SSO login protokolining amalga oshirilishi ko‘rsatilgan. Qisqartirish uchun foydalanuvchi 2-rasmda ko‘rsatilmagan va foydalanuvchi tizimga kirish tugmasini bosish yoki foydalanuvchi hisob ma’lumotlarini kiritish kabi kerak bo‘lganda Android bilan o‘zaro aloqada bo‘ladi.

1) SP va SP ga kirish uchun foydalanuvchi so‘rovlari Facebook SDK ga foydalanuvchi kirish tokenini so‘rab so‘rovni boshlaydi.

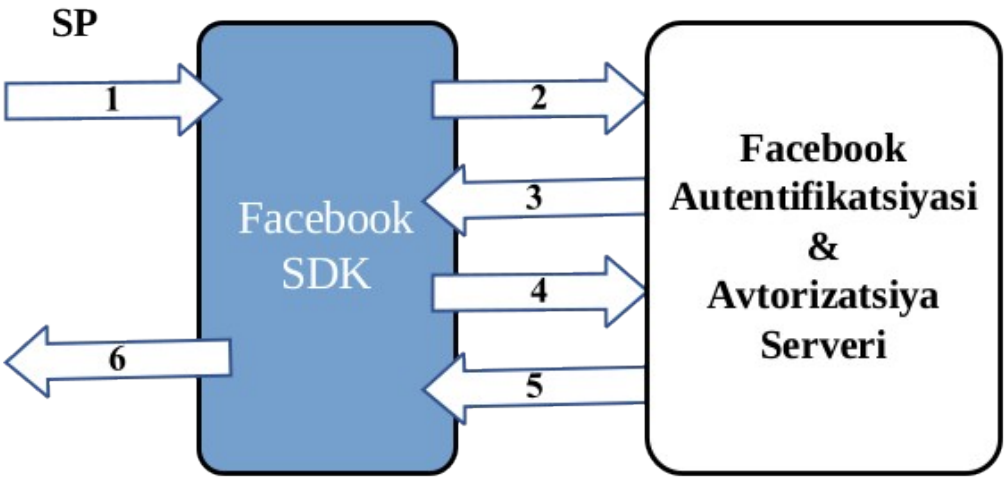
2) Facebook SDK so‘rovni Facebook serveriga o‘zining Facebook akkaunti identifikatori foydalanuvchi hisob ma’lumotlari bilan yuboradi.

3) Facebook serveri foydalanuvchining hisob ma’lumotlarini tekshiradi va muvaffaqiyatli tekshirishdan so‘ng cookie-fayllar foydalanuvchiga SP foydalanuvchining Facebook akkauntiga qanday ma’lumotlarga kirishini ko‘rsatuvchi shakl bilan qaytariladi.

4) Foydalanuvchi avtorizatsiyaga rozilik beradi.

5) Facebook kirish tokenini yaratadi va uni Facebook SDK-ga qaytaradi.

6) Facebook SDK SP ga kirish tokenini yetkazib beradi va SP foydalanuvchini tizimga kiritadi.



2-rasm: Odatda SSO tizimga kirish jarayoni

Taklif etilayotgan usul tavsifi

Facebook SSO joriy etilishini rasman tekshirish uchun uni amalga oshirishdan oldin protokolning rasmiy modelini yaratishi kerak.

Asosan, tahlil to‘rt bosqichdan iborat. Ular protokolni olish bosqichi, protokolni modellashtirish bosqichi, tekshirish bosqichi va yakuniy natijalarni tahlil qilish bosqichi. Har bir bosqichda artefaktlar yaratiladi va artefaktlar keyingi bosqichda kirish sifatida ishlatiladi. Xavfsizlik bo‘yicha tahlilchi modeldagi mumkin bo‘lgan zaifliklarni aniqlash va tasdiqlash uchun yakuniy bosqichda yaratilgan artefaktlarni qo‘lda tahlil qilishi kerak.

1) Protokolni chiqarish: Facebook SSO protokolini qanday amalga oshirishini hujjatlashtirmaganligi sababli, rasmiy modelni to‘g‘ri yaratish uchun Facebook SDK va Facebook serveri o‘rtasida nima uzatilishini va uzatilgan xabarlarning semantikasini tushunish kerak. Ushbu ma’lumotlarni bilish uchun Facebook SDK ning statik tahlili o‘tkaziladi, uning manba kodini qo‘lda tekshiradi va kirish jarayonida SDK nima

qilishini va SDK SP va Facebook serveri bilan qanday bog‘lanishini tushunish uchun. Keyin, protokolni dinamik ravishda ishga tushirish orqali Facebook SDK va Facebook serveri o‘rtasidagi tarmoq trafigini ushlaydi. Shundan so‘ng, ortiqcha xabarlar va parametrlarni olib tashlash orqali olingan tarmoq trafigini modellashtirish jarayonining qulayligi uchun tozalanadi.

2) Protokolni modellashtirish: Oldingi bosqichda olingan takomillashtirilgan protokol bilan muallif rasmiy modelni yozilgan Pi-hisobida quradi, bu Proverif [9] da qo‘llaniladigan modellashtirish tili bo‘lib, rasmiy modelni tanlovini tekshiradi. Ushbu bosqichdagi asosiy to‘siq - bu aniq amalga oshirish va yuqori darajadagi model namoyishi o‘rtasidagi bo‘shliq.

Ushbu muammoni yengillashtirish uchun avval intuitiv ravishda aniqlangan protokolni Pi-hisobiga yaqin bo‘lgan oraliq tasvirga aylantiradi. Asosiy modelga asoslanib, model ustidagi to‘rt xil tajovuzkorni taqdim etadi va tekshirilishi kerak bo‘lgan xususiyatlarga ega to‘rtta rasmiy modelni oladi. Birinchi tajovuzkor modeli - bu tajovuzkor aloqa kanalida, ya’ni tarmoqda tinglaydigan tarmoq hujumchisi, ikkinchisi zararli SP bo‘lib, u foydalanuvchiga xizmatlarni taqdim etadi va foydalanuvchilarga IdPda o‘z identifikatorlari bilan kirishga imkon beradi, uchinchi va to‘rtinchisi tizimdagi zararli dastur bo‘lib, ular faqat tizimdagi zararli dastur ildiz huquqini qo‘lga kirita oladimi yoki yo‘qligi bilan farqlanadi. Xavfsizlik tahlilchisi tomonidan ushbu to‘rtta tajovuzkor modelida aniqlangan xususiyatlar protokol xavfsizligi va foydalanuvchi maxfiyligiga eng mos keladigan autentifikatsiya xususiyati, avtorizatsiya xususiyati va maxfiylik xususiyatini o‘z ichiga oladi.

3) Tekshirish va tahlil: Oxirgi bosqichda olingan aniqlangan protokolning to‘rtta rasmiy modeli ushbu bosqichda xavfsizlik tahlilchisi tomonidan belgilangan xususiyatlar bilan tekshirilishi kerak bo‘lgan kirishlar sifatida ishlatiladi. Tekshiruvdan so‘ng Proverif modellar uchun tekshirish hisobotlarini yaratadi. Hisobotlarni tekshirish orqali xavfsizlik tahlilchisi tekshirilayotgan xususiyatlarning buzilishini va protokolning mumkin bo‘lgan zaifliklarini aniqlaydi. Agar shunday bo‘lsa, xavfsizlik bo‘yicha tahlilchi haqiqiy dunyo qurilmasiga hujumlarni qayta tiklaydi.

Tekshirish natijalari

Tasdiqlash jarayoni tugagandan so‘ng Proverif to‘rtta tajovuzkor modeli uchun tekshirish hisobotlarini yaratadi. Avtorizatsiya xususiyatlaridan faqat bittasi to‘g‘ri, ikkinchisi noto‘g‘ri yoki isbotlanmaydi. Tasdiqlangan modellar shuni ko‘rsatadiki, barcha tajovuzkor modellarida Facebook serveri avtorizatsiya jarayonini “foydalanuvchi” ning xohishiga ko‘ra tugatadi, xoh u haqiqiy foydalanuvchi bo‘ladimi, xoh foydalanuvchining hisob ma’lumotlarini buzgan va o‘zini shu foydalanuvchi sifatida ko‘rsatayotgan tajovuzkor bo‘ladimi. Natijalar shuni ko‘rsatadiki, ba’zi hollarda SP uchun takroriy hujum bo‘lishi mumkin. Biroq, bu tarmoq aloqasida keng tarqalgan *https* protokoli tufayli real dunyoda zaiflik emas va bu modellarni tekshirish natijalarida noto‘g‘ri ijobiydir.

Tarmoq tajovuzkori va tizimdagi zararli dastur uchun ildiz huquqiga ega bo‘lmagan tajovuzkor modellari uchun foydalanuvchi Facebook serveridan kiritgan va qaytargan barcha sirlar xavfsizdir, maxfiylik xususiyatlarining barchasi haqiqat ekanligi isbotlangan. Chunki tarmoq tajovuzkori uchun, tajovuzkor kanalni tinglashi mumkin bo‘lsa-da, lekin kanal shifrlanganligi sababli, u xabarlarni parolini hal qila

olmaydi yoki soxtalay olmaydi. Ildiz huquqiga ega bo‘lmagan zararli dastur uchun u boshqa ilovalarning shaxsiy ma’lumotlariga kira olmaydi, shuning uchun u foydalanuvchi va Facebook serveridan sirlarni ololmaydi. Zararli SP tajovuzkor modeliga kelsak, foydalanuvchi kiritilgan barcha hisob ma’lumotlari o‘g‘irlanishi va maxfiylik xususiyatlarining barchasi yolg‘on ekanligiga shubha yo‘q.

Ildiz huquqiga ega zararli dastur natijasida foydalanuvchining hisob ma’lumotlari xavfsiz ekanligi isbotlangan, maxfiylik xususiyatlari to‘g‘ri isbotlangan, Facebook serveridan qaytarilgan hisob ma’lumotlari esa xavfsiz emas. Bu, aslida, Yagona Origin Siyosatini (SOP) [10] buzganligi sababli amalga oshirishning katta kamchiliklarini ochib beradi. Kirish tokenini SP ning shaxsiy xotirasida saqlash oqilona bo‘lsa-da, lekin Facebookga tegishli bo‘lgan Facebook cookie-fayllarini SP xotirasida saqlash to‘g‘ri emas, chunki bu SOPni buzadi.

Amalga oshirishning ushbu kamchiligini maqsad qilib, SP shaxsiy xotirasiga kira oladigan har bir kishi Facebook cookie-fayllarini o‘g‘irlashi va jabrlanuvchining Facebook akkauntiga kirish uchun brauzerda cookie-fayllardan foydalanishi mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

1. S. Steiner, “The dangers of identity theft,” Aug 2013. [Online]. Available: http://goo.gl/ONKbLm

2. P. Oliver, “What’s most dangerous kind of identity theft?” Mar 2015. [Online]. Available: http://goo.gl/BXtoUP

3. R. Wang, S. Chen, and X. Wang, “Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services,” in S&P, 2012.

4. E. Y. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague, “Oauth demystified for mobile application developers,” in CCS, 2014.

5. R. Wang, Y. Zhou, S. Chen, S. Qadeer, D. Evans, and Y. Gurevich, “Explicating sdks: Uncovering assumptions underlying secure authentication and authorization.” in USENIX Security, 2013.

6. H. Bagheri, E. Kang, S. Malek, and D. Jackson, “Detection of design flaws in the android permission protocol through bounded verification,” in FM, 2015.

7. G. Bai, J. Sun, J. Wu, Q. Ye, L. Li, J. S. Dong, and S. Guo, “All your sessions are belong to us: Investigating authenticator leakage through backup channels on android,” in ICECCS, 2015.

8. C. Bansal, K. Bhargavan, and S. Maffeis, “Discovering concrete attacks on website authorization by formal analysis,” in CSF, 2012.

9. B. Blanchet, B. Smyth, and V. Cheval, “Proverif 1.86: Automatic cryptographic protocol verifier, user manual and tutorial,” INRIA Paris-Rocquencourt, LSV, ENS Cachan & CNRS & INRIA Saclay IIle-de-France, Paris, France, 2013.

10. M. Zelwski, “Browser security handbook, part 2,” 2011. [Online]. Available: https://goo.gl/Vi3dGO