ՀԱՍՏԱՏՈՒՄ ԵՄ՝

Հայաստանի ազգային պոլիտեխնիկական

համալսարանի գիտության և գիտատեխնոլոգիական

համագործակցության գծով պրոռեկտոր՝

տ.գ.դ., պրոֆ.

Ա. Խ. ԳՐԻԳՈՐՅԱՆ

«1» 12 2021 թ.

ԱՌԱՋԱՏԱՐ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ԿԱՐԾԻՔ

Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ներկայացված Ջիվան Անդրանիկի Հակոբյանի «Ֆազզ-թեստավորման արդյունավետությունը բարձրացնող մեթոդների հետազոտում և իրականացում» թեմայով ատենախոսության վերաբերյալ:

Ատենախոսության նպատակն է հետազոտել հայտնի եղանակները, մշակել և իրականացնել ֆազզ-թեստավորման արդյունավետությունը բարձրացնող նոր մեթոդներ: Մշակված մեթոդները պետք է թույլ տան հայտնաբերել առավել լայն դասի սխալներ, ինչպես նաև կիրառելի լինեն Linux, Windows և MacOS օպերացիոն համակարգերում:

Ատենախոսության արդիականությունը

Ծրագրային համակարգերը դարձել են մարդու կյանքի անբաժանելի մասը, և դրանց դերը գնալով մեծանում է: Հաճախ այդպիսի համակարգերը պարունակում են ծրագրային թերություններ և խոցելիություններ, ինչը կարող է ի հայտ գալ կիրառման ընթացքում: Նման սխալները կարող են ոչ միայն ֆինանսական վնաս պատճառել, այլև վտանգել մարդկանց կյանքն ու առողջությունը:

Ծրագրային ապահովման ստեղծման ընթացքում օգտագործվում են տարատեսակ թեստային համակարգեր և վերլուծության գործիքներ, որոնք թույլ են տալիս հայտնաբերել սխալները: Հնարավորինս անվտանգ ծրագրային ապահովումներ ստեղծելու համար կան հատուկ մշակված ստանդարտներ, որոնց համաձայն ֆազզ-թեստավորումը համարվում է անհրաժեշտ մեթոդներից մեկը, որը տեղի է ունենում ծրագրի կատարվող կոդի հիման վրա: Ֆազզ-թեստավորման գործիքները աշխատանքի ընթացքում մեկնարկում են թիրախային ծրագիրը՝ որպես մուտք փոխանցելով նախապես գեներացված/ձևափոխված տվյալներ, ապա հետևում ծրագրին: Ծրագրի վթարային ավարտի դեպքում տեղեկացնում են դրա մասին՝ տրամադրելով համապատասխան մուտքային տվյալները, ինչը հնարավորություն է տալիս վերարտադրել հայտնաբերված սխալը:

Գոյություն ունեն այնպիսի ծրագրային համակարգեր, որոնք մուտքային տվյալները ստանում են մեկից ավել ճանապարհներով՝ ցանցի, ֆայլերի, միջավայրի փոփոխականների, մուտքային դրոշների և ստանդարտ մուտքի հոսքի միջոցով: Քանի որ առկա թեստավորման գործիքները ապահովում են սահմանափակ քանակով մուտքերի թեստավորում (սովորաբար ֆայլի և ստանդարտ մուտքի հոսքի), ապա վերոնշյալ ծրագրային համակարգեր բոլոր հնարավոր մուտքերը թեստավորելու համար անհրաժեշտ է օգտվել մի քանիսից: Նման մոտեցումը բերում է վերլուծության գործընթացի բարդացման, ինչպես նաև ստեղծում է հավելյալ ֆինանսական ծախսեր և, որ ամենակարևորն է, ամբողջությամբ չի լուծում խնդիրը: Այդ գործիքները չեն փոխգործակցում միմյանց հետ, այսինքն՝ չեն օգտագործում միմյանց կողմից թեստավորման ընթացքում ձեռք բերված տվյալները: Գրեթե բոլոր թեստավորման գործիքները հաշվի չեն առնում մուտքային տվյալների կառուցվածքային առանձնահատկությունը և գեներացնում են այնպիսի մուտքային տվյալներ, որոնց մեծ մասն անտեսվում է թիրախային ծրագրի կողմից՝ որպես խոտան կամ վնասված: Իսկ նրանք, որոնք հաշվի են առնում, կիրառելի են սահմանափակ թվով մուտքային տվյալների տիպերի դեպքում:

Ատենախոսության կառուցվածքը

Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրակացությունից և հավելվածներից: Ատենախոսության ամբողջ ծավալը

կազմում է 102 էջ՝ ներառյալ 21 նկարներ և 4 աղյուսակներ, ինչպես նաև պարունակում է 106 անուն հղում:

Առաջաբանում հիմնավորվում է ատենախոսության թեմայի արդիականությունը, ներկայացվում են հետազոտության նպատակն ու խնդիրները, գիտական նորույթը, պաշտպանությանը ներկայացվող հիմնական դրույթները, հետազոտության տեսական և գործնական նշանակությունը:

Առաջին գլխում նկարագրված է հետազոտական ակնարկ այն գործիքների և մեթոդների մասին, որոնք կապ ունեն ատենախոսության թեմայի հետ, մասնավորապես՝ նկարագրվում են ֆազզ-թեստավորման հիմնական մեթոդները, ինչպես նաև առավել հայտնի թեստավորման գործիքները: Խոսվում է Java լեզվով գրված գրադարանների և իրերի համացանց (IoT) համակարգերի թեստավորման մասին, դիտարկվում են թեստավորման ժամանակ մուտքային տվյալներ գեներացնելու մեթոդները և դուրս են բերվում թվարկված գործիքներում առկա խնդիրներն ու թերությունները:

Երկրորդ գլխում ներկայացված է մշակված ISP – Fuzzer ֆազզ-թեստավորման միջավայրը: Այն իրականացված է որպես միջավայրից անկախ համակարգ, որը կարելի է գործարկել բաշխված և զուգահեռ համակարգերում՝ բարձրացնելով թեստավորման արդյունավետությունը:

ISP-Fuzzer–ն օժտված է հավելվածների ղեկավարման համակարգով, որի շնորհիվ այն հեշտորեն ընդլայնվում է՝ ներառելով նոր ֆունկցիոնալ հնարավորություններ: Սույն գլխում ներկայացված են նաև մշակված հավելվածները, որոնք թույլ են տալիս բարձրացնել թեստավորման արդյունավետությունը:

Երրորդ գլխում ներկայացված է Java լեզվով գրված գրադարանների ֆազզ-թեստավորման համար նախատեսված մեթոդ, որն իրականացված և ներդրված է ISP-Fuzzer միջավայրում: Մեթոդն ամբողջությամբ ինքնուրույն է և չի պահանջում որևէ նախնական տեղեկատվություն գրադարանային ֆունկցիաների կամ դասերի մասին:

Ի տարբերություն առկա այլ գործիքների, առաջարկվող տարբերակն աչքի է ընկնում API (Application Programming Interface) ֆունկցիաների կանչերի կապակցված հաջորդականությունների գեներացիայով: Համակարգը

թեստավորման ընթացքում ձևավորում է կանչերի այնպիսի հաջորդականություններ, որոնցում օգտագործված ֆունկցիաները կարող են լինել տարբեր դասերի: Նման մոտեցումն ապահովում է API ֆունկցիաների օգտագործման հնարավոր կոմբինացիաների ավելի մեծ շրջանակի թեստավորում:

Չորրորդ գլխում ներկայացված է մուտքային տվյալների միջակայքային ձևափոխության մեթոդը, որն օգնում է կրճատել թիրախային ծրագրի կողմից խոտան համարվող մուտքային տվյալների գեներացիան: Առաջարկվող մեթոդն իրականացնելու համար նախագծվել և իրականացվել է առանձին գործիք, որն ստատիկ վերլուծության միջոցով պարզում է մուտքային տվյալների առանցքային հատվածներն ու դրանց համապատասխան արժեքները, որոնց խախտման դեպքում մուտքային տվյալները համարվում են խոտան: Այս ամենի արդյունքում մուտքային տվյալներն այնպես են գեներացվում, որ բանալիային հատվածների ճիշտ արժեքները պահպանվեն: Վերլուծության արդյունքները կիրառվում են ISP-Fuzzer գործիքում՝ մուտքային տվյալների ձևափոխության ժամանակ, որի շնորհիվ, բոլոր բանալիային հատվածները պահպանում են ճիշտ արժեքները:

Ատենախոսության առավել կարևոր գիտական արդյունքները հետևյալն են.

- Առաջարկվել և իրականացվել է ֆազզ-թեստավորման միջավայր, որն ընդլայնվելիության հաշվին կարող է աշխատել ինչպես Linux այնպես էլ Windows և MacOS օպերացիոն համակարգերում: Միջավայրում ներդրվել է հավելվածների մեխանիզմ, որի շնորհիվ օգտատերը կարող է ավելացնել սեփական հավելվածը, ապահովելով նոր ֆունկցիոնալ հնարավորություններ: Արագագործության բարձրացման նպատակով մշակվել է լրացուցիչ գործիք, որը թույլ է տալիս միջավայրը գործարկել բաշխված և զուգահեռ համակարգերում:
- Միջավայրում իրականացվել է Java լեզվով գրված գրադարանների ֆազզ-թեստավորման մեթոդ: Այն թույլ է տալիս թեստավորել ցանկացած գրադարան նախապես չիմանալով վերջինիս կառուցվածքային առանձնահատկությունները: Մեթոդի կարևորագույն հատկություններից մեկը կայանում է նրանում, որ այն կարող է աշխատել նաև իրական սարքի վրա, ինչն ապահովում է բարձր արագագործություն:
- Իրականացվել է ծրագրի մուտքային տվյալների գլխագրերի կառուցվածքային առանձնահատկությունների կանխագուշակման մեթոդ: Առաջարկվող մեթոդը ստատիկ վերլուծության միջոցով հայտնաբերում է

մուտքային տվյալների այն հատվածներն ու դրանց համապատասխան արժեքները, որոնք անհրաժեշտ են գլխագրերը ընդունելի համարվելու համար: Մեթոդն օգտագործում է թեստավորման ընթացքում հայտնաբերված կատարման հետագծերը և դրանց համապատասխան մուտքային տվյալները:

- Մշակվել է թեստավորման ընթացքում մուտքային տվյալների գեներացիայի արդյունավետությունը բարձրացնող միջակայքային ձևափոխությունների մեթոդ, որի նպատակն է կրճատել այնպիսի մուտքային տվյալների գեներացիան, որոնք թիրախային ծրագրի կողմից կարող են անմիջապես անտեսվել՝ կառուցվածքի անհամապատասխանության պատճառով:

Ցավոք, աշխատանքը զերծ չէ որոշ թերություններից, որոնց թվում են.

- 4-րդ գլխի երկրորդ բաժնում նկարագրված են չափորոշիչներ նախատեսված միջակայքին ձևափոխությունների աշխատանքին բաժին ընկնող ժամանակի և ստատիկ վերլուծության կիրառման պարբերության համար: Ցանկալի կլիներ չափորոշիչների ընտրությունը կատարվեր ավելի լայն վերլուծության արդյունքում:
- 3-րդ գլխում նկարագրված է Java գրադարանների թեստավորման մեթոդ, սակայն մեթոդի արդյունավետությունը ստուգվել է միայն մեկ գրադարանի համար: Ցանկալի կլիներ համակարգի միջոցով թեստավորվեին մի քանի այլ գրադարաններ ևս:

Նշված թերությունները, սակայն, սկզբունքային չեն, կրում են խորհրդատվական բնույթ և չեն ազդում ատենախոսության ընդհանուր դրական գնահատականի վրա:

Աշխատանքում ստացված հիմնական արդյունքները հրապարակված են հեղինակի 4 գիտական հոդվածներում (մեկը՝ Scopus):

Սեղմագիրը ամբողջությամբ համապատասխանում է ատենախոսությանը և արտացոլում նրա բովանդակությունը: Հետազոտության թեման և ստացված արդյունքները լիովին համապատասխանում են Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությանը:

Ջիվան Անդրանիկի Հակոբյանի «Ֆազզ-թեստավորման արդյունավետությունը բարձրացնող մեթոդների հետազոտում և իրականացում» թեմայով թեկնածուական

ատենախոսությունը ավարտուն գիտական աշխատանք է, որը կարող է գնահատվել որպես կիրառական կարևոր խնդրի լուծում ապահովող, գիտականորեն հիմնավորված տեխնիկական մշակում:

Աշխատանքում առաջադրված խնդրի արդիականությունն ու ստացված արդյունքների նշանակությունը վկայում են այն մասին որ ատենախոսությունը լիովին համապատասխանում է թեկնածուական ատենախոսություններին ներկայացվող պահանջներին, իսկ հեղինակն արժանի է Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհման:

Քննարկմանը ներկա էին «Տեղեկատվական անվտանգություն և ծրագրային ապահովում» ամբիոնի վարիչ, տ.գ.թ., պրոֆ. Գ.Ի.Մարգարովը, պրոֆ. Ա.Խ.Պալյանը, դոց. Վ.Ս.Հակոբյանը, դոց. Ռ.Գ.Հակոբյանը, դոց. Ասլանյան Ա.Կ., տ.գ.թ. Լ.Ա.Թադևոսյանը, տ.գ.թ. Ա.Գ.Խաչատուրովը, ամբ.վար.տեղ. Վ.Ղ.Ղուկասյանը, դաս. Մ.Գ.Ուսեպյանը, դաս. Հ.Վ.Մարկոսյանը:

«Տեղեկատվական անվտանգություն և ծրագրային ապահովում»
ամբիոնի վարիչ, տ.գ.թ., պրոֆեսոր՝ Գ.Ի.Մարգարով

«Տեղեկատվական անվտանգություն և ծրագրային ապահովում»
ամբիոնի գիտ.քարտուղար, տ.գ.թ., դոցենտ՝ Ռ.Գ.Հակոբյան

Ստորագրությունները հաստատում եմ՝
ՀԱՊՀ գիտական քարտուղար, տ.գ.թ., դոցենտ՝ Ծ.Ս.Հովհաննիսյան
29.11.21թ.