ՊԱՇՏՈՆԱԿԱՆ ԸՆԴԴԻՄԱԽՈՍԻ ԿԱՐԾԻՔ

Համբարձում Դավիթի Մինասյանի

«Իրերի համացանցի սարքավորումների անվտանգության ապահովման մեթոդների և գործիքամիջոցների մշակումը» թեմայով Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության վերաբերյալ:

Ատենախոսությունը վերաբերում է IoT սարքերի անվտանգության ապահովմանը՝ կենտրոնանալով երեք հիմնական ուղղությունների վրա՝ գաղտնագրական համակարգերի արդյունավետության գնահատում, բանալիների կառավարում և սարքերի կարգավիճակի հավաստագրում: Աշխատանքը նշանակալի է իր համապարփակ մոտեցմամբ և գործնական կիրառելիությամբ:

1. Աշխատանքի արդիականություն

Ատենախոսության մեջ արձանագրված է IoT ոլորտի հիմնարար հակասությունը. ժամանակակից կիբեռհարձակումների բարդությունը կտրուկ աճում է, մինչդեռ IoT եզրային սարքերի ռեսուրսային բազան մնում է ծայրաստիճան սահմանափակ: Ըստ ատենախոսության մեջ բերված վիճակագրության, IoT սարքերի վրա կատարվում են օրական մոտ 820,000 հարձակում, իսկ խախտումների տարեկան աճը կազմում է 84%: Այս ֆոնին ատենախոսը ճիշտ նկատել է, որ ոչ թե սարքավորումների ավելի ժամանակակից տարբերակների անցումն է լուծումը, այլ կիրառվող ապարատային անվտանգության մոդուլների (ARM CryptoCell-310, TrustZone) արդյունավետ, համակողմանի և ստանդարտացված շահագործման մեթոդաբանության մշակումը: Թեմայի ձևակերպումն ու հիմնավորումն արդիական է և արտացոլում է ոլորտի ռազմավարական կարիքները:

Ոլորտում կան բազմաթիվ աշխատանքներ, որոնք ուսումնասիրում են կամ սարքի սպառման էներգիան, կամ համակարգի աշխատանքի արագությունը, կամ հիշողությունը, կամ անվտանգությունն առանձին-առանձին, սակայն դրանք ամբողջությամբ ինտեգրող, կշռված, կիրառական ձևաչափ ունեցող մեկ միասնական ինդեքս հազվադեպ է հանդիպում: Հատկապես գնահատելի է UCEI-ի ոչ միայն տեսական, այլ նաև չորս տարբեր հարթակների (VisionFive 2, Nordic nRF9161, ESP32-S3, Arduino Uno) վրա գործնական կիրառությունը՝ ապահովելով ալգորիթմների փաստացի Պարետո-օպտիմալ ընտրություն կոնկրետ տեղակայման սցենար:

CSM (Composite Security Metric) ձևաչափի ներկայացումն ևս արժեքավոր է, քանի որ այն փորձում է կապ հաստատել դասական անվտանգության գնահատման և հետքվանտային կայունության չափման, ինչպես նաև ֆիզիկական հասանելիության ռիսկի հաշվառման միջև: Գործնական կիբեռանվտանգության

տեսանկյունից, որտեղ սպառնալիքի մոդելը հաճախ ներառում է տարասեռ հակառակորդներ, CSM-ն ուղղակիորեն արտացոլում է իրական կիրառման բարդությունը: Հատկապես արժեքավոր է λ և μ պարամետրերի կիրառմամբ CSM-ի հարմարեցումը կոնկրետ տեղակայմանը, ինչն ատենախոսությանը հաղորդում է հավելյալ ճկունություն:

Աշխատանքում ներկայացվում է DANE/DANCE արձանագրությունների հիման վրա բազմակլաստերային մառախլապատ ճարտարապետությամբ բանալիների կառավարման համակարգը: Մշակված համակարգը ոչ միայն տեխնիկապես հմուտ լուծում է, այլ ռազմավարորեն ճիշտ ընտրված ուղղություն: Ապակենտրոնացված, մառախլապատ ճարտարապետությանն անցումն, ըստ ատենախոսության ցուցանիշների, ոչ միայն անվտանգության, այլ նաև գործառնական արդյունավետության բարելավում է:

Հիբրիդային բանալու ձևավորման ռազմավարությունը ևս արժանի է ուշադրության: Հետքվանտային գաղտնագրության անցման ժամանակաշրջանն այսօր ինտենսիվ բանավեճի թեմա է մասնագիտական հանրությունում, և հիբրիդային մոտեցումը, որն արդեն ընդունել են Chrome, Signal, iMessage հարթակները, ճշտորեն ընտրված ռազմավարություն է ատենախոսի կողմից: Կարևոր է, որ ատենախոսը ոչ թե հետքվանտային ստանդարտների «կեցվածք է ընդունել», այլ հստակ ձևակերպել է, թե կոնկրետ ինչ կոնֆիգուրացիայի դեպքում և ինչ ռիսկ-մոդելի ենթատեքստում է հիբրիդային մոտեցումը ողջամիտ ընտրություն:

Աշխատանքում ներկայացվում է RFC 9783 PSA ատեստավորման թոքենների իրականացումը ARM TF-M-ի վրա ռեսուրսներով սահմանափակ IoT սարքերի պայմաններում: Մշակված տարբերակը ոչ թե ինժեներական կատարողականություն է, այլ արդի ստանդարտի (2025 թ. հրատարակված RFC 9783) փաստացի կիրառում սահմանափակ ռեսուրսներով սարքերի համար, ինչը, ըստ ատենախոսի արձանագրության, մինչ այդ գործնականում ապացուցված չի եղել:

2. Ատենախոսության կառուցվածքը և բովանդակությունը

Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրահանգումից, 119 անուն գրականության ցանկից, թվով 1 հավելվածից և հապավումների ցանկից: Ատենախոսության ծավալը կազմում է 118 էջ, իսկ հավելվածի, նկարների և աղյուսակների ցանկի հետ միասին 131 էջ:

Ներածության մեջ հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և հիմնական դրույթները, որոնք ներկայացվում են պաշտպանության:

Գլուխ 1-ում ներկայացվում է ատենախոսությունում կիրառված տեխնոլոգիաների և մոտեցումների նկարագրությունը: Աշխատանքի այս հատվածում ներկայացվել է առկա հետազոտություններում հինգ կարևոր բացթողում. բանալիների կառավարման ապարատային արագացմամբ շրջանակների բացակայությունը,

բանալիների կառավարման նախագծման մեջ էներգիա-անվտանգություն փոխզիջումներին ոչ բավարար ուշադրությունը, մառախլապատ (fog-assisted) անվտանգության ճարտարապետությունների սահմանափակ մասշտաբայնությունը, IoT սահմանափակումներին հարմարեցված սարքերի ստանդարտացված հավաստագրման բացակայությունը և գաղտնիությունը պահպանող ու քվանտային կայուն մեխանիզմների ոչ բավարար ինտեգրումը:

Գլուխ 2-ում ներկայացվել են սահմանափակ ռեսուրսներով IoT սարքերի վրա ապարատային գաղտնագրման համակարգերի մոդելավորման և քանակական գնահատման համար մաթեմատիկական մոդելներ: Ներկայացված համակարգը հնարավորություն է տալիս կազմել էներգիայի սպառման, անվտանգության մակարդակի, հիշողության օգտագործման և հաշվողական ծախսերի միջև կապերը՝ օպտիմալացման մոդելի միջոցով, որը ենթարկվում է անվտանգության և ռեսուրսների հստակ սահմանափակումների:

Գլուխ 3-ում ներկայացվել է երեք փոխկապակցված մեթոդ, որոնք միասին լուծում են լայնածավալ բջջային IoT տեղակայումների բանալիների կառավարման և տվյալների անվտանգության ապահովման պահանջները:

Գլուխ 4-ում ներկայացվել է մշակված գործիքների և առաջարկվող մեթոդների համապարփակ փորձարարական վավերացում: ARM TF-M-ի (Trusted Firmware-M) վրա կիրառվել է RFC 9783 PSA հավաստագրման թոքենների համակարգը՝ ապահովելով իրական ժամանակում սարքի կարգավիճակի մշտադիտարկում:

3. Գիտական ներդրումը

Առաջին գիտական նորույթն է գաղտնագրության արդյունավետության միասնական ինդեքսի (Unified Cryptographic Efficiency Index - UCEI) մշակումը, որը ի տարբերություն առկա լուծումների, ինտեգրում է էներգասպառումը, հաշվարկային ցիկլերը, հիշողության սահմանափակումները և անվտանգության մակարդակը մեկ համադրելի սկալյար չափանիշի մեջ: UCEI-ն սահմանվում է որպես կշռված երկրաչափական միջին: Չորս IoT հարթակների վրա կատարված փորձարկումները ցույց են տվել, որ AES-128-L ալգորիթմն ապահովում է UCEI=2.847 մարտկոցով սնուցվող տվիչի պրոֆիլում՝ AES-128 ելակետի նկատմամբ 47% էներգախնայողություն, հիշողության 62% նվազում և թողունակության 35% բարելավում՝ պահպանելով 128-բիթանոց բանալու անվտանգության մակարդակը: Ատենախոսությունում ներկայացվել է նաև անվտանգության բաղադրյալ չափորոշիչ, որն ինտեգրում է դասական անվտանգության մակարդակը, հետքվանտային դիմացկունությունը և կողմնակի ալիքների կայունությունը: Կողմնակի ալիքների վերլուծությամբ հաստատվել է, որ ապարատային իրականացումները նվազեցրել են հզորության կոռելյացիայի գործակիցը մինչև 0.03, ինչն ապահովել է անսարքությունների 99.7% հայտնաբերում:

Երկրորդ նորույթը՝ համագործակցային բազմակլաստերային մառախլապատ (fog) ճարտարապետության օգտագործումն է DANE/DANCE արձանագրություններով բանալիների մասշտաբային կառավարման համար՝

քառաստիճան հիերարխիկ կառուցվածքով: Մշակվել է բանալիների կառավարման ապարատային արագացմամբ շրջանակ՝ ARM CryptoCell-310 և TrustZone տեխնոլոգիաների հիման վրա, որն ապահովում է մեկուսացված պայմաններում բանալիների անվտանգ գեներացում ապարատային էնտրոպիայի աղբյուրների միջոցով:

Երրորդ նորույթը՝ RFC 9783 PSA հավաստագրման թոքենների իրականացումն է ARM TF-M (Trusted Firmware-M) վրա՝ իրական ժամանակում սարքի կարգավիճակի մշտադիտարկման համար: Անոմալիաների հայտնաբերման գործառույթն իրականացնում է սահող ելակետային վիճակի մշտադիտարկման և ահազանգման գործառույթներ (լռելյայն τ=3, 99.7% վստահությամբ):

4. Գործնական արժեքը

Մշակված լուծումների գործնական արժեքը հաստատված է խելացի կառավարվող լուծումների անվտանգության բարձրացման նպատակով «Ար Փի Ի Քոնթրոլս» ՍՊԸ-ում(RPE Controls LLC) ներդրմամբ: Մշակված լուծումները կիրառելի են խելացի տների, արդյունաբերական արտադրության ավտոմատացման, առողջապահության ոլորտում և խելացի քաղաքների ենթակառուցվածքներում: Ապարատային արագացմամբ բանալիների կառավարման մեթոդը զգալիորեն բարելավում է մարտկոցով աշխատող սարքերի կենսունակությունը.. տնտեսական վերլուծությամբ հաստատվել է, որ սարքի ինքնարժեքի մոտ 15% աճը փոխհատուցվում է մարտկոցի կյանքի երկարացմամբ և ռիսկերի նվազեցմամբ, ինչն ուղղակիորեն ազդում է դժվար հասանելի վայրերում տեղակայված տվիչների շահագործման արժեքի վրա:

Հատկանշական է նաև,. որ մաթեմատիկական մոդելները և դրանց ծրագրային իրականացումը օգտագործվում են ՀԱՊՀ-ի «Տեղեկատվական անվտանգության և ծրագրային ապահովման» ամբիոնի ուսումնական գործընթացում:.

5. Հրապարակումներ

Ատենախոսը ունի 7 հրատարակված գիտական աշխատություն ընդ որում՝ հրատարակությունների ցանկն ընդգրկում է ինչպես Հայաստանյան, այնպես էլ ճանաչված միջազգային հարթակներ. Springer-ի «Programming and Computer Software» ամսագիրը, IEEE ACDSA 2026 կոնֆերանսը (Boracay Island), IEEE EWDTS 2025 սիմպոզիումը, CSIT-2025 կոնֆերանսը: Հիմնական արդյունքների հրապարակումն այս հեղինակության հարթակներում ապահովում է միջազգային գիտական հանրության կողմից վերանայված և ճանաչված ներդրում:

Ատենախոսության արդյունքների հավաստիությունը հիմնավորվում է կիրառված մաթեմատիկական մոդելների ճշգրտությամբ և գործնական ներդրմամբ:

«Ար Փի Ի Քընթրոլս» ՍՊԸ-ում կատարված ներդրումը ապահովում է արդյունքների ոչ թե լաբորատոր, այլ արտադրական միջավայրում գործնական կիրառությունը:

ՀԱՊՀ-ի ուսումնական գործընթացում UCEI մոդելի կիրառումն ու ֆորմալ ինտեգրումը ապահովում է կրթական համակարգի մեջ շոշափելի ռեզոնանս:

Ատենախոսության թեմայով հրատարակված աշխատանքները և սեղմագիրը լիովին արտացոլում են ատենախոսության հիմնական բովանդակությունն ու արդյունքները:

7. Դիտողություններ

1. Իրերի համացանցը հաճախ ենթադրում է հարյուր հազարավոր կամ միլիոնավոր սարքերի համաժամանակյա աշխատանք: Ատենախոսության մեջ էմպիրիկ տվյալները հիմնականում ստացվել են լաբորատոր կամ տեղային ենթակառուցվածքների փորձարկումներից: Ցանկալի կլիներ տեսնել սիմուլյացիոն արդյունքներ, որոնք ցույց կտային բանալիների կառավարման և հեռահար մշտադիտարկման մեթոդի պահվածքը խիստ գերբեռնված (stress test) պայմաններում:

2. Ապարատային արագացմամբ բանալիների կառավարման և PSA ատեստավորման մեթոդների (ըստ Աղյուսակ 4.1 և 4.3) կիրառումը ենթադրում է ժամանակակից միկրոկոնտրոլերների և հատուկ ճարտարապետության առկայություն: Որպես թերություն կարելի է նշել, որ լուծված չէ կամ բավարար չափով դիտարկված չէ հին սերնդի կամ խիստ պարզագույն (legacy) սենսորների ինտեգրման և պաշտպանության հարցը, որոնք ի սկզբանե զուրկ են նման ապարատային աջակցությունից:

3. Հեղինակը հիմնական շեշտը դրել է հաշվողական ռեսուրսների, էներգասպառման և հիշողության սահմանափակումների վրա: Սակայն սահմանափակ թողունակությամբ ցանցերում գաղտնագրման բանալիների գեներացման ու փոխանակման գործընթացը կարող է առաջացնել ցանցային նշանակալի հավելյալ ծանրաբեռնվածություն: Աշխատանքում բաց է մնում այն հարցը, թե ինչպես է մշակված մոդելն ազդում կապի հապաղումների (latency) և փաթեթների կորստի դեպքում համակարգի կայունության վրա:

8. Եզրակացություն

Ատենախոսությունը ներկայացնում է ամբողջական և համակարգված հետազոտություն IoT սարքերի անվտանգության ապահովման ոլորտում՝ հստակ տրամաբանությամբ, որտեղ UCEI մոդելը ծառայում է որպես ճարտարապետական ձևավորման քանակական հիմք, իսկ CSM-ով պայմանավորված անվտանգության պահանջները սահմանում են հիբրիդային ատեստավորման ռազմավարությունը: Ատենախոսության գլուխները ոչ թե անկախ ուսումնասիրություններ են, այլ փոխկապակցված, ամբողջական հետազոտություն, ինչն ատենախոսությանն ամբողջականություն է հաղորդում:

Ատենախոսը իր հետազոտությամբ դուրս է եկել զուտ «ապարատային-ֆիզիկական» կամ «ծրագրային» մտածողության սահմաններից և փորձ է կատարել ստեղծել անվտանգության ապահովման ամբողջական, բազմաշերտ,

փոխկապակցված շրջանակ, որտեղ ֆորմալ մոդելները, ապարատային վստահության արմատները և ճարտարապետական ձևավորումները աշխատում են որպես մի ամբողջություն:

Հաշվի առնելով աշխատանքի գիտական նորույթը, տեսական և փորձարարական արդյունքների հիմնավորվածությունը, արդյունքների գործնական ներդրումը և հրապարակումների որակը, գտնում եմ, որ Համբարձում Դավիթի Մինասյանի ատենախոսությունը լիովին բավարարում է Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ թեկնածուական ատենախոսություններին ներկայացվող պահանջներին, իսկ հեղինակը արժանի է տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհմանը:

Պաշտոնական ընդդիմախոս՝ տ.գ.դ. Ս.Սարգսյան

ՌՀՀ գիտքարտուղար ..... Ռ.Կասաբաբովա

«21» 05 2026