A.H. MANUKYAN, H.G. MANUKYAN

ANALYSIS AND COMPARISON OF THE PROCESSORS OF MOBILE DEVICES WITH DIFFERENT ARCHITECHTURES

Devices of mobile processors, processor characteristics and their impact on the productivity and energy consumption are considered. Types of processor architechtures of mobile devices are introdueed.

Keywords: mobile processors, ARM architechture, Intel architechture x86 processor, CPU frequency, processor core, graphic card, graphic core.

ՀՏԴ 004.312.26:621.394.147.8

Ա.Ա. ԽԵՄՉՅԱՆ, Ա.Կ. ԱՍԼԱՆՅԱՆ, Ա.Հ. ԱՐՇԱԿՅԱՆ, Գ.Հ. ԽԱՉԱՏՐՅԱՆ

ՀԱՄԱԿԱՐԳՉԱՅԻՆ ԳԱՂՏՆԱԳՐԱՅԻՆ ՍԱՐՔԱՎՈՐՄԱՆ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ՀԱԿԱՌԱԿՈՐԴԻ ԿՈՂՄԻՑ ՎԵՐԱՀՍԿՄԱՆ ԱՆՈՐՈՇՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ

Գաղտնագրման սարքավորումներում կարևոր հիմնահարց է դրանց պաշտպանության իրականացումը հասանելիության քաղաքականություններ իրագործելիս: Ցույց է տրվում, որ կիրառելով կոշտ տրամաբանությամբ աշխատող գաղտնագրող և վերծանող օժանդակ սարքավորումները՝ ստանում ենք ինքնավար գաղտնագրային ենթահամակարգի ելքում հիմնական գաղտնագրված տեղեկույթը: Այն թույլ է տալիս օգտատերերին՝ զերծ մնալ վնասաբեր ծրագրերի (ներդրված սարքավորումների) ազդեցությունից, ինչը ստիպում է հնարավոր գաղտնավերլուծողին կիրառել ոչ ավանդական գաղտնավերլուծման մեթոդներ:

Առանցքային բառեր. վնասաբեր ծրագիր, գաղտնագրման համակարգ, ներդրված սարքավորումներ, գաղտնավերլուծություն:

Գաղտնագրման սարքավորումներում կարևոր հիմնահարց է դրանց պաշտպանության իրականացումը հասանելիության քաղաքականություններ իրագործելիս: Դա է պահանջում նաև տեղեկատվական համակարգերի կարևորությունը տեղեկույթի պահպանության և պաշտպանության գործում: Տարբերվում են երաշխավորված և չերաշխավորված միջավայրերում գաղտնագրման համակարգի պահպանությունը և պաշտպանությունը [1]: Առաջարկվող միջոցները բարդ են, և դրանց իրագործումը կարող է պահանջել մեծ ծախսեր:

Գաղտնագրման համակարգչային համալիրի համար կարելի է առաջարկել մեկ այլ լուծում. մշակենք անվտանգության քաղաքականություն իրականացնող մեթոդ, որով պրոցեսորների և ծրագրային ապահովման մասին սահմանափակ տեղեկությունների պայմաններում հնարավոր լինի չեզոքացնել վնասաբեր ծրագրերի (օրինակ “տրոյական ձի”, “ստեղնաշարային լրտես” և այլն), ինչպես նաև

տեղեկույթի արտահոսք ստեղծող ներդրված տարբեր սարքավորումների կիրառումը: Այսպիսի անվտանգության քաղաքականությունն առավել արդյունավետ կլինի այն դեպքում, երբ օգտագործվում են բաց համացանցով տրամադրվող կապուղիները: Մեթոդը ենթադրում է ոչ լիարժեք տեղեկություններ պրոցեսորների և ծրագրային ապահովման, ինչպես նաև պրոցեսորների մեջ հնարավորինս առկա ներդրված սարքավորումների և տարբեր վնասաբեր ծրագրերի գործառույթների մասին:

Ներկայիս համակարգերի տեղեկատվական հոսքերի թույլտվությունից հետևում է.

- վնասաբեր ծրագրերը, եթե դրանք գոյություն ունեն ենթահամակարգում, կարող են հասնել և ստանալ ցանկացած տեղեկույթ, վերագրանցել այն ցանկացած օբյեկտում՝ առանց տեղեկույթի վարկաբեկման,
- ենթահամակարգում նպատակահարմար չէ իրականացնել որևէ տեղեկատվական հոսքի կառավարման համար վերահսկման մեխանիզմներ:

Խնդրի ձևայնացված լուծման համար հստակեցնենք միակողմանի կապուղի հասկացությունը: Տեղեկույթի առաքողը և ստացողը ունեն հետևյալ հատկանիշները. առաքողը կարող է ուղարկել ցանկացած հաղորդագրություն, իսկ ստացողը կարող է ուղարկել առաքողին միայն այն տեղեկույթը, որը հայտնի է երկուսին (միակողմանի կապուղի կիրառող համակարգերը կոչվում են միամակարդակ համակարգեր) [1]:

Միամակարդակ համակարգը կարելի է զննել ոչ թե որպես առանձին համակարգիչ, այլ հավաստագրված պաշտպանություն իրականացնող ճկուն միջոց (տեղեկատվական համակարգի ցանկացած ենթահամակարգ կարելի է դիտարկել որպես միամակարդակ համակարգ), որում հնարավոր չէ մանրամասն վերլուծել տեղեկատվական հոսքերը, բայց կարելի է կատարել դրան կցված բոլոր կապուղիների լիակատար վերլուծությունը: Այսպիսով՝ միամակարդակ համակարգ կարող է հանդիսանալ ծրագրային ապահովման ինչ-որ առանձին մաս (եթե հայտնի են սկզբնական կոդերը, կամ առկա են դրա փաստաթղթերը հետագա վերլուծության համար) կամ ամբողջությամբ մեկուսացված տեղեկատվական համակարգ, որում մշակվում է գաղտնի տեղեկույթ, և դա մեկուսացված է շրջապատող միջավայրի վնասակար ազդեցությունից հուսալի պաշտպանությամբ:

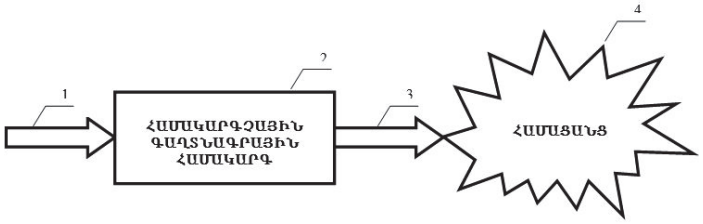
Ենթադրենք՝ ունենք ցանցի (լոկալ) տարածական տեղաբաշխմամբ երկու ենթացանցեր (գաղտնագրային սարքավորումներ), որոնք համակցված են գլոբալ ցանցի (համացանց) միջոցով: Օգտատերերը և տեղեկույթը տեղային ենթացանցերում միամակարդակ են, շրջանառվող տեղեկույթը՝ կարևոր (գաղտնագրվող տեքստ, ձևափոխման հաշվեկանոն, գաղտնաբանալիներ, գաղտնագրված տեքստ և այլն): Համացանցն ունի վստահության նվազագույն աստիճան.

հակառակորդը, չունենալով ֆիզիկական հասանելիություն տեղական ցանցում, փորձում է կարևորագույն տեղեկույթ կորզել գլոբալ ցանցից: Ընդունենք նաև, որ սարքավորումները (համակարգչային տեխնիկան, ներառյալ պրոցեսորները, ղեկավարող սարքերը և այլն) և ծրագրային ապահովումը (օպերացիոն համակարգերը՝ Microsoft Windows, Linux, կիրառական ծրագրերը՝ Microsoft Office, Open Office և այլն) հիմնականում ստեղծված են, մեր տեսակետից, ոչ հուսալի կազմակերպությունների վերահսկողության ներքո և կարող են ունենալ ապարատային ու ծրագրային ներդրված տարրեր: Ենթադրենք նաև, որ հակառակորդը տիրապետում է տեղեկույթի՝ տեղեկատվական համակարգի չփաստաթղթված հնարավորությունների (ՉՓՀ) մասին: Ենթադրում ենք նաև, որ ծրագրային միջավայրում գործում է ծրագիր-գործակալ, որի գործունեությունն իրականացվում է որոշակի հրահանգներով ու տեսանելի չէ համակարգչի և տեղային ցանցի պաշտպանական միջոցների համար (օրինակ՝ աշխատում են “rootkit” տեսակի ծրագրերի քողարկման ներքո): Եթե ծրագիր-գործակալը հաստատում է կապ հակառակորդի հետ համացանցում, ապա նա կարող է ստանալ հրահանգներ, հավելյալ ծրագրային ապահովում՝ տվյալների մշակման համար, ինչպես նաև փոխանցել կարևորագույն տեղեկույթը նրա «տիրոջը»՝ հակառակորդին: Կարելի նաև ենթադրել, որ հակառակորդի հնարավորությունները բավարար են՝ վերծանելու գաղտնագրված տեղեկույթը, մշակելու մեր կողմից կիրառվող տվյալները և բացահայտելու օգտագործվող ծրագրային ապահովումը: Դրա հետ մեկտեղ ծրագիր-գործակալներն ունեն սահմանափակումներ կապի բացակայության դեպքում. առանց հստակ հրահանգների՝ նա չի կարող հասկանալ ոչ ստանդարտ տվյալների կառուցվածքը, ոչ վերականգնել ձևափոխումների ամենահասարակ պարամետրերը: Ծրագիր-գործակալի կապը հակառակորդի հետ իրականացվում է ՉՓՀ-ով պաշտպանության միջոցների համար անտեսանելի հետևյալ կապուղիներով [1].

- հաստիքացուցակային կապուղի. փաթեթների իրար փոխանցում տեղային բաղադրամասերից համացանցով,
- կիսահաստիքացուցակային կապուղի. հաստիքացուցակային կապուղի ու օգտագործում՝ կիրառելով հաղորդվող տվյալների և կապի պարամետրների մասին տեղեկույթը,
- ծածուկ կապուղի. սարքավորումների և ծրագրային ապահովման օգտագործման ոչ հաստիքացուցակային մեթոդ՝ տեղային ցանցից հաղորդագրություն փոխանցելու համար:

Այսպիսով՝ խնդիրը գլոբալ ցանցի միջոցով այնպիսի կապուղու ստեղծումն է, որով կապահովվի տեղեկույթի առավել հուսալի պաշտպանություն՝ դրա արտահոսքը բացառելու միջոցով:

Պարզագույն դեպքում գաղտնագրային համակարգը հնարավոր է ներկայացնել միամակարդակ համակարգի մոդելով (նկ.1) [1].

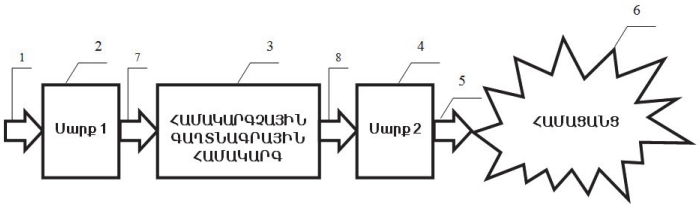


Նկ. 1. Գաղտնագրային համակարգի մոդելը

1 – տեղեկույթի մուտք, 2 – համակարգչային գաղտնագրային համակարգ,
3 – տեղեկույթի ելք, 4 – համացանց

Այսպիսով՝ I(x,t) որոշակի տեղեկույթը (1) ներմուծվում է գաղտնագրային սարք (2), որտեղ որոշակի A(I(x,t),K) հաշվեկանոնով և K գաղտնաբանալիով այն վերափոխվում է: Ենթադրելով, որ գաղտնագրային սարքում կարող են առկա լինել ներդրված սարքավորում, վնասաբեր ծրագրային ապահովում, կարող ենք նաև վստահ համոզված լինել, որ ստեղծվում է V(I(x,t)) տեսակի տեղեկույթ, ինչն էլ համացանցի միջոցով կհասնի հասցեատիրոջը և կվարկաբեկի մեր գաղտնագրային համակարգը: Փաստորեն, սարքավորման (2) ելքում կունենանք՝ A(I(x,t),K) + V(I(x,t)): Եվս մեկ անգամ նշենք, որ գաղտնագրային համակարգը հագեցած է պաշտպանող ծրագրային ապահովմամբ, բայց այն չի տեսնում վտանգը և չի տալիս համապատասխան արձագանք:

Այս իրավիճակը շտկելու համար առաջարկվում է հետևյալը. գաղտնագրային համակարգը կատարելագործել՝ լրակազմելով այն ևս 2 սարքավորումներով (նկ.2.):



Նկ. 2. Կատարելագործված գաղտնագրային համակարգի սխեման

1 – տեղեկույթի մուտք, 2–սարք1 (գաղտնագրային համակարգ A_1 հաշվեկանոնով և K_1 գաղտնաբանալիով), 3–համակարգչային գաղտնագրային համակարգ A_2 հաշվեկանոնով և K_2 գաղտնաբանալիով, 4–սարք2 (վերծանող համակարգ A_1^{-1} հաշվեկանոնով և K_1 գաղտնաբանալիով), 5 – տեղեկույթի ելք, 6 – համացանց, 7 – միջանկյալ ելք 1,
8 – միջանկյալ ելք 2:

Այսինքն՝ հիմնական գաղտնագրման համակարգերը լրակազմվում են 2 սարքավորումներով, որոնք ներկայացնում են նույն հաշվեկանոնը և գաղտնաբանալին կիրառող գաղտնագրող և վերծանող համակարգեր: Գաղտնագրման հայտնի բանաձևի [1] մաթեմատիկական ձևափոխությունները հանգում են հետևյալին.

1 - տեղեկույթ I(x,t),

7 – $A_1(I(x,t),K_1)$,

8 – $A_2(A_1(I(x,t),K_1),K_2) + V(A_1(I(x,t),K_1)$,

5 – $A_1^{-1}(A_2(A_1(I(x,t),K_1),K_2),K_1) + A_1^{-1}(V(A_1(I(x,t),K_1),K_1)$,

Հաշվի առնելով այն, որ գաղտնագրումն ու վերծանումը գծային մաթեմատիկական ձևափոխումներ են, և A1 ու A2 հաշվեկանոնները դարձելի են, գործում է գաղտնագրման հիմնական աքսիոմը՝ A1-1(A1(I(x,t),K1),K1) = I(x,t), և կատարելով տարրական գործողություններ, (5) կետում կստանանք՝

$$A_2(I(x,t),K_2) + A_1^{-1}(V(A_1(I(x,t),K_1),K_1):$$

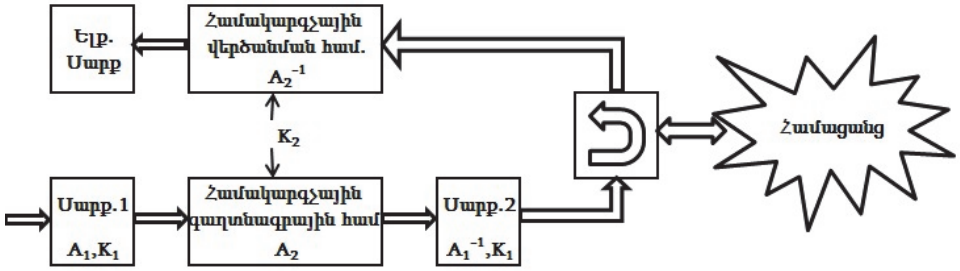
Բայց, կիրառելով սարք1 և սարք2, անհրաժեշտ է անպայման կատարել սարքավորումներին վերաբերող հետևյալ պահանջները.

- պետք է կառուցված լինեն "երկաթի" հիմքի վրա, այլ խոսքով՝ էլեկտրոնային սկզբունքային սխեման կառուցված լինի հնարավորինս առավելապես տեղական արտադրության դիսկրետ և ինտեգրալ սարքերի վրա,
- պետք է ունենան աշխատանքի կոշտ տրամաբանություն (software-ի պարտադիր բացակայություն),
- գաղտնագրման հաշվեկանոնին ու գաղտնաբանալուն ներկայացվող գաղտնակայունության նվազագույն պահանջներ:

Եզրակացություն: Կիրառելով կոշտ տրամաբանությամբ աշխատող գաղտնագրող և վերծանող օժանդակ սարքավորումները՝ ստանում ենք ինքնավար գաղտնագրային ենթահամակարգի ելքում հիմնական գաղտնագրված տեղեկույթը, ինչպես նաև վնասաբեր ծրագրերի (ներդրված սարքավորումների) ստեղծած ծայրաստիճան աղավաղված բիթերի զանգված, երբ վերծանող սարքում փոփոխվում է և բուն տեղեկույթը, և հնարավոր հակառակորդի հասցեն, ինչը թույլ է տալիս համակարգչային գաղտնագրային սարքավորումը պաշտանել հակառակորդի կողմից վերահսկման անորոշության պայմաններում, այսինքն՝ հնարավոր ներդիր սարքերի և վնասաբեր ծրագրային ապահովման առկայության դեպքում:

Փաստորեն հակառակորդին մնում է հայտնաբերել գաղտնագրված տեղեկույթը համացանցի տեղեկատվական միջավայրում և փորձել վերծանել այն իրեն հայտնի մեթոդներով:

Քանի որ իրական համակարգչային գաղտնագրային համակարգը ներկայացնում է գաղտնագրող և վերծանող միամակարդակ համակարգերի ամբողջություն, ապա լրակազմ սխեման կընդունի այլ տեսք, որը ներկայացված է ստորև (նկ.3).



Նկ. 3. Կատարելագործված գաղտնագրային սարքավորման սխեման

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Грушо А.А., Применко Э.А., Тимонина Е.Е.** Теоретические основы компьютерной безопасности. - М.: Издательский центр “Академия”, 2009. -272 с.

А.А. ХЕМЧЯН, А.К. АСЛАНЯН, Г.Г. ХАЧАТРЯН

ЗАЩИТА КОМПЬЮТЕРНОГО ШИФРОВАЛЬНОГО ОБОРУДОВАНИЯ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ КОНТОЛЯ ПРОТИВНИКОМ

Защита шифровального оборудования является фундаментальным вопросом при применении разных политик доступности. Показано, что, применяя внешние шифровальное и дешифровальное оборудования, работающие на жесткой логике, получаем независимую шифровальную систему и на выходе основную зашифрованную информацию, которая даст потребителям возможность защититься от действий вредоносных программ (внедренных оборудований), что заставит возможного криптоанализера использовать нестандартные методы дешифрования.

Ключевые слова: вредоносная программа, система шифрования, встроенные устройства, криптоанализ.

**A.A. KHEMCHYAN, A.K. ASLANYAN, A.H. ARSHAKYAN,
G.H. KHACHATRYAN**

PROTECTION OF COMPUTER CRYPTOGRAPHIC EQUIPMENT AT UNCERTAINTY OF THE FOE CONTROL

The protection of encryption equipment is a fundamental issue in application of different accessibility policies. It is shown that by applying external encryption and decryption equipment working on hard logic, an independent cryptographic system and its main output encrypted information are obtained which will allow the consumers to protect themselves from the actions of malicious programs (embedded devices). It makes possible to use non-standard methods of decryption.

Keywords: malware, encryption system, embedded devices, cryptanalysis.

ՀՏԴ 681.3

Ռ.Հ. ԳԵՂԱՄՅԱՆ, Ա.Կ. ՍԱՂԱԹԵԼՅԱՆ, Ա.Գ. ՔԱՄԱԼՅԱՆ

ԵՌԱՆԿՅՈՒՆԱՉԱՓԱԿԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ ՀԱՇՎԱՐԿ ԻՐԱԿԱՆԱՑՆՈՂ ՍԱՐՔԻ ԱՊԱՐԱՏԱՅԻՆ ԻՐԱԳՈՐԾՈՒՄԸ

Դիտարկված են արագագործության տեսակետից արդյունավետ եռանկյունաչափական ֆունկցիաների հաշվարկման սարքի նախագծման եղանակը և տրամաբանական սինթեզումը ժամանակակից միջոցների կիրառմամբ:

Առանցքային բառեր. Եռանկյունաչափական ֆունկցիաներ, ապարատային իրագործում, աղյուսակային ընտրում, PROM հիշողություն:

Ուսումնասիրելով եռանկյունաչափության հիմնական ֆունկցիաները և օրենքները՝ կարելի է պնդել, որ լայնորեն կիրառվող և հաշվարկվող ֆունկցիաների դասին են պատկանում sin, cos, tg, ctg պարզ ֆունկցիաները, և այդ ֆունկցիաների արժեքների որոշումն ունի որոշակի պարբերականություն: Եռանկյունաչափական օրենքների հիման վրա կատարելով նաև գումարման/հանման գործողությունը և ունենալով sinα և tgα արժեքները, կարելի է ստանալ համապատասխանաբար cosα և ctgα ֆունկցիաների արժեքները:

Այս ձևափոխումները հիմնված են բերման բանաձևերի և եռանկյունաչափության պարբերականությունը և զույգությունը պահպանող օրենքների վրա:

Որպես սկզբնական տեղեկություն առաջարկվում է ձևավորել 2 աղյուսակ՝ $\sin(0^0)$-$\sin(90^0)$ արժեքները պահող աղյուսակը և $tg(0^0)$-$tg(90^0)$ արժեքները պահող աղյուսակը: Այդ նպատակով օգտագործվում է ծրագրավորվող 2 հիշող սարք (PROM)՝ սինուս (PROM1) և տանգենս (PROM2) արժեքների համար, յուրաքանչյուրը 128x16 ծավալով: Այս որոշումը հիմնված է մշակվող սարքի ապարատային