Т.А. БАГДАСАРЯН

МЕТОД ВЫБОРА ОПТИМАЛЬНОГО ПОРОГА ДЛЯ СХЕМЫ РАСПРЕДЕЛЕНИЯ СЕКРЕТА. ОПРЕДЕЛЕНИЕ ГРАНИЧНОГО ЗНАЧЕНИЯ ПОРОГА

Разработан метод выбора оптимального порога для систем распределения секрета. Метод основан на двух вероятностных критериях оценки защищенности пороговых схем распределения секрета: вероятности раскрытия частей секрета и вероятности потери и/ или искажения частей секрета. В качестве примера использована пороговая схема Шамира.

Ключевые слова: распределение секрета, пороговая схема, оптимальный порог, схема Шамира.

T.A. BAGHDASARYAN

THE OPTIMAL THRESHOLD SELECTION FOR SECRET SHARING SCHEMES. DETERMINING THE BOUNDARY VALUE OF THE THRESHOLD

A method for optimal threshold selection is proposed for systems in which secret sharing schemes are used. The method is based on two probabilistic criteria of the secret sharing threshold scheme security assessment. These criteria are the probability of the share disclosure and the probability of the share loss and/or distortion. Shamir's threshold scheme is used as an example.

Keywords: secret sharing, threshold scheme, optimal threshold, Shamir's scheme.

ՀՏԴ 005.312.26

Վ.Հ. ՀՈՎՍԵՓՅԱՆ

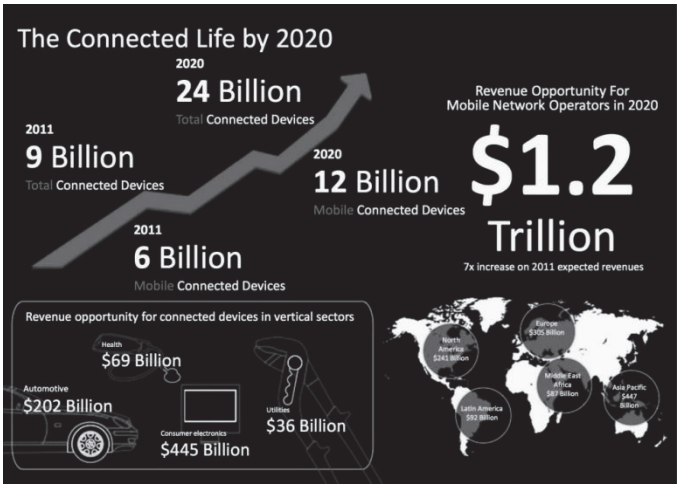
ՇԱՐԺԱԿԱՆ ԲԱՆԱԼՈՒ ԿԻՐԱՌՈՒՄԸ ԱՄՊԱՅԻՆ ՄԻՋԱՎԱՅՐՈՒՄ

Մշակված է գաղտնագրման համակարգ՝ շարժական բանալու ստեղծմամբ, որն ապահովում է տվյալների անվտանգ տեղափոխումը: Շարժական բանալի է անլար ցանցի ցրիչը, որը մշակելով փոխանցվող փաթեթը, գաղտնագրում է այն: Առաջարկված համակարգը հարմար է կիրառել այն ցանցային միացումների դեպքում, որտեղ բացակայում է գաղտնագրումը: Ներկայացված է տվյալների փոխանցման անվտանգությունն ապահովող նոր սկզբունք:

Առանցքային բառեր. գաղտնագրում, անլար ծածկույթ, շարժական բանալի, անվտանգ համացանց:

Ներածություն: Աշխարհում գոյություն ունեն ավելի քան 7.5 միլիարդ սարքեր, որոնք կապված են համացանցին ուղղակի կամ միջանկյալ սարքերով: Արդեն իսկ նոր սերնդի հեռախոսների քանակը գերազանցել է երկրում ապրող մարդկանց քանակը: Ըստ բազմաթիվ հեղինակավոր ընկերությունների, որոնցից են Intel,

Guardians և Apple, 2020 թվականին համացանցին կապված սարքերի թիվը կմոտենա 24 միլիարդի: 2015 թվականին համացանցին միացած սարքերի 20% կապված են անլար ցանցով, օգտագործելով WI-FI 802.11 ստանդարտը: Այս տոկոսային հարաբերակցությունը մեծանում է, և WI-FI-ի կիրառումը դառնում է ավելի արդիական: Կարելի է հստակ ենթադրել, որ ապագայում անլար ցանցային կապ օգտագործող սարքերի քանակը կգերազանցի մի քանի միլիարդը (նկ.1):



Նկ. 1. Յանցային կապ օգտագործող սարքերի քանակը

Ներկայումս արտադրվում են WiFi ընդունիչով հեռախոսներ, համակարգիչներ, բժշկական սենսորներ, ժամացույցներ և նույնիսկ սառնարաններ: Թվարկված սարքերի ցանկում գոյություն ունեն այնպիսիները, որոնք պատկանում են պարզագույն սարքերի դասին: Տվյալ դասի սարքերը ստեղծված են որոշակի գործառույթ կատարելու համար և ունեն ցածր հզորություն: Օրինակ, սրտի սենսորն ունակ է միայն չափելու և համացանցով փոխանցելու սրտի աշխատանքը բնութագրող տարբեր պարամետրեր, կամ օդափոխության համակարգը կարգավորող սարքը, որը համացանցի միջոցով կարող է փոխել կամ փոխանցել սենյակային ջերմաստիճանը: Այս դասի սարքերը չունեն համակարգչին կամ հեռախոսին համապատասխան տեխնիկական և ծրագրային հնարավորություններ: Այդ իսկ պատճառով այս սարքերն ունեն անվտանգության լուրջ խնդիր: Տեխնիկական կամ ծրագրային սահմանափակումներից բացի պետք է նաև հասկանալ, որ այս սարքերը գտնվում են զարգացման առաջնային փուլում, որը որոշակիորեն արդարացնում է գոյություն ունեցող անվտանգության խնդիրները:

Հիմնական անվտանգության խնդիրը կապված է տվյալների փոխանցման հետ: Սարքի սահմանափակումները թույլ չեն տալիս կիրառել անվտանգ հաղորդակցման ստանդարտները: https արձանագրության օգտագործումը ենթադրում է

30մբ հավելյալ հիշողություն, պրոցեսոր և համապատասխան ծրագրային ապահովում: Այս պահանջները բավական համեստ են, բայց կարող են պարտադրել՝ կատարելու սարքի տեխնիկական փոփոխություններ, որոնք զգալիորեն կբարձացնեն նրա սկզբնական արժեքը:

Վերը նշված խնդիրն ունեցող սարքերի քանակն այսօր անցնում է մեկ միլիոնը, բայց հիմնվելով տարբեր հեղինակավոր ընկերությունների կանխագուշակման արդյունքների վրա՝ հստակ կարելի է ասել, որ մոտ ապագայում այդպիսի սարքերի քանակը կշատանա մի քանի տասնյակ անգամ:

Վերոնշյալ խնդրի լուծման համար անհրաժեշտություն է առաջանում ստեղծել միկրոհամակարգիչ՝ իր ծրագրային ապահովմամբ, որը պետք է ընդունի փոխանցվող փաթեթները, գաղտնագրի և փոխանցի համացանցով: Այդ սարքը պետք է հանդիսանա շարժական բանալի համացանցի և պարզագույն դասի սարքերի միջև:

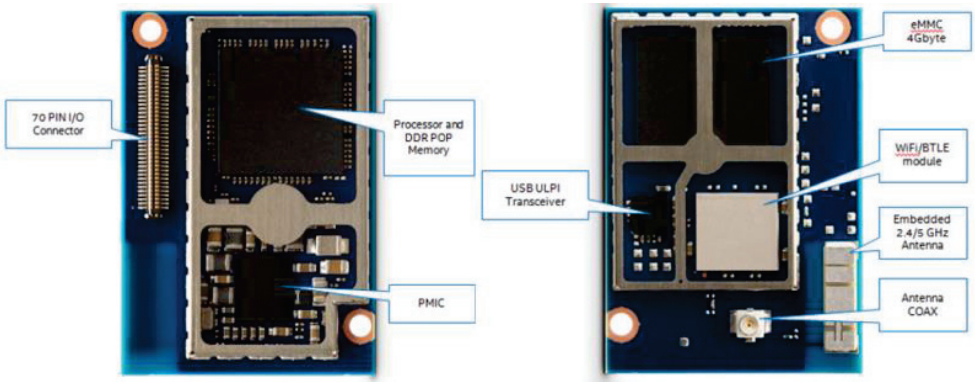
Շարժական բանալի: Փոխանցվող տվյալների գաղտնագրման համար ստեղծված սարքը պետք է բավարարի 4 կարևոր պահանջներ՝

1. միաժամանակ աշխատի մի քանի սարքերի հետ,
2. գաղտնագրումը պետք է լինի արագ,
3. լինի փոքր և շարժական,
4. պետք է ունենա ծրագրային թարմացման և հավելվածների կցման հնարավորություն:

Որպես սարքի հիմք օգտագործվել է Intel-ի Edison մոդուլը [1]: Այն տրամադրում է համապատասխան միջավայր՝ տեխնիկական փոփոխություններ և լրացումներ կատարելու համար: Օգտագործելով Edison Breakout Board Kit, հնարավոր է հեշտությամբ փոխել սարքի կարգավորումները, տեղադրել օպերացիոն համակարգ և կառավարել բոլոր ծրագրային պրոցեսները: Որպես նախնական Օպերացիոն համակարգ օգտագործված է Yocto ՕՀ, որը բաց կոդով նախագիծ է և տրամադրում է գործիքներ և մեթոդներ, որոնք օգնում են՝ ստեղծելու Linux ՕՀ-ի վրա հիմնված համակարգն՝ անկախ սարքի ապարատային ճարտարապետությունից: Տվյալ համակարգն ունի որոշակի բարդույթներ, որոնցից մեկը ՕՀ-ի տեղադրումն է՝ ամեն անգամ հավելված ավելացնելու դեպքում: Այդ իսկ պատճառով որոշում կայացվեց օգտագործվել Ubilinux: Այս ՕՀ-ը հիմնված է հանրահայտ DEBIAN ՕՀ-ի վրա: Այն լիովին համապատասխանում է նախագծի պահանջներին և հնարավորություն է տալիս առանց բարդույթների ինտեգրել անլար ցանցային կապի համար նախատեսված ծրագրային ապահովումը: Շարժական բանալու տեսքը և գծանկարը պատկերված են նկ. 2-ում: Նրա հիմնական տեխնիկական բնութագրերն են.

1) բարձր կատարողականություն ունեցող երկմիջուկ CPU,
2) 1ԳԲ DDR օպերատիվ հիշողություն,
3) 4ԳԲ FLASH հիշողություն,

4) անլար հաղորդակցության սարքեր ,ինչպիսիք են՝ Wi-Fi և Bluetooth 4.0,
5) հնարավորություն ՝տեղադրելու Linux-ի հիման վրա ստեղծված ՕՀ,
6) փոքր չափեր (25 *մմ* և 35.5 *մմ*) և թեթև քաշ (0.2 *կգ*):



Նկ. 2. Շարժական բանալու կառուցվածքը

Այս սարքի շնորհիվ հնարավոր դարձավ ստեղծել անլար Wi-Fi ցանց, որը կարող է սպասարկել միաժամանակ մինչև 8 ակտիվ օգտվող սարք: Սահմանափակումը կապված է սարքի գաղտնագրման համակարգի արտադրողականության հետ: Այն նաև հնարավորություն է տալիս օգտագործել WEP, WAP 1 և WAP 2 համակարգերը՝ անլար ցանցային կապը դարձնելով անվտանգ:

Տվյալ սարքի համար ստեղծվել է ՕՀ և հավելումների տեղադրման և կարգավորման փաթեթ, որի շնորհիվ կարելի է սարքը կարգավորել՝ օգտագործելով միայն մի հրահանգ:

Ծրագրային ապահովում: Հիմնական ֆունկցիան՝ գաղտնագրումը, կարգավորելու համար ստեղծվել է վեբ ինտերֆեյս: Շարժական բանալին ունի աշխատանքային 2 վիճակ: Ստեղծված ինտերֆեյսի շնորհիվ հնարավոր է ընտրել սարքի աշխատանքային 2 վիճակներից մեկը և կարգավորել այն: Այստեղ կներկայացվի միայն մեկ աշխատանքային վիճակը:

Առաջին վիճակը ենթադրում է հավելյալ ծրագրային փաթեթի օգտագործում, սարքից ուղարկվող հարցումների մշակող միջավայրում (սերվերում): Օգտատերը, օգտվելով սարքի ինտերֆեյսից, պետք է մուտքագրի հասցեներ, որոնց ուղարկվող փաթեթները պետք է գաղտնագրվեն և գեներացնեն գաղտնի բանալի: Հետագայում այդ գաղտնի բանալին պետք է ներբեռնվի ուղարկվող հասցեի սերվեր: Սերվերին կտրամադրվի ծրագրային գրադարան, որից օգտվելու դեպքում այն կկարողանա ապակոդավորել ստացվող փաթեթները: Գաղտնագրումը կատարվում է հայտնի AES ալգորիթմի փոփոխված տարբերակի հիման վրա, շարժական բանալիում, մինչև համացանց հասնելը [2]: Շարժական բանալին, ստանալով անլար ցանցին միացած

սարքավորումներից տվյալների փաթեթը, ստուգում է՝ ուղարկվող հասցեն համընկնու՞մ է մինչ այդ վեբ ինտերֆեյսով մուտքագրած հասցեներից որևէ մեկին, թե՞ ոչ: Եթե հասցեն համընկնում է, ապա նախագծած սարքը գաղտնագրում է ուղարկվող փաթեթի մարմինը և փաթեթի գլխում (header) ավելացնում է համապատասխանող բանալու համարը՝ PRIVATE-KEY-ID անվամբ: Եթե հասցեի համընկնում չկա, փաթեթն ուղարկվում է առանց փոփոխության: Սերվերը, իր հերթին ստանալով ցանկացած փաթեթ, ստուգում է PRIVATE-KEY-ID առկայությունը, հայտնաբերելու դեպքում օգտագործում է այդ համարին համապատասխանող բանալին և ապակոդավորում մարմնի դաշտում առկա տվյալները, որից հետո միայն շարունակում բնականոն աշխատանքը: Ծրագրային փաթեթը ստեղծվել է՝ օգտագործելով c++ միջավայրը:

AES ալգորիթմում կատարվել է 2 փոփոխություն: Նախ՝կոդավորման համար պրոցեսորի մեկ միջուկի փոխարեն օգտագործվել են շարժական բանալիում առկա 2 միջուկները, ինչը զգալիորեն բարձացրել է ալգորիթմի արագագործությունը: Կատարվում է է Intel AES լրացումների կիրառմամբ: 2010 թվականին Intel ընկերությունն իր պրոցեսորների համար թողարկել է նոր հրամանների ցուցակ, որոնք նախատեսված են՝ կատարելու AES ալգորիթմում օգտագործվող ցնցումներից մի քանիսը, միանգամից օգտագործելով ընդամենը մեկ հրաման: Հրամանների ցանկը թվարկված է ստորև.

AESENC (AES Encrypt Round), AESENCLAST (AES Encrypt Last Round), AESDEC (AES Decrypt Round), AESDECLAST (AES Decrypt Last Round), AESKEYGENASSIST (AES Key Generation Assist), AESIMC (AES Inverse Mix Columns) [3]:

Եզրակացություն: Այսպիսով, մշակվել է գաղտնագրման նոր համակարգ այն սարքերի համար, որոնք չունեն համապատասխան ապարատային կամ ծրագրային ապահովում: Տվյալ համակարգի առավելությունն այն է, որ այն կարողանում է գաղտնագրել մինչև 8 տարբեր սարքերից ուղարկված տվյալները և աշխատում է այդ սարքերից անկախ. այսինքն՝ չի պահանջում գոյություն ունեցող սարքի ապարատային կամ ծրագրային փոփոխություն: Այն փոփոխություն է պահանջում միայն սերվերային մասից, այն էլ փաթեթները ստանալու փուլում ,որն ապահովում է առկա ծրագրային կոդի հետ լիարժեք համատեղելիություն: Այս մեթոդն ավելի շատ նախատեսված է մոտ ապագայի համար, երբ ,օրինակ, «խելացի տան» կառավարումը անվտանգ դարձնելու և օգտագործվող սարքերի գինը ցածր պահելու խնդիր կառաջանա: Այսօր այն կարող է օգտագործվել տարբեր սենսորներից տվյալների անվտանգ փոխանցման նպատակով, ինչպես, օրինակ, սրտի և ուղեղի աշխատանքի վերաբերյալ տվյալների անվտանգ փոխանցումն է:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Guermonprez Paul.** IoT with Galileo and Edison: Course Modules from Intel Experts. - Intel Exhibition, 2015. - P.1-25.
2. **Joan Daemen** and **Vincent Rijmen.** The Design of Rijndael, AES - The Advanced Encryption Standard. - Springer-Verlag, 2012.-238 p.
3. Shay Guero. Advanced Encryption Standard (AES) New Instructions Set.- Israel Development Center, 2010.

В.О. ОВСЕПЯН

ИСПОЛЬЗОВАНИЕ ПОРТАТИВНОГО КЛЮЧА В ОБЛАЧНОЙ СРЕДЕ

Разработана система шифрования, которая основана на создании портативного ключа в целях обеспечения безопасной передачи данных. Портативным ключом является роутер беспроводной сети, который преобразовывает входящий пакет посредством криптографии. Система пригодна для использования в незащищённых сетевых соединениях. Предлагается новый принцип для обеспечения безопасности данных, передаваемых в незащищённых сетях.

Ключевые слова: криптография, беспроводная сеть, портативный ключ, безопасная система.

V.H. HOVSEPYAN

PORTABLE KEY USAGE IN CLOUD ENVIRONMENT

An encryption system based on the creation of a portable key to ensure a secure data transfer is developed. The Portable Key is the wireless network router, encrypting the transferred data packages. The system is suitable to be used in the network connections non-protected network is proposed where there is no encryption. A new principle of ensuring the data security transmitted in non-protected network is proposed.

Keywords: wireless network, portable key, secure data transmission.