ENCRYPTION | ԳԱՂՏՆԱԳՐՈՒՄ

Katarina Gevorgyan | Կատարինա Գևորգյան
ISOC Armenia Chapter Board Member
«Ինտերնետ հասարակության Հայաստան Հատված» ՀԿ-ի խորհրդի անդամ

Lianna Galstyan | Լիաննա Գալստյան
Coordinator | Համակարգող
ISOC Armenia Chapter Board Chair
«Ինտերնետ հասարակության Հայաստան հատված» ՀԿ-ի խորհրդի նախագահ

ՆԵՐԱԾՈՒԹՅՈՒՆ

Համացանցի անվտանգության ապահովման վերաբերյալ քննարկումների կարևորագույն հարցերից է գաղտնագրման հիմնախնդիրը կամ գաղտնագրային պահպանությունը, որը վերաբերում է փոխանցվող տվյալների պաշտպանության համար օգտագործվող գործիքներին:

Գաղտնագրումը սովորական տեքստը գաղտնագրման համակարգի (մաթեմատիկական որոշակի ալգորիթմների) միջոցով կողմնակի անձանց համար անհասկանալի տեքստի վերածելն է:

Այն կիրառվում է ինչպես համակարգիչներում պահվող տվյալների (չփոխանցվող տեղեկատվություն), այնպես էլ համացանցի միջոցով փոխանցվող տվյալների պաշտպանության համար (փոխանցման մեջ գտնվող տեղեկատվություն):

END-2-END(E2E) ԳԱՂՏՆԱԳՐՈՒՄ

Տվյալ դեպքում գաղտնագրված հաղորդագրությունը կարող են կարդալ միայն ուղարկողը և վերջնական ստացողը:

- Որևէ այլ անձ և նույնիսկ կապի ծառայություն մատուցող ընկերություն չունեն գաղտագրումը բացող բանալի:
- E2E գաղտնագրումը ամենաապահով եղանակն է, ուստի հնարավորության դեպքում նպատակահարմար է կիրառել այդ տարբերակը՝ ձեզ և ձեր տվյալները պաշտպանելու համար:
- Գաղտնագրման միջոցով հաղորդակցման ծառայությունների օրինակ են WhatsApp, Signal, Telegram և Threema հավելվածները:

ԳԱՂՏՆԱԳՐՄԱՆ ԿԻՐԱՌՈՒՄԸ

Մեր օրերում մենք միշտ ստիպված ենք ապավինել գաղտնագրմանը համացանցում տարբեր գործողություններ կատարելիս:

Կայքերի զննարկում (Web browsing)
Զննարկիչները (browsers) և կայքերը կիրառում են HTTPS արձանագրություններ՝ ապահով հաղորդակցություն տրամադրելու և տվյալների փոխանցման ժամանակ հանցագործների կողմից կարդալուց պաշտպանելու համար:

Էլեկտրոնային առևտուր
Առցանց ապրանքներ գնելիս կամ բանկային հավելվածներից օգտվելիս օգտատերերը վստահում են ընկերություններին՝ պաշտպանելու իրենց անձնական և ֆինանսական տվյալները, որը նույնպես իրականացվում է գաղտնագրման միջոցով:

Ապահով հաղորդագրություն
Տարբեր հավելվածների միջոցով հաղորդագրություն ուղարկելիս երկու կողմերն էլ համոզված են, որ այն անձնական է և միայն իրենք կարող են կարդալ: Հաղորդակցման որոշ հավելվածներ կիրառում են գաղտնագրումը օգտատերերի անվտանգությունը և պաշտպանվածությունը ապահովելու համար: Որոշները կիրառում են նույնիսկ E2E գաղտնագրումը, որի դեպքում միայն ուղարկողը և ստացողը կարող են կարդալ հաղորդագրությունը:

ԳԱՂՏՆԱԳՐՄԱՆ ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Գաղտնագրումը համացանցում մեր տվյալների պաշտպանության, ինչպես նաև անվտանգ փոխանցման և պահպանման հիմնաքարն է: Այն շատ կարևոր է հասարակության առցանց գործունեության տարբեր փուլերում, քանի որ պաշտպանում է օգտատիրոջ տվյալները տեսանելի դառնալուց, ինչպես նաև.

- կանխում է տվյալների (փաստաթղթերի, քարտարանների) կեղծումը,
- նպաստում է վստահության ձևավորմանը՝ այսինքն, դուք տեղյակ եք, թե ում հետ եք իրականում կապ հաստատում,
- թվային ստորագրության անհրաժեշտության դեպքում հաստատում է օգտագործողի վավերականությունը:

Շատերը սխալմամբ կարծում են, որ գաղտնագրումը և անձնական տվյալների պաշտպանությունն այնքան էլ անհրաժեշտ չեն, եթե թաքցնելու ոչինչ չունեն:

Բայց եթե ձեր տվյալները հայտնվեն «վատ» ձեռքերում, այդ դեպքում կարող են առնվազն՝

- վնասել անձի հեղինակությանը,
- ֆինանսական վնաս հասցնել՝ ինքնությունը պարզելու միջոցով,
- ուրիշի փոխարեն ստորագրելով վերահասցեավորել վճարումները,
- հանրային դիտարկման առարկա դարձնել անհատի անձնական կյանքը:

ԿԱՌԱՎԱՐՈՒԹՅՈՒՆՆԵՐԻ ՄՈՏԵՑՈՒՄԸ

Որոշ երկրների կառավարություններ բողոքում են, որ E2E գաղտնագրումը խոչընդոտում է իրավապահ և ազգային անվտանգության մարմինների աշխատանքին՝ բացահայտելու հանցագործներին, ահաբեկիչներին և այլոց, որոնք պլանավորում են երկրների անվտանգությանը սպառնող գործողությունների կազմակերպում:

Արդյո՞ք E2E գաղտնագրումը խնդիր է առաջացնում:

Բնավ ոչ:
Գաղտնագրումը հիմնարար նշանակություն ունի համացանցում մեր հասարակության անվտանգ և արդյունավետ գործունեության համար՝ ներառյալ իրավապահ և ազգային անվտանգության մարմինների, ինչպես նաև բիզնես գործողությունների համար:

ԳԱՂՏՆԱԳՐՄԱՆ ՀԵՏՆԱՄՈՒՏՔ

- Որոշ երկրների կառավարություններ փորձում են ստիպել հաղորդակցման և համացանցում ծառայություն տրամադրող ընկերություններին հասանելի դարձնել իրենց համակարգերի կողմից գաղտնագրված տեղեկատվությունը: Այստեղ ի հայտ է գալիս նոր տերմին՝ «գաղտնագրման հետնամուտք»:

- Մյուսները պահանջում են թուլացնել գաղտնագրումը՝ տեղակատվությունը ֆիլտրելու կամ արգելափակելու հնարավորություն ստանալու նպատակով:

- Որոշ դեպքերում էլ փորձում են մուտքի թույլտվություն ստանալ դեպի գաղտնագրված տվյալներ՝ դրանք դրամայնացնելու նպատակով:

ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՏԵՍԱԿՆԵՐԸ

Օրենսդրական
Նոր օրենքներ, որոնք ստեղծվում են հետնամուտքերի հասանելիություն ապահովելու համար՝ կասկածյալ հանցագործ տարրերին, ահաբեկիչներին թիրախավորելու նպատակով:

Իրավական
Գործող օրենքների մեջ փոփոխություններ, որոնք կատարվում են իրավապահ մարմինների համար հետնամուտքերի հասանելիություն ստեղծելու համար՝ կասկածյալ հանցագործ տարրերին և ահաբեկիչներին թիրախավորելու նպատակով:

Շոշափելի
Կենտրոնացած չէ գաղտնագրման վրա, բայց միևնույն է, սպառնում է գաղտնագրման անվտանգությանը: Այս դեպքում իրականացվում է հաղորդագրության բովանդակության զտում, որը E2E գաղտնագրումը դարձնում է պարզապես անհնար:

Անկախ մեթոդից՝ հնարավոր չէ ստեղծել այնպիսի հետնամուտք, որը հնարավոր լինի կիրառել վերապահորեն միայն լիազորված մարմինների կողմից և միևնույն ժամանակ չխաթարել գաղտնագրման անվտանգությունը:

Խնդիրն այն է, որ հանցագործ տարրերը կարող են հայտնաբերել և կիրառել նույն մեթոդը՝ ձեռք բերելով հետնամուտքի հասանելիություն, ինչպես նաև փոփոխել գաղտնագրված հաղորդագրությունը:
Նման այլընտրանքները լայնորեն հասանելի են և, որ ամենակարևորն է, գտնվում են կառավարական և իրավապահ մարմինների հսկողությունից դուրս:

Քանի որ հանցագործ տարրերը նույնպես կարող են կիրառել գաղտնագրումը այս դեպքում իրենց գործունեությունը թաքցնելու նպատակով, իրավապահ և կառավարական մարմինները խիստ անհանգստացած են: Փաստորեն այդ նույն գաղտնագրման հնարավորությունը կարող է խանգարել պաշտպանելու քաղաքացիների իրավունքները և պահպանելու օրենքները:

ՀԵՏՆԱՄՈՒՏՔԻ ՏԻՊԵՐԸ

Ցանկացած տիպի հետնամուտք ունի խոցելի կետեր, որոնք մեծացնում են հանցագործ տարրերի կողմից արժեքավոր տեղեկատվության և անձնական տվյալների հայտնաբերման, գողացման, վերարտադրման և չարաշահման վտանգը:

Հիմնական պահպանումն (Key Escrow) այն պայմանավորվածությունն է, որի համաձայն գաղտնագրված տվյալների գաղտնազերծման բանալիները պահվում են հատուկ պահոցում, որպեսզի որոշակի հանգամանքների դեպքում լիազորված երրորդ կողմը կարողանա հասանելիություն ստանալ այդ բանալիներին: Այնուամենայնիվ ցանկացած բանալի հանցագործ տարրերի կողմից հայտնաբերման և կիրառման ռիսկի տակ է գտնվում:

Գաղտնագրման հետնամուտքի կողմնակիցները կիրառում են արտահայտություններ՝ «**պատասխանատու ծածկագրում**», «**բացառիկ մուտք**» կամ «**օրինական մուտք**», որոնք բոլորն էլ հանդիսանում են գաղտնագրման հետնամուտքի տիպեր:

Ուստի, հետնամուտքի հասանելիությունը կհանգեցնի բազում խնդիրների՝ առանց էֆեկտիվ լուծումների:

ԳԱՂՏՆԱԳՐՄԱՆ ԳՐԱԳԻՏՈՒԹՅԱՆ ԽԹԱՆՈՒՄ

- Օգնել հասարակության տարբեր խավերին, ինչպես նաև կառավարական և իրավապահ մարմիններին հասկանալ գաղտնագրման իրական կարևորությունը,
- Ցուցադրել ապահով գաղտնագրման օրինակներ և կազմակերպել դասընթացներ,
- Սովորեցնել օգտագործել գաղտնագրումը, օրինակ՝ ինչպիսի հավելվածներից օգտվել
- Դարձնել գաղտնագրումը ճանաչելի և կիրառելի,
- Համագործակցել կառավարությունների հետ, որպեսզի վերջիններս լիովին պատկերացնեն և գնահատեն գաղտնագրման բարձր կարևորությունը երկրների և իրենց քաղաքացիների ապահովության և անվտանգության համար:

ՀԱՄԱՇԽԱՐՀԱՅԻՆ ԳԱՂՏՆԱԳՐՄԱՆ ԿՈԱԼԻՑԻԱ

2020թ. մայիսի 14-ին «Ինտերնետ հասարակություն» կազմակերպությունը հայտարարեց **«Գլոբալ Գաղտնագրման Կոալիցիա»**-ի գործարկման մասին:

Ավելի քան 30 հասարակական կազմակերպություններ համատեղում են իրենց ջանքերը միասին զարգացնելու և պաշտպանելու գաղտնագրումը առավել խոցելի երկրներում և համայնքներում՝ կրթելով հասարակությանը և տեղեկացնելով գաղտնագրման հիմունքների, կարևորության և սպառնալիքների մասին:

https://www.globalencryption.org/events/