Criptú ceann go ceann, mínithe i ndáiríre

An méid a deir soláthraithe nuair a deir siad E2EE, agus an méid nach ndeir siad. Míniú oideachasúil ar an meicníocht agus ar na teorainneacha, gan an timfhilleadh fógraíochta.

Le bheith soiléir: Deir WhatsApp go bhfuil do theachtaireachtaí criptithe ceann go ceann. Tá sé fíor — agus ní leor é. Má théann an cúltaca chuig iCloud nó Google Drive gan aon chriptiú breise, bristear an criptiú ar do ghuthán féin. Ní hé an cheist oibríochtúil an bhfuil sé criptithe, ach cá bhfuil na heochracha.

Cad is brí le criptiú, i ndáiríre

Ciallaíonn criptiú teachtaireachta í a chlaochlú go rud éigin a bhfuil cuma torainn air d'aon duine nach bhfuil faisnéis áirithe acu ar a dtugtar eochair. Déantar an oibríocht ar ghléas an tseoltóra agus, leis an eochair cheart, déantar í a chealú ar ghléas an ghlacadóra. Idir an dá linn, taistealaíonn an teachtaireacht mar chomharbas de bheartanna gan bhrí shoiléir. Sin an smaoineamh simplí. Déileálann an chuid eile den alt leis na miondifríochtaí a athraíonn é, ag brath ar an gcás, go ráthaíocht iarbhír nó go lipéad margaíochta.

Cuireann an t-aidiacht *ceann go ceann* — i mBéarla *end-to-end*, giorraithe E2EE — cruinneas leis. Ní dhéantar criptiú ionas gur féidir le freastalaí idirmheánach é a léamh agus a sheachadadh. Déantar é ionas nach mbeidh an eochair ach ag an dá cheann — gléas an tseoltóra agus gléas an ghlacadóra. Feiceann aon fhreastalaí a théann an teachtaireacht tríd an torann, ní an teachtaireacht. Sin an difríocht theicniúil le criptiú *faoi bhealach*, áit a dtaistealaíonn an t-ábhar criptithe ó fhreastalaí amháin go dtí an chéad cheann eile, ach déanann gach freastalaí a théann sé tríd é a dhícriptiú chun é a chur ar aghaidh, ag athshlánú an téacs go soiléir go sealadach.

Paradacsa an rún comhroinnte

Tá fadhb shoiléir ann. Ionas go mbeidh beirt in ann teachtaireachtaí a chriptiú agus a dhícriptiú eatarthu féin, teastaíonn an eochair chéanna ón mbeirt acu. Ach conas a aontaíonn siad ar an eochair seo má théann gach rud a sheolann siad chuig a chéile, de réir sainmhínithe, trí chainéal ina bhféadfadh duine a bheith ag éisteacht? Is cosúil go bhfuil sé dodhéanta aontú ar an eochair sa chainéal céanna ina n-úsáidfidh siad níos déanaí í: má chloiseann an t-ionsaitheoir í agus iad ag aontú uirthi, beidh siad in ann gach rud ina dhiaidh sin a dhícriptiú. Ar feadh na mblianta, réitigh an chripteagrafaíocht chlasaiceach é seo ar an mbealach crua: seachadadh eochracha go pearsanta, sula dtosaíodh á n-úsáid, i dteagmhálacha fisiceacha. D'iompair ambasadóirí málaí eochracha fuaite isteach i líneáil a gcóta.

Sa ríomhphost comhaimseartha, ní fhéadfaidh an réiteach sin scálú. Dá mbeadh orainn dul go fisiciúil chuig teach gach duine a raibh sé i gceist againn cumarsáid chriptithe a dhéanamh leo, ní bhfaighimis deis labhairt le duine ar bith. Ba í seo an cheist a chuir an pobal cripteagrafach os comhair caoga bliain ó shin: an féidir le beirt nach n-aithníonn a chéile agus nach bhfuil acu ach cainéal poiblí aontú, sa chainéal poiblí céanna sin, ar rún nach féidir le duine ar bith atá ag éisteacht leis an gcainéal a bheith ar eolas acu?

Galántacht Diffie-Hellman

I 1976, léirigh beirt mhatamaiticeoir darbh ainm Whitfield Diffie agus Martin Hellman rud éigin a raibh cuma dodhéanta air: gur féidir le beirt, ag caint trí chainéal poiblí amháin — cainéal inar féidir le duine ar bith gach rud a deir siad a chloisteáil — aontú ar fhocal faire rúnda gan aon éisteoir a bheith in ann é a fháil amach. Tá cuma draíochta air. Ní draíocht é: is matamaitic é. Is é malartú eochracha Diffie-Hellman, mar is eol dó ó shin, an bonn do gach cumarsáid chriptithe ar an idirlíon beagnach, agus deimhníonn leathchéad bliain de dhlúthúsáid agus de ghrinnscrúdú acadúil domhanda a thacaíocht. Is féidir le duine ar bith ar mian leo an t-iomas amhairc nó an mhatamaitic a fheiceáil leanúint ar aghaidh ag léamh. Is féidir le duine ar bith ar fearr leo muinín a bheith acu as go n-oibríonn sé leanúint ar aghaidh freisin gan snáithe an ailt a chailleadh.

D'aon duine ar mian leo é a shamhlú in íomhá, tá analaí aitheanta ann le dathanna. Samhlaigh go n-aontaíonn Eilís agus Bruno go hoscailte ar bhundath — abair buí — os comhair Éabha, a éisteann leo. Roghnaíonn gach duine an dara dath rúnda go príobháideach agus meascann siad a rún leis an mbuí. Faigheann Eilís oráiste áirithe; faigheann Bruno glas áirithe. Malartaíonn siad na torthaí os comhair Éabha. Anois meascann gach duine an dath a fuarthas lena rún féin, agus sroicheann an bheirt an dath deiridh céanna, mar nach cuma faoi ord na meascán. Chonaic Éabha an buí agus an dá mheascán idirmheánacha, ach ní na rúin; gan aon cheann de na rúin ní féidir leo an dath deiridh a bhaint amach. Athraíonn an mhatamaitic iarbhír na dathanna le haghaidh easpónantú i ngrúpaí modúlacha nó i gcuair éilipseacha, ach is é an smaoineamh céanna é: tógann an rún comhroinnte go poiblí gan aon duine sa chainéal a bheith in ann é a atógáil.

In uimhríocht, don té ar fearr leis an mheicníocht a fheiceáil: Roghnaíonn Eilís uimhir rúnda a, roghnaíonn Bruno b. Malartaíonn siad g^a agus g^b go hoscailte thar an gcainéal. Ríomhann Eilís $(g^b)^a$ agus ríomhann Bruno $(g^a)^b$; sroicheann an bheirt acu an g^{ab} céanna. Feiceann Éabha g, g^a agus g^b ag dul tríd an gcainéal, ach teastaíonn am ríomhaireachta réalteolaíoch chun a a fháil ó g^a — an fhadhb logartaime scoite mar a thugtar uirthi — níos mó ná aois na cruinne nuair a roghnaítear g i ngrúpa matamaitice oiriúnach.

Dóibh siúd ar mian leo é a sheiceáil le huimhreacha beaga. Is féidir malartú Diffie-Hellman a dhéanamh ina iomláine le figiúirí atá beag go leor chun na ríomhanna a dhéanamh de láimh. Is féidir le haon duine ar fearr leo gan dul i ngleic le huimhríocht an chuid seo a scipeáil gan snáithe an ailt a chailleadh; gheobhaidh aon duine ar mian leo an mheicníocht a fheiceáil ag obair céim ar chéim anseo é. **Na rialacha poiblí**, ar féidir le haon duine a léamh: uimhir phríomha $p = 11$ (sa bhfíor-Diffie-Hellman tá thart ar thrí chéad digit ann; úsáidimid a haon déag chun go n-oirfidh na ríomhanna ar leathanach amháin), bunáit $g = 2$, agus an coinbhinsiún go ndéantar gach uimhríocht *modúl p* — ríomhann tú, roinneann tú ar p, agus coimeádann tú an fuílleach, cosúil le clog aon suíomh déag a thilleann go nialas nuair a théann sé thar a deich. **Na roghanna príobháideacha**, ceann an duine agus nach roinntear go deo: roghnaíonn Eilís $a = 4$. Roghnaíonn Bruno $b = 7$.

Céim 1. Ríomhann Eilís $2^4 = 16$, ansin $16 \bmod 11 = \mathbf{5}$. Seolann sí an cúigear. Déanann Éabha é a thaifeadadh.

Céim 2. Ríomhann Bruno $2^7 = 128$, ansin $128 \bmod 11 = \mathbf{7}$. Seolann sé an seachtar. Déanann Éabha é a thaifeadadh freisin. Tar éis an dá tharchur, tá ceithre phíosa sonraí i leabhar nótaí Éabha: $p = 11$, $g = 2$, A = 5, B = 7. Tá an uimhir chomhroinnte a bhfuil Eilís agus Bruno ar tí a dhíorthú ar iarraidh uirthi — agus ní bheidh Éabha in ann í a athchruthú.

Céim 3. Tógann Eilís an seachtar a sheol Bruno chuici agus hardaíonn sí é go dtí a heaspónant príobháideach $a = 4$. Chun láimhseáil $7^4 = 2401$ a sheachaint, ríomhtar é ina chodanna agus an modúl á chur i bhfeidhm ag gach céim:

$7^2 = 49$

$49 \bmod 11 = 5$

$7^4 = (7^2)^2 = 5^2 = 25$

$25 \bmod 11 = 3$

Faigheann Eilís an uimhir **3**.

Céim 4. Tógann Bruno an cúigear a sheol Eilís chuige agus hardaíonn sé é go dtí a easpónant príobháideach $b = 7$. Arís ina chodanna:

$5^2 = 25 \bmod 11 = 3$

$5^4 = (5^2)^2 = 3^2 = 9 \bmod 11 = 9$

$5^6 = 5^4 \times 5^2 = 9 \times 3 = 27 \bmod 11 = 5$

Faoi dheireadh $5^7 = 5^6 \times 5 = 5 \times 5 = 25 \bmod 11 = \mathbf{3}$.

Faigheann Bruno **3** freisin.

Tá an bheirt tar éis an uimhir chéanna, 3, a shroicheadh agus iad ag obair go comhthreomhar. Níor sheol ceachtar acu a n-easpónant príobháideach ag aon am. Níl a fhios ag Eilís gurb é $b = 7$; níl a fhios ag Bruno gurb é $a = 4$. D'úsáid gach duine an luach poiblí a sheol an duine eile in éineacht lena n-easpónant príobháideach féin, agus bhuail siad ag an gceann scríbe céanna. **Cén fáth a sroicheann siad an uimhir chéanna?** An méid a ríomh gach duine: Eilís, $(g^b)^a = 2^{7\times4} = 2^{28} \bmod 11$. Bruno, $(g^a)^b = 2^{4\times7} = 2^{28} \bmod 11$. Is í an méid céanna í mar níl aon tábhacht le hord iolrú na n-easpónant ($7 \times 4 = 4 \times 7$). Shroich gach duine trí chonair dhifriúil go dtí an ceann scríbe céanna.

Agus Éabha? Tá aici ina leabhar nótaí $p = 11$, $g = 2$, A = 5, B = 7, agus ba mhaith léi an 3. Chun é a ríomh bheadh uirthi eolas a bheith aici ar a nó b — ach níor thaistil ceachtar acu tríd an gcainéal. Is é an t-aon bhealach atá aici ná í féin a cheistiú: «cén t-easpónant a a gcomhlíontar $2^a \bmod 11 = 5$ ina leith?». Le p chomh beag sin is féidir léi 0, 1, 2, 3, 4... a thriail agus é a aimsiú níos lú ná nóiméad. Ach in áit 11, úsáid uimhir phríomha trí chéad digit, beidh níos mó dúile sa spás easpónant féideartha ná mar atá d'adaimh sa chruinne inbhraite. **Faoi láthair níl aon algartam ar eolas ag an gcine daonna ar féidir leis an spás sin a thrasnú níos lú ná na billiúin bliain.** Is í seo an fhadhb logartamach scartha mar a thugtar uirthi (*discrete logarithm problem*): éasca ar aghaidh, ríomhiolraithe dodhéanta siar. Agus is í seo an chúis a sheasann an criptiú in aghaidh Éabha fiú má tá sí tar éis an comhrá iomlán a leanúint litir ar litir.

Trí chomhábhar shimplí — uimhríocht chloig, easpónantú, agus cómhalartacht an iolraithe ($a \cdot b = b \cdot a$) — ceangailte le chéile iad ag táirgeadh prótacal ar a mbraitheann leath an chine daonna gach lá dá gcumarsáid phríobháideach. Níl aon cheann de na trí phíosa, scartha óna chéile, ag breathnú go speisialta. Is é an tionól atá cinntitheach.

Ó Diffie-Hellman go dtí prótacal Signal

An criptiú ceann go ceann a úsáideann feidhmchláir teachtaireachtaí gairmiúla an lae inniu, tá sé bunaithe, gan aon eisceacht beagnach, ar leagan galánta agus crua de mhalartú Diffie-Hellman. Is é prótacal Signal, deartha ag Trevor Perrin agus Moxie Marlinspike idir 2013 agus 2016, an tagairt. Comhcheanglaíonn sé dhá phríomhsmaoineamh. An chéad cheann, malartú eochracha i gcuair éilipseacha (X25519), a tháirgeann an rún comhroinnte tosaigh idir dhá ghléas. An dara ceann, an Double Ratchet mar a thugtar air — raitseád dhúbailte — a dhéanann na heochracha a athnuachan go huathoibríoch le gach teachtaireacht, ionas nach gceadaíonn comhréiteach an ghléis inniu teachtaireachtaí san am atá thart a dhíchriptiú, ná teachtaireachtaí amach anseo nuair a bheidh an raitseád rothlaithe.

In Zig, luíonn an malartú X25519 a tháirgeann an rún comhroinnte idir dhá ghléas i sé líne, ag baint úsáide as an leabharlann chaighdeánach:

```
const std = @import("std");
const X25519 = std.crypto.dh.X25519;
```

```
// Alicia y Bruno generan cada uno un par (privada, pública).
const par_alicia = X25519.KeyPair.generate(io);
const par_bruno  = X25519.KeyPair.generate(io);

// Cada parte recibe la clave pública de la otra y deriva el mismo secreto.
const secreto_alicia = X25519.scalarmult(par_alicia.secret_key, par_bruno.public_key) catch unreachable;
const secreto_bruno  = X25519.scalarmult(par_bruno.secret_key,  par_alicia.public_key) catch unreachable;
// secreto_alicia == secreto_bruno  (32 bytes)
```

Cad a tharlaíonn sna sé líne sin: Taistealaíonn na heochracha poiblí go hoscailte. Ní fhágann na heochracha príobháideacha an gléas faoi seach go deo. Díorthaíonn gach páirtí, óna chuid príobháideach agus poiblí an duine eile, an rún céanna de thríocha a dó beart nach féidir le duine ar bith sa chainéal a aisghabháil. Feidhmíonn an rún sin níos déanaí mar shíol chun na teachtaireachtaí malartaithe a chriptiú. Cuireann Double Ratchet an phrótacail Signal rothlú leanúnach ar an ábhar sin ionas nach gcuirfidh comhréiteach miontraic isteach ar an gcuid eile den chomhrá.

Agus cad go díreach atá taobh istigh de `std.crypto.dh.X25519`? Níl aon draíocht fholaithe ann. Is dhá fheidhm ghearra iad is féidir a léamh ina n-iomláine i leabharlann chaighdeánach Zig féin. Díorthaíonn an chéad cheann an eochair phoiblí ón gceann príobháideach — an «g^{a}» sa mhalartú:

```
pub fn recoverPublicKey(secret_key: [secret_length]u8) IdentityElementError![public_length]u8 {
    const q = try Curve.basePoint.clampedMul(secret_key);
    return q.toBytes();
}
```

I dteanga an ailt: «iolraítear» an eochair phríobháideach — sa chiall éilipseach, ní sa chiall d'uimhríocht bhunúsach — faoi bhunphointe chuair Curve25519, agus déantar an toradh a shraitheáil i dtríocha a dó beart. Is é an oibríocht `clampedMul` an leagan cruaite den iolrú scálach sin: ionchorpraíonn sé na coimircí a chuir an pobal cripteagrafach leis thar na blianta chun seasamh in aghaidh clanna ionsaithe atá ar eolas. Dhá líne do chorp na feidhme.

Nascann an dara feidhm d'eochair phríobháideach leis an eochair phoiblí a sheolann an páirtí eile chugat. Is é an «$(g^{b})^{a}$» sa mhalartú, a tháirgeann an rún comhroinnte tríocha a dó beart nár tharchuir ceachtar agaibh riamh:

```
pub fn scalarmult(secret_key: [secret_length]u8, public_key: [public_length]u8) IdentityElementError![shared_length]u8 {
    const q = try Curve.fromBytes(public_key).clampedMul(secret_key);
    return q.toBytes();
}
```

Dhá líne eile. Léirmhínítear an eochair phoiblí a fhaightear mar phointe ar an gcuar, agus «iolraítear» í faoina eochair phríobháideach féin. Trí chómhalartacht na hoibríochta cuair — cosúil le cómhalartacht iolrú na n-easpónant a chonaic muid san sampla uimhriúil — faigheann an dá pháirtí an pointe sraitheáilte céanna: go díreach an rún comhroinnte a labhraíonn an t-alt faoi.

Sin é. An rud a bhreathnaíonn mar dhraíocht in iarratas, i ndáiríre, dhá fheidhm de thrí líne an ceann. Tá an chastacht theicniúil comhchruinnithe in aon oibríocht amháin, `clampedMul`, atá scríofa níos faide síos sa leabharlann chaighdeánach chéanna, athbhreithnithe ar feadh blianta ag an bpobal cripteagrafach idirnáisiúnta, agus ar fáil d'aon duine ar mian leo é a léamh litir ar litir. Níl aon bhosca dubh ann inár bhfeidhmchlár ná i leabharlann chaighdeánach Zig. Tá cód foinse oscailte ann is féidir le duine a thuiscint, ag roghnú an luais inar mian leo dul isteach ann.

Cad a chosnaíonn criptiú ceann go ceann

An rud a chosnaíonn E2EE go maith, ag glacadh le cur i bhfeidhm ceart, ná ábhar na teachtaireachta agus í faoi bhealach. Feicfidh freastalaí idirmheánach a fhaigheann agus a chuireann na sonraí criptithe ar aghaidh comharbas de bheartanna do-thuigthe. Feicfidh ionsaitheoir a bhfuil rochtain aige ar an gcábla, ar an ródaire, ar an bpointe rochtana wifi, an rud céanna. Ní bheidh soláthraí seirbhíse a choinníonn cóipeanna den trácht in ann é a léamh níos déanaí. Gheobhaidh Rialtas a ordaíonn d’oibreoir na seirbhíse an t-ábhar a sheachadadh na beartanna do-thuigthe céanna a bhí ag an bhfreastalaí sa chéad áit.

Is mór an méid sin, i dtéarmaí praiticiúla. Is é an difríocht idir litir a scríobh laistigh de chlúdach teimhneach agus í a scríobh ar chárta poist. Sroicheann an dá cheann. Ní chosnaíonn ach ceann amháin an t-ábhar ón bpostaire.

Cad nach gcosnaíonn criptiú ceann go ceann

Is fiú go mór é a bheith ar eolas agat freisin. Ní chosnaíonn E2EE meiteashonraí: tá a fhios ag an bhfreastalaí fós go seolann úsáideoir A sonraí chuig úsáideoir B, cén t-am, cé chomh minic agus cén áit, cé nach bhfuil a fhios aige cad a deir siad. Na meiteashonraí seo, mar atá maíte againn cheana féin i *Ní hionann criptiú agus a bheith príobháideach*, is minic gur mó a nochtann siad ná an t-ábhar. Má bhíonn a fhios agat gur ghlaoigh duine éigin ar ghnólacht dlí a dhéanann sainfheidhmiú ar cholscaradh ar an Aoine ag 22:00 ar feadh tríocha nóiméad, insíonn sé scéal nár inis ábhar an ghlao riamh. Is é an cás céanna é duine a fheiceáil ag dul isteach agus ag teacht amach as clinic oinceolaíochta go minic: ní gá duit aon rud a chloisteáil faoi na rudaí a deirtear istigh chun a shamhlú cad atá ag tarlú. Is féidir nach gciallaíonn meiteashonraí aonair amháin rud ar bith; tarraingíonn roinnt meiteashonraí tras-tagartha rud éigin atá róchosúil leis an bhfírinne. Ní chosnaíonn E2EE na foircinn: má tá gléas an ghlacadóra i gcontúirt ag clár mailíseach, dícriptítear an teachtaireacht de ghnáth don ghlacadóir sin agus léann an clár mailíseach í. Ní chosnaíonn E2EE in aghaidh fhéiniúlacht an idirghabhálaí ann féin: má chreideann Eilís go bhfuil sí ag caint le Bruno ach go bhfuil ionsaitheoir idircheaptha ag an tús (*man in the middle*) agus nach n-áirítear fíorú neamhspleách sa phrótacal, críochnaíonn an dá pháirtí ag caint leis an ionsáiteoir ag ceapadh go bhfuil siad ag caint lena chéile.

Tá ceathrú rud ann ar fiú é a fhoirmiú gan débhrí. Ní chuireann E2EE cosc ar sholáthraí a mhaíonn go dtairgeann sé é cóip den teachtaireacht neamhchriptithe a choinneáil ina chórais féin freisin. Ní hionann an ráiteas «tá mo chuid teachtaireachtaí criptithe ceann go ceann» agus an

ráiteas «ní choinníonn an soláthraí m’ábhar». Is féidir le feidhmchlár an chéad cheann a chomhlíonadh agus an dara ceann á shárú; chonaiceamar i gceannlínte preasa é arís agus arís eile ó 2018. Mura bhfuil cód an chliaint infhíoraithe, níl aon bhealach teicniúil ag an úsáideoir cás amháin a aithint ón gcás eile gan imscrúdú saineolach. An cás is mó a bhfuil aithne ag an bpobal air: déanann WhatsApp teachtaireachtaí a chriptiú ceann go ceann faoi bhealach, ach má ghníomhaíonn an úsáideoir an cúltaca in iCloud nó Google Drive gan criptiú breise, stóráiltear an chóip sin inléite i mbonneagar tríú páirtí, agus briseadh an criptiú ag deireadh an úsáideora féin.

An cheist nach mian leis an oibreoir a chloisteáil

Is féidir le feidhmchlár a mhaíonn go ndéanann sé criptiú ceann go ceann, go teicniúil, ceann amháin de thrí rud a dhéanamh maidir leis na heochracha:

1. **Tá cónaí ar na heochracha ar na gléasanna amháin.** Gineann siad agus tá cónaí orthu go heisiach ar ghléasanna na n-úsáideoirí; níl a fhios ag an oibreoir iad ná ní stórálann sé iad. Is é seo an cás is fearr.
2. **Is féidir leis an oibreoir rochtain a fháil más mian leo.** Tá eochracha na n-úsáideoirí ag an oibreoir (nó is féidir leo iad a ghiniúint de réir mar is mian leo) agus stórálann siad iad ina gcuid bunachar sonraí. Más mian leo nó má chuirtear d’oibleagáid orthu é, is féidir leo an t-ábhar a léamh. Is amhlaidh atá an cás i gcás fhormhór na seirbhísí 'sa scamall'.
3. **Ní féidir leis an oibreoir rochtain a fháil trí dhearadh, ach rialaíonn siad an rochtain.** Níl na heochracha ag an oibreoir, ach tá smacht acu ar an bhfeidhmchlár a ghineann iad. Má chuirtear d’oibleagáid orthu é, is féidir leo nuashonrú mailíseach a sheoladh a ghabhann na heochracha nó an t-ábhar sula ndéantar é a chriptiú. Is amhlaidh atá an cás i gcás go leor seirbhísí tráchtála E2EE.

Ní hé an cheist oibríochtúil, dá bhrí sin, an bhfuil rud éigin criptithe, ach cé ag a bhfuil smacht ar an ngléas agus ar an mbogearra a bhainistíonn na heochracha. In Solo2, tá cónaí ar na heochracha i do Bhoghta amháin (IndexedDB criptithe le d’fhocal faire) agus is foinse oscailte infhíoraithe é an bogearra.

Don léitheoir gairmiúil

Is uirlis don cheannasacht dhigiteach é criptiú ceann go ceann. Ach cosúil le gach uirlis, braitheann a éifeachtúlacht ar an lámh a úsáideann í agus ar an talamh ar a luíonn sí.

1. Cá ngintear na heochracha cripteagrafacha agus cá bhfuil cónaí orthu go fisiciúil? Más féidir leis an oibreoir rochtain a fháil orthu (fiú go sealadach, fiú faoi leithscéal an aisghabhála), is ainmniúil atá an E2EE.
2. An bhfuil fíorú neamhspleách ann ar an idirghabhálaí (uimhreacha slándála, cóid QR, comparáid lasmuigh den bhanda) a chuireann cosc ar ionsaí man-in-the-middle le linn bhunú na comhrá?
3. An bhfuil cód an chliaint in-iniúchta — oscailte, foilsithe, in-atáirgthe — nó an dteastaíonn muinín as focal an tsoláthraí maidir leis an méid a dhéanann an cliant i ndáiríre?
4. Cad iad na meiteashonraí a ghineann agus a choinníonn an tseirbhís, agus cá fhad? Fiú má tá an t-ábhar teimhneach, is féidir le meiteashonraí cuid mhaith den fhaisnéis íogair a atógáil.

Ní iarrann na ceithre cheist seo faisnéis theicniúil chun cinn; iarrann siad faisnéis ar féidir le haon oibreoir macánta a fhreagairt ina dhoiciméadú poiblí. Insíonn cáilíocht agus cruinneas an fhreagra an oiread faoin táirge is a dhéanann an freagra féin.

Is é criptiú ceann go ceann, nuair a dhéantar i gceart é, ceann de na tógálacha is deise atá tugtha ag an gcripteagrafaíocht chomhaimseartha do chleachtas an lae inniu. Is le Whitfield Diffie agus Martin Hellman, 1976, an smaoineamh bunaidh — gur féidir le beirt teacht ar chomhaontú faoi rún ar chainéal poiblí; leathchéad bliain níos déanaí táimid fós ag maireachtáil ina iarmhairt. Ach, mar a tharlaíonn le haon gheallúint theicniúil, braitheann a luach ar chomhlíonadh iarbhír, ní ar an lipéad. Ní hé ceist an ghairmí macánta ná «an bhfuil sé criptithe?», ach «cé a bhfuil na heochracha aige?». Tá iarmhairtí difriúla ag na freagraí. Is fiú iad a bheith ar eolas agat.

Foinsí agus léitheoireacht bhreise

- Diffie, W.; Hellman, M. — *New Directions in Cryptography*, IEEE Transactions on Information Theory, Samhain 1976. Alt bunaitheach na cripteagrafaíochta eochrach poiblí.
- Perrin, T.; Marlinspike, M. — *The Double Ratchet Algorithm*, sonraíocht phoiblí ó Open Whisper Systems, athbhreithniú 2016. Bunús an phrótacail Signal agus a dhíorthaigh thionsclaíocha.
- RFC 7748 — Elliptic Curves for Security (IETF, Eanáir 2016). Sonraíocht normatach de na cuair X25519 agus X448 a úsáidtear i malartuithe eochracha nua-aimseartha.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Caibidlí ar mhalartú eochracha agus ar phrótacail chriptithe fhíordheimhnithe.
- Rialachán (AE) 2024/1183 maidir le creat féiniúlachta digiteach Eorpach (eIDAS 2) — bunaíonn sé creataí inar féidir le fíorú neamhspleách an idirghabhálaí tacaíocht institiúideach a fháil, agus inar féidir le hiarmhairtí dlíthiúla difriúla a bheith ag an idirdhealú idir criptiú ainmniúil agus criptiú fíor.

← Roimhe seoKill switch agus an gabháil institiúideachAr aghaidh →An tsamhail ghnó mar chomhartha muiníne

Léitheoireacht le déanaí

- Anailís · 18 Bealtaine 2026 Príobháideacht iarbhír vs príobháideacht dhealraitheach: na ceisteanna ba chóir duit a chur ort féin
- Anailís · 18 Bealtaine 2026 Féin-óstáil mar chleachtas gairmiúil

- Coincheap · 18 Bealtaine 2026 Na 24 focal: cad is féiniúlacht chripteagrafach ann

Beir an t-alt seo leat áit ar bith a dteastaíonn sé uait.

↓ Markdown ↓ Téacs simplí ↓ PDF

Íoslódálfar an comhad chuig do ghléas. Ón áit sin is féidir leat é a shábháil, é a iompórtáil go Solo2 nó é a roinnt cibé áit is mian leat. Ní chinneann Cuadernos an ceann scríbe duitse.

Séala céir · SHA-256 283ec065b50aa2cf87b023d1d8ce2aff53627ad21747a2a62c36b360d7b6ded9

Cuadernos Lacre · Foilseachán de chuid Menzuri Gestión S.L. ·
scríofa ag R.Eugenio · curtha in eagar ag foireann Solo2.

Ní úsáideann an suíomh seo fianáin agus ní lódálann sé acmhainní ó thríú páirtithe. Úsáideann sé córas tomhais anaithnid arna óstáil (Umami, ar ár bhfreastalaí Eorpach) agus an t-íosmhéid JavaScript is gá don dá rialaitheoir ceanntáisc: téama solais nó dorcha, agus roghnóir teanga. Gan rianairí, gan próifíliú, gan comhroinnt sonraí. Más mian leat sinn a leanúint: RSS.