COMHAD FÍRICÍ: TEICNEOLAÍOCHT DHIGITEACH GCE

AS2: BUNPHRIONSABAIL NA TEICNEOLAÍOCHTA DIGITÍ: TEICNEOLAÍOCHT GHRÉASÁIN AGUS ILMHEÁIN

FORBAIRT SUÍOMH GREASÁIN 2

Torthaí Foghlama

Ba chóir do dhaltaí a bheith ábalta:

- Criptiúchán (lena n-áirítear eochracha poiblí agus príobháideacha);
- Prótacal slánaistrithe hipirtéacs (*https*);
- Sraith Soicéad Slán (*SSL*);
- Síniú digiteach nó deimhniú digiteach.

Inneachar i bhFeidhmchláir Ghréasáin 2

- ✔ Is modh slándála thar an Idirlíon é criptiúchán
- ✔ Síniú Digiteach agus Deimhniú Digiteach
- ✔ Prótacal Slánaistrithe Hipirtéacs (*https*) agus Sraith Soicéad Slán

Is modh slándála thar an Idirlíon é criptiúchán

Is í an eolaíocht a bhaineann le rudaí a chur i bhfolach í cripteagrafaíocht. Tugtar criptiúchán ar phróiseas an aistrithe féin. Baintear úsáid as algartam nó rúnscríobh leis na sonraí a chriptiú.

Is modh é criptiú le slándáil a chur ar fáil do shonraí nuair atá siad á stóráil go leictreonach agus nuair atá siad á dtarchur. Déantar na sonraí a 'scrobhadh' ag úsáid eochair chriptiúcháin. Tá na sonraí criptithe seo gan chiall do dhuine ar bith a dhéanann rochtain orthu. Ní mór na sonraí a dhíchriptiú ag úsáid eochrach, ionas gur féidir iad a thuiscint.

Roinnt córas, úsáideann siad an eochair chéanna don chriptiú agus don díchriptiú, go háirithe mura bhfuil líon na n-úsáideoirí ach iontach beag.

Cripteagrafaíocht le heochair phoiblí, baineann sé úsáid as dhá eochair dhifriúla, ceann amháin leis na sonraí a chriptiú agus ceann eile leis na sonraí a dhíchriptiú. Tá an péire eochracha seo, Poiblí agus Príobháideach, tá siad nasctha agus tá an dá eochair de dhíth le sonraí a chriptiú agus a dhíchriptiú.

Tá an eochair phoiblí ar fáil do gach duine ach tá an Eochair Phríobháideach rúnda agus sainiúil do ghlacadóir ar leith. Tá an péire eochracha gaolta de réir matamaitice, mar sin de, cibé rud a dhéantar a chriptiú le hEochair Phoiblí, ní féidir é a dhíchriptiú ach leis an Eochair Phríobháideach atá ag freagairt dó agus an bealach eile thart.

Más mian le húsáideoir A teachtaireacht chriptithe a chur chuig úsáideoir B, déanfaidh úsáideoir A na sonraí a chriptiú ag úsáid Eochair Phoiblí úsáideoir B. Níl an Eochair Phríobháideach chomhfhreagrach leis an teachtaireacht a dhíchriptiú ach ag úsáideoir B. Mar sin de, má dhéanann tríú páirtí rochtain ar na sonraí criptithe, ní bheidh siad ábalta iad a léamh nó a dhíchriptiú mar nach bhfuil an Eochair Phríobháideach acu. Tá an Eochair Phoiblí ar fáil do dhuine ar bith, mar sin de, b'fhéidir go gcuirfí teachtaireacht bhréige chuig úsáideoir B. Leis seo a sheachaint, úsáidtear sínithe digiteacha.

Síniú Digiteach

Is cuid de theachtaireacht é síniú digiteach atá criptithe ag an tseoltóir. Úsáidtear é lena dhearbhú gurb ionann an seoltóir agus an duine atá in ainm a bheith ann. Ar dtús, dearbhaíonn an duine a fhaigheann an teachtaireacht an síniú ag úsáid

eochair phoiblí an tseoltóra. I ndiaidh bailíocht an tsínithe a chinntiú, gheobhaidh an faighteoir na sonraí trí dhíchriptiú ag úsáid an Eochair Phríobháideach atá aige/aici féin.

Deimhniú Digiteach

Úsáidtear Deimhniú digiteach fosta le fíordheimhneacht seoltóra a dheimhniú. Baintear úsáid as go forleathan le suíomhanna gréasáin.

Comhlachtaí nó daoine a bhfuil deimhnithe digiteacha de dhíth orthu, caithfidh siad iarratas a dhéanamh le tríú páirtí iontaofa ar a dtugtar Údarás Deimhnithe (*CA*), comhlacht a chuireann deimhniúchán ar líne ar fáil. Is sampla amháin é de *CA* Verisign. Cuireann an *CA* deimhniú digiteach criptithe ar fáil ina bhfuil, i measc rudaí eile, eochair phoiblí an úsáideora. Ceanglaíonn seo duine nó suíomh gréasáin le heochair phoiblí áirithe, mar sin de, déanann an tríú páirtí iontaofa a n-aitheantas a dheimhniú. Nuair a iarrann comhlacht deimhniú, ní mór dóibh faisnéis a thabhairt faoin fhreastalaí gréasáin agus suíomh an chomhlachta. Déanfaidh *CA* an fhaisnéis seo a dheimhniú. Ansin, cruthaíonn an t-údarás *CA* deimhniú agus síníonn é. Tugtar an deimhniú ar ais don chomhlacht a shuiteálann ar an fhreastalaí é.

Seoltar brabhsálaithe le faisnéis maidir le deimhnithe. Go háirithe an Eochair Phoiblí do na deimhnithe agus mar sin de, thig leo fíordheimhneacht an chuid is mó de na deimhnithe a sheiceáil.

Is féidir le deimhnithe digiteacha bheith:

- Pearsanta – in úsáid ag daoine a bhfuil r-phost slán de dhíth orthu;
- Eagraíocht – úsáideann eagraíochtaí iad d'fhostaithe a bhfuil idirbheartaíochtaí slán r-phoist agus gréasáin de dhíth orthu;
- Freastalaí le húinéireacht a chruthú ar ainm fearainn nó le húsáid le *SSL;*
- Forbróir – le húinéireacht a chruthú ar bhogearraí/ríomhchláir.

Prótacal Slánaistrithe Hipirtéacs (*https*) agus Sraith Soicéad Slán (*SSL*)

Gach sonraí atá tarchurtha thar cheangail *HTTP*, tá siad i bhfoirm 'gnáth-théacs' agus is féidir aon duine iad a léamh atá ábalta haiceáil isteach sa cheangal idir brabhsálaí agus suíomh gréasáin. Prótacal Slánaistrithe Hipirtéacs (*https*), úsáidtear é le sonraí a chriptiú nuair atá siad á dtarchur thar an Idirlíon. Leathanach ar a bhfuil https:// i dtús an tseolta gréasáin, bainfidh sé úsáid as criptiú le tarchur sonraí a dhéanamh slán. Baineann leathanaigh ghréasáin *HTTPS* úsáid as *SSL* (nó *TLS* – Slándáil Shraith an Iompair). Le linn an phróisis seo, úsáidtear Eochair Phoiblí agus Eochair Phríobháideach le chéile maraon le deimhniú digiteach. Cinntíonn seo, má bhriseann haiceálaí isteach sa cheangal, ní bheidh siad ábalta cuid ar bith de na sonraí a dhíchriptiú.

Is prótacal é *SSL* a úsáidtear le bealach slán a oscailt nó nasc criptithe idir an dá ríomhaire ar líne. Úsáidtear é nuair is gá do bhrabhsálaí gréasáin ceangal go slán le freastalaí gréasáin. Tá deimhnithe *SSL* ann le sonraí a chriptiú agus le suíomhanna gréasáin a shainaithint. Ligeann seo do bhrabhsálaí gréasáin muinín a chur i suíomh gréasáin ionas gur féidir sonraí íogaire a tharchur go sábháilte.

Is é an cuspóir ná cumarsáid iontaofa ceann go ceann.

Déanann *SSL* criptiú láithreach ar théacs lom mar uimhreacha cárta creidmheasa ionas gur sonraí atá ann nach dtig le duine ar bith ach an t-úsáideoir agus an suíomh gréasáin iad a dhíchriptiú. Cinntíonn *SSL* nach ndéantar athruithe ar na sonraí agus deimhníonn sé suíomhanna gréasáin. Lena dhearbhú go bhfuil *SSL* ag cosaint leathanaigh, cuardaigh seoladh gréasáin a thosaíonn ar https:// agus íocón de ghlas fraincín druidte. Comhlachtaí a úsáideann bailíochtú sínte, taispeánann siad na sonraí i mbarra seoltaí glas. Taispeánann deimhniú digiteach *SSL* go bhfuil an suíomh gréasáin slán agus is féidir le cuairteoirí a bheith ar a suaimhneas go mbeidh a gcuid sonraí cosanta agus iad á úsáid.

Mura bhfuil suíomh gréasáin ag úsáid *SSL*, is féidir ríomhaire ar bith ar an líonra rochtain a dhéanamh ar shonraí ar bith atá á dtarchur. Agus muid ag déanamh baincéireachta ar líne, bíonn *SSL* agus *HTTPS* in úsáid againn. Tarlaíonn na céimeanna seo a leanas:

- Iarrann ríomhaire an chliaint ceangal *SSL*
- Freagraíonn an freastalaí agus cuireann deimhniú *SSL* ar fáil, ina bhfuil eochair phoiblí
- Bailíochtaíonn an ríomhaire cliaint an deimhniú agus an eochair phoiblí
- Gineann an ríomhaire cliaint eochair seisiúin agus cuireann sé faoi bhráid an fhreastalaí í
- Tá an ceangal *SSL* bunaithe

Ceisteanna

1 Déantar brabhsálaithe a sheoladh le deimhnithe digiteacha. Fiosraigh cé acu deimhnithe atá seolta i ríomhaire agus cuir síos ar an dóigh a gcuireann seo le slándáil fhoriomlán na sonraí agus an tIdirlíon á úsáid.

2 Cruthaigh léiriú grafach a chuireann síos ar phróiseas criptithe agus díchriptithe sonraí ag úsáid eochracha poiblí agus príobháideacha.

3 Fiosraigh an dóigh a n-éascaíonn na brabhsálaithe seo a leanas aistriú sonraí slán.

- Safari
- Opera
- Firefox
- Internet Explorer

Leabharliosta
BCS Academy Glossary Working Party, 2013, *BCS Glossary of Computing and ICT*, 13 Ú hEagrán, Swindon, BCS Learning and Development Ltd