EFF'S SURVEILLANCE SELF-DEFENSE

DHANA MUHIMU KATIKA USIMBAJI FICHE

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Katika hali fulani, usimbaji fiche unaweza kuwa wa kiotomatiki na rahisi. Lakini kuna njia ambapo usimbaji fiche unaweza kwenda vibaya. Kadiri unavyouelewa, ndivyo utakavyokuwa salama dhidi ya hali kama hizi. Tunapendekeza usome mwongozo wa "Ninapaswa Kujua Nini Kuhusu Usimbaji Fiche?" kwanza ikiwa hujausoma.

Katika mwongozo huu, tutaangalia mawazo matano makuu. Hizi ni dhana muhimu za kuelewa usimbaji fiche data inaposambazwa:

- Kisimbuaji fiche, cha kibonye
- Usimbaji fiche unaoutumia msimbo mmoja kusimba na kusimbua na unaotumia misimbo tofauti kwa kusimba na kusimbua
- Vibonye vya binafsi na umma
- Uthibitishaji wa utambulisho wa watu (kibonye cha umma cha alama za vidole)
- Uthibitishaji wa utambulisho wa nyavuti (vyeti vya usalama)

Kisimbuaji fiche, Cha Kibonye

Labda umeona kitu ambacho, kwa muonekano wake, hakieleweki. Labda inaonekana kama iko katika lugha nyingine, au kama ni hayaleti maana—kuna aina fulani ya kizuizi cha kuweza kuisoma na kuielewa. Hii haimaanishi kuwa imesimbwa kwa njia fiche.

Je, ni nini hutofautisha kitu ambacho hakieleweki na ambacho *kimesimbwa kwa njia fiche*?

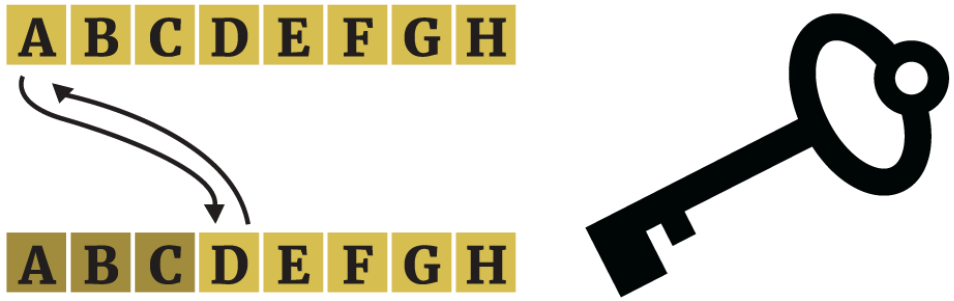
Usimbaji fiche ni mchakato wa hisabati unaotumiwa kuficha taarifa, ili ziweze kufichuliwa tu kwa ujuzi maalum. Mchakato huu unahusisha usimbuaji fiche na kibonye.

Kisimbuaji fiche **ni seti ya kanuni (algoriti) ya usimbaji fiche na usimbuaji. Hizi ni hatua zilizoainishwa vyema ambazo zinaweza kufuatwa kama fomula.**

Kibonye **ni sehemu ya taarifa inayoelekeza algoriti ya usimbaji fiche na usimbuaji jinsi ya kusimba na kusimbua. Vibonye ni mojawapo ya dhana muhimu zaidi za kuelewa usimbaji fiche.**

Kibonye Kimoja na Vibonye Vingi?

Katika **usimbaji fiche unaoutumia msimbo mmoja kusimba na kusimbua,** kuna kibonye kimoja cha kusimba na kusimbua taarifa.



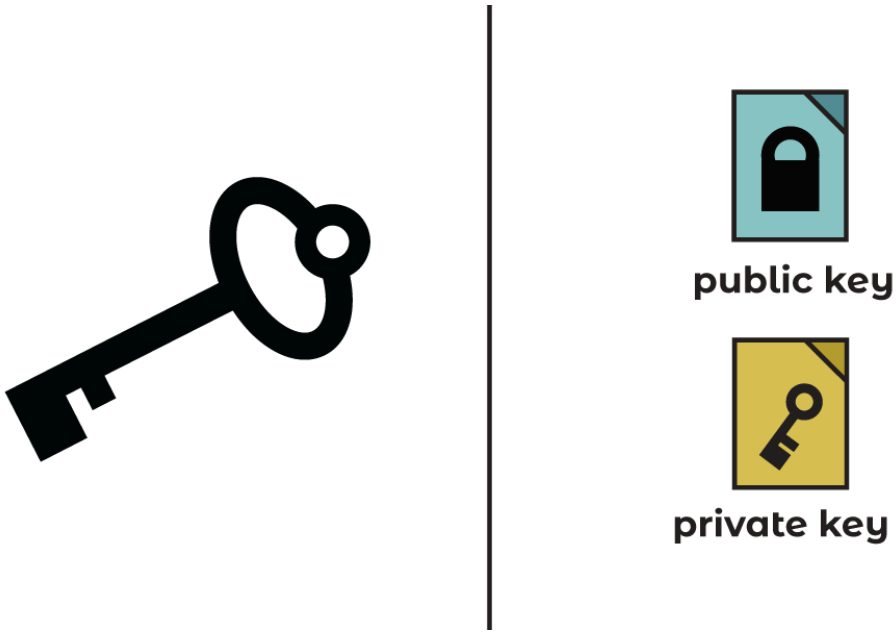
Njia za awali za usimbaji fiche zilikuwa na msimbo mmoja wa kusimba na kusimbua. Kwa "Algoriti ya usimbaji fiche na usimbuaji Caesar" iliyotumiwa na Julius Caesar, kibonye cha kusimba na kusimbua ujumbe ulikuwa kubadilisha kwa alfabeti tatu. Kwa mfano, "A" ingebadilishwa kuwa "D." Ujumbe "ENCRIPTION IS COOL" ungesimbwa kwa njia fiche kuwa "HQFUBSWLRQ LV FRRO" kwa kutumia msimbo kubadilisha kwa alfabeti tatu. Kibonye hicho hicho kingetumika kusimbua ujumbe huo hadi kwenye ujumbe asili.

Usimbaji fiche unaotumia msimbo mmoja kusimba na kusimbua bado unatumika leo—mara nyingi huja kwa njia ya "algoriti za mkondo" na "algoriti za vikundi," ambazo hutegemea michakato changamano ya hisabati kufanya usimbaji wao kuwa mgumu kuusimbua. Usimbaji fiche sasa hivi unajumuisha hatua nyingi za kuficha data ili kuifanya iwe vigumu kufichua maudhui asili bila msimbo halali. Algoriti za kisasa za usimbaji unaoutumia msimbo mmoja kusimba na kusimbua, kama vile algoriti ya Kiwango cha Juu cha Usimbaji Fiche (AES), ni thabiti na ya haraka. Usimbaji fiche unaotumia msimbo mmoja kusimba na kusimbua hutumiwa sana na kompyuta kwa kazi kama vile usimbaji wa faili, usimbaji wa sehemu za kompyuta, usimbaji kamilifu wa vifaa na wa kompyuta zinazotumia diski nzima na usimbaji wa hifadhidata kama zile za vidhibiti nenosiri. Ili kusimbua taarifa hizi zilizosimbwa kwa kutumia msimbo mmoja wa kusimba na

kusimbua, utaombwa kuweka nenosiri mara kwa mara. Hii ndiyo sababu tunapendekeza utumie manenosiri thabiti na kutoa mafunzo ya kuunda manenosiri thabiti ili kulinda taarifa hizi zilizosimbwa kwa njia fiche.

Kuwa na kibonye kimoja kunaweza kuwa sawa ikiwa wewe ndiye mtu pekee ambaye anayehitaji kufikia taarifa hizo. Lakini kuna tatizo la kuwa na kibonye kimoja: je, na ikiwa ungependa kushiriki taarifa zilizosimbwa na rafiki aliye mbali? Je, na ikiwa hukuweza kukutana na rafiki yako ana kwa ana ili kushiriki msimbo huo wa binafsi? Je, unawezaje kushiriki kibonye hicho na rafiki yako kupitia muunganisho wazi wa Tovuti?

Usimbaji fiche unaotumia misimbo tofauti ya kusimba na kusimbua, unaojulikana pia kama **usimbaji fiche wa msimbo wa umma**, hushughulikia matatizo haya. Usimbaji fiche huu unaotumia misimbo tofauti unahusisha misimbo miwili: msimbo wa binafsi (wa kusimbua) *na* kibonye cha umma (kwa usimbaji fiche).



Usimbaji Fiche Unaoutumia Msimbo Mmoja kusimba na Kusimbua	Usimbaji Fiche Unaotumia Misimbo Tofauti kwa Kusimba na Kusimbua
• Haraka	• Polepole
• Hauhitaji uwezo mkubwa wa kompyuta	• Unahitaji uwezo mkubwa wa kompyuta

Usimbaji Fiche Unaoutumia Msimbo Mmoja kusimba na Kusimbua	Usimbaji Fiche Unaotumia Misimbo Tofauti kwa Kusimba na Kusimbua
• Ni muhimu kwa usimbaji fiche wa jumbe kubwa na ndogo	• Unahitaji usimbaji fiche wa ujumbe mdogo
• Unahitaji kushiriki kibonye kwa usimbaji fiche na usimbuaji	• Kibonye cha kusimbua hakihitaji kusambazwa - ni "kibonye cha umma" pekee cha usimbaji unachosambazwa
• Hakiwezi kutumika kuthibitisha utambulisho (uthibitishaji)	• Kinaweza kutumika kwa uthibitishaji wa utambulisho (uthibitishaji)

Usimbaji fiche unaotumia msimbo mmoja kwa kusimba na kusimbua na unaotumia misimbo tofauti mara nyingi hutumiwa pamoja kwa usimbaji fiche wa data wakati wa usambazaji.

Usimbaji Fiche Unaotumia Misimbo Tofauti kwa Kusimba na kusimbua: Vibonye Binafsi na vya Umma

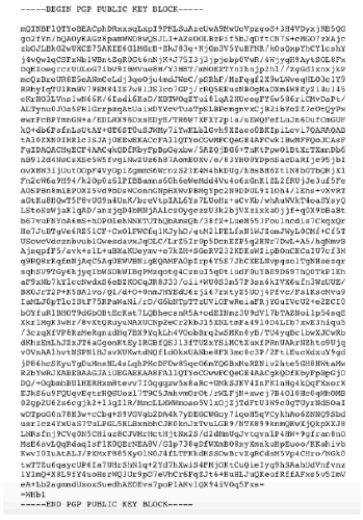
Vibonye binafsi na vya umma huja kama jozi zinazolingana, kwa sababu kibonye cha binafsi na kibonye cha umma kimefungwa pamoja kihisabati. Unaweza kukifikiria kama mwamba uliogawanywa mara mbili. Vinapoletwa pamoja, nusu hizo mbili hulingana na kuwa moja kamili. Hakuna nusu nyingine ya mwamba italingana hivyo. Faili za kibonye cha umma na cha kibonye cha binafsi ni sawa, lakini hatimaye hujumuishwa na uwasilishaji unaoweza kusomwa na kompyuta wa *idadi kubwa sana*.

public

private

----- BEGIN PUBLIC KEY BLOCK -----

----- BEGIN PRIVATE KEY BLOCK -----



----- END PUBLIC KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

Ingawa unaitwa "kibonye cha umma," inaweza kutatanisha kufikiria kuwa msimbo wa umma ni kama msimbo halisi, wa kufungua vitu. Hautumiki kabisa kwa kazi hiyo. Kwa maelezo zaidi kuhusu misimbo ya umma na ya binafsi, angalia maelezo ya kina ya SSD kuhusu kriptografia ya misimbo ya umma.

----- BEGIN PUBLIC KEY BLOCK -----

----- END PUBLIC KEY BLOCK -----

Kibonye cha umma ni faili ambayo unaweza kumpa mtu yeyote au kuchapisha hadharani. Mtu anapotaka kukutumia ujumbe uliosimbwa kutoka kwa mtuma ujumbe hadi mpokeaji, atahitaji msimbo wako wa umma kufanya hivyo.

----- BEGIN PRIVATE KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

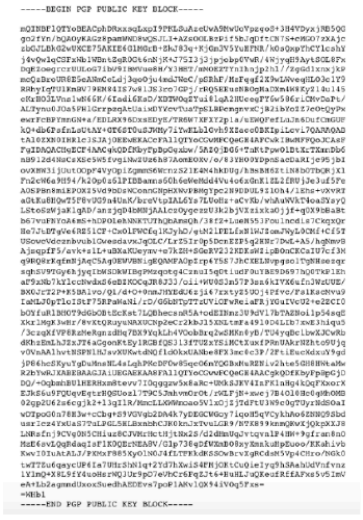
Kibonye chako cha binafsi hukuruhusu kusimbua ujumbe huu uliosimbwa. Kwa sababu kibonye chako cha binafsi hukuruhusu kusoma ujumbe uliosimbwa kwa njia fiche, ni muhimu sana kulinda kibonye chako cha binafsi. Zaidi ya hayo, msimbo wako wa binafsi unaweza kutumika kutia sahihi kwenye hati ili watu wengine waweze kuthibitisha kwamba kwa kweli zilitoka kwako.

Kwa kuwa kibonye chako cha binafsi hatimaye ni faili kwenye kifaa kinachohitaji ulinzi, tunakuhimiza ulinde kwa kutumia nenosiri na usimbaji sehemu ambayo kibonye chako cha binafsi umehifadhiwa. Kwenye Ufuatiliaji wa Kujilinda, tuna miongozo ya manenosiri thabiti na usimbaji fiche wa kifaa.

public

private

----- BEGIN PUBLIC KEY BLOCK -----



----- BEGIN PRIVATE KEY BLOCK -----

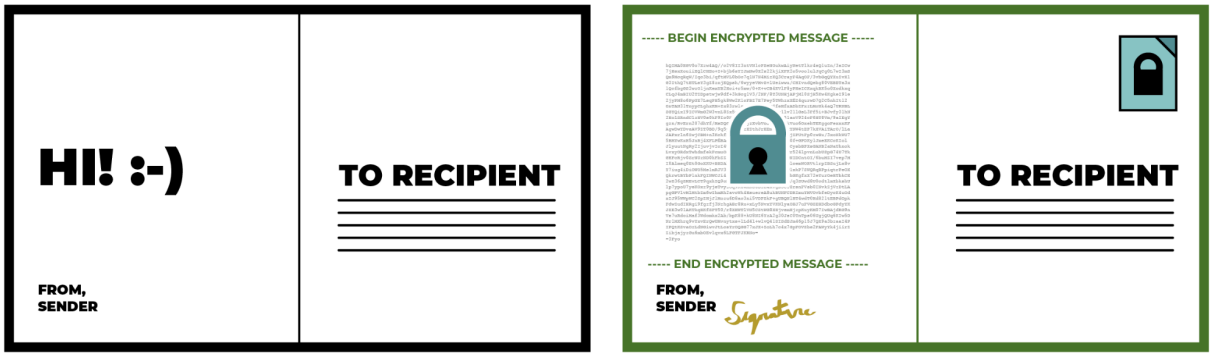
----- END PUBLIC KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

Kibonye cha Umma	Kibonye cha Binafsi
• Faili inayoweza kusambazwa sana (inaweza kusambazwa Mtandaoni kwa urahisi)	• Faili ambayo sharti iwekwe salama na ilindwe
• Mtumaji anahitaji kibonye cha umma ili kusimba taarifa kwa mpokeaji kwa njia fiche	• Hutumika kusimbua ujumbe uliosimbwa kwa njia fiche ambao umeelekezwa kwa kibonye cha umma unaolingana

Kibonye cha Umma	Kibonye cha Binafsi
• Huku ikiwakilishwa na "alama za vidole za kibonye cha umma," ambacho hutumika kuthibitisha utambulisho (uhalalishaji)	• Hutumiwa kwa sahihi za kidijitali, ikiruhusu njia ya kuthibitisha utambulisho wa mtumaji (uhalalishaji)
• Unaweza kuchapishwa kwa hiari kwenye hifadhidata za kudumu, zinazoweza kufikiwa na umma, kama vile "seva zinazotumika kudhibiti misimbo ya usimbaji fiche" (seva zinazotumika kudhibiti misimbo ya usimbaji fiche ni maarufu katika baruapepe iliyosimbwa ya PGP)	

Kwa njia fulani, unaweza kufikiria kutuma taarifa zinazosambazwa kama vile kutuma postikadi. Katika kielelezo cha postikadi kwenye upande wa kushoto (chini), mtumaji anaandika: “HI! :-)” Mtumaji huielekeza kwa mpokeaji ujumbe. Ujumbe huu haujasimbwa na mtu yeyote anayepatana nao anaweza kuusoma.



Kwenye upande wa kulia ni postikadi hiyo hiyo, yenye ujumbe uliosimbwa kwa njia fiche kati ya mtumaji na mpokeaji. Ujumbe bado unaonyesha “Hi! :-)” lakini sasa unaonekana kama ujumbe uliosimbwa kwa sisi wengine.

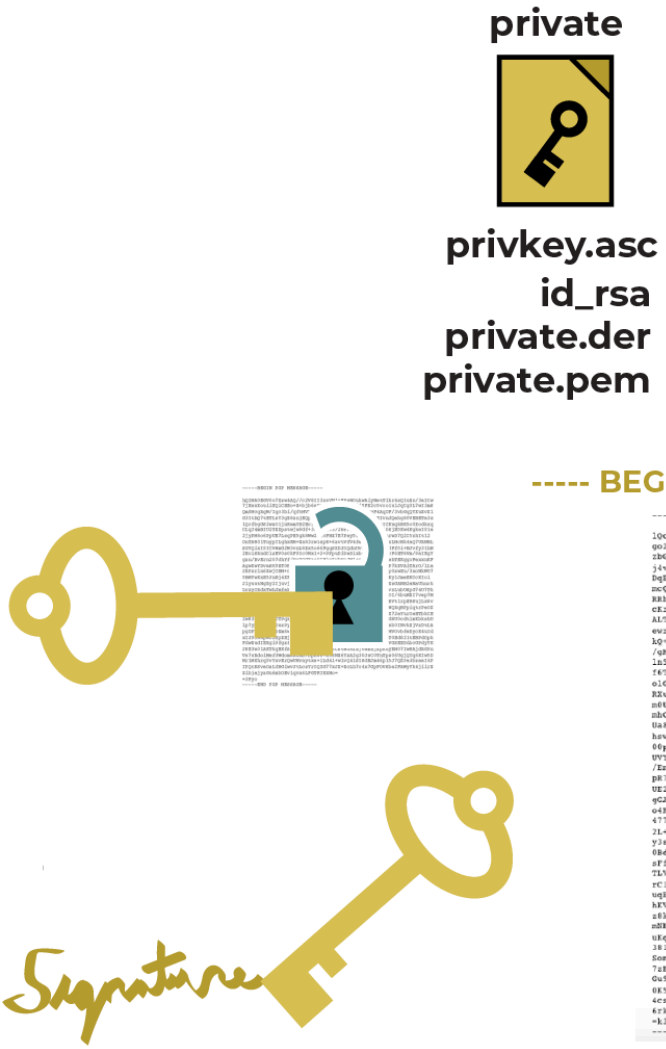
Je, hii hufanywaje? Mtumaji amepata kibonye cha umma wa mpokeaji. Mtumaji huelekeza ujumbe kwa msimbo wa umma wa mpokeaji, ambao husimba ujumbe huo kwa njia fiche. Mtumaji huyo pia amejumuisha sahihi yake ili kuonyesha kwamba ujumbe uliosimbwa kwa njia fiche umetoka kwake.

Kumbuka kuwa metadata—ya anayetuma na anayepokea ujumbe huo, pamoja na taarifa za ziada kama vile saa za kutumwa na kupokewa, mahali ulipopitia na kadhalika—bado zinaonekana. Tunaweza kuona kwamba mtumaji na mpokeaji wanatumia usimbaji fiche, tunaweza kujua kwamba wanawasiliana, lakini hatuwezi kusoma maudhui ya ujumbe wao.

Je, Unasimbia Nani Kwa Njia Fiche? Je, Ni Wao Kwa Kweli?

Sasa, unaweza kuwa unashangaa: "Ninaelewa kuwa kibonye changu cha umma huruhusu mtu kunitumia ujumbe uliosimbwa na msimbo wangu binafsi huniruhusu kusoma ujumbe huo uliosimbwa. Lakini na ikiwa mtu anajifanya kuwa mimi? Je, na akiunda msimbo mpya wa umma na wa binafsi na kuniiga?"

Hapo ndipo kriptografia ya msimbo wa umma ni muhimu sana: Hukuwezesha kuthibitisha utambulisho wako na wa mpokeaji wako. Hebu tuangalie uwezo wa msimbo wa binafsi kwa kina zaidi.



Mbali na kukuruhusu kusome ujumbe uliosimbwa kwa njia fiche unaotumwa kwa msimbo wako wa umma, msimbo wako wa binfsi hukuruhusu kuweka sahihi za kidijitali zisizoweza kubadilishwa kwenye ujumbe unaotuma kwa watu wengine, kana kwamba unaonyesha "ndiyo, ni mimi ninayetuma ujumbe huu."

Mpokeaji wako ataona sahihi yako ya kidijitali pamoja na ujumbe wako na kuulinganisha na taarifa zilizoorodheshwa kwenye kibonye chake cha umma.

Hebu tuangalie jinsi hii inavyofanya kazi katika vitendo.

Uthibitishaji wa Utambulisho wa Watu: Kitambulisho cha Kipekee cha Kibonye cha Umma

Tunapotuma aina yoyote ya ujumbe, tunategemea imani nzuri ya watu wanaoshiriki. Ni kama katika ulimwengu halisi: Hatutarajii mtu anayewasilisha barua aingilie maudhui ya barua zetu, kwa mfano. Hatutarajii mtu kuchukua barua ya rafiki iliyotumwa kwetu, kuifungua na kuirekebisha na kuituma kwetu, kana kwamba hakuna kilichobadilishwa. Lakini kuna hatari hii inaweza kutokea.

Ujumbe uliosimbwa kwa njia fiche una hatari kama hii ya kurekebishwa, hata hivyo, kriptografia ya kibonye cha umma huturuhusu kukagua ikiwa taarifa zimebadilishwa, kwa kukagua utambulisho wa kidijitali wa mtu na utambulisho wake wa halisi.

Kibonye cha umma ni kizuizi kikubwa cha maandishi kwenye faili. Pia huwakilishwa katika njia ya mkato inayoweza kusomeka na binadamu inayoitwa kitambulisho cha kipekee cha msimbo.

Neno "kitambulisho cha kipekee" linamaanisha vitu vingi tofauti katika sekta ya usalama wa kompyuta.

Mojawapo ya matumizi ya neno hili ni "kitambulisho cha kipekee cha kibonye." msururu wa herufi kama vile "65834 02604 86283 29728 37069 98932 73120 14774 81777 73663 16574 23234" ambao unapaswa kukuruhusu kuangalia kama mtu kwenye Tovuti anatumia msimbo sahihi wa kibinafsi kwa njia ya kipekee na salama.

Katika baadhi ya programu, taarifa hizi zinaweza kuwasilishwa kama msimbo wa QR ambao wewe na rafiki yako huchanganua kwa kutumia vifaa vyenu.

Unaweza kukagua kama kitambulisho cha kidijitali cha mtu kinalingana na mtu huyo kupitia kitu kinachoitwa "uthibitishaji wa kitambulisho cha kipekee."

Uthibitishaji wa kitambulisho cha kipekee hufanywa vyema zaidi katika hali halisi. Iwapo unaweza kukutana na rafiki yako ana kwa ana, kuwa na kitambulisho cha kipekee cha msimbo wako wa umma na umruhusu rafiki yako akague kwamba kila herufi kwenye kitambulisho cha kipekee cha msimbo wako wa umma inalingana kitambulisho alicho nacho. Kuangalia mfuatano mrefu wa herufi kama vile "342e 2309 bd20 0912 ff10 6c63 2192 1928" kunachosha, lakini ni muhimu kukagua. Ikiwa huwezi kukutana ana kwa ana, unaweza kufanya kitambulisho chako cha kipekee kipatikane kupitia kituo kingine salama, kama vile mfumo mwingine wa kutuma ujumbe uliosimbwa kutoka kwa mtuma ujumbe na mpokeaji, au uliochapishwa kwenye tovuti ya HTTPS.

Kuthibitisha kitambulisho cha kipekee cha mtu hukupa uhakika wa hali ya juu kuwa ni wao. Lakini si kamili kwa sababu ikiwa misimbo ya binafsi imenakiliwa au kuibiwa (labda una programu hasidi kwenye kifaa chako, au mtu fulani alifikia kifaa chako na kunakili faili hiyo), mtu mwingine ataweza kutumia kitambulisho hicho cha kipekee. Kwa sababu hii, ikiwa msimbo wa binafsi "umeibiwa," utahitaji kuunda jozi mpya ya misimbo ya umma na wa binafsi na uwape marafiki zako utambulisho mpya wa kipekee wa msimbo wako wa umma.

Muhtasari: Uwezo wa Usimbaji wa Kibonye cha Umma

Kwa ujumla, kutumia usimbaji fiche wa kibonye cha umma kinaweza kuwapa watumiaji:

Usiri: Ujumbe uliosimbwa kwa njia fiche kwa kutumia kriptografia ya kibonye cha umma huruhusu mtumaji kuunda ujumbe ambao ni wa siri, ili mpokeaji aliyekusudiwa tu aweze kuusoma.

Uhalisi: Mpokeaji ujumbe uliotiwa sahihi kwa kutumia kriptografia ya kibonye cha umma anaweza kuthibitisha kuwa ujumbe huo uliundwa kihalisi na mtumaji ikiwa ana msimbo wa umma wa mtumaji.

Uadilifu: Ujumbe uliotiwa sahihi au uliosimbwa kwa kutumia kriptografia ya kibonye cha umma, kwa ujumla, hauwezi kubadilishwa, vinginevyo ujumbe hautasimbuliwa au kuthibitishwa ipasavyo. Hii inamaanisha kuwa hata kukatizwa kwa ujumbe bila kukusudia (k.m. kwa sababu ya tatizo la muda la mtandao) kutaonekana.

Uthibitishaji wa Utambulisho wa Wavuti na Huduma: Vyeti vya Usalama

Unaweza kushangaa: “Ninaweza kuthibitisha utambulisho wa kipekee wa kibonye cha umma, lakini na katika wavuti? Je, ninawezaje kukagua kama ninatumia huduma ambayo kwa hakika ni ya kweli? Je, ninawezaje kuwa na uhakika kwamba hakuna mtu anayeingilia muunganisho wangu na huduma?"

Mtu anayetumia usimbaji fiche kutoka kwa mtuma ujumbe hadi mpokeaji hushiriki kibonye chake cha umma sana ili wengine waweze kuthibitisha kuwa kwa hakika ni yeye. Vile vile, unapotumia usimbaji fiche wakati wa usambazaji wa data, kompyuta yako hukagua kiotomatiki ili kuthibitisha kama kibonye cha umma kwa kweli ni wa huduma inayoonyeshwa na kwamba unasimba kwa huduma inayokusudiwa: hii inaitwa cheti cha usalama.

Hapa chini, unaweza kuona mfano wa cheti cha usalama cha SSD kutoka kwa kivinjari cha kawaida cha Wavuti. Taarifa hizi mara nyingi zinaweza kufikiwa kwa kubofya kufuli ya HTTPS kwenye kivinjari chako cha Wavuti na kupata maelezo ya cheti.

Kivinjari cha Wavuti kwenye kompyuta yako kinaweza kufanya miunganisho iliyosimbwa kwa tovuti kwa kutumia HTTPS. Wavuti mara nyingi hutumia vyeti vya usalama ili kuthibitisha kwa kivinjari chako kuwa una muunganisho salama kwenye tovuti halisi na si kwa mfumo mwingine ambao unatatiza muunganisho wako. Vivinjari vya wavuti huchunguza vyeti ili kuangalia misimbo ya umma ya majina ya vikoa—(kama vile www.google.com, www.amazon.com, au ssd.eff.org). Vyeti ni njia mojawapo ya kujaribu kubaini ikiwa unajua msimbo sahihi wa umma kwa mtu au wavuti, ili uweze kuwasiliana nao kwa usalama. Lakini je, kompyuta yako hujuaje msimbo sahihi wa umma kwa tovuti unazotembelea?

Vivinjari vya kisasa na mifumo ya uendeshaji inajumuisha orodha ya Mamlaka za Cheti zinazoaminika (CAs). Misimbo ya umma ya CA hizi huunganishwa mapema unapopakua kivinjari hicho au kununua kompyuta. Mamlaka za Cheti hutia sahihi msimbo wa umma wa wavuti mara baada ya kuzithibitisha kama zinazoendesha kikoa kihalali (kama vile www.example.com). Kivinjari chako

kinapotembelea tovuti ya HTTPS, huthibitisha kuwa cheti ambacho tovuti iliwasilisha kimetiwa sahihi na CA ambayo inaiamini. Hii inamaanisha kuwa mhusika mwingine anayeaminika amethibitisha kuwa tovuti hiyo ni ya kweli.

Kwa sababu tu cheti cha usalama cha tovuti kimetiwa sahihi na Mamlaka ya Cheti, hakumaanishi kuwa tovuti hiyo sharti iwe tovuti salama. Kuna vikomo kwa mambo ambayo CA inaweza kuthibitisha—haiwezi kuthibitisha kwamba tovuti ni ya kweli au ya kuaminika. Kwa mfano, tovuti inaweza kuwa "imelindwa" kwa kutumia HTTPS, lakini bado ina ulaghai na programu hasidi. Kuwa makini na upate maelezo zaidi kwa kusoma mwongozo wetu kuhusu programu hasidi na hadaa.

Mara kwa mara, utaona ujumbe wa makosa yanayohusiana na cheti kwenye Wavuti. Mara nyingi hii ni kwa sababu mtandao wa hoteli au mkahawa unajaribu kuingilia muunganisho wako kwenye tovuti ili kukuelekeza kwenye tovuti yao ya kuingia kabla ya kufikia wavuti huo au kwa sababu ya makosa ya ukiritimba katika mfumo wa vyeti. Lakini mara nyingine ni kwa sababu mdukuzi, mwizi, au polisi au wakala wa kijasusi anayejaribu kufikia muunganisho huo uliosimbwa. Kwa bahati mbaya, ni vigumu sana kutofautisha kati ya hali hizi.

Hii inamaanisha kuwa usiwahi kuendelea kubofya unapoona onyo la cheti ikiwa linahusiana na wavuti ambayo una akaunti au unasoma taarifa yoyote nyeti.

Kuleta Zote Pamoja: Misimbo Inayotumia Msimbo Mmoja wa Kusimba na Kusimbua, Misimbo Inayotumia Misimbo Tofauti ya Kusimba na Kusimbua na Vitambulisho vya Kipekee vya Msimbo wa Umma.

Mfano wa Mchakato Unaotumika Kuanzisha Muunganisho Salama Kati ya Mteja na Seva

Unapotumia usimbaji fiche wa muunganisho salama kati ya mteja na seva, kivinjari cha kompyuta yako na kompyuta ya tovuti unayotembelea hutumia algoriti zinazotumia msimbo mmoja wa kusimba na kusimbua na algoriti zinazotumia misimbo tofauti ya kusimba na kusimbua.

Hebu tuchunguze mfano halisi wa jinsi mawazo haya yote yanavyofanya kazi pamoja: unapojiunganisha kwenye tovuti hii ya HTTPS (https://ssd.eff.org/), ni nini kinachotokea?

Wavuti inapotumia HTTPS, kivinjari chako na seva ya wavuti huwa na mwingiliano wa haraka sana unaoitwa "muunganisho wa kwanza salama kati ya kivinjari na wavuti." Kivinjari chako—kama vile Google Chrome, Mozilla Firefox,

Tor Browser na kadhalika—kinazungumza na seva (kompyuta) inayopangisha tovuti yetu, https://ssd.eff.org.

Kwenye muunganisho wa kwanza salama kati ya kivinjari na wavuti, kivinjari na seva hutumiana vidokezo kwanza ili kuona kama zina mapendeleo yoyote ya pamoja ya algoriti za usimbaji (hizi zinajulikana kama "algoriti za kulinda mawasiliano ya muunganisho"). Unaweza kuichukulia kama vile kivinjari chako na seva yetu ya ssd.eff.org zina mawasiliano ya haraka: zinaulizana ni njia gani za usimbaji ambazo zote zinajua na zinapaswa kuwasiliana nazo na vile vile mbinu za usimbaji fiche zinazopendelea. (“Je, sote tunajua jinsi ya kutumia algoriti inayotumia misimbo tofauti ya kusimba na kusimbua kama vile RSA pamoja na algoriti inayotumia msimbo mmoja wa kusimba na kusimbua kama AES? Ndiyo, sawa. Ikiwa muunganisho huu wa algoriti za usimbaji fiche haufanyi kazi kwetu, ni algoriti gani nyingine za usimbaji ambazo sisi sote tunajua?")

Kisha, kivinjari chako hutumia usimbaji fiche unaotumia misimbo tofauti kwa kusimba na kusimbua: hutuma cheti cha kibonye cha umma kwa ssd.eff.org ili kuthibitisha kuwa kwa hakika ni wewe. Seva ya tovuti hukagua cheti hiki cha kibonye cha umma dhidi ya msimbo wako wa umma. Hii ni kuzuia kompyuta hasidi kuingilia muunganisho wako.

Baada ya utambulisho wako kuthibitishwa, seva ya tovuti hiyo hutumia usimbaji fiche unaotumia msimbo mmoja wa kusimba na kusimbua: hutengeneza faili mpya, inayotumia msimbo mmoja wa kusimba na kusimbua na ya siri. Kisha husimba kwa kutumia misimbo tofauti ya kusimba na kusimbua msimbo wa umma wa kivinjari chako, na kuutuma kwa kivinjari chako. Kivinjari chako hutumia msimbo wake wa binafsi kusimbua faili hii.

Ikiwa kibonye hiki kinaotumia misimbo tofauti ya kusimba na kusimbua utafanya kazi, kivinjari chako na seva ya wavuti huutumia kusimba mawasiliano yao mengine. (Seti hii ya mwingiliano ni muunganisho wa kwanza salama kati ya kivinjari na wavuti (TLS).) Kwa hivyo, ikiwa kila kitu kitaenda sawa katika muunganisho wa kwanza salama kati ya kivinjari na wavuti, muunganisho wako kwa ssd.eff.org huonekana kama Salama na HTTPS kando ya ssd.eff.org.

Kwa maelezo zaidi kuhusu kibonye cha umma na ya binafsi, pamoja na uthibitishaji, soma mwongozo wetu wa SSD kuhusu usimbaji fiche wa kibonye cha umma unaofuata.