

AUÐKENNING

Sjálfstætt verkefni í Tölvuöryggi

Háskólinn í Reykjavík, Tölvunarfræðideild, Haustönn 2004.

Leiðbeinendur: Dr. Gísli Hjálmtýsson og Björn Brynjúlfsson.

Nemandi: Sigurjón Sveinsson.

1 Inngangur

Aðgangur manna að heiminum er nokkuð opinn. Við getum farið hvert sem við viljum, þó í einhverjum tilfellum sé það takmörkunum háð. Stundum þarf að kaupa aðgang, borga svokallaðan aðgangseyri. Stundum þarf leyfi stjórnvalda til að komast inn á svæði, til dæmis vegabréfaáritun fyrir viðkomandi land. Svo eru til staðir, stórir sem smáir, þar sem aðgangur er takmarkaður við ákveðna aðila.

Í þessari greinagerð verður aðgangsstýringum manna og tækja inn á tölvur eða tölvukerfi gerð nokkur skil. Ýmsar aðferðir til auðkenningar verða kynntar og kostir þeirra og gallar skoðaðir.

2 Auðkenning fólks

Auðkenning er að staðfesta einkenni einhvers (persónu eða hlutar) á áreiðanlegan máta. Að auðkenna eftir lykilorði getur verið flókið mál. Því lengri sem lykilorðið er því betra. Að dulrita lykilorðið er ennþá betra. Því má ætla að lykilorð, sem er til dæmis 128 bitar og þar að auki dulritað með DES, sé mjög gott. Tölvur geta notað slík lykilorð en ekki fólk. Fólk er oftast mjög takmarkað þegar kemur að því að muna mjög löng lykilorð og ennþá takmarkaðra ef það á síðan að dulrita lykilorðið eftir mjög flóknum aðferðum og reiknireglum.

Auðkenning notenda byggist aðallega á aðferðum sem byggjast á þremur þáttum [1]:

- Hvað notandinn veit.
- Hvað notandinn hefur.
- Hver notandinn er.

Notkun á lykilorðum er ein leið til að auðkenna notendur eftir því sem þeir *vita*. Lyklar að húsum er dæmi um að fólk sé auðkennt, eða veittur aðgangur, eftir því sem það *hefur* og fingraför er auðkenning eftir því hver viðkomandi *er*.

2.1 Auðkenning með hlutum

Í dag eru til margir hlutir sem fólk notar til auðkenningar. Lyklar, greiðslukort, vegabréf, PIN kort í símum og margt fleira. Þessir hlutir eru oft tengdir því hvað notandinn *veit* (lykilorð) og hver notandinn *er* (myndir, undirskrift, fingrafar, lífsýni). Sem dæmi má nefna kröfur Bandaríkjanna um að á næstunni verði erlendir borgarar sem vilja koma til Bandaríkjanna að hafa vegabréf sem í eru lífsýni viðkomandi, s.s. ekki bara hvað hann hefur (vegabréfið) heldur líka hver hann er (lífsýnið). Einnig fara lykilorð og

hlutir oft saman. Til dæmis þarf að slá inn fjögurra stafa PIN (e. Personal Identification Number) númer þegar bankakort er notað í hraðbanka.

Helsti öryggisgalli við þessa hluti er að það er hægt að týna þeim. Ef hlutur týnist getur sá sem finnur hann auðkennt sig sem eigandinn ef engar aðrar öryggisráðstafanir eru notaðar með þeim hlut, eins og til dæmis PIN númer með greiðslukortum. Annar stór öryggisgalli við þessa hluti er að þó svo að notandinn slái ekki inn neinar upplýsingar, eins og til dæmis í rafrænum hurðapnara fyrir bílskúra, þá eru ákveðnar upplýsingar að flæða milli staða [1]. Þessar upplýsingar er hægt að hlera. Sem dæmi má nefna er með einföldum tækjum sem hægt er að kaupa út í búð, hægt að hlusta eftir þeim útvarpsbylgjum sem hurðapnararnir senda, vista þær og svo nota síðar á sömu hurð til að opna hana.

Nýlega hafa komið fram svokölluð VIT kort (e. smart card). Þau geta haft eigin örgjörva og eigið minni. Við notkun þess fara fram samskipti milli kortsins og þess tækis sem kortið er að auðkenna sig gagnvart, í stað þess einfaldlega að lesa inn gögn í aðra áttina eins og greiðslukort gera. Þessi kort eru af mismunandi toga. PIN kortin eru einfaldasta útgáfan og eru notuð í til dæmis GSM síma. Þau geyma upplýsingar í minni en við ræsingu þarf að slá inn svokallað PIN númer til að fá aðgang að þeim upplýsingum sem kortið geymir. Ef rangt númer er slegið inn of oft læsir kortið sér og er þá engan veginn hægt að lesa kortið nema með löngum aðgangsstreng, mun lengri en PIN númerið.

2.2 Auðkenning eftir líffræðilegum einkennum

Hægt er að bera kennsl á fólk eftir líkamseinkennum þess. Við gerum þetta reyndar á hverjum degi þegar við hittum fólk og berum kennsl á það eftir útliti. Við berum einnig kennsl á það eftir því hvernig það hljómar í síma. En það eru til aðferðir fyrir tæki til að bera kennsl á fólk eftir líkamlegum einkennum þess. Þessar aðferðir eru mis dýrar í útfærslu. Kosturinn við þær er að erfitt er að þykjast vera einhver annar því að til þess að villa á sér heimildir þarf að fá "lánaða" hluta af þeim einstaklingi sem á auðkennið.

Dæmi um auðkenningu eftir líffræðilegum einkennum [1]:

- Sjónhimmuskanni: Tæki sem skoðar örsmáar æðar í augnbotnum viðkomandi. Hver augnbotn er einstakur og því er hægt að auðkenna eftir því. Gallinn við þessi tæki er að þau eru dýr og geta virkað ógnandi fyrir þá sem þarf að auðkenna.
- Fingrafaraskanni: Sú tækni að lesa fingraför hefur verið til lengi. Fingraför eru einstök fyrir hvern einstakling og því er hægt að auðkenna fólk eftir þeim. En þrátt fyrir mikla reynslu af þessari tækni hafa komið upp vandamál við að gera þessa tækni sjálfvirka.
- Handafaraskanni: Þessi tæki eru útbreiddari en fingrafaraskannar. Þessi tæki lesa upplýsingar um hönd viðkomandi, breidd, hæð, fingralengd og fleira. Þessi tæki eru ekki jafn nákvæm og fingrafaraskannar vegna þess að þau geta lesið tvær hendur eða fleiri sem sömu höndina. En þau eru ódýrari en fingrafaraskannar og þeim fylgja færri vandamál.

- Raddlesari: Þessi tækni ber kennsl á rödd fólks og raddir eru nokkurn veginn jafn einkvæmar og fingraför. Þessi tækni er líka nokkuð ódýr. Gallinn við þessi tæki er að það er hægt að blekkja þau með upptöku af rödd (og þar með er ekki verið að auðkenna manneskju heldur tæki) auk þess sem þau geta neitað að auðkenna fólk ef rödd þeirra hefur breyst vegna veikinda, til dæmis hálsbólgu.

Það er einn stór galli við að geyma upplýsingar um þessi líkamlegu einkenni á stafrænan máta. Það er hægt að komast í gagnabanka þeirra sem geyma upplýsingarnar og þar með senda þær upplýsingar sem auðkenningu. Það er því nauðsynlegt, ætli aðilar að geyma þessar upplýsingar á stafrænan máta, að dulrita þau gögn, hvort heldur sem það er á geymslustaðnum eða þegar þessar upplýsingar eru sendar milli auðkenningartækisins og geymslumiðils.

2.3 Auðkenning með lykilorðum

Auðkenning með lykilorði er þegar notandinn, hvort sem notandinn er persóna eða hlutur, þarf að gefa upp leynilegan streng af táknum til að fá aðgang að kerfi eða auðlindum. Lykilorðið er oftast venslað við notendanafn og er notendanafnið í raun það sem ákvarðar aðgang að kerfinu, auðkennir notandann, en lykilorðið er nokkurs konar sönnun þess að sá sem á viðkomandi notendanafn sé raunverulegur eigandi þess.

Lykilorðið er þekkt í kerfinu sem aðgangur er veittur að. Lykilorðið á að vera leynt, þ.e. það á enginn annar að vita þennan streng nema notandinn. Reyndar er lykilorð notandans yfirleitt ekki þekkt í kerfunum sem eru að auðkenna. Það er algengast að svokölluð prófsumma af lykilorðinu sé það gildi sem er geymt.

Það eru nokkrir þættir við notkun lykilorða sem draga úr því öryggi sem þau veita. Einhver getur, annar en notandinn sjálfur, séð lykilorðið þegar notandinn slær það inn. Fylgst með lykilorðinu eða komið fyrir hugbúnaði á tölvunni sem skráir innsláttur á lykilorð og "les" þannig lykilorð. Tölvuþrjotar geta komist í gagnabankann fyrir lykilorðin. Lykilorðið getur verið gegnsætt, þ.e. of auðvelt að giska á það (til dæmis nöfn barna og gæludýra, tölur úr kennitölu viðkomandi o.s.frv). Hægt er að reyna frátengdar orðagiskanir (e. off-line password guessing) með ákveðnu mengi af lykilorðum eins og orðabók. Einnig geta aðgerðir kerfisstjóra til að auka gæði lykilorða, með því að þröngva notendum til að velja erfið lykilorð, orsakað það að notendur fara að skrifa lykilorð niður og geyma þau til dæmis undir lykilorðinu. Um þetta er fjallað í undirkaflanum "Lykilorð og kærulausir notendur".

2.3.1. Tengdar orðagiskanir

Tengd orðagiskun er sú aðgerð að giska á lykilorð á því kerfi sem lykilorðið gengur að með það í huga að ramba á rétt lykilorð. Stundum getur það verið auðvelt því að lykilorð verða ekki betri en þau sem notendur velja sér. Margir notendur nota nafn sitt sem lykilorð, notendanafnið sjálft, nafn barna sinna, hluta úr kennitölu, sambland af nafni og afmælisdegi o.s.frv. Persónubundnar upplýsingar, sem auðvelt er að verða sér úti um og reyna í tengdri orðagiskun, eru því ekki æskileg sem lykilorð.

Svona ágiskanir er hægt að koma í veg fyrir með því að kerfi leyfa takmarkaðan fjölda af röngum ágiskunum. Til dæmis er hægt á Domain Controller á Windows Server 2000 og 2003 að stilla þannig að kerfisstjóri leyfir ákveðinn fjölda af röngum tilraunum og þeim fjölda er náð þá læsist sá notendaaðgangur í ákveðinn tíma. Einnig er Windows þannig að eftir að ákveðnum fjölda af röngum ágiskunum er náð þá stoppar stýrikerfið, bíður í ákveðinn tíma, og tefur þannig ágiskanir. Þessar aðferðir eru einnig útfærðar í hraðbönum. Ef rangt PIN númer er slegið inn of oft, er reyndar ekki svo oft, u.þ.b. 4 tilraunir, þá tekur hraðbankinn kortið til sín og eigandinn þarf að ná í það í bankann sjálfan. Sum kerfi skrá það niður ef þau verða vör við óeðlilega mörg röng lykilorð. Þannig geta kerfisstjórar verið varaðir við ef einhver er að reyna að giska á lykilorð.

2.3.2. Frátengdar orðagiskanir

Stundum geta tölvuþrjótur komist yfir prófsummu lykilorðs eða dulritað lykilorð. Þeir komast jafnvel yfir allan lykilorðagagnabankann. Þó svo að þrjótanir geti ekki brotið dulritunina og lesið beint hvað lykilorðið er þá geta þeir reynt að giska á hvaða lykilorð gögnin standa fyrir. Reikniritin fyrir dulrituninni eða tætifallinu sem reiknar prófsummuna eru yfirleitt kunn og opinber gögn. Þar af leiðandi getur tölvuþrjótur tekið rafræna orðabók sem inniheldur kannski u.þ.b. 500.000 orð og prófað öll orðin. Það eina sem hann þarf að gera er að útfæra sama reiknirit, til dæmis dulkóðaði það lykilorð sem hann er með, dulrita hvert orð með því reikniriti og bera niðurstöðuna saman við lykilorðið. Þessi aðferð er fýsilegur kostur því tölva sem reynir tíu orð á sekúndu, sem er frekar léleg afköst, á þennan máta er tæplega 14 tíma að fara í gegnum orðabók.

Ef þrjóturinn hefur komist yfir öll lykilorð í einu kerfi getur hann beitt ofangreindri aðferð á öll lykilorðin, þ.e. fyrir hvert orð í orðabókinni og athugað hvort það passar við eitthvert þeirra. Það eru miklir möguleikar á því að þrjóturinn finni eitthvað lykilorð sem hefur þann eiginleika að vera til í orðabók. Það er hægt að komast fyrir þessa leið með því að "salta" lykilorðin.

Salt er notað á mat til að bæta bragð hans. Á sama hátt er settur smá broddur í aukningu með lykilorði til að bæta algrímið. Þegar lykilorð er búið til fyrir einhvern notanda er búin til tilviljunarkennd tala á sama tíma, hið svokallaða saltgildi. Þessi tala er geymd ásamt frálagi tætifalls með tölunni og lykilorðinu, samskeyttum (`auðkenna(saltgildi, lykilorð)`). Þegar notandinn skráir sig inn finnur kerfið saltgildi þess notanda, skeytir því saman við það lykilorð sem notandinn gaf upp og reiknar tætifallið `auðkenna(saltgildi, lykilorð)`. Ef frálagið úr tætifallinu fyrir lykilorðið er það sama og er geymt í lykilorðaskránni þýðir það að rétt lykilorð var slegið inn. Þessi aðferð gerir það ekki erfiðara í sjálfu sér að giska á lykilorð en það sem hún gerir er að það er ómögulegt að reyna að dulrita lykilorð, með reikniriti kerfisins, og bera það saman línulega við heilt mengi af lykilorðum [1]. Þannig margfaldast sá tími sem tekur að giska á öll lykilorð í mengi lykilorða (með til dæmis orðabók) með þeim fjölda lykilorða sem í menginu eru. Þetta stafar af því að það þarf að bera saman orðabókina alla fyrir hvert og eitt lykilorð í menginu.

Afköst við frátengdar orðagiskanir fyrir mengi lykilorða m með orðabók n eru því $O(n^m)$ ef saltgildi er notað en ef saltgildi er ekki notað eru afköstin $O(n)$.

Dæmi um notkun á salti á lykilorð:

Notendanafn	saltgildi	dulritað lykilorð
sigurjons01	6877	tætifall(6877 lykilorð _{sigurjons01})
gisli	5984	tætifall(5984 lykilorð _{gisli})
bjorninn	9834	tætifall(9834 lykilorð _{bjorninn})

2.3.3. Forrit til að hlera eftir lykilorðum

Tölvuprjótar hafa lengi notað forrit til að finna út lykilorð. Þessi forrit geta verið í formi viðmóts sem líkir eftir því viðmóti sem innskráning kerfisins notar. Þegar notandinn slær inn sínar upplýsingar, notendanafn og lykilorð, skráir forritið þær upplýsingar. Þessar upplýsingar geta svo verið sendar til utanaðkomandi aðila. Þessi forrit geta verið í formi vírusar eins og PWSteal.Trojan.D. Einnig hafa komið fram forrit sem hlusta á samskipti á tölvuneti og geta borið kennsl á lykilorð. Dæmi um þetta er Ace Password Sniffer frá [EffeTech](#) sem getur veitt út lykilorð í samskiptastöðlum á borð við FTP, POP3, HTTP, SMTP og Telnet.

Einnig eru til forrit sem taka öll slög notenda á lykilorð og vista þau í skrá sem svo er send með tölvupósti til þess sem er að safna þessum upplýsingum.

2.3.4. Lykilorð og kærulausir notendur

Fólk lítur oft frekar á öryggi sem óþurft frekar en nauðsyn [1]. Það sem verra er er að aukið öryggi tefur oft notendur eða setur hindranir á tölvuaðgang/tölvunotkun þeirra. Það er því oft gæfulegt að fræða notendur um tölvuöryggi, nauðsyn þess og reyna að gera öryggismál nógu þolanleg til þess að notendur geti lifað með þau í sátt og samlyndi.

Lykilorð geta orðið mjög mikill áhættuþáttur í öryggi tölvukerfa. Notendur geta skrifað þau niður og límt á tölvuskjáinn hjá sér því þau eru of löng til að muna. Notendur geta einnig farið óvarlega með þau eins og að gefa þau upp fyrir hverjum sem er.

Notendur eiga það oft til að nota sama lykilorðið að mörgum kerfum. Til dæmis að innra neti vinnustaðarins, heimabankanum, MSN, tölvupóstinum og að tölvunni heima hjá sér. En það er erfitt að sjá í fljótu bragði hvort það sé betra að nota mismunandi lykilorð að mismunandi kerfum því um leið og aðgangi að kerfum fjölgar, og þar með fjölda lykilorða sem þarf að muna, því meiri verður freistingin að skrifa þau bara niður notandanum til hægðarauka.

Kerfisstjórar geta valið að setja reglur um lengd og flækjustig lykilorða og þessar reglur geta verið mjög flóknar og erfiðar. Einnig geta þeir valið að láta þau renna út eftir ákveðinn tíma. En að beita þessum aðferðum getur verið tvíeggja sverð eins og eftirfarandi atburðarás gefur dæmi um [1]:

- Kerfisstjóri stillir kerfið þannig að lykilorð verður að vera 6 stafir

- Notandinn velur að setja nafn dóttur sinnar sem lykilorð, elisabet.
- Kerfisstjórinn lætur lykilorð renna út eftir mánuð.
- Eftir mánuð, þegar lykilorð notandans rennur út, velur notandinn að breyta lykilorðinu og slær inn nafn dóttur sinnar aftur, elisabet.
- Kerfisstjórinn kemst að þessari "hjáleidd" notenda og lætur kerfið framfylgja því að nýtt lykilorð geti ekki verið síðasta lykilorð.
- Notandinn slær inn nýtt lykilorð eftir mánuð en breytir því strax aftur í elisabet.
- Kerfisstjórinn lætur þá kerfið geyma síðustu n lykilorð og að nýtt lykilorð geti ekki verið eitt af þeim.
- Notandinn, næst þegar lykilorðið rennur út, breytir um lykilorð $n+1$ sinnum í einum rykk og slær svo inn elisabet sem nýtt lykilorð.
- Kerfisstjórinn lætur kerfið hefta notendur í því að breyta um lykilorð nema með m daga millibili.
- Notandinn skeytir tölunni 1 aftan við elisabet og hækkar töluna um einn í hvert sinn sem hann breytir um lykilorð. Þegar talan er orðin n slær notandinn inn elisabet og er þannig kominn aftur á byrjunarreit.
- Kerfisstjórinn býr til reglu í kerfinu þannig að ný lykilorð geta ekki verið of keimlík gömlu n lykilorðum.
- Notandinn springur á limminu, ákveður að samþykkja eitthvað ómögulegt lykilorð sem erfitt er að muna og skrifar það á miða sem hann límur svo á skjáinn.

Allar þessar aðferðir hafa verið reyndar með misjöfnum árangri. En þegar allt kemur til alls þá er illmögulegt að gera kerfi öruggt nema með samvinnu við notendur. Ef kvaðir á lykilorðum eru vegna raunverulegrar hættu þá þarf að upplýsa notendur um þá hættu. Ef það er ekki hægt þá er það ekki þess virði að setja þröngar skorður á lykilorð [1].

2.3.5. Geymsla á lykilorðum

Það er hægt að geyma lykilorð notenda á mörgum mismunandi stöðum eftir því hvers eðlis aðgangurinn er. Yfirleitt eru tvenns konar leiðir sem farnar eru [1]:

- Að geyma lykilorð á hverri útstöð sem notandinn hefur aðgang að.
- Að geyma lykilorð miðlægt á netstjóra eða öðru aðgangsyfirvaldi.

En hvort sem lykilorðið er geymt miðlægt eða á útstöðvum þá er mjög óæskilegt að lykilorð séu geymd ódulkóðuð á þeim miðli sem auðkennir. Ef þær upplýsingar yrðu afhjúpaðar væri hætt á að óprúttir aðilar geti auðkennt sig sem hvaða löglegur notandi kerfisins sem er. Einnig getur notandi á einu kerfi notað sama lykilorð að öðru kerfi þannig að aðgangstakmarkanir annars staðar gæti orðið ótryggar af þeim sökum.

Það er til leið til að geyma lykilorðin á góðan máta og það er að geyma ekki strenginn sjálfan heldur frálag tætifalls fyrir hvert lykilorð. Ef einhver kemst yfir það gagnasafn sem heldur utan um lykilorðin á því formi verður viðkomandi að reyna frátengdar orðagiskanir. Í þessu tilviki er mikilvægt að notendur hafi valið lykilorð sitt af kostgæfni því að reikniritið sem tætifallið notar er ekki leyndarmál, frekar má reikna með því að það sé vel þekkt.

Einnig er hægt að geyma lykilorðin dulrituð í gagnagrunni. Sem dæmi um þetta þá nefna `crypt()` fallið í UNIX sem dulritar lykilorð notanda. Í því falli er lykilorð notandans notað sem lykill til að dulrita 64 0 bita. Reikniritið er byggt á DES dulrituninni og virkar aðeins í eina átt, þ.e. ekki er hægt að nota sama reiknirit til að dulráða lykilorðið. 64 bita útkoman úr dulrituninni er breytt í 11 tákna streng sem er geymdur í `/etc/passwd` skránni [2]. Þegar svo notandinn auðkennir sig gagnvart kerfinu þá er lykilorðið notað sem lykill í `crypt()` falli og útkoman borin saman við lykilorðið í `/etc/passwd` skránni. Ef bæði orðin eru eins þá hefur rétt lykilorð verið slegið inn og notandinn er auðkenndur.

3 Auðkenningarkerfi

Auðkennið er ekki bundið við perónur. Til dæmis þurfa tölvur á Windows neti að auðkenna sig gagnvart netstjóranum (e. Domain Controller) fyrir ýmsar aðgerðir. Til eru mismunandi aðferðir til að láta nethnúta auðkenna sig gagnvart hvor öðrum og eftirfarandi eru tvær aðferðir við að gera þetta með traustum milliliðum: Lykladreifistöðvar og vottorðayfirvald.

3.1 Traustir milliliðir

Á neti, sem í eru n margir nethnútar sem þurfa að auðkenna sig sín á milli, þarf hver nethnútur að halda utan um aðgangsupplýsingar $n-1$ hnúta. Ef nýjum hnút er svo bætt í netið þarf að senda upplýsingar um auðkenningu þess hnúts á alla hina n hnútana [1]. Þetta er kannski ekki mikið mál fyrir lítil net en ef um stór net er að ræða er utanumhaldið mjög viðamikið. Breyting á einum hnút kallar á uppfærslu á auðkenningu á $n-1$ hnútum. Til þess að minnka flækjustig þessa utanumhalds hafa komið fram kerfi sem gera þetta miðlægt.

3.1.1. Lykladreifistöðvar

Lykladreifistöðvar (e. Key Distribution Center, KDC) halda utan um aðgangsorð, allra hnúta á netinu. Ef hnútur A vill hafa samskipti við hnút B auðkennir A sig gagnvart dreifistöðinni (KDC). Þegar því er lokið biður A KDC um aðgang að B. KDC býr til dulritaðan lykil, með þeim upplýsingum sem KDC hefur um A og B og sendir svo til B og A. Þeir nota svo þennan lykil í þeirra samskiptum. Þessi aðferð auðveldar alla stjórnun á aðgangi milli hnúta og auðkenningu þeirra. Gallinn við þetta er aftur á móti sá að ef óviðkomandi aðili kemst inná KDC og nær stjórn á honum eru aðgangstakmarkanir allra hnúta á

netinu í hættu. Að sama skapi er hættu á því að KDC bili og þar með getur enginn hnútur haft samband við annan hnút, svokallaður "single point of failure". Lykladreifistöðvar geta líka lent í því að anna ekki því álagi sem á þær er lagt og því geta þær orðið flöskuhálsar og hægt á öllum afköstum netsins.

3.1.2. Vottorðayfirvald

Í dulritun með dreifilyklum þarf þar af stærðfræðilega tengdum lyklum, annar er dreifilykill og öllum aðgengilegur og hinn er einkalykill og á enginn að hafa hann nema eigandinn. Það getur verið vandkvæðum bundið að halda utanum alla dreifilyklana á einum stað svo að vel sé. Hvað gerist ef tölvuþrjótur komast inn á þann aðila sem geymir alla lyklana?

Vottorðayfirvald (e. Certificate Authority, CA) er traustur aðili sem heldur utanum alla dreifilykla hnúta á ákveðnu neti. Þau vottorð sem vottorðayfirvaldið (CA) gefur frá sér eru í raun dreifilykill og nafn þess sem á dreifilykilinn. Þeir hnútar sem hafa samskipti við CA verða að hafa dreifilykil CA til að staðfesta heilindi vottorðsins, að það sé í raun frá CA. Þannig að ef að hnútur A vill koma á samskiptum við B hefur hann samband við CA og biður um dreifilykil B. A fær vottorð frá CA sem í er nafn B og dreifilykill hans ("B", dreifilykill_B) og A getur staðfest það að það var sannarlega CA sem sendi lykilinn, því stafræn undirskrift CA er á vottorðinu og A getur sannreynt heilindi hennar með dreifilykli CA. En veikleiki vottorðayfirvalda er sá sami og hjá lykladreifistöðvum. Ef heilindum CA er stofnað í hættu eru heilindi heils nets þar með í hættu.

4 Heimildaskrá

- [1] Charlie Kaufman, Radia Perlman og Mike Speciner, 1995. *Network Security: Private Communication in a Public World*. Prentice-Hall, Inc.
- [2] Simson Garfinkel og Gene Spafford, önnur útgáfa, 1996. *Practical UNIX and Internet security*. Kafli 8, Defending Your Accounts.
http://www.unix.org.ua/oreilly/networking/puis/ch08_06.htm
- [3] Bruce Schneier, 2000. *Secrets & Lies – Digital Security in a Networked World*.