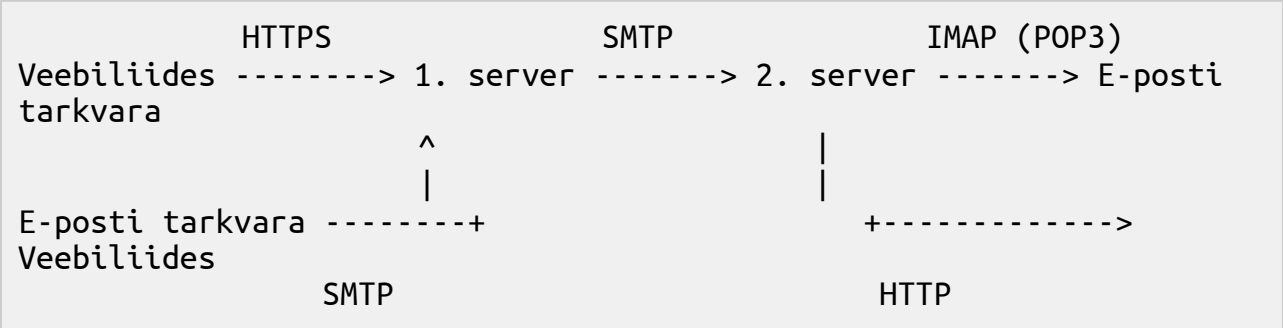
https://lauri.xn--vsandi-pxa.com/2017/03/encrypted-email.html

E-posti krüpteerimine30. Mar '17

Sissejuhatus

Reaalsus on see, et kui saadad kirja, siis juhtub umbestäpselt midagi säärast:



Igal sammul on erinevad puudused, veebiliidese puhul ei ole kindel kas veebiliidesele minnakse ligi HTTPS abil (turvatuna). E-posti serverite vahel liiguvad kirjad päris tihti krüpteerimata. E-post ei kao nii pea kuskile kuna kiirsuhtlusplatvormid on äärmiselt fragmenteerunud ning otspunktist-otspunkti sisu krüpteerimine on toetatud varieeruva eduga.

E-posti turvamise juures on meil kaks aspekti:

- Krüpteerimine, et keegi teine sidet pealt kuulates ei saaks sõnumit lugeda
- Allkirjastamine saatja identiteedi tõendamiseks

Otspunktide vahel mõlemi jaoks on sisuliselt kolm varianti:

- ID-kaardi abil, kasutades ID-kaardi tarkvara
- S/MIME abil (ID-kaart e-posti klienttarkvaras või ise genereeritud X.509 sertifikaadid)
- PGP/GPG abil, tükk maad keerukam aga fooliummütsikestele kõige sobivam

E-posti klienttarkvara

E-posti tarkvara on vajalik selleks et suhelda e-posti serveriga. Gmaili puhul on põhiline postkastile ligisaamise viis veebiliides ise. Suuremates ettevõtetes on kasutusel Microsoft Outlook. Aga need ei ole ainsad viisid postkastile ligi pääsemiseks, üks populaarsemaid avatud lähtekoodiga programme on Mozilla Thunderbird. E-postiserverid kasutavad SMTP protokolli kirjade saatmiseks ning IMAP protokolli kirjade lugemiseks serverist. POP protokolli tänapäeval kasutada pole mõistlik kuna inimesel on rohkem kui üks seade. Thunderbirdi nii nagu pea suvalise e-posti tarkvara saab seadistada kirju alla laadima e-posti serverist IMAP protokolli abil ning saatma SMTP protokolli abil.

Kui kasutad veebiliidest veendu et lähed veebilehele ligi HTTPS abil, indikaatoriks roheline tabalukk aadressiribal

E-posti tarbimiseks kohalikust masinast paigalda Mozilla Thunderbird, seadistamisel veendu et kasutad SMTPS/IMAPS (TLS abil turvatud variante SMTP/IMAP protokollidest):

- Windows, Mac OS X puhul aadressilt https://www.mozilla.org/et/thunderbird/
- Ubuntu, Debian puhul: apt install thunderbird
- Fedora, Red Hat puhul: dnf install thunderbird

Isegi kui kasutad praegu kolmanda osapoole e-posti serverit siis proovi oma arvutis seadistada e-posti klienttarkvara seadistada.

GPG

PGP ehk Pretty Good Privacy oli 1991 aastal loodud tarkvara sõnumite krüpteerimiseks ja allkirjastamiseks. Sellest tarkvarast loodi tagasiulatuvalt OpenPGP avalik standard. GPG ehk GNU Privacy Guard on PGP protokolli avatud lähtekoodiga realisatsioon. GPG kasutab RSA võtmeid, kõige suurem vaev ongi võtmete üles seadmine ning oma usaldusvõrgustiku ehitamine. Näiteks minu

GPG võtme sõrmejälg on E1BC859AFC900AA925F1BAF33E1E3B1EE82AD8C0, võtmeserverist saad alla laadida minu võtme E82AD8C0 lühendi järgi, so viimased 8 sümbolit võtme sõrmejäljest. Enne kui asud allkirjastama minu võtit (sümboliseerib sinu usaldust minu võtmemajanduse vastu) peaksid enne allkirjastamist veenduma et selle võtmega on tõepoolest seotud minu identiteet - helista, tule külla vms.

Paigalda võtmete haldamiseks tarkvara:

- Windows puhul GPG4Win
- Mac OS X puhul GPG Suite
- Linuxiliste puhul kõige lihtsam piirduda käsurea tööriistadega: apt install gpg2

Paigalda Thunderbirdi pistikprogramm:

- Windows puhul ava peamenüüst Lisad ning paigalda Enigmail
- Ubuntu, Debian puhul: apt install thunderbird-enigmail
- Fedora, Red Hat puhul: dnf install thunderbird-enigmail

Pikemas perspektiivis otstarbekas hankida riistvaraline seade võtmete hoiustamiseks a'la Yubikey, selle kohta leiab juhendi siitsamast blogist.

Kuidas täiesti oma postkast teha
Tehtav kui on juba kuskil avalikus internetis tiksumas mõni Linuxiga arvuti, nt Zone pilveserver(~10€/kuu), DigitalOcean virtuaalmasin (5USD/kuu). Õiged häkkerid on vähemalt kord elus käima pannud Linuxi serveri oma koduse ruuteri taha, selle jaoks piisab SMTP ja IMAP portide ringi suunamisest (port forward), hea oleks kui on staatiline IP aadressiga internetiühendus (~6€/kuu).

Lisaks on vaja registreerida domeen (~8-9€ aastas). Domeeni registrari DNS serverisse lisa MX kirje mis ütleb missugune masin

sinu domeeni e-posti teenindab ning SPF kirje, et teised kirju vastu võtvad serverid oskaks kindlaks teha, et sinu domeeniga saadetud kirjad tõepoolest sinu serverist pärinevad.

Paigalda ning seadista Postfix ja Dovecot. Seadista Postfixi jaoks spämmifiltrid a'la Spamhaus. Seadista TLS sertifikaadid Let's Encrypt abil, et sinu serverisse kirju üldse saaks saata üle turvatud kanali.

Kui sul on juba olemas domeenikontroller (Microsoft Active Directory või Samba 4.x) liida e-posti server domeeni realmd abil, vastasel korral loo kohalikud kasutajakontod kes postkasti kasutada saavad.

Kui üksi teha tundub üle mõistuse ehk oleks vaja luua kommuun säärase teenuse jaoks a'la nagu rootslastel on Fripost.

Kui oma postkasti ei julge teha siis uuri Protonmail teenuse kohta.