Elu mõttest andmeturbe valguses

Ühe unise krüptograafi ääremärkusi

Jan Willemson, TÜ 2005

Disclaimer

- Kogu järgnev käsitleb ühe väljamõeldud firma näidet
- Igasugune kokkulangevus reaalsete asjaolude, sündmuste või inimestega on juhuslik ning ettekavatsemata

Ettekande kondikava

- Sissejuhatus
- 1. lugu
- 2. lugu
- 3. lugu
- 4. lugu
- 5. lugu
- 6. lugu
- Boonuslugu
- Õnne definitsioon
- Elu mõte

Sissejuhatus. Firma

- ... toodab klient-server arhitektuuril põhinevat tarkvara teenuse pakkumiseks Internetis
- ... ise seda teenust ei paku, tema klientideks on teised firmad, kes suhtlevad lõpptarbijatega
- ... omab palju kontoreid üle maailma
- ... on oma turusegmendis maailma esikolmikus

Firma ajaloost

- Firmale panid aluse paar noormeest, kes progesid alguses oma lõbuks, siis aga leiti välismaised investorid, kes haistsid kasvupotentsiaali
- Firma hakkaski jõudsalt kasvama ja enamust kerkivaid probleeme lahendati lahenduse valmimise kiirust optimeerides (loe: häkkidega)
- Ühel hetkel otsustati olukorda parandada ja palgati krüptograaf nurka magama

1. lugu. Kommunikatsioon

- Klient-server arhitektuur tähendab palju võrgusuhtlust
- Mis saab siis, kui keegi seda pealt kuulab või vahele surgib?
- Niisiis tuleb suhtlust krüptida. Millega?
- Leiutame oma krüptosüsteemi!
- Paraku oli selle leiutanud juba Blaise de Vigenère ... ja see süsteem murti väga katki juba 400 aastat tagasi
- Firma kasutas toda süsteemi aastaid
- Mitu korda murti see Firma rakenduses?
- Null!

1. loo jätk

- Vaatamata sellele, et fikseeritud parooliga Viegenère'i süsteem polnud Firmat kordagi alt vedanud, otsustati see välja vahetada
- Mis tuli asemele?
- SSL
- Firmas ei huvita kedagi, mida see SSL täpselt teeb, peaasi, et midagi teeb
- Firma krüptograaf ei pruukinud selle lahenduse tarvis isegi üles ärgata

2. lugu. Bitikinnistus

- Firma rakenduse protokoll on kahekäiguline:
  - Klient valib mõned numbrid
  - Server ütleb, palju see klient nende numbrite eest raha saab
- Kui server juhtub paha olema, siis võib ta mõnele kliendile alati käkki keerata
- Korrektne oleks teha bitikinnistust:
  - Klient valib numbrid ja saadab serverile nende kinnistuse
  - Server ütleb, mis numbrite eest raha saab
  - Klient avab kinnistuse

2. loo jätk

- Bitikinnistuse realiseerimisest on kasu ainult siis, kui lõpptarbija suudab veenduda, et protokoll on õige ja seda järgitakse. Selleks
  - peaks ta lugema rakenduse lähtekoodi (mida talle ei anta),
  - olema suuteline sellest aru saama (mida ta ei ole) ning
  - mõistma turvatõestusi (mida ta ei mõista)
- Seega pole korrektsel protokolli realiseerimisel Firmas mingit mõtet

2. loo jätk

- Lisaks on bitikinnistusega protokoll kolmekäiguline ja iga lisakäik tekitab lisaprobleeme protokolli katkemisel
- Veendumaks, et serverid kliente ei peta, tehakse sõltumatute organisatsioonide poolt koodiauditit ja ulatuslikku statistikat ning petvad serverid jäävad kiiresti ärist ilma. See on osutunud piisavaks turvagarandiks
- Ja krüptograaf võib edasi magada

3. lugu. Krediitkaardid

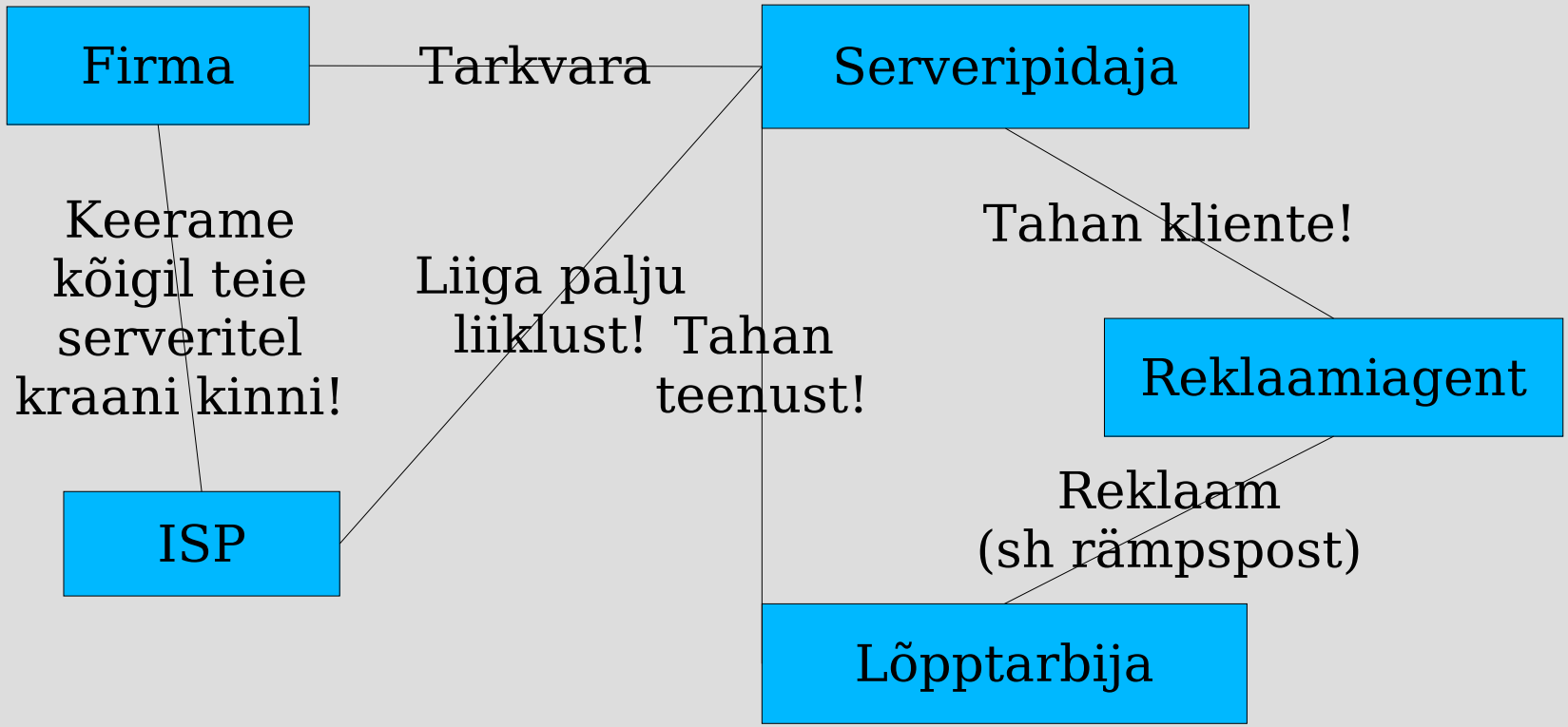
- Juuni lõpus 2005 läks puuduliku käitluse tõttu kaduma ~40.000.000 krediitkaardinumbrit
- VISA ja Mastercard hakkasid seepeale krediitkaardikäitlejatelt nõudma teatud tingimuste täitmist
- Näiteks krediitkaardinumbrite krüptimist
- Krüptograaf tegi ühe silma lahti ja selgitas, kuidas DESi otsa 3DESi ehitada (sest Oracle 8 toetab ainult DESi)

3. loo jätk

- Aga kahe silma vahele jäi ...
- Võtmehaldus!
- Käideldavusnõuetest lähtuvalt tuleb võtit hoida serveris
- Oracle soovitab (ma kahjuks ei naljata):
  - hoidke võtit andmebaasis või
  - hoidke võtit failis või
  - jagage võti mitmeks osaks
- Krüptograaf mõistis, et head lahendust ei olegi, ja kui kunagi midagi välja mõeldakse, realiseerib Oracle selle ise. Krüptograaf vajus tagasi unne

4. lugu. Rämpspost

- Kuidas rämpspost sünnib?



4. loo jätk

- Rämpspost võib olla tüütu koorem postkastile, aga ta töötab ...
- ... ja on majanduslikult kõigile kasulik
  - Serveripidaja saab kliente ja kasumit
  - Firma teenib rohkem
  - ISP teenib rohkem
  - Riik saab maksudena rohkem tulu
- Seega pole rämpsposti võimalik kaotada
- Spämmi hulga määrab ISP murdumispunkt
- Süsteem tuksub selle punkti läheduses
- Majandusteadlased, appi!!!
- Krüptograaf teeb senikaua ühe uinaku

5. lugu. Tarkvara kaitse

- Suur osa Firma väärtusest peitub tema koodibaasis
  - Tarkvara arhitektuur
  - Suhtlusprotokollid
  - Tehnilised lahendused
- Samas selleks, et raha teenida, tuleb koodi mingil kujul müüa
- Kompileeritud kuju pole piisav privaatsuse tagamiseks
- Mida siis teha?

5. loo jätk

- Põhimõtteliselt on võimalik binaarkoodi loetamatumaks muuta nii, et funksionaalsus säilib (*sogastada*)
- Nt PHP jaoks on olemas Zend Encrypt
  - Kui keegi suudab välja uurida, mida see elukas teeb, siis ma oleksin tänulik
- Midagi on olemas ka Java jt asjade jaoks
- Samas on nad kõik “häkid” ja nende murdmise raskuse kohta ei teata midagi
- Puuduvad isegi head mudelid sogastamise kohta väidete tõestamiseks

5. loo jätk

- On teada, et sogastamine väga üldises mõttes pole võimalik
- Praktiline vajadus on aga väga suur – tööpõld tulevastele teadlastele!
- Samuti tuleks uurida riistvarale toetuvaid tarkvarakaitsemeetodeid
- Krüptograaf ärkas külm higi otsa ees, sest sogastamisest ei teadnud ta mitte midagi

6. lugu. Pettused

- Firma kliendid teenivad serveritele tuginevate teenuste müügist raha
- Kus on raha, seal on pettused
- Lõppkasutajaid on palju (üle 2 miljoni), sestap nii transaktsioone kui ka pettusi palju
- Kuidas pettustele jälile jõuda?
- Võtta tööle 20 onu ja lasta neil kõik transakstioonid üle vaadata ...
- ... see aga läheb mingist hetkest alates liiga kalliks

6. loo jätk

- Tüütuid asju aitab teha arvuti!
- Pettusi saab leida lihta lineaarse mudeliga
  - Defineeritakse binaarsed tunnused
  - Igale tunnusele määratakse kaal
  - Iga transaktsiooni korral liidetakse aktiivsete tunnuste kaalud
  - Kui summa ületab ettemääratud läve, antakse pettusealarm
- Kuidas määrata kaalud ja läved?
- Jälle onud ..?

6. loo jätk

- Läveprobleemi jah/ei küsimuste juures ei teki ja kaalude juures oskab meid taas arvuti aidata
- Tehnika nimi on Bayesi õppimine ja seda kasutatakse väga edukalt rämpsposti filtreerimisel
- Jälle valdkond noorteadlastele
- Krüptograaf ringutas ja leidis, et statistikakursused olid omal ajal täitsa kasulikud

Boonuslugu. Turvalisuse hindamine

- Ülemus – krüptograaf:
  - Make sure we will be secure.
  - How secure?
  - Well, so that nothing bad would happen.
  - Can't do that. We can be hit by an asteroid, a member of the board can sell company secrets ...
  - Cut the mumbo-jumbo. Then do as well as you can!
- Kui turvaline Firma olla saab?
- Kas onu Sidi käest on mõtet meteoriidikindlustust osta?

Boonusloo jätk

- Mis on turvalisuse ühik?
- Raha!
- Iga turvavidin, mis ostetakse (kaamera, PGPDisc, raudkapp, Tripewire, ...) on investeering, mis peab ära tasuma
- Majandusteadlased, appi!!!
- Krüptograaf viis hommikul paberid majandusteaduskonna kaugõppesse ja hakkas öösiti olümpiaadiraamatuid kirjutama

Kokkuvõtteks

- Asjad, millega on mõtet tegeleda:
  - Tarkvara kaitse
  - Majanduslikud meetodid (riskianalüüs)
  - Masinõpe
- Asjad, millega ei ole mõtet tegeleda:
  - Protokollide ja algoritmide väljatöötamine
    - Vähemalt praegu ja Eestis on see nii, sest kõik krüpto saabub meile karbis
  - Majanduslike probleemidega võitlemine tehnoloogiliste ja seadusandlike meetoditega
    - Näiteks rämpsposti saatmise seadusega ärakeelamine

Mis on õnn?

- Õnn on see, kui sinu teadmistest ja oskustest kellelgi tulu tõuseb
- Kas inimene ise saab enda õnne nimel midagi teha?
- Loomulikult, tuleb omandada kasulikke teadmisi ja oskusi!

Mis on elu mõte?

- Let's stop for discussions here.