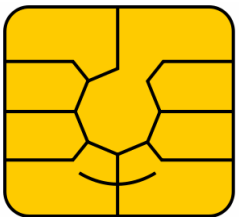
Kako je mali 7-Zip pobijedio pametnu karticu



Možete li zamisliti poslovni scenarij koji favorizira pametne kartice kao najbolje rješenje za dosezanje visoke razine zaštite podataka, naposljetku se implementira 7-zip - i sve bude baš kako treba?! Tja, čujte, ili sam - blago meni - jaaako promućuran ili sam napravio neku gadnu "grešku u koracima". Priča ide ovako...

Poznanik koji vodi omanje knjigovodstveno poduzeće školovani je ekonomist i računalni zanesenjak. Značajan dio svakodnevnih poslova on i njegovi radnici odrađuju uz podršku pametnih kartica, tipično, https-om se spoje na web uslugu neke banke, autenticiraju posredstvom kartice pa onda provode svakojake financijske transakcije... klasika za tu djelatnost. Kad nešto zapne, a uzrok je tehničke prirode, moj poznanik poletno se primi *tshootanja*, ponešto riješi sam, ponešto uz asistenciju likova poput mene, i tako se to kotrlja godinama. U trenutku nadahnuća, bijaše to pred samu Novu godinu, odlučio je tipične funkcionalnosti pametne kartice - enkripcija podataka i digitalni potpis - primijeniti na elektroničku razmjenu poruka sa senzitivnim podacima između svog poduzeća (nadalje: Centrala) i poduzeća-klijenata. Ideja se zasnivala na spoznaji da su već godinama u optjecaju RDC-ovi poslovni certifikati, štoviše, sve više ljudi ima eOI koja omogućuje uporabu identifikacijskog i potpisnog certifikata, i zašto se time ne okoristiti.

Kad mi je poznanik priopćio tu svoju odluku o štićenju važnijih poruka e-pošte pametnim karticama, brzopotezno sam se složio jer od svih postojećih rješenja baziranih na tehnologiji javnog ključa (PKI), ona je uistinu najsigurnija. Zašto je, recimo, pametna kartica sa certifikatom za digitalno potpisivanje sigurnija od certifikata iste namjene instaliranog u OS računala? Zbog toga što privatni ključ nikada nije dostupan operativnom sustavu ili bilo kojoj aplikaciji računala, sve operacije s njime odrađuje operativni sustav pametne kartice lokalno. Da, do sada su evidentirani raznovrsni uspješni napadi na pametne kartice ali uzrok je traljava implementacija konkretnog smart card rješenja, recimo, driver ili aplikacija za upravljanje karticom imaju sigurnosni propust, ili je čip na kartici određenog proizvođača loše konstruiran... ma to je priča za sebe, idemo mi dalje s temom.

Kako sam sve bolje upoznavao konkretno poslovno okruženje, postajao sam sve neodlučniji. Sama po sebi, ideja zaštite određenih podataka u porukama e-pošte sasvim je opravdana, posebice u ozračju GDPR uredbe kojom se svi poslovni subjekti obvezuju na zaštitu osobnih podataka. Očito je da osobni podaci u porukama e-pošte moraju biti enkriptirani kako ih kradljivac ne bi mogao pročitati, digitalni potpis tu nije dovoljan. A osobni podaci, pored onih financijskih, uistinu povremeno cirkuliraju na relaciji Centrala - klijenti. Ti klijenti, nek se zna, razna su omanja poduzeća, njih desetak, raštrkana po Zagrebu i okolnim gradovima: ima tu restorana, mesnica, trgovina odjećom i drvenim (polu)prerađevinama... Za njih poduzeće mog poznanika obavlja sve knjigovodstvene i računovodstvene poslove, zato ga i poimam kao Centralu. Saznao sam u jednom trenutku da su izvorište poruka sa potencijalno senzitivnim podacima klijenti, Centrala uglavnom potvrđuje primitak, podsjeća na nešto ili traži podatke. Saznao sam i još važnije: e-poruke šalju ili vlasnik poduzeća-klijenta ili, češći slučaj, od njega ovlašteni djelatnik koji sretnim stjecajem okolnosti znade poslati neku poruku s privitkom kako bi Centrala odradila svoj posao (nekakvu uplatu/isplatu, obračun plaće, ovakav-ili-onakav podnesak Poreznoj upravi ili tzv. trećoj strani, i slično). Nadalje, iako su sva klijentska računala Windows, sami klijenti kao pravne osobe dozlaboga su šareni po odabiru sustava i klijenata e-pošte - neki rabe Gmail, drugi Yahoo, treći su se opredijelili za uslugu e-pošte telekom operatera koji im iznajmljuje Internet vezu; manjina koristi Outlook, jedan ima Thunderbird a većina rabi Internet preglednik... i tu sam puko, dreknuh "NEMERE!".

Navodim razloge za svoje kontriranje:

* Klijenti su, u najboljem slučaju, obični korisnici računala, štoviše, sa pametnim karticama kojima će enkriptirati i/ili potpisivati poruke nemaju baš nikakva iskustva. To znači da bi ih se trebalo educirati, odraditi nabavu i inicijalno podešavanje čitača i programske podrške, kupiti certifikate, podesiti klijenta e-pošte te, naposljetku, organizirati efikasnu tehničku podršku. Treba misliti i na višegodišnje arhiviranje privatnih ključeva jer bez odgovarajućeg ključa nećemo moći pročitati poruku enkriptiranu isteklim certifikatom. Iz iskustva znam da su, kad rade s pametnim karticama, bez stručne podrške korisnici bespovratno izgubljeni u praktično svim problemskim situacijama. U istoj se situaciji često nađu i neiskusniji informatičari jer infrastruktura javnog ključa jest sveprisutna, ali i vrlo specifična u odnosu na sve druge računalne teme & dileme.

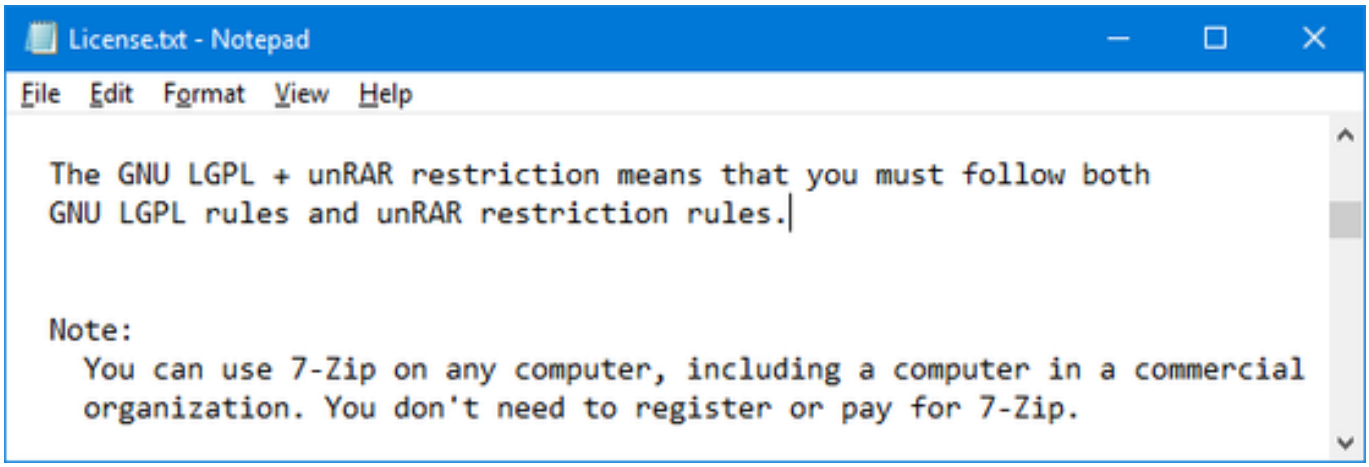
* Napomena glede osposobljavanja klijenata: očito bi to trebali biti djelatnici koji neće nakon edukacije "zbrisati" na novi posao, pri čemu je jasno da je poduzeću najprivrženiji kadar - njegov gazda! A ti ljudi su 24 sata dnevno okupirani problematikom preživljavanja svog poduzeća, računalo im je "zadnja rupa na svirali" pa nije teško pretpostaviti kako će se postaviti naspram prijedloga da se obrazuju za uporabu pametnih kartica u dopisivanju.

* Ne treba zanemariti troškovni aspekt priče, kao i volju klijenta da uvede pametnu karticu u svoje radne procese - dovoljno je da jedan odbije to učiniti i evo odstupanja koje ruši koncept kao cjelinu jer tada za sigurniju mail komunikaciju s tim klijentom treba osmišljavati neko drugo rješenje.

* Pametna kartica s RDC-ovim poslovnim certifikatima poslužiti će svrsi, ali ne i AKD-ova elektronička osobna iskaznica (eOI) jer na nju "zaprženi" identifikacijski i potpisni certifikati ne omogućavaju niti enkripciju podataka niti digitalno potpisivanje e-poruka. Zašto tako korisne funkcionalnosti nisu implementirane, ne znamo, ali znamo da nam baš eOI može poslužiti kao odličan primjer gnjavaže s pametnim karticama: nakon instalacije drivera za čitač i aplikacije za upravljanje certifikatima, evo problema kao na slici - iz poruke nitko živ ne može dokučiti da Windows računalo nema AKD-ov *root* certifikat u Trusted root spremištu certifikata. Za potrebe ovog članka provjerih on-line uputu za instalaciju eOI softverskog paketa i mogu reći da AKD-ov *root* certifikat kao preduvjet u uputi nije spomenut (možda je u nekoj od nekolicine drugih uputa, ali tada čitatelj mora imati fotografsko pamćenje). Da poantiram: iz poruke niti informatičar ne može shvatiti stvarni uzrok greške, snaći će se samo onaj koji već ima pozamašnog iskustva iz tog područja, potom treba znati dohvatiti i instalirati taj certifikat = neriješivo običnom korisniku!

* Značajan broj klijenata rabi Internet preglednik kao klijenta e-pošte a čak niti Gmail, zasigurno najmasovniji i najnapredniji besplatni sustav e-pošte, nema integriranu podršku za enkriptiranje i digitalno potpisivanje poruka. Znači, trebali bismo pokrenuti pravu kampanju konsolidacije klijentske strane po tom pitanju = *mission impossible*. Istina je da danas na ovim prostorima vjerojatno nema komercijalne usluge e-pošte koja nije zaštićena TLS-om na relacijama korisnik <-> mailbox i SMTP server <-> SMTP server ali opet - dovoljan je jedan izuzetak da sruši cijeli koncept.

I tako, počeo sam tragati za nekim primjerenijim rješenjem... ubrzo "napikirah" općepoznati 7-zip, besplatan i za osobnu i za poslovnu primjenu. Čime su ispunjeni svi preduvjeti za početak jednog divnog prijateljstva! :o)



Dodatne su vrline 7-zip alata:

* Postavljanje ovog programa na računalo nije niti za dlaku složenije od instalacije neke pasijans, mah-jong, fliper i slične igre kakve si obični smrtnici redovito priušte na poslu ili doma. Veliki plus za većinu koja još uvijek ne vlada engleskim je lokalizirano sučelje. Što se tiče uporabe alata, višestruko je jednostavniji od bilo kakve igre i u to ćemo se odmah uvjeriti.

* Ako mu tako naredimo, 7-zip će tijekom sažimanja podataka odraditi i enkriptiranje, rabeći vrlo siguran AES256 algoritam, ujedno će nam omogućiti postavljanje lozinke. Ovo je sve što klijent treba učiniti:

- desni klik na dokumentu prikazanom u Windows Exploreru > 7-Zip > Dodaj u arhiv > unos lozinke i potvrda (eventualno uključi prikaz upisane lozinke kako bi se uvjerio u njenu ispravnost);

- otvoriti mail klijenta, priložiti doc-arhiva.7z i poslati Centrali.

Jednostavnije ne može! U stvari, može ako nam je klijent e-pošte registriran u sustav, naime, tada u WinExploreru, iz 7-zip izbornika, odaberemo naredbu Sažimanje i slanje e-poštom pa 7-zip sam doda paket u novu poruku.

* Centrala može raspakiravati pakete iz GUI-a ili skriptno, iz komandne linije, ovako:

7z x doc-arhiva.7z -pLozinka

* Naravno da sam dobro ispitao ranjivost produkta i zaštitu jednom postavljene lozinke, ta neću poslovnim ljudima uvaliti "rupičasti" softver! Ukupan broj spomena vrijednih ranjivosti u zadnjih 10 godina je 8, niti jedna nije razine High, kažu CVE Details, također, autor 7-zip alata vrlo brzo reagira.

A sada par riječi o najslabijoj karici rješenja - lozinki. Dogovoreno je da svaki klijent postavi svoju lozinku, koju potom telefonom ili poštom priopći Centrali. Unikatna lozinka identificira klijenta, što je koristan detalj u praksi. Lozinka se mijenja jednom godišnje. Vjerojatnost probijanja lozinke samo je teorijska jer se od klijenata očekuje postupanje prema uputi koju sam izradio, slijedi njen sažetak:

a) Minimalna duljina lozinke je 16 znakova.

b) Pored slova engleske abecede, brojeva i posebnih znakova, uključujući razmak, u lozinki **mora** biti prisutno poneko veliko i/ili malo slovo palatala hrvatske abecede.

c) Lozinka se formira tako da se složi od izobličenih ili presloženih riječi, idealno od žargonizama.

d) Operativni sustav i antimalware softver poslovnog računala treba pažljivo održavati, ne skitarati po webu s tog računala.

Primjer 1: RuužnaŠaškastaDžuke11a (nap.: miks deformiranih riječi književnog hrvatskog i žargonizma **džukela** kojega smo dodatno "začinili")

Primjer 2: Sowa-ČŽŠ-Cuck0v1a (nap.: postoji sova vrste kukuvija, iz te riječi izvodimo riječ Cuckovia, potom neke samoglasnike zamijenimo brojevima)

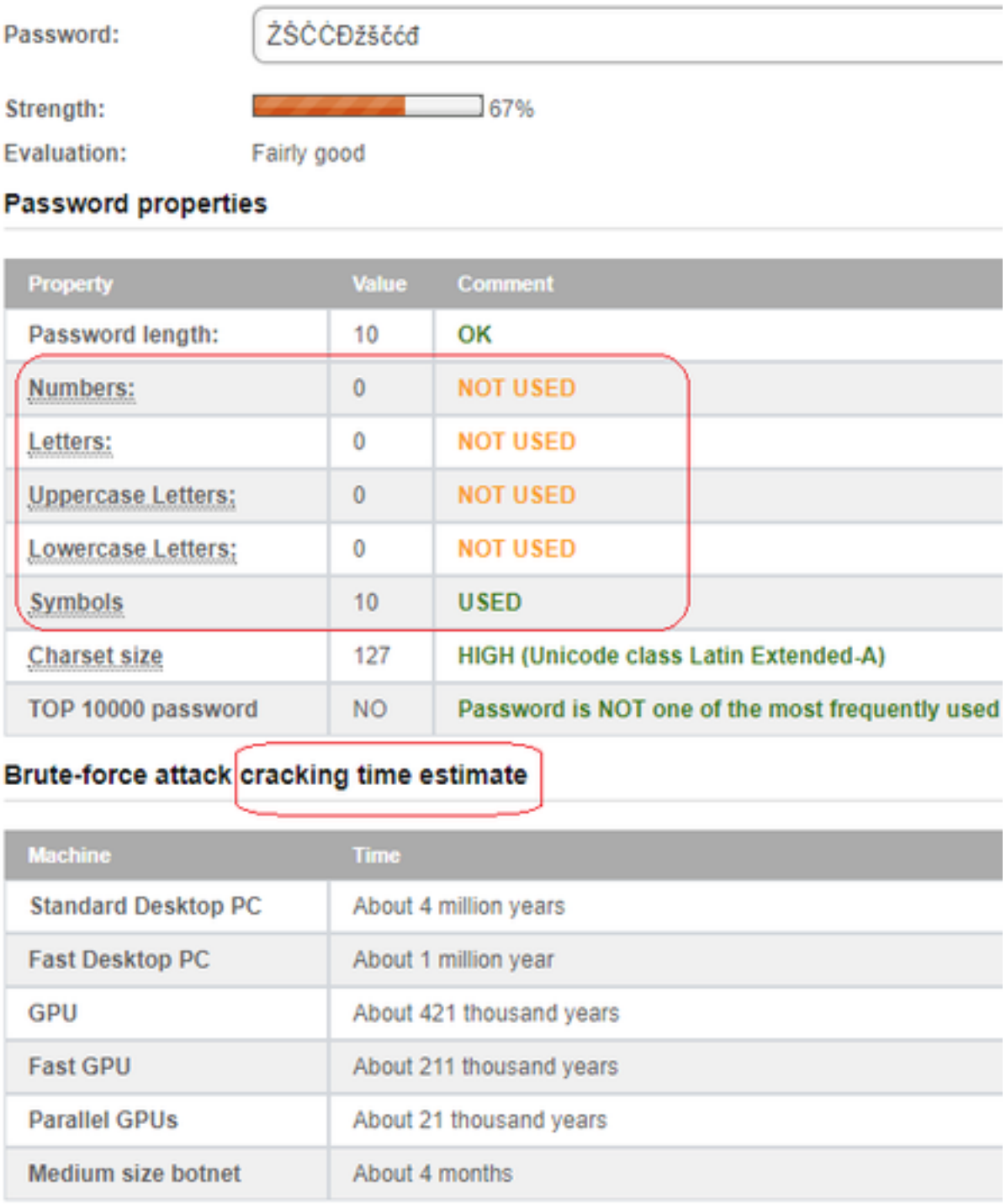
Kad promislimo gornje upute i primjere, primijetit ćemo:

- iako deformirane, lozinke su pamtljive Hrvatima i onima koji se tako osjećaju, utoliko, ne treba ih zapisivati;

- napad rječnikom je zamalo pa nemoguć odn. primjenjivi su samo vrlo sofisticirani napadi, uz brojne prateće modifikacije izvorne morfologije riječi;

- preostaje "brute force" napad ali njemu se suprotstavljamo duljinom lozinke i uporabom slova s dijakritičkim znacima. Utoliko, i taj tip napada mora biti sofisticiran.

Za *dictionary* i *brute force* napade vrijedi: moraju biti podržani superračunalom ili klasterom računala sa snažnim grafičkim karticama i prvoklasnim sofverom ukoliko se želi probiti lozinka u nekom razumnom vremenu. Lako ćemo naći razne izračune na webu. U pripremnom periodu isprobao sam tucet poznatih lokalno instaliranih i on-line *password crackera*, većina bi "otkačila" kad bih im uvalio sekvencu čšž i slično. Uočite da se uključivanjem u lozinku naših slova s dijakritičkim znakovima, za 10 slova povećava osnovni skup slova - onaj temeljen na engleskoj abecedi - koje *cracker* mora obraditi, što je samo po sebi veliki dobitak u smislu zaštite lozinke. Tako smo svojevremenu noćnu moru hrvatskih informatičara - palatale hrvatske abecede - pretvorili u prednost!



Password: ŽŠČĆĐžšććđ

Strength: 67%

Evaluation: Fairly good

Password properties

Property	Value	Comment
Password length:	10	OK
Numbers:	0	NOT USED
Letters:	0	NOT USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	0	NOT USED
Symbols	10	USED
Charset size	127	HIGH (Unicode class Latin Extended-A)
TOP 10000 password	NO	Password is NOT one of the most frequently used

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 4 million years
Fast Desktop PC	About 1 million year
GPU	About 421 thousand years
Fast GPU	About 211 thousand years
Parallel GPUs	About 21 thousand years
Medium size botnet	About 4 months

Cyber kriminalci su dosjetljivi i uporni likovi, kvalificirani za svoj nečasni posao, također, mogu upogoniti izvanredno jak hardver... ali sve to košta i para i vremena! I tu dolazimo do kategorije motiviranosti - kolika je vjerojatnost da će napadač uložiti golema sredstva u razbijanje lozinke prisutne u mailu nekog omanjeg poduzeća ili obrta?! Za one koji smatraju da koncept ruši *keylogger* koji će jednostavno "pocicati" lozinku: u uputi je smjernica d) kao obveza korisnika računala, dodatno, prisjetimo se da je to slaba točka i *smart card* tehnologije, znači, po tom smo pitanju "na pozitivnoj nuli". Mislim da u konačnici možemo zaključiti kako je sigurnost ovog besplatnog rješenja zaštite osjetljivih osobnih i poslovnih podataka na vrlo visokom nivou.

7-zip smo upogonili tijekom prvog mjeseca ove godine. Svi su se brzo snašli. Sva Windows računala u startu su imala dobro podešene Language, Keyboard i prateće regionalne kerefekice pa lozinka sa ććđšž nikome nije bila problem. Čak je zadovoljena i kategorija interoperabilnosti - ako na Android smartfon instalirate Zarchiver, pa tijekom zipanja postavite kodnu stranicu 12521 (European Western

ANSI) i paket zaštitite lozinkom koja uključuje naša "problematična" slova, primatelj s ispravno podešenim Windows 10 bez problema će sa 7-zip raspakirati zaprimljeni paket. Luud1ll000ćžš! :o)

čet, 2018-04-05 09:21 - Ratko Žižek**Vijesti:** Sigurnost [1]
Kategorije: Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: sigurnost [3]
zaštita [4]
mail [5]
e-pošta [6]
windows [7]
7zip [8]
enkripcija [9]
GDPR [10]

Source URL: https://sysportal.carnet.hr./node/1801

Links
[1] https://sysportal.carnet.hr./taxonomy/term/13
[2] https://sysportal.carnet.hr./taxonomy/term/30
[3] https://sysportal.carnet.hr./taxonomy/term/82
[4] https://sysportal.carnet.hr./taxonomy/term/204
[5] https://sysportal.carnet.hr./taxonomy/term/228
[6] https://sysportal.carnet.hr./taxonomy/term/229
[7] https://sysportal.carnet.hr./taxonomy/term/76
[8] https://sysportal.carnet.hr./taxonomy/term/230
[9] https://sysportal.carnet.hr./taxonomy/term/231
[10] https://sysportal.carnet.hr./taxonomy/term/210