Što treba znati o vjerodajnici tipa „ime/lozinka“

Nedavno je Vlada RH gromoglasno (i opravdano!) izmarketirala uvođenje u javnu uporabu e-usluga poput NIAS, ePass, Korisnički pretinac... (itd.). Ne dvojim da znate o čemu je riječ - radi se o sustavu komunikacije građana s državom putem mreže, bez čekanja pred šalterima. Na adresi https://gov.hr [1] je on-line podsjetnik. Prevođenje projekta e-Građani s razine planova i koncepata na razinu konkretnih web usluga, koje sada postaju dio naše svakodnevice, donosi građanima razne benefite, ali i problemčić kojega mnogi zacijelo još nisu niti osvijestili u cijelosti - kako sačuvati svoj digitalni identitet.

Već sam pisao na temu zaštite računala [2] od provala s računalnih mreža, pa ovaj članak možemo tretirati kao nastavak te teme. Postoji, naime, neraskidiva međuzavisnost: vjerodajnicama otpornim na provale i krađu štitimo svoje računalo (tj. sebe), a na provale i krađe otpornim računalom štitimo svoje vjerodajnice (tj. sebe)!

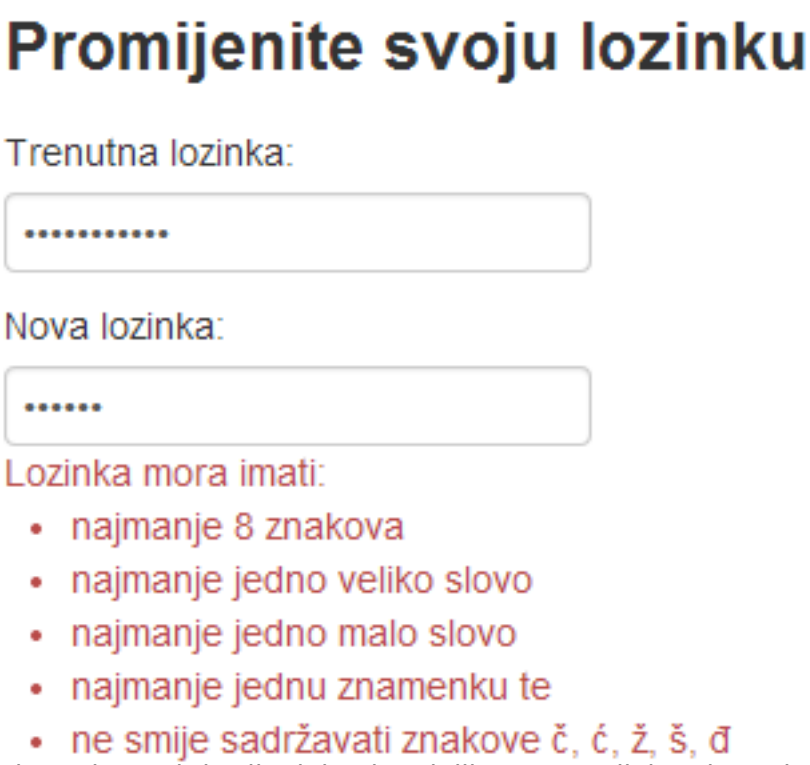
Uslugy ePass omogućuje svakome od nas da bez troškova postane posjednik vjerodajnice tipa „ime/lozinka“. S tom vjerodajnicom možemo rabiti e-usluge TDU-a koje prihvaća vjerodajnicu kao dostatno sigurnu za korištenje predmetne usluge. Tisuće nas već je iskoristilo tu pogodnost i imamo svoju ePass vjerodajnicu. Koju je, nema u to sumnje, svaki od nas oblikovao po vlastitom nahođenju, u skladu sa osobnim (ne)znanjem. I po istom kriteriju organizirao si njeno čuvanje, zaštitu od otuđenja.

S druge strane, prisjetimo se, vjerodajnica tipa „ime/lozinka“ dokazano je najranjiviji tip vjerodajnice, u stručnim krugovima etiketirana je kao relikt iz neke ranije informatičke ere... Ali dobra vijest: ta proskribirana vjerodajnica uopće nije tako loša. Ako mi građani, kao njeni vlasnici, i Fina, kao njen izdavatelj (*Identity Provider*), znademo što nam je činiti, još će nad dugo i vjerno služiti!

Što treba učiniti vlasnik vjerodajnice „ime/lozinka“?

- Prvi dio vjerodajnice - korisničko ime - uopće ne mora zrcaliti naše stvarno ime i prezime. U mom slučaju, umjesto da svoju ePass vjerodajnicu imenujem kao ratko.zizek ili rzizek (i slično), mogu je nazvati Ratpass. Izdavatelj vjerodajnice znade upariti ovakvo ime samnom kao fizičkom osobom, jer sam morao proći proces identifikacije i registracije za izdavanje vjerodajnice, a tijekom tog procesa Fina je dobila sve podatke koji nedvosmisleno povezuju vjerodajnicu samnom. S druge strane, ovim postupkom značajno demotiviramo hackera da se posveti probijanju lozinke jer, čak i kada shvati da postoji neka vjerodajnica imena Ratpass, ne zna stvarni identitet njenog vlasnika.

- Drugi dio vjerodajnice – lozinka – ključ je za očuvanje našeg digitalnog identiteta. Niža slika pokazuje da usluga ePass nameće 8 znakova kao minimum za lozinku. Sa strane usluge to je korektno, ona traži minimalni broj znakova da bi lozinka bila prihvaćena od strane ePass sustava, problem je u korisnicima utoliko što golem broj njih, dokazano je, minimalnu duljinu lozinke bez ikakvog pravog razloga tretira kao jedinu moguću duljinu! Pa se, pritisnuti i ostalim preduvjetima koje moraju ispuniti za koliko-toliko sigurnu lozinku (eno i njih na slici) trude smisliti nešto, štogod to bilo, ali duljine 8 znakova!



Zaboravite na kriterij minimalne duljine, postavljajte ekstradugačke lozinke! I dostatno kompleksne, dakako. Temeljem dugogodišnjeg osobnog iskustva mogu reći da se vrlo brzo upisuje kompleksna lozinka koja je ujedno i više no dvostruko dulja od minimalne! Naime, nakon što neko vrijeme iole redovitije rabimo neku ekstradugačku lozniku, prsti se „osamostale“, virtuozno zaplešu po tipkovnici i upis traje 2 -3 sekunde. Dodatna pogodnost za vlasnika extradugačke lozinke je ta što ju ne mora mijenjati u nekim kraćim intervalima. Uz preduvjet da vlasnik takve lozinke, te izdavatelj vjerodajnice, provode i odgovarajuće mjere čuvanja / zaštite vjerodajnice, vjerojatnost probijanja ekstradugačke lozinke graniči sa nevjerojatnošću!

- Umijeće oblikovanja lozinke ima višestruki pozitivan učinak, naime, umješno oblikovana lozinka toliko je otporna na razne metode probijanja da ju ne moramo učestalo mijenjati, upisuje se brzo poput neke kratke a totalno nerazumljive lozinke (npr. O7_hx“G!s) te, naposljetku, ne moramo ju nigdje zapisivati pa potom brinuti o štićenju te bilješke od znatiželjnih očiju.

Ovako ćemo stvoriti neprobojnu a humanu (brzoupisivu i pamtljivu) lozinku:
a) Prisjetimo se nečije fraze, mudrolije, opaske; ako je neki žargonizam ili možda u nekom narodskom dijalektu - još bolje! Kao izvorište odlično će poslužiti baština obiteljske komunikacije, pisane ili govorne.
b) Odabrani izraz modificiramo poštujući pritom načelo dosljednosti: presložimo određene slogove u riječima, određena slova zamijenimo brojevima i posebnim znacima.

Uzmimo za primjer lozinku Naze1e-Nad01i. Riječ je o dijelu imena američkog filma *How green was my walley* (Kako je zelena bila moja dolina). Lozinka je stvorena od dvije riječi iz tog imena, točnije, preoblikovan je dio „zelena dolina“ tako što je zadnji slog svake riječi postavljen na njen početak a slovo l je dosljedno zamijenjeno brojem 1.

Jačanje procesorske snage i tehnika probijanja lozinke nagnali su me da tu lozinku zamijenim duljom, koju sam potom opet godinama rabio: Mal1.Schep0n1a!. Kad je moja kći bila malena, razrezala je stopalo pa je danima šepala, snuždena poput napuštenog ptića, a ja sam ju oslovljavao izrazom „Moj mali šeponja!“. Nema šanse da tu frazu zaboravim, zar ne?! Niti postoji šansa da ju provali bilo kakav *password guessing* softver, čovjek pogotovo. Uočite da riječ Scheponia ne postoji, također, dosljedno sam neka slova zamijenio brojevima.

Dakako, lozinku možemo još bolje „zvuzlati“, zašto ne, samo treba naći mjeru kako se opet ne bismo

našli u situaciji da je moramo zapisati jer ju ne možemo upamtiti. Tu važi načelo: Bolje produljiti nego zakomplicirati.

- Pravilno čuvanje i uporaba vjerodajnice sljedeći je čimbenik kojime štitimo svoj digitalni identitet. Vjerodajnica kojom se bavimo u ovom članku – „ime/lozinka“ -ne čuva se nigdje drugdje osim u glavi. Vlastitoj. Što je lako izvedivo ako smo ispoštovali gornje savjete. Glede uporabe vjerodajnice, prije upisivanja imena i lozinke provjerit ćemo kome smo u vizualnom dometu. Rečeno se ne odnosi samo na ljude nego i na kamere, ta ove umjetne oči su posvuda – eno ih na stropovima, stupovima, stolovima, monitorima, mobitelima... Nadalje, svoju vjerodajnicu ćemo rabiti samo ako je konekcija na web servis tipa HTTPS (pri čemu ćemo, prije upisivanja vjerodajnice, provjeriti autentičnost tog web mjesta, vidi članak Zaštita računala od provala s računalnih mreža), te samo ako smo dostatno uvjereni da cyber-zločestobe nisu ugnijezdile neki backdoor ili, ne-daj-Bože, keylogger u računalo kojime se služimo. Prevedeno – ne rabiti tuđa ili javna računala!

Što treba učiniti izdavatelj vjerodajnice „ime/lozinka“?

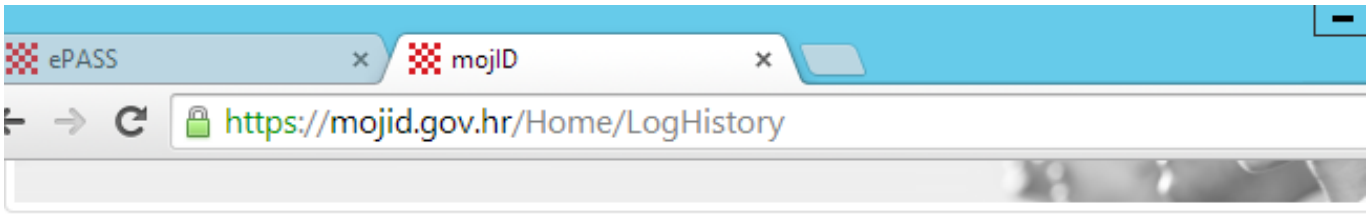
Za svaki uspješno izvršen password harvesting nije odgovoran korisnik nego izdavatelj vjerodajnica. Nažalost, korisnik je taj koji ispašta. Svjedočimo postojanju izdavatelja vjerodajnica koji svoju ulogu shvaćaju isuviše olako pa im hackeri „u jednom cugu“ iščitaju tisuće i desetke tisuća vjerodajnica. Dakle, oni Identity Provideri koji žele zadržati svoj kredibilitet, nemaju izbora, oni moraju primjenjivati high-security politike, i to ne samo na sve komponente koje tvore sustav za izdavanje i čuvanje vjerodajnica nego i na sve komponente s kojima taj sustav komunicira. Možemo se mi non-stop baviti zaštitom jezgrenih komponenata sustava, ali ako napadač provali u naš sigurnosno zanemareni pomoćni serverčić za transfer logova i backupova, a jezgra s njime priča... razumijemo se, zar ne?!

Slijedi par dodatnih bitnih sastavnica *high-security* politike:

- obveza je IT arhitekata osmisliti i dalje razvijati sustav koji je arhitekturalno otporan ne samo na ispade već i na napade; programeri su dužni stvarati aplikacije usklađene sa suvremenim sigurnosnim standardima; sistemci-admini su obvezni primijeniti sigurnosne zakrpe na upogonjeni softver što je prije moguće;
- repozitorij sa digitalnim identitetima je access listama izoliran od front-end sloja i enkriptiran; pristup tom repozitoriju imaju samo ovlaštene, dokazano pedantne osobe (i to samo sa tzv. management mreže); rezervna kopija tog repozitorija na internoj je mreži i podliježe istoj politici;
- front-end sloj sustava dostupan je samo kroz SSL port; ispred tog sloja nisu samo reverzni proxy i firewall nego i IDS/IPS logika koja će brzo „nanjušiti“ neočekivane / neželjene aktivnosti na mrežnoj ili aplikativnoj razini te, uz alarmiranje osoblja, pokrenuti kontraakciju;
- periodično se rade sigurnosne provjere – fokus je na front-end sloju - poput penetracijskih testova, kako bi se pravovremeno uočile i otklonile ranjivosti;
- postoje jasno definirani procesi / procedure djelovanja za predviđene i nepredviđene situacije;
- korisniku treba omogućiti kreiranje imena po izboru, a nameće mu se kreiranje dugačke i kompleksne lozinke;
- praćenje uporabe računa i obavještavanje korisnika kad se primijeti istovremena uporaba istog računa sa raznih lokacija / računala, ili ako se desi da u kratkom vremenskom periodu netko ubrzano unosi netočnu lozinku (potonje je indikator *password guessing* napada);
- dobrodošlo je uvođenje teholoških rješenja usmjerenih na dodatnu zaštitu vjerodajnice, poput podrške za *two-step* autentikaciju: korisnik se predstavi „ime/lozinka“ vjerodajnicom, potom

mu se na ranije registrirani uređaj (mobitel, PC) dostavi jednokratni kod kojim dodatno potvrđuje svoj identitet – za detalje skoknuti na https://accounts.google.com/SmsAuthConfig [3] jer je Google jedan od Identity Providera koji to omogućuje korisnicima svojih e-servisa.

Niže vidimo da MojID, jedna od aplikacija NIAS suite, omogućuje građaninu praćenje uporabe svojih vjerodajnica.



Povijest pristupa e-uslugama

Datum od:
17.06.2014

Datum do:
24.06.2014

Vrijeme	E-usluga	Detalji razmjene podataka između NIAS-a i e-usluge
24.06.2014. 15:40:05	mojID	prikaži/sakrij detalje...
20.06.2014. 09:53:52	mojID	prikaži/sakrij detalje...
20.06.2014. 09:51:36	mojID	prikaži/sakrij detalje...
20.06.2014. 09:50:33	mojID	prikaži/sakrij detalje...

Što treba učiniti napadač na vjerodajnicu „ime/lozinka“?

Pa, ako izdavatelj i vlasnik vjerodajnice dobro odrađuju svoj dio posla, zločestobe će trebati naći neku novu zanimaciju! :-)

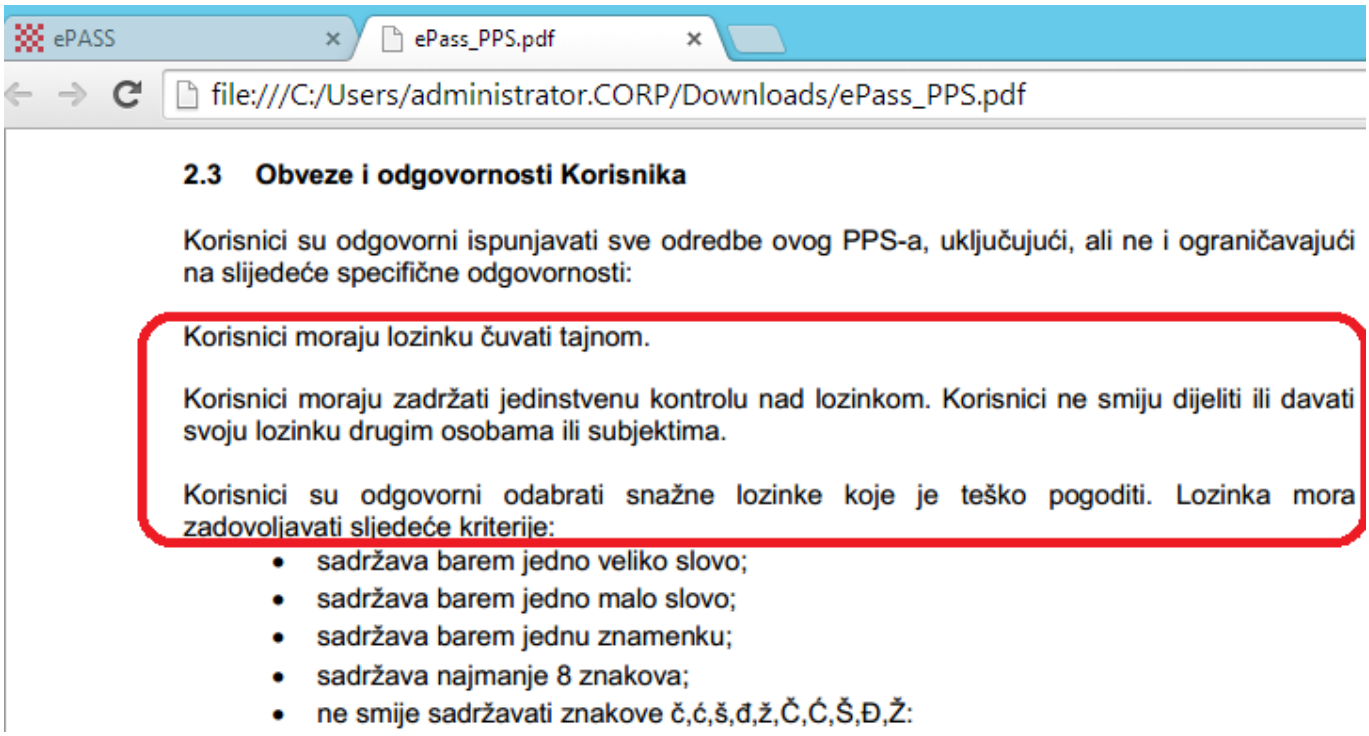
Šalu na stranu, negativcu realno preostaje socijalni inženjering, znači, pokušat će „nasukati“ vlasnika vjerodajnice. Što se u praksi često dešava, nažalost. Slijedi, za pouku, opis jako dobre smicalice. Uočite kako njen izumitelj vješto kombinira poznavanje ljudske naravi i računalnih tehnologija.

a) U neposrednoj okolici naciljane ustanove, na par međusobno udaljenih ali lako uočljivih mjesta, rano ujutro postavi se po jedan dopadljiv USB stick;
b) tijekom dolaska na posao, djelatnik ustanove uoči stick, zahvali Bogu što mu je omogućio posjedovanje ovakve spravice za 0 kuna i, dakako, gurne stick u USB utor svog računala;
c) svi iole moderniji desktop operativni sustavi automatski mountaju stick... a na sticku je *spyware* koji koristi tu funkciju kako bi se ugnijezdio u operativni sustav; prvi modul *spywarea* (*keylogger*)

vrijedno bilježi sva korisnikova kvrckanja po tipkovnici a drugi modul (*backdoor*) spaja se Internetom na računalo pod kontrolom prevaranta i prenosi mu te informacije... neminovno, u jednom trenutku prenijet će mu i „ime/lozinka“ vjerodajnicu.

Drage sistemašice, dragi sistemci, svjedočimo masovnom uključivanju građana Republike Hrvatske u kompjutorizirane interakcije s tijelima državne uprave. Većina tih ljudi je slabo ili nikako osposobljena za zaštitu svog računala (PC desktop, prijenosnik, tablet, mobitel...) i svog digitalnog identiteta. Pomozite im jer time i sebi pomažete: vaši korisnici i poznanici obratit će vam se za pomoć kad možda bude prekasno da se njihov problem bezbolno riješi.

Na kraju samo podsjećam: za sve nas kao korisnike ePass vjerodajnice, odn. bilo kakve vjerodajnice tipa „ime/lozinka“, vrijedi niži imperativ:



sub, 2014-06-28 09:03 - Ratko Žižek**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1413

Links
[1] https://gov.hr
[2] https://sysportal.carnet.hr/node/1386
[3] ttps://accounts.google.com/SmsAuthConfig