Generator pametnih šifri

Viktor Braut, Matija Osrečki i Dino Sulić

7. siječnja 2014.

Sažetak

Za većinu korisnika sigurnost na računalnim sustavima bazira se na kvalitetnoj šifri. Ovaj rad predstavlja pristup generiranju kvalitetnih šifri na temelju lakoće utipkvanja istih. Za analizu lakoće utipkavanja naučili smo neuronsku mrežu da regresijom ocjeni lakoću utipkavanja nizova znakova fiksne duljine (engl., *n-gram*), u našem slučaju veličine 3. Optimalne parametre neuronske mreže odredili smo unakrsnom validacijom nad skupom od oko 440 podnizova koristeći 4 preklopa. Iako rezultati jako variraju, u konačnici smo dobili dovoljno dobre rezultate za izradu generatora. Sam generator koristi jednostavnu tehniku gdje kreće s kvalitetnim nizom duljine 3 i svaki sljedeći znak odabire slučajnim odabirom, čija je vjerojatnost odabira proporcionalna kvaliteti zadnjeg dobivenog podniza.

1. Uvod

Sigurnost privatnosti na računalnim sustavima danas je bitna više nego ikada. Za većinu korisnika to znači jednu stvar – kvalitetna šifra. I dok sustavi poput GMail-a ugrađuju metode dodatne verifikacije korisnika putem tokena generiranih primjerice mobilnim uređajem te postoje rješenja sigurnosti uporabom kriptografskih metoda javnih i privatnih ključeva (SSH, GPG, itd.), za većinu web servisa, operacijskih sustava i ostalih oblika programske potpore kvalitetna šifra je najzastupljenije rješenje.

Više je svojstava kvalitetne šifre. Najbitnije svojstvo je sigurnost – mora biti dovoljne duljine, sadržavati dovoljno različitih vrsta znakova (mala i velika slova, brojevi i ostali znakovi) koji bi trebali biti slučajno raspoređeni, kako pojedini dijelovi šifre ne bi bile konkretne riječi. Drugo poželjno svojstvo je da je šifru lagano zapamtiti. Nažalost, za većinu je to najbitnije svojstvo zbog čega za šifre koriste imena svojih djevojki, velikih kantautora (Bob) i slično.

U ovom radu predstavljamo ideju izbora, odnosno generiranja šifre na temelju lakoće utipkavanja iste. Prva pretpostavka je da će takav način zastupati sve znakove na tipkovnici u podjednakoj mjeri te da zbog slučajne prirode generiranja šifri neće doći do podnizova koji se mogu naći u rječnicima, prema tome bi trebalo biti zadovoljeno svojstvo sigurnosti. Druga pretpostavka je da lakoća utipkavanja olakšava mehaničko pamćenje i da će time biti zadovoljeno drugo stvojstvo dobre šifre, iako možda tek nakon kraćeg perioda uvježbavanja šifre.

Uži aspekt ovog zadatka koji je i ujedno najteži jest analiza lakoće utipkavanja proizvoljnih nizova znakova na tipkovnici određenog rasporeda znakova. Pristup koji smo prirodno prihvatili jest uporaba subjektivnih ocjena skupa kraćih nizova u nadi da postoje nekakva statistička ili geometrijska korelacija između transformiranih nizova znakova i naših subjektivnih ocjena. Konkretno, koristili smo neuronske mreže kako bi regresijom odredili lakoće utipkvanja nizova znakova koje nismo vidjeli.

2. Metode

akllk

2.1. Analiza lakoće tipkanja

oaks

2.2. Stohastički generator šifri

jkik

3. Rezultati

3.1. Implementacija

3.2. Učenje neuronske mreže

4. Zaključak