Povzetek Zaključnega Dela

Jakob Povšič

June 20, 2021

1 Uvod

Tehnologija in internet sta radikalno preobrazila našo družbo v zadnjih desetletjih, in z vsakim dnevom je naše življenje bolj zlito z digitalnim. Vendar niso vse spremebe pozitivne, še posebej na področju zasebnosti, danes se zdita pojma digitalnega življenja in zasebnosti samo izključujoča. Zaradi poslovnih modelov velikih tehnoloških podjetji, ki temeljijo na dostopanju osebnih podatkov uporabnikov, dobiva zasebnost vsak dan večji pomen.

Zero-Knowledge Proofs (ZKPs) so eno od orodji, ki bi lahko spremenila naš pristop do obdelave podaktkov. Njihove aplikacije omogočijo odločitve nad podatki, brez razkirvanja podatkov samih.

V zaključnem delu bomo raziskali uporabo ZKP v avtentikacijskem sistemu, kot metodo dokazovanja pravilnosti gesla.

2 Avtentikacija in EAP

Avtentikacija je proces preverjanja resničnosti trditev, ki jih predstavlja neka entiteta o sebi ali predmetih. V informacijski varnosti se avtentikacija pogosto uporablja za uspostavljanje dostopa med uporabniki in zasčitenimi sistemi. Avtentikacija z uporabniškim imenom in geslom je pogost model s katerim se danes srečujejo uporabniki.

V zaključnem delu bomo zasnovali avtentikacijski sistem kot metodo v "extensible authentication protocol" ogrodju (EAP). EAP [1] je razširljivo ogrodje za pogajanje in izvršitev mnogih avtentikacijskih metod (EAP metod). Sistem bo omogočal avtentikacijo z uporabniškim imenom in geslom preko omrežja, in bo uporabljal ZKP kot mehanizem preverjanja gesla.

Uporaba gesel prinese določene ranljivosti, zato je industrija posvojila varnostne metode, ki onemogočajo določene napade na sistem. Ena od teh metod je raztegovanje ključev, uporaba ZKP mora omogočati uporabo takšnih metod za zagotavljanje minimalne varnosti.

3 Zero-Knowledge Proofs

ZKPs [3] so zanimiv koncept z področja kriptografije, ki omogočajo dokazovanje metematičnih izjav brez razkrivanja *zakaj* so resnične. To omogoča izredno zanimive aplikacije, saj lahko takšen sistem izvaja "operacije" nad podatki brez, da bi do njih dostopal v surovi obliki. V takem sistemu lahko dokažemo, da smo polnoletni oz državljani neke države oz, da imamo določen znesek na bančnem računu, brez razkrivanja občutljivih osebnih podatkov. Kriptovalute kot Monero in Zcash uporabljajo ZKPs za dokazovanje veljavnosti transakcij, brez razkrivanja identitete pošiljatelja, prejemnika ali vrednosti poslanega zneska. Projetki kot Idemix [2] uporabljajo ZKPs kot orodoje za operiranje nad osebnimi podatki na dokumentih izdanih z strani organizaciji oz avtoritet.

ZKP sistemi obstajajo za vrsto matematičnih problemov. V našem avtentiakcijskem sistemu, bomo uporabili ZKP sistem za problem kvadratnih ostankov.

4 Dizajn Avtentikacijskega Sistema in EAP Metode

Naš avtentikacijski sistem razširja ZKP sistem za problem kvardatnih ostankov z metodami razširjevanja ključev, kar onemogoča napade nad podatki, ki ji uporablja sam sistem za preverjanje gesla. Avtentikacijski sistem je dodatno definiran kot EAP metoda.

References

[1] Bernard Aboba, Larry Blunk, John Vollbrecht, James Carlson, Henrik Levkowetz, et al. Extensible authentication protocol (eap). 2004.

[2] Jan Camenisch and Els Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 21--30, 2002.

[3] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186--208, 1989.