Autentifikacija decentraliziranim verifikatorima zasnovana na znanju

Kristian Skračić
mentor: izv. prof. dr. sc. Mile Šikić
Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva

1. Uvod

Autentifikacija korisnika je ključan element svakog sigurnog informacijskog sustava. Većina modernih metoda autentifikacije korisnika se zasniva na statičkim podacima kao što su lozinke i biometrijski predlošci, ili se koriste posebnim uređajima za proizvodnju jednokratnih lozinki. Cilj ovog istraživanja je stvoriti metodu autentifikacije korisnika koja zadovoljava sljedeće uvijete:

- Presretanjem ispravnog odgovora napadač ne može iskoristiti za iduću prijavu,
- Korisnik unaprijed ne može znati niti pitanje niti odgovor,
- Ispravan odgovor se ne može pogoditi uporabom javno dostupnih informacija.

2. Opis problema

U ostvarivanju navedenih cilja potrebno je riješiti problem postizanja dogovora oko autentičnosti korisnika u sustavu s decentraliziranim verifikatorima, te problem automatske proizvodnje verifikatora zasnovanih na znanju.

3. Metodologija

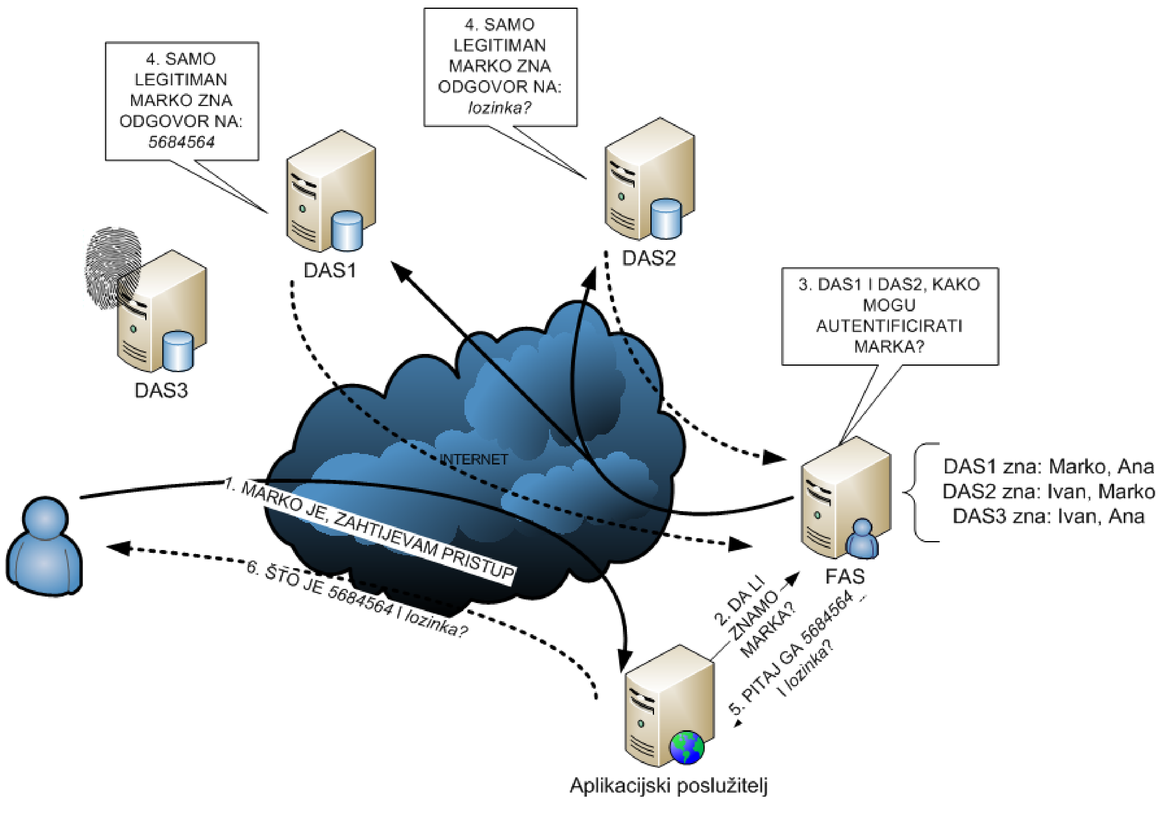
Problem postizanja dogovora oko autentičnosti korisnika u sustavu s decentraliziranim verifikatorima riješen je razvojem raspodijeljenog protokola za sigurnu razmjenu. Protokol se sastoji od tri glavna elementa:

- **Klijent** koji pokreće zahtjev za autentifikaciju,
- **FAS** (Front-end Authentication Server) primarni čvor koji upravlja komunikacijom,
- **DAS** (Distributed Authentication Server) koji sadrži verifikatore za autentifikaciju korisnika.

Problem automatske proizvodnje verifikatora zasnovanih na znanju riješit će se izradom generičkog modela koji će moći obuhvatiti širok skup podataka iz raznih transakcijskih baza. Model će sadržavati sljedeće atribute:

- oznaku vremena u kojemu se događaj ili transakcija dogodila,
- lokaciju na kojoj se događaj ili transakcija dogodila,
- akcija koja opisuje tip događaja ili transakcije,
- količinu koja se pripisuje događaju ili transakciji.

Cilj je iz tako strukturiranih podataka proizvoditi jednokratne verifikatore na koje samo legitiman korisnik može dati točan odgovor.



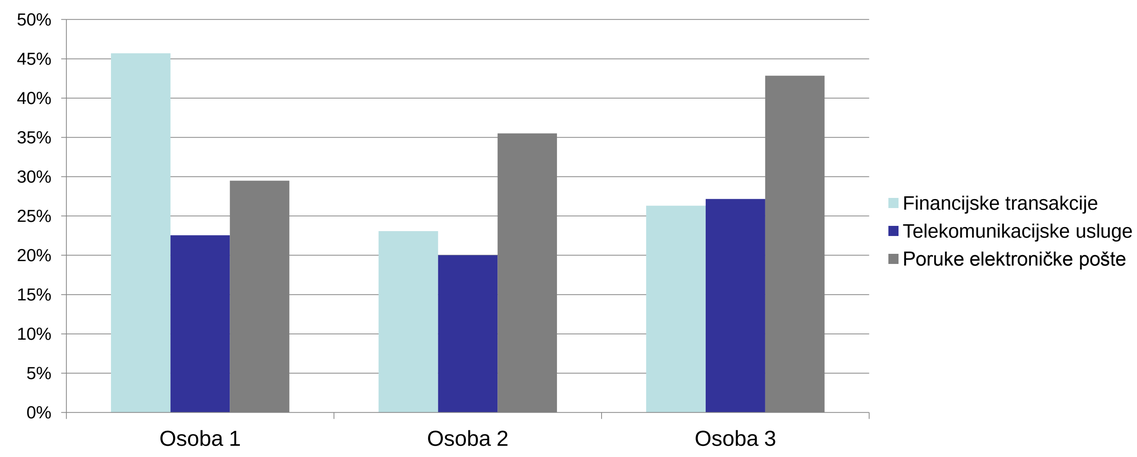
Skica protokola

4. Rezultati

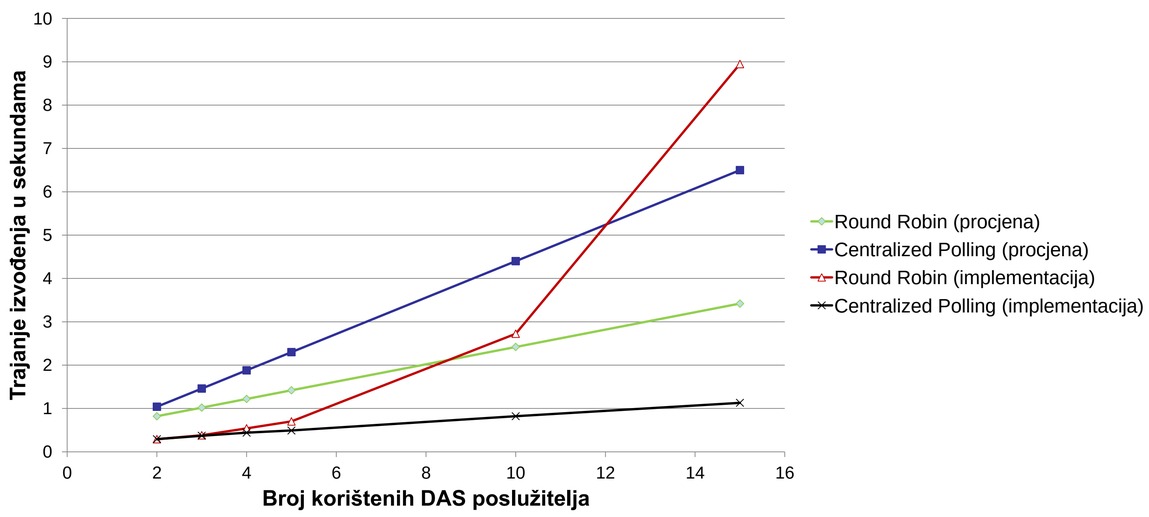
Preliminarni rezultati istraživanja pokazuju kako legitimni korisnici nisu u stanju ispravno odgovoriti na pitanja koja zahtijevaju:

- precizno prisjećanje događaja,
- svijest o frekvenciji pojavljivanja događaja.

Iz tog razloga će se daljnje istraživanje usmjeriti na postavljanje pitanja vezana uz najviše dva atributa iz generičkog modela. Također, iz dosadašnjih rezultata može se zaključiti kako je moć prisjećanja određenih događaja individualna.



Postotak točno odgovorenih pitanja



Usporedba izvođenja protokola u podržanim načinima rada

Razvijeni protokol ima dva načina rada:

- Kružno dodjeljivanje (**Round Robin**) u kojemu FAS samo inicijalizira postupak autentifikacije. Svaki DAS neovisno proizvodi verifikator i provjera korisnikov odgovor, i tek kada svi DAS poslužitelji daju svoj sud, FAS poslužitelj dobiva odgovor svih DAS poslužitelja,
- Centralizirano pozivanje (**Centralized Polling**) u kojemu FAS zasebno inicira autentifikaciju sa svakim DAS poslužiteljem.

Zanimljivo!

Podatci o ponašanju korisnika prikupljenih iz transakcijskih baza ne mogu se grupirati u skupine koje se značajno razlikuju po frekvenciji.

5. Zaključak

Preliminarni rezultati istraživanja pokazuju kako je moguće korisnike autentificirati temeljem znanja, no ujedno i da se treba u obzir uzeti uporabljivost konačnog rješenja. Razvijeni protokol omogućava autentifikaciju korisnika bez uporabe unaprijed razmijenjenih informacija, te osigurava tajnost i integritet digitalnog identiteta korisnika čak i u situacijama kada se autentifikacijski poslužitelj kompromitira.