Sustav aktivnog otkrivanja uljeza na sjedištu WWW.HR

Krešimir Pripužić, Denis Salopek, Valter Vasić, Marin Vuković

Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

CUC 2015, studeni 2015., Dubrovnik

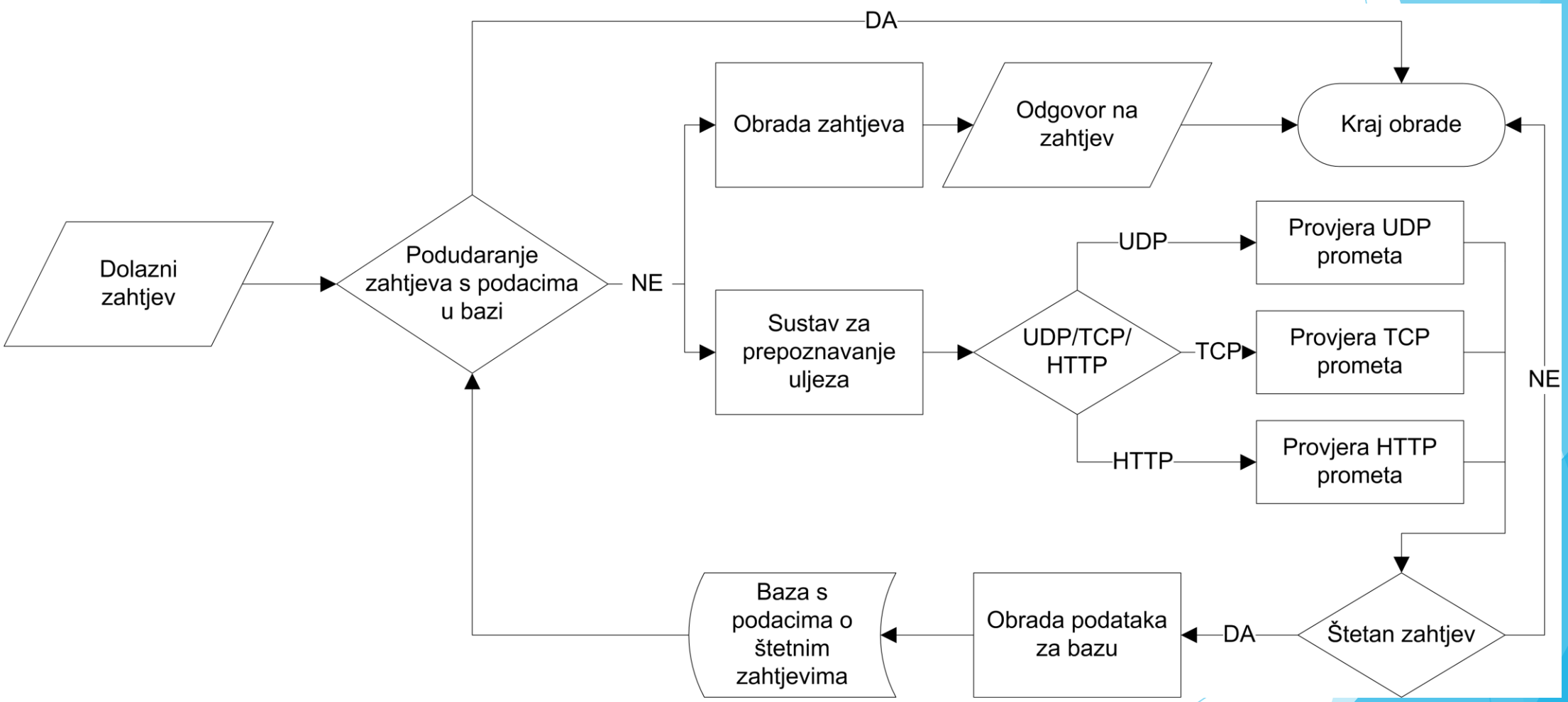
Uvod

- Prepoznavanje i filtriranje dolaznog mrežnog prometa na poslužitelju WWW.HR
  - Početna stranica Hrvatske već 20 godina
  - više od 20,000 aktivnih registiranih sjedišta
- Sustavi za otkrivanje uljeza u računalnom sustavu
  - Pasivni sustavi – sigurnosna stijena (engl. *firewall*)
  - Aktivni sustavi – IDS (engl. *Intrusion Detection Systems*)
- Cilj sustava:
  - Prepoznavanje nelegitimnog i neispravnog prometa upućenog na pokrenute servise
  - Jednostavna primjena sustava na druge poslužitelje

Prepoznavanje uljeza

- Problem filtriranja i tumačenja prometa koji dolazi do sjedišta
- Raspodjela dolaznog prometa na protokole:
  - Promet protokolom UDP
    - sav dolazni promet koji nije iniciran od strane poslužitelja
  - Promet protokolom TCP
    - sumnjivi sadržaj zaglavlja
  - Zahtjevi HTTP
    - dozvoljene metode dohvata, ispravnost zahtjeva i podaci u zaglavlju
- Potrebno je izuzeti automatizirane sustave za dohvat sadržaja (engl. *crawler*) Google, Bing, Yahoo

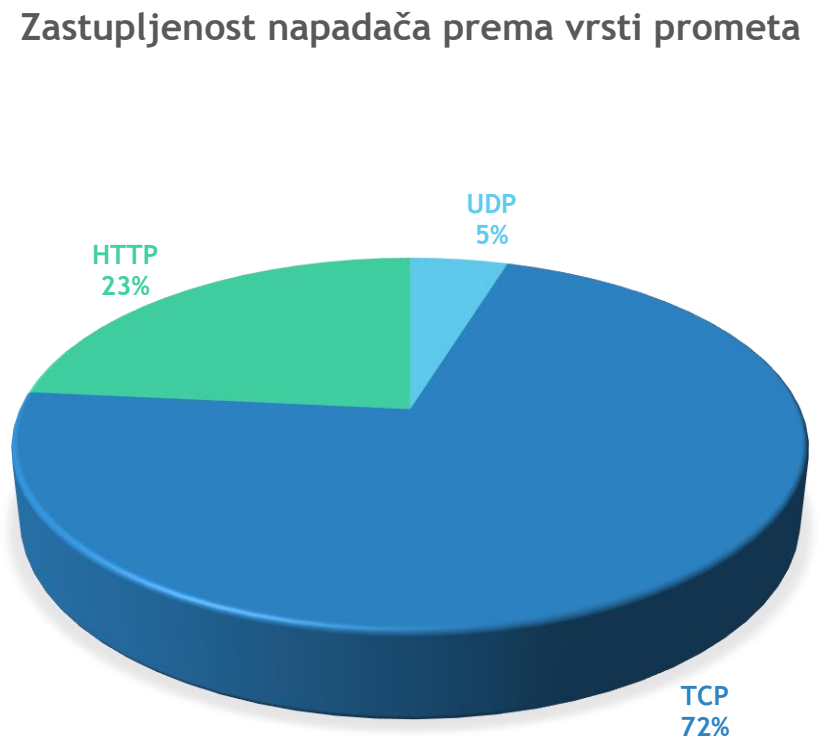
Sustav za prepoznavanje uljeza



Provjera dolaznog prometa

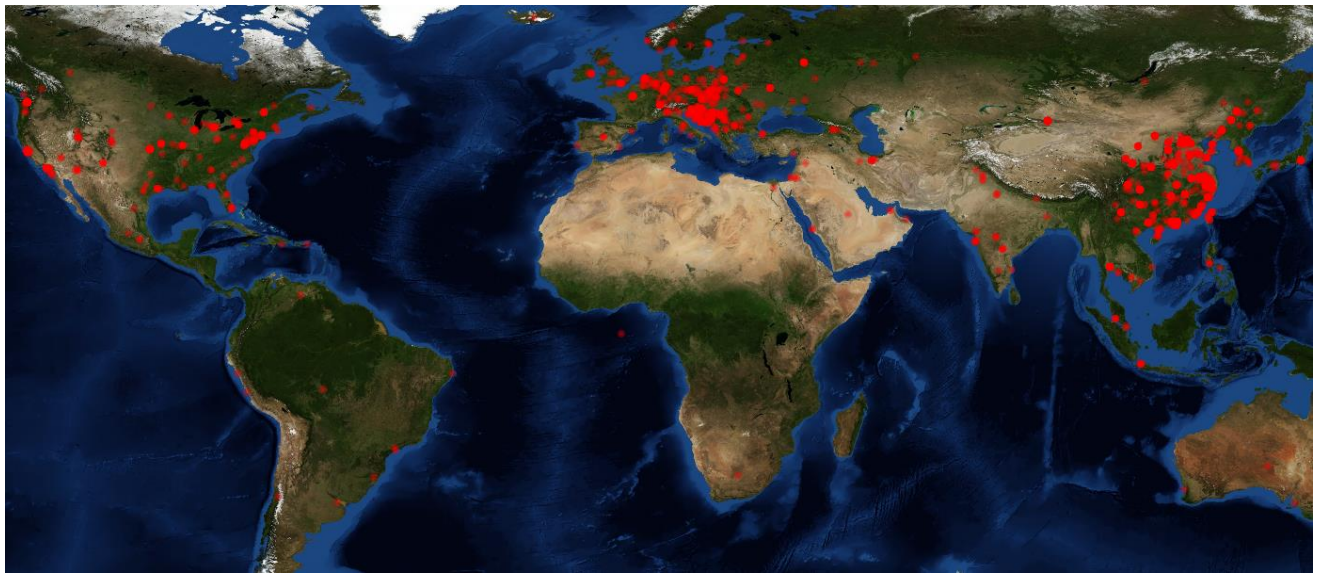
- Zahtjevi su štetni ako vrijedi jedna od sljedećih tvrdnji:
  - Zahtjevi koji dolaze protokolom **UDP**, a nisu inicirani od strane poslužitelja
  - Zahtjevi koji dolaze protokolom **TCP** s vrata koja su niža od 20000 – to upućuje na nestandardni softver koji je najčešće zloćudan
  - Zahtjevi protokolom **HTTP**:
    - koji nemaju popunjene sve potrebne podatke (polja Host, User-Agent) i ne koriste metode GET i POST na način predviđen na sjedištu WWW.HR
    - koji traže pristup administratorskom sučelju sustava za upravljanje sjedištima (CMS, engl. Content Management System) poput Wordpressa

Rezultati sustava za prepoznavanje uljeza



Analiza podataka o uljezima

- Podaci o uljezima su prikupljani u rasponu od jednog tjedna
- Provedena je gelokacijska analiza prikupljenih podataka
  - Europa (središnja i sjeverna), Kina, zapadna i istočna obala SAD-a



Zaključak

- Omogućeno je sprječavanje i bilježenje mrežnih napada na poslužitelj WWW.HR
- Metodologija je primjenjiva za druga sjedišta
- Moguće je pratiti i spriječiti sav neželjeni i štetan promet
- Uz standardne napade moguće je detektirati i nove vrste nelegitimnog prometa upućenog prema sjedištu
  - Veća razina sigurnosti od standardnih rješenja za aktivno otkrivanje uljeza
- Naknadnom obradom prepoznatog štetnog prometa mogu se identificirati novi mehanizmi za otkrivanje uljeza