Sigurnost operacijskih sustava i aplikacija

Stabla napada

Ian Marković, 11.4.2025.

Pregled predavanja

- Pitanja za ispite
- Motivacija
- O stablima napada
- Metrike prijetnji pomoću stabla napada
- Varijacije i primjene
- Zaključak
- Literatura

Pitanja za ispite

- Što je stablo napada i po čemu se razlikuje od grafa napada
- Nabrojite prednosti modela stabla napada nad drugim modelima prijetnja
- Objasnite strukturu stabla napada
- Opišite načine definiranja metrika napada u stablu napada
- Napravite primjer jednostavnog stabla napada koristeći kontinuirane vrijednosti čvorova te označite najefektivniji put po tim svojstvima

Motivacija

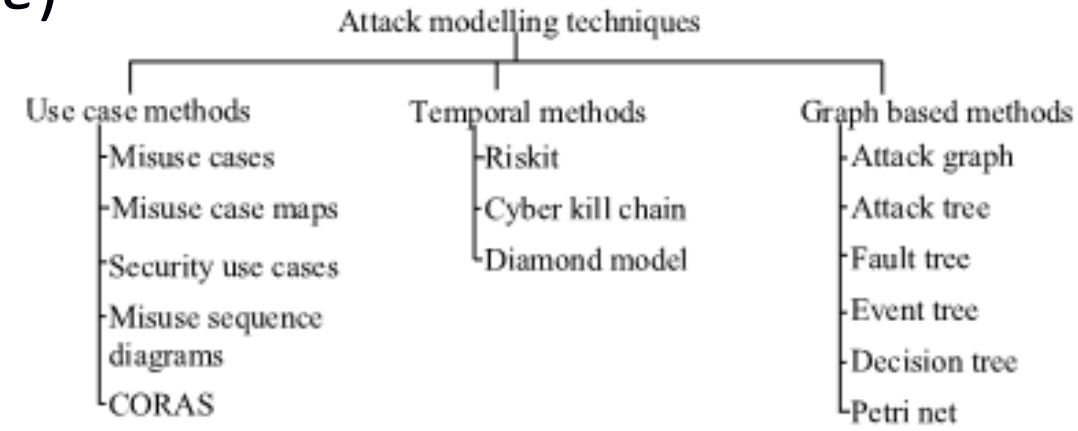
- Napadači neće uvijek koristiti samo očite napade
- Napadi u prilici
- Razvojem kompleksnosti napada i protumjera potrebni su sustavi za pregledni prikaz oboje
  - Kognitivna efikasnost

Motivacija

- Tražena svojstva modela prijetnji
  - Potpuna pokrivenost ciljeva i načina realizacije napada na sustav
  - Shvaćanje koji napadi su više vjerojatni
  - Saznati koje su sigurnosne pretpostavke sustava i gdje se fokusirati pri njegovom dizajnu
  - Jednostavna i skalabilna preglednost modela

Modeliranje prijetnji [2]

- Modeliranje događaja koji vode do napada
- Tri generalne kategorije
  - Modeli bazirani na grafovima (*graph based)*
  - Fokus na vrijeme (*temporal perspective*)
  - Slučaj primjene (*use-case)*



Slika 1. Pregled kategorija tehnika modeliranja prijetnji [2]

Što je stablo napada? [1]

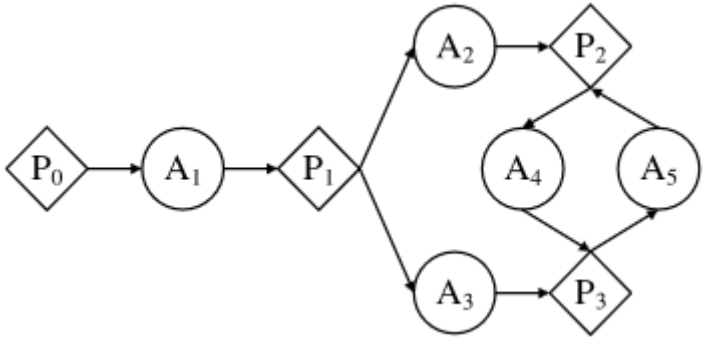
- Prikaz napada i protumjera u strukturi stabla
- Proizlazi iz analize međusobne zavisnosti napada
- Pripada kategoriji modela prijetnji baziranih na grafovima
  - Podskup grafova napada

Zašto stablo napada?

- Prednosti
  - Može se definirati za više različitih ciljeva
  - Grananjem pokriva sve moguće putove do ostvarenja cilja napadima
  - Pruža jednostavan pregled mogućih koraka do ostvarenja cilja
  - Lagano se proširi za dodatne putove i napade (podstabla)
- Par nedostataka
  - Postane relativno nepregledno pri povećanju kompleksnosti
  - Jednostavnost otežava definiranje kompleksnijih napada

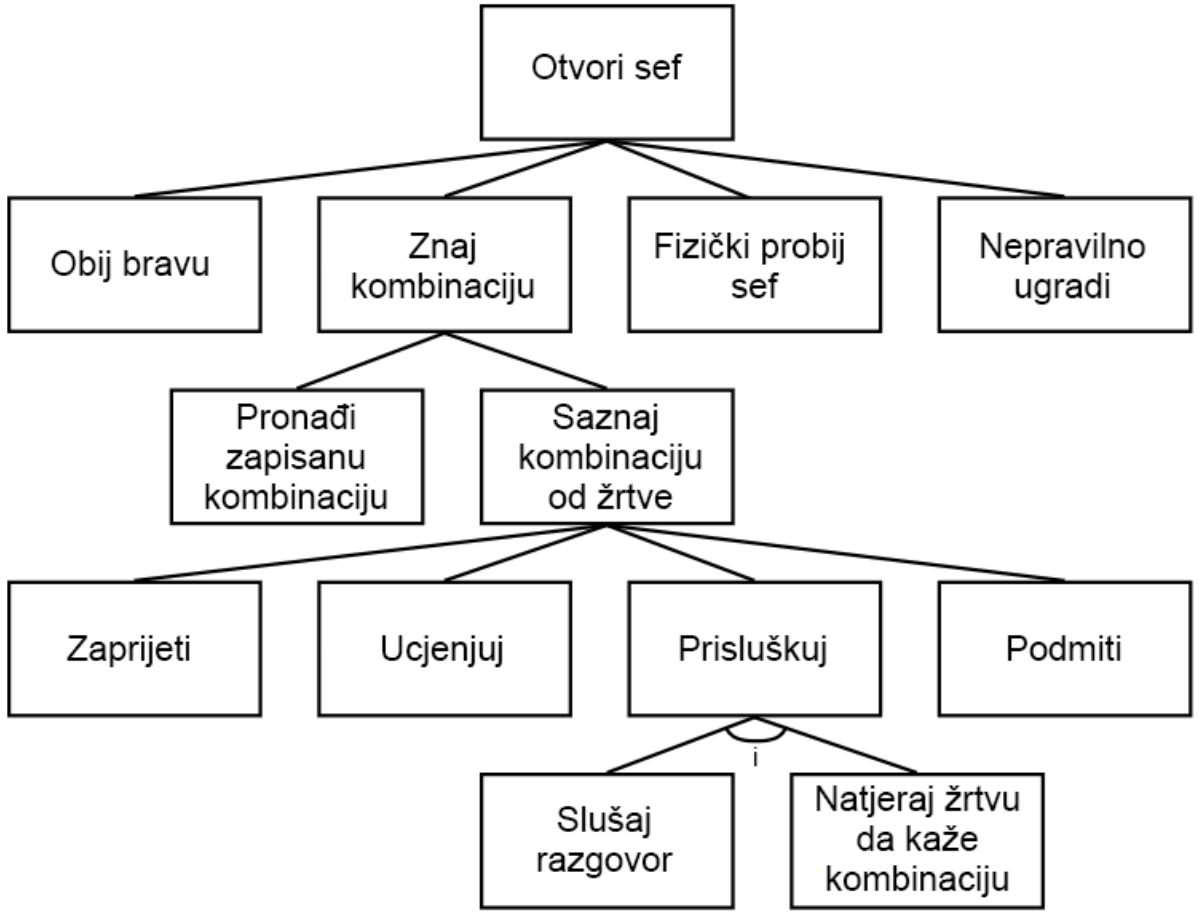
Stablo i graf napada

- Graf napada je najopćenitiji oblik modela prijetnji baziranog na grafu
- Grafovi napada imaju proširenu definiciju
  - Koriste različite oblike i oznake za razlikovanje ranjivosti i preduvjeta
  - Mogu imati više od jednog roditelja
  - Mogu biti ciklički



Slika 2. Primjer cikličkog **grafa** napada [2]

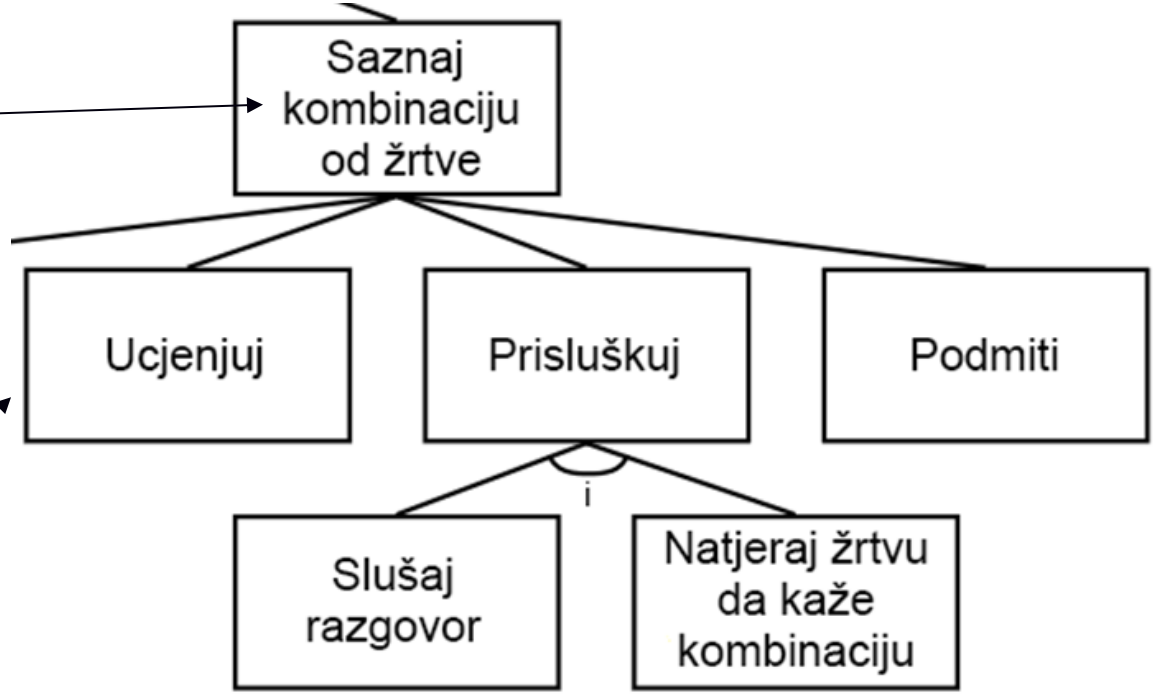
Jednostavan primjer stabla



Slika 3. Jednostavan primjer stabla napada [1]

Jednostavan primjer stabla

- Naziv i opis napada
- Napadi koji vode do saznavanja kombinacije
- Napadi koje se mora izvršiti za ostvarivanje prisluškivanja



Slika 3.1 Isječak iz primjera jednostavnog stabla napada (Slika 3)

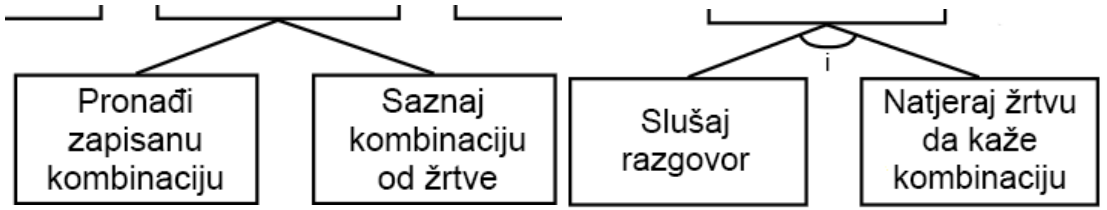
Struktura

- Korijenski čvor je cilj napada
- Listovi su pod-napadi ili preduvjeti koji služe kao koraci do izvršavanja napada čvora roditelja
- Bridovi prikazuju smjer tijeka ostvarivanja cilja kroz povezane napade

Pravila i sintaksa

- Dvije vrste poveznica
  - „ili” poveznica – različiti putevi ostvarenja napada čvora roditelja
  - „i” poveznica – oba napada listova moraju biti ostvareni za ostvarenje napada čvora roditelja
- Svaka dva čvora su međusobno povezana samo jednim putem
  - Svaki čvor ima točno jednog roditelja
- Neusmjereni bridovi

Slika 4. Primjeri poveznica [1]



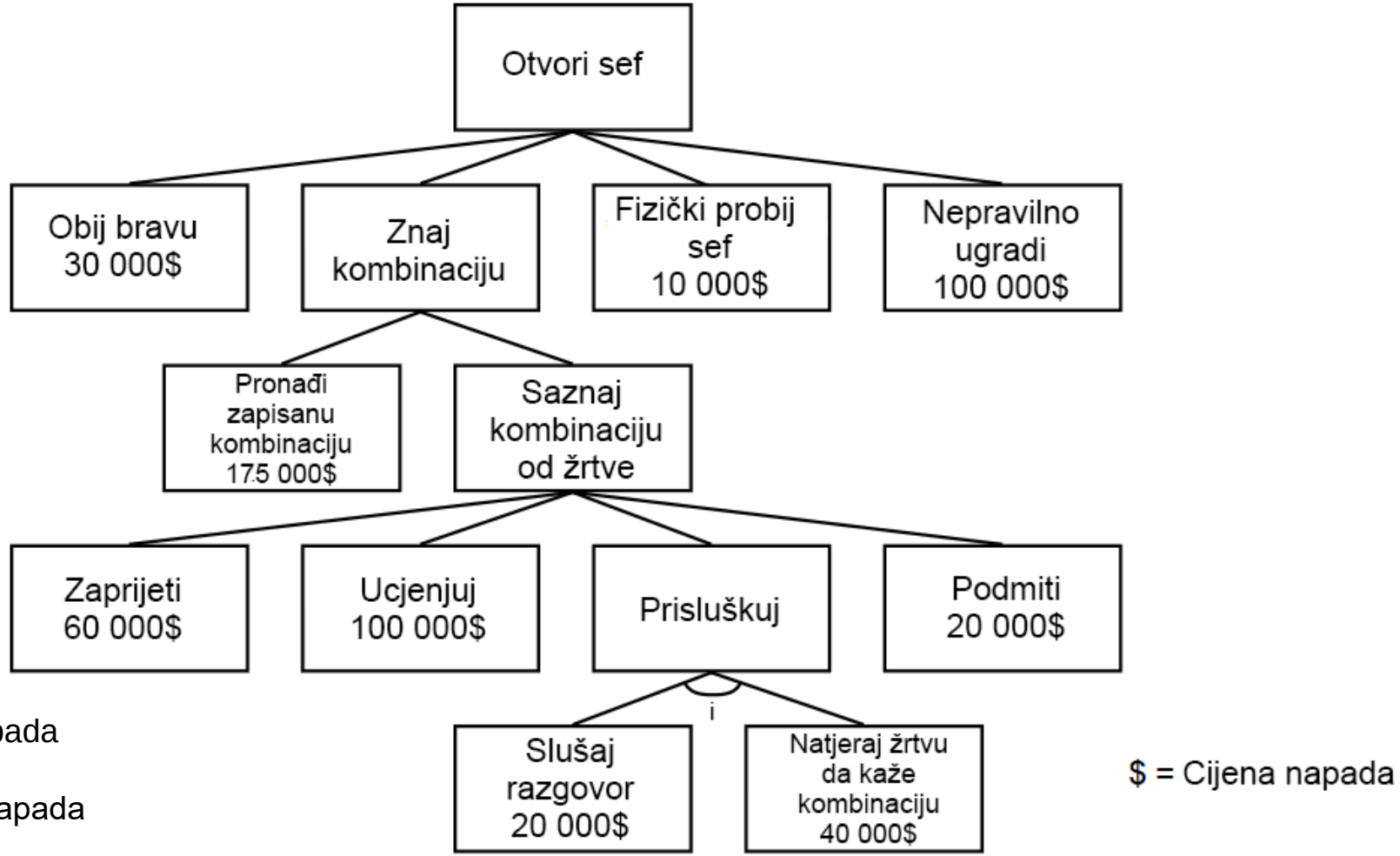
Vrijednosti čvorova

- Opcionalne vrijednosti za kasniju analizu
- Definiranje ovisno o napadačima koje trenutno analiziramo
  - Vrijednosti onda opisuju njihove vještine i sredstva
- Definiranje relativno obrani
  - Vrijednosti onda služe za generalnu prioritizaciju obrane (npr. po cijeni)

Vrste vrijednosti

- Booleove vrijednosti
  - Logičke vrijednosti
  - Jesu li potrebna posebna sredstva, je li legalno, …
- Kontinuirane vrijednosti
  - Numeričke vrijednosti
  - Potrebno vrijeme, cijena izvedbe/obrane, …

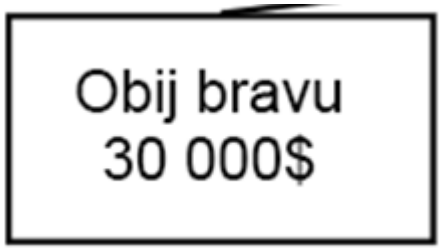
Primjer stabla sa kontinuiranim svojstvima



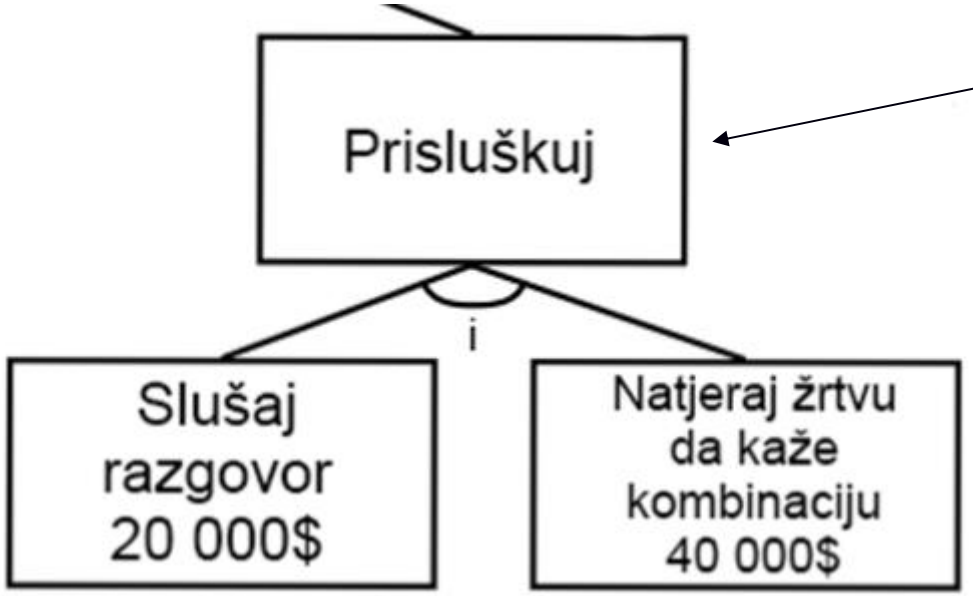
Slika 4. Primjer stabla napada sa vrijednostima cijena ostvarenja pojedinačnih napada [1]

Primjer stabla sa kontinuiranim svojstvima

- Kontinuirana vrijednost čvora, označava cijenu potrebnu za izvršiti napad



Slika 4.1 Čvor iz primjera stabla napada (Slika 4)



- Ovdje je cijena za prisluškivanje zbroj oba napada djeteta -> 60 000$

Slika 4.2 „i” poveznica iz primjera stabla napada (Slika 4)

Skalabilnost

- Svaki dio stabla može se analizirati kao zasebno podstablo
- Podstabla manjih napada
- Jednostavna usporedba napada po svojstvima korijena njihovih podstabala

Konstruiranje stabla napada

- Korak 0: Identificirati ciljeve napadača
  - Ciljevi mogu biti više korijena ili zasebna pod-stabala
- Korak 1: Postepeno identificirati napad koji vodi do ostvarenja cilja
  - Krećemo se od korijena prema listovima
- Korak 2: Dodati postojeća stabla kao pod-stabla

Metrike prijetnji [3]

- Potrebna metrika za usporedbu različitih napada
  - Npr. koji je napad vjerojatniji za pokušati od slučajnih ili specifičnih napadača
- Važnost metrike zbog nepreciznosti ulaznih podataka modela
  - Moramo znati gdje je slaba sigurnost neovisno o napadaču

Put napada

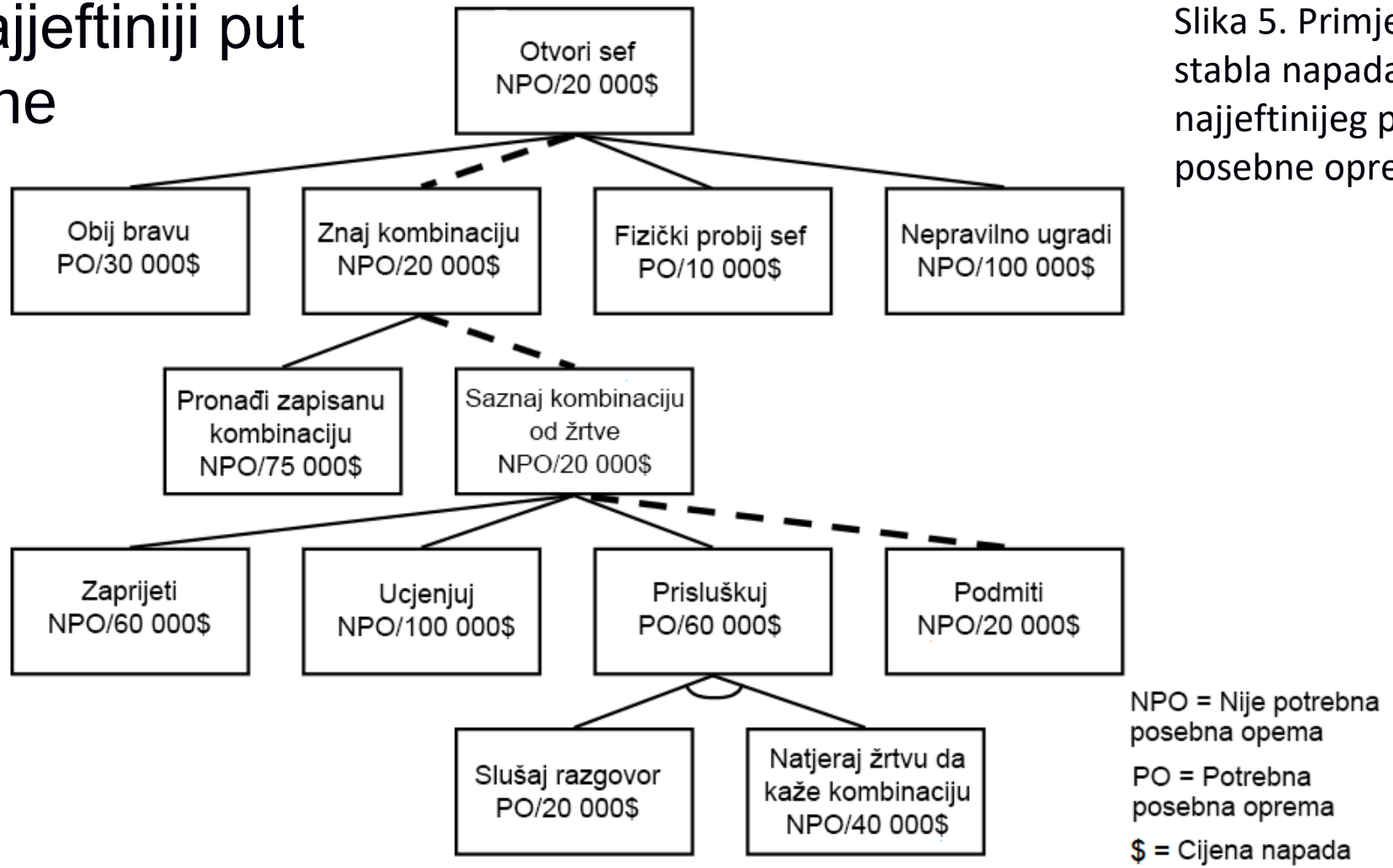
- Put od krajnjeg lista do korijena stabla
- Predstavlja jedan način ostvarenja cilja kroz uzastopne napade
- Ako je put uspješan znači da je obrana na svakom čvoru puta bila neuspješna
  - Preglednost pri biranju gdje treba pojačati obranu
- Mogu biti različitih duljina

Metrika prijetnji u stablu napada

- Stablo napada pruža intuitivnu metriku prijetnje
- Booleove vrijednosti – pronalazimo sve puteve koji vode kroz čvorove sa samo traženom vrijednošću
- Kontinuirane vrijednosti – tražimo put sa najvećom ili najmanjom sumom

Primjer analize potpunog stabla napada

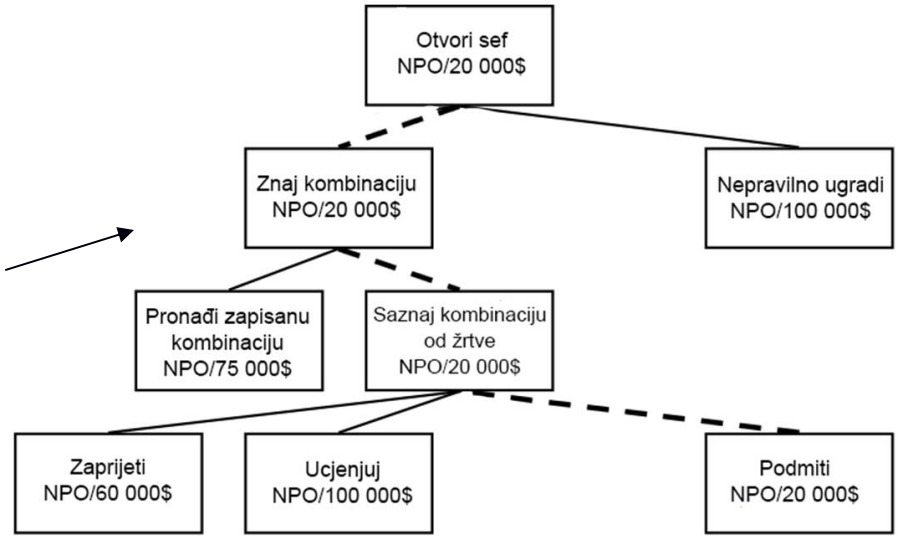
- Tražimo najjeftiniji put bez posebne opreme



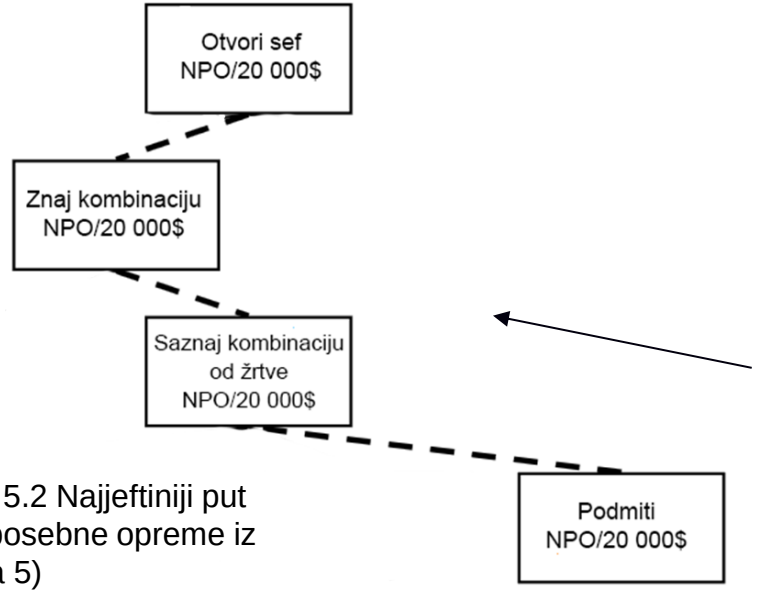
Slika 5. Primjer potpunog stabla napada i analiza najjeftinijeg puta napada bez posebne opreme [1]

Primjer analize potpunog stabla napada

1. Uočimo sve putove napada koje je moguće izvršiti bez posebne opreme



Slika 5.1 Putevi bez posebne opreme iz (Slika 5)



Slika 5.2 Najjeftiniji put bez posebne opreme iz (Slika 5)

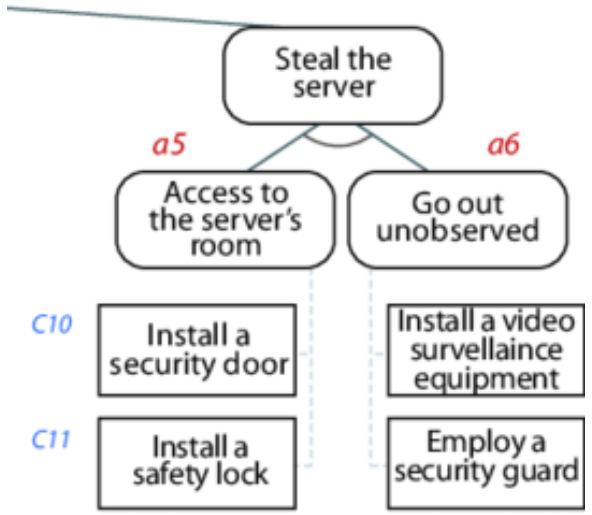
2. Pronađemo put koji napadača košta najmanje za izvršiti

Problemi

- Svaki čvor ne sadrži sve potrebne vrijednosti ili su teški za odrediti
  - Kako odrediti vrijeme potrebno za prisluškivanje razgovora
- Kompleksnost pri dodavanju novih zahtjeva
  - Sakupi se puno vrijednosti na čvorovima

Varijacije stabla napada

- Stablo obrane [5]
  - Dodatni pod-čvorovi metoda obrane od napada u listovima stabla



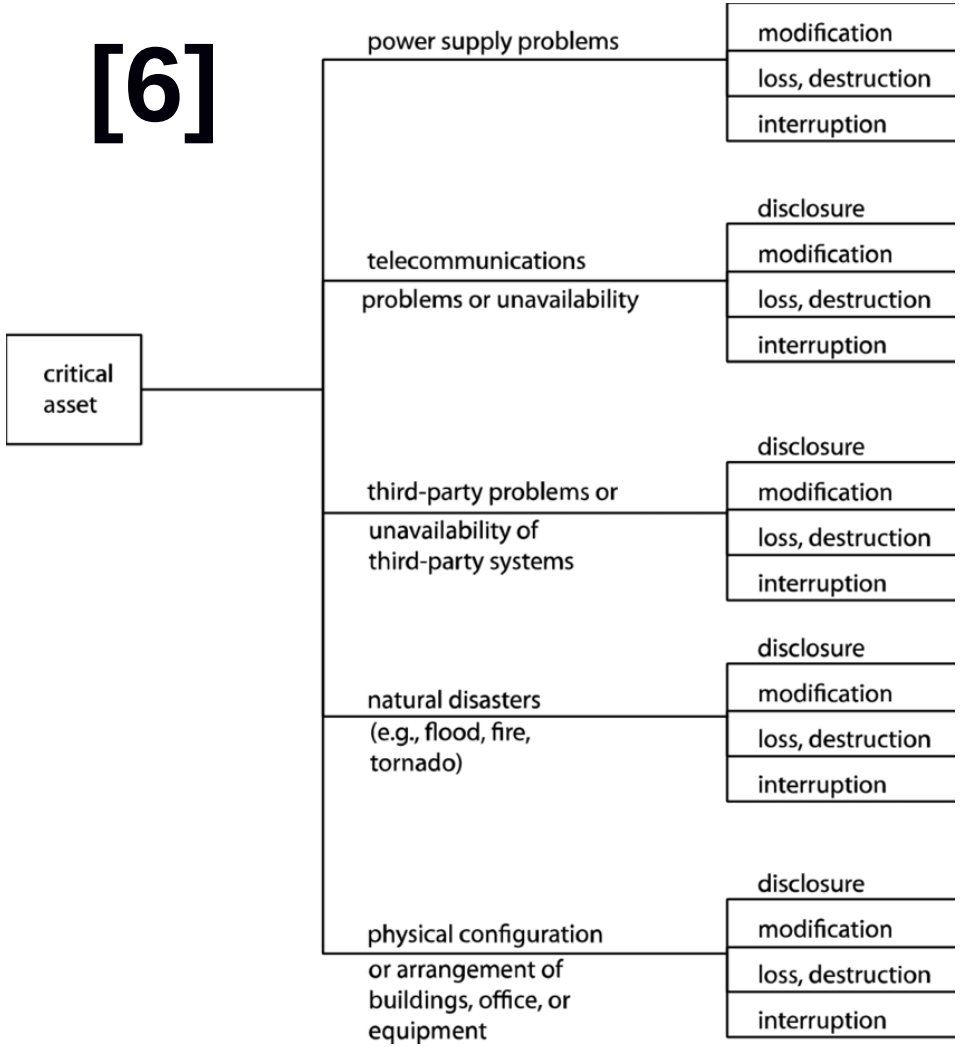
Slika 6. Isječak iz stabla obrane

Stabla prijetnji [4]

- Općenitiji koncept stabla napada
  - Stabla napada su proizašli iz njih
- Prikazuje prijetnje umjesto napada
- Preferirani u primijenjenim modelima prijetnji

Primjena: OCTAVE [6]

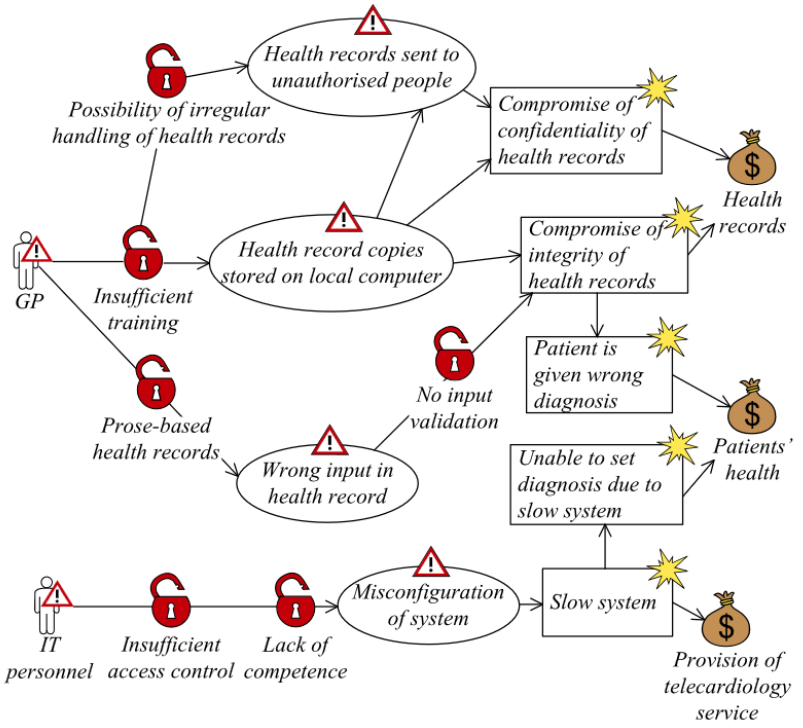
- Jedna od razvijenih metoda identificiranja informacijskih sigurnosnih rizika
- Koristi stabla prijetnji, varijaciju stabla napada



Slika 7. Primjera stabla prijetnji korištenog u OCTAVE pristupu [6]

Primjena: CORAS [7]

- Generaliziran pristup za obrambenu analizu rizika
- Također koristi stablo prijetnji, uz olakšanje pravila jednog roditelja



Slika 8. Primjer stabla prijetnji korištenog u CORAS pristupu [7]

Zaključak

- Stabla napada su moćni modeli za pokrivanje mogućih napada i prijetnji na sustav
- Spajaju jednostavnost i intuitivnost sa efektivnim izračunom potrebne metrike za analizu sigurnosnih rizika
- Jedini nedostatak su kompleksnost i ograničenja koji proizlaze iz jednostavnosti modela

Literatura

1. Schneier, Bruce. "Attack trees." *Dr. Dobb's journal* 24.12 (1999): 21-29. *(jedna od najranijih obrada teme)*
2. Lallie, Harjinder Singh, Kurt Debattista, and Jay Bal. "A review of attack graph and attack tree visual syntax in cyber security." Computer Science Review 35 (2020): 100219.
3. Homer, John, et al. "Aggregating vulnerability metrics in enterprise networks using attack graphs." Journal of Computer Security 21.4 (2013): 561-597.
4. Amoroso, Edward G. Fundamentals of computer security technology. Prentice-Hall, Inc., 1994.

Dodatna literatura

5. (stabla obrane)
   Bistarelli, Stefano, Pamela Peretti, and Irina Trubitsyna. "Analyzing security scenarios using defence trees and answer set programming." *Electronic Notes in Theoretical Computer Science* 197.2 (2008): 121-129.
6. (OCTAVE pristup)
   Caralli, Richard A., et al. "Introducing octave allegro: Improving the information security risk assessment process." Hansom AFB, MA (2007).
7. (CORAS pristup)
   Lund, Mass Soldal, Bjørnar Solhaug, and Ketil Stølen. „Model-driven risk analysis: the CORAS approach.” Springer Science & Business Media, 2010.

Hvala!