SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 6:

Sistemi za otkrivanje i sprečavanje upada

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Sistemi za otkrivanje i sprečavanje upada

- Sadržaj poglavlja i predavanja:
  - 6.1 Sistemi za otkrivanje upada (IDS)
  - 6.2 Teorija sistema za otkrivanje upada
  - 6.3 Sistemi za sprečavanje upada (IPS)
  - 6.4 Primena sistema sa veštačkom inteligencijom

Quote

"Keep your friends close and your enemies even closer"

The Art of War by Sun Tzu

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

Sistemi za otkrivanje i sprečavanje upada

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)

Šta je upad (engl. *intrusion*)

- Jim Anderson - u ranim osamdesetim godinama dvadesetog veka
- Anderson definiše **upad kao svaki neovlašćen pokušaj da se informacijama pristupi, manipuliše, da se one izmene ili unište, ili da se sistem učini nepouzdanim ili neupotrebljivim**
- Sistem za detekciju upada pokušava da otkrije ovakav tip aktivnosti

6.1 Sistemi za otkrivanje upada (IDS)

- Podela
- Karakteristike
- Teorija
- Primeri

Podela IDS sistema

- Kriterijum podele: **šta se detektuje**?
  - Detekcija zloupotreba (engl. *misuse intrusion detection*)
  - Detekcija anomalija (engl. *anomaly intrusion detection*).

- Kriterijum podele: **gde je sistem smešten**?
  - IDS koji je smešten na računaru i štiti taj računar (engl. *host based IDS*, HIDS)
  - Mrežni IDS (engl. *network based IDS*, NIDS)
  - Aplikativni IDS

Podela IDS sistema...

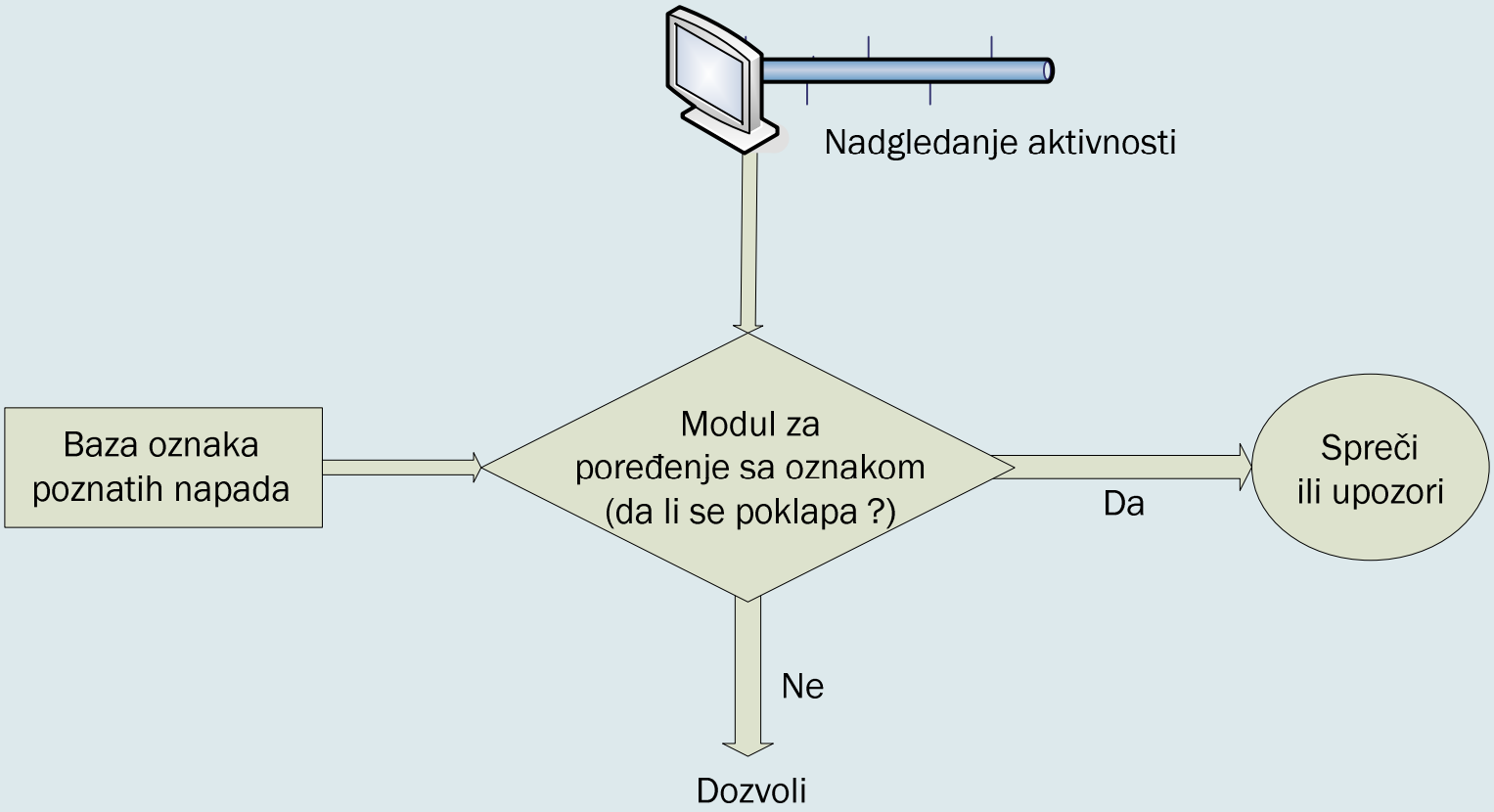
- Kriterijum podele: **kada je napad otkriven**?
  - U realnom vremenu (engl. *real time*) i
  - Naknadno, tj. nakon dešavanja (engl. *after the fact*, *post-mortem*).

- Kriterijum podele: **reakcija na napad**
  - Pasivni sistemi
  - Reaktivni sistemi

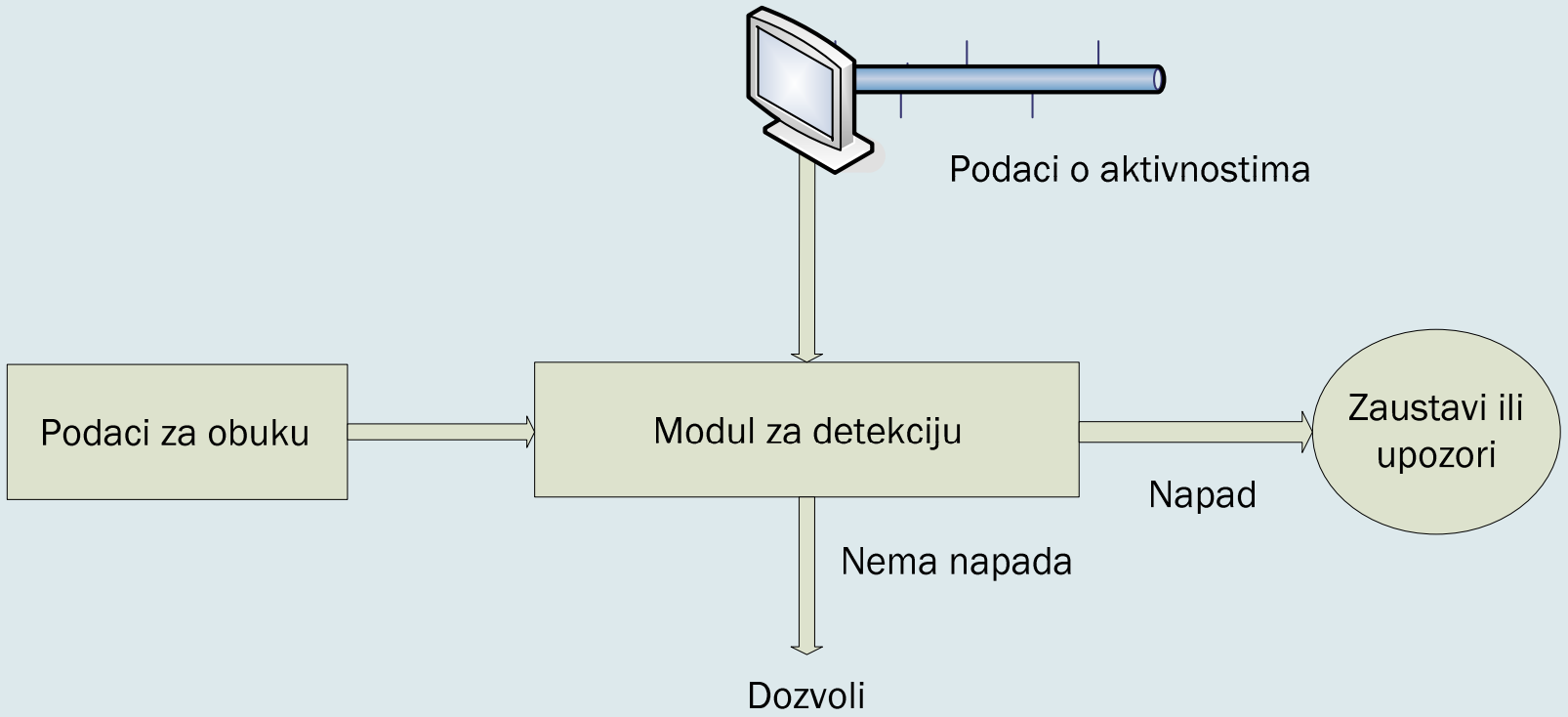
Kriterijum podele: šta se detektuje?

- Detekcija zloupotreba (engl. *misuse intrusion detection*)
- Detekcija anomalija (engl. *anomaly intrusion detection*).

Sistem za detekciju zloupotreba



Sistem za detekciju anomalija



Kriterijum podele: gde je sistem smešten?

- IDS koji je **smešten na računaru** i štiti taj računar (engl. ***host based IDS***, HIDS)
- **Mrežni** IDS (engl. ***network based IDS***, NIDS)
- **Aplikativni** IDS

Kriterijum podele: kada je napad otkriven?

- **U realnom vremenu** (engl. *real time*) i
- **Naknadno,** tj. nakon dešavanja (engl. *after the fact*, *post-mortem*).

Kriterijum podele: reakcija na napad

- **Pasivni** sistemi
- **Reaktivni** sistemi

Faze odgovora na napad prema Bishopu

- Priprema (engl. *preparation*)
- Identifikacija (engl. *identification*)
- Ograđivanje (engl. *containment*)
- Iskorenjivanje (engl. *eradication*)
- Oporavak (engl. *recovery*)
- Nastavak (engl. *follow-up*)

* Matt Bishop, "Computer Security: Art and Science", Addison Wesley Professional, 2003

Postojeći sistemi za detekciju upada

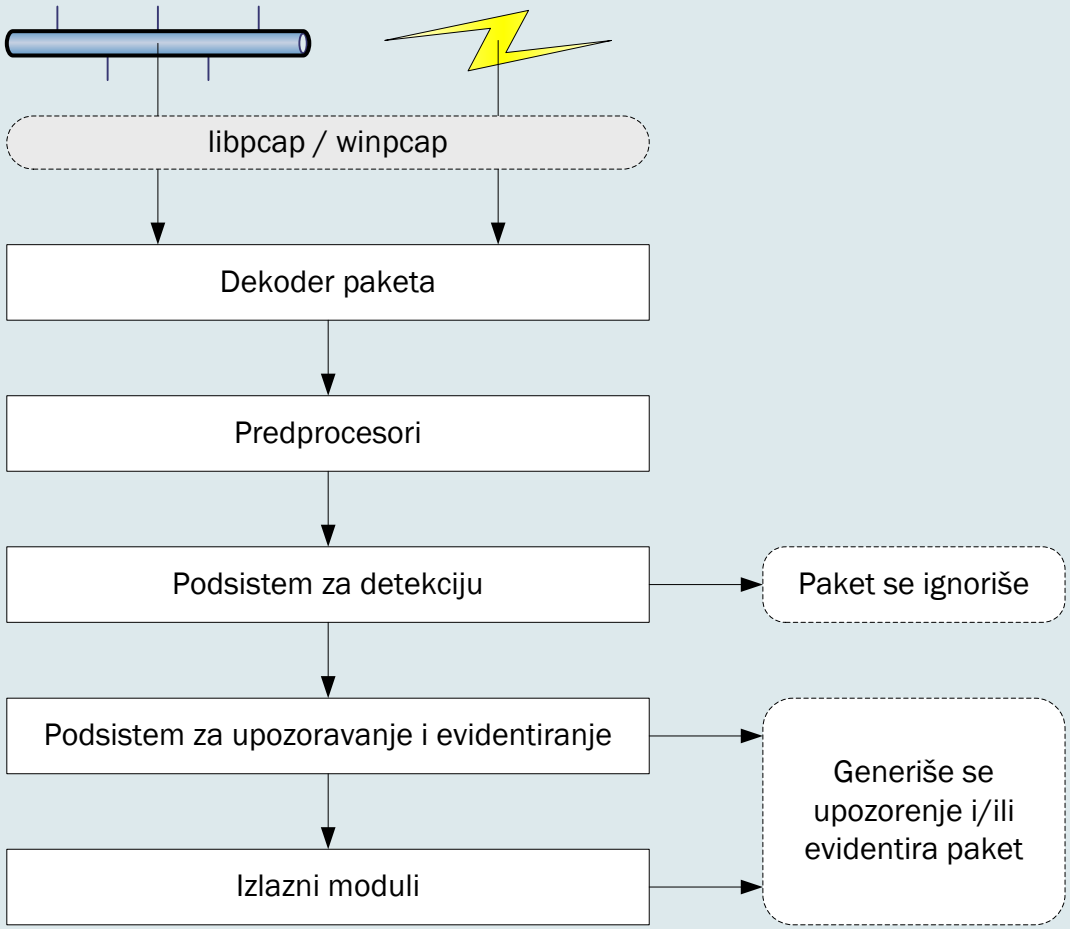
- Najjednostavniji sistemi za detekciju upada su monitori dnevničkih datoteka (engl. *Log File Monitors*)
  - SWATCH, što je skraćenica od Simple WATCHer
- Monitor integriteta (engl. *integrity monitor*)
  - Tripwire
- Skeneri "potpisa" (engl. *signature scanners*)
  - Snort
  - Snort Wireless

Postojeći sistemi za detekciju i prevenciju upada…

- IBM
- Cisco
- Juniper
- TippingPoint
- McAfee
- Enterasys Dragon
- Network Chemistry
- Airdefense

- WIDZ
- Garuda (open source)
- …

Snort - Komponente



IDS sistemi…

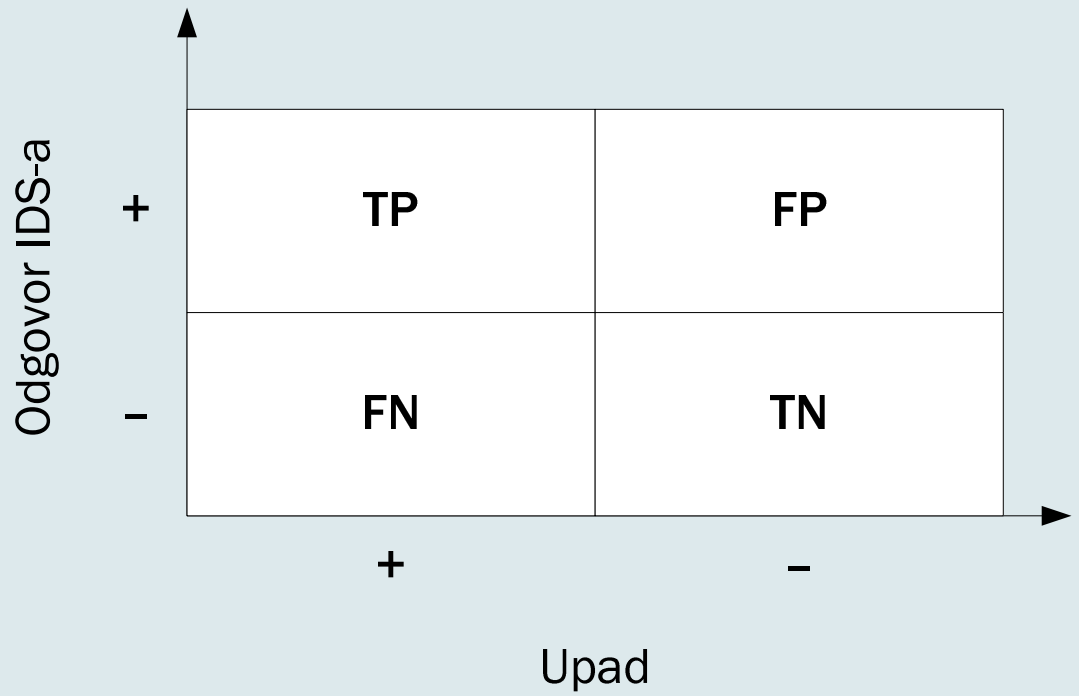
- Snort
  - www.snort.org
- Snort Wireless
  - www.snort-wireless.org
- Fortego All-Seeing Eye
  - www.fortego.com/en/ase.html

- Više na vežbama

6.2 Teorija sistema za otkrivanje upada

- Osetljivost
- Određenost
- Tačnost

Dijagram reakcije IDS-a na aktivnosti



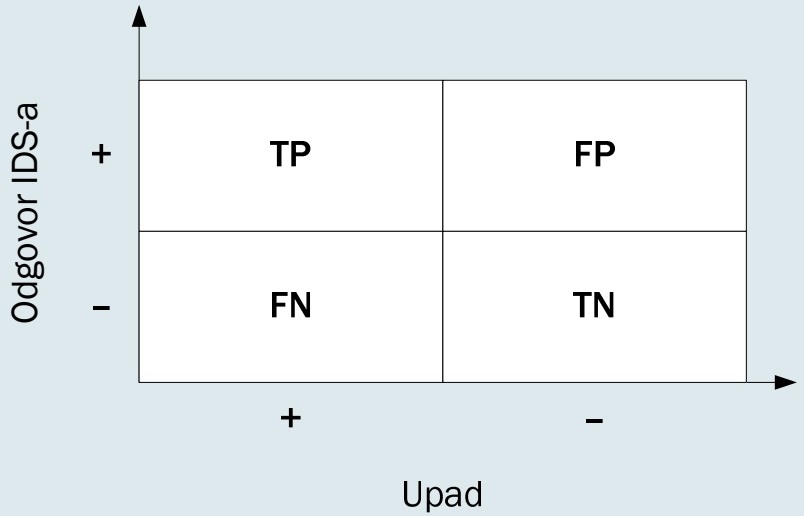
Reakcija IDS-a na aktivnosti

- TP (***True Positive***, pravi alarm) označava da je upad ispravno detektovan, tj. da je IDS otkrio napad koji se stvarno desio.
- FP (***False Positive***, lažni alarm) označava da je IDS detektovao nepostojeći napad, tj. da do napada nije došlo, a da je IDS tekuću legitimnu aktivnost registrovao kao napad (takozvani).
- FN (***False Negative***, propušten alarm) označava da je IDS propustio da detektuje napad, tj. da je do napada došlo a da IDS to nije registrovao.
- TN (***True Negative***, ispravno legitiman) označava da IDS nije detektovao nepostojeći napad, tj. da je tekuću aktivnost korektno registrovao kao aktivnost iz skupa dozvoljenih aktivnosti.

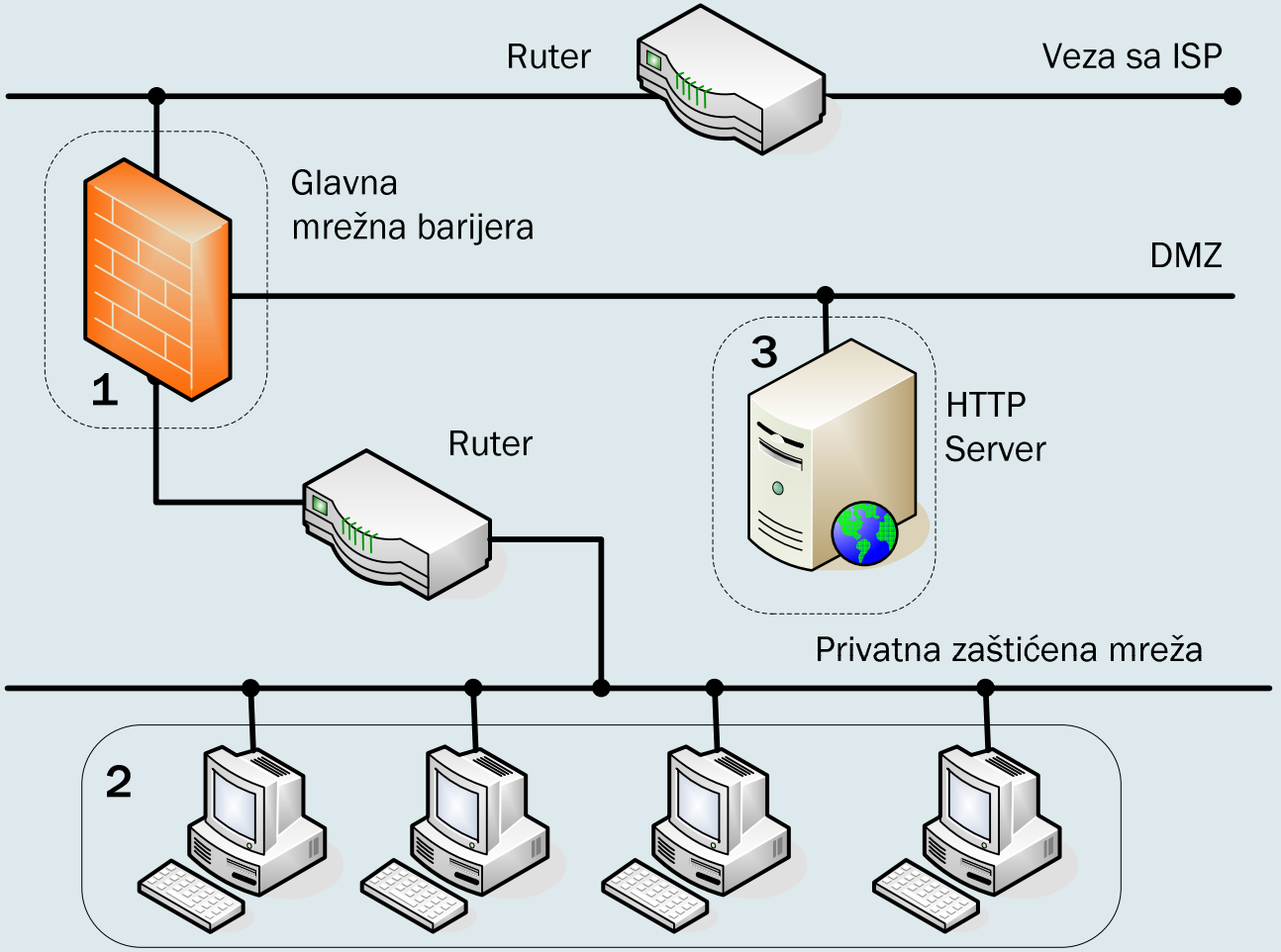
Osetljivost (engl. *sensitivity*)

- Osetljivost = TPR = TP / (TP + FN)

- Učestalost propuštenih alarma (engl. *false negative rate*)
  - FNR = FN / (TP + FN) = 1 – TPR = 1 – osetljivost.

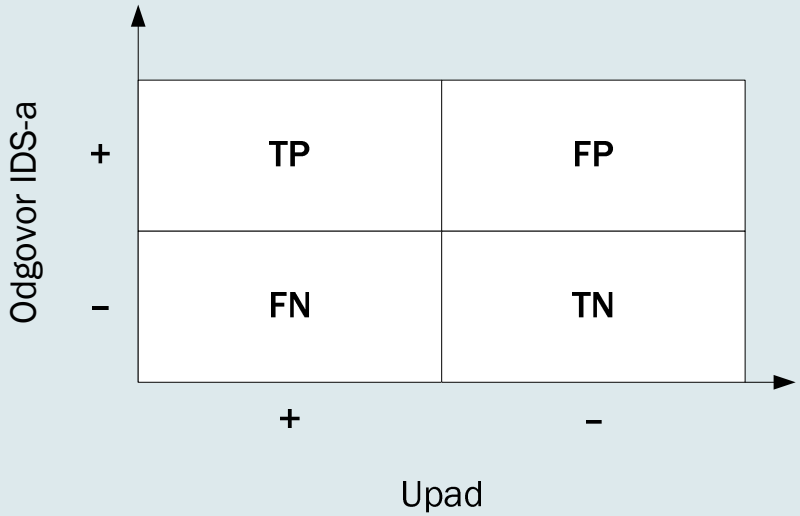


IDS visoke osetljivosti



Određenost (engl. *specificity*)

- Određenost = TNR = TN / (TN + FP)
- Učestalost lažnih alarma (engl. *False Positive Rate*)
  - FPR = FP / (TN + FP) = 1 – TNR = 1 - određenost



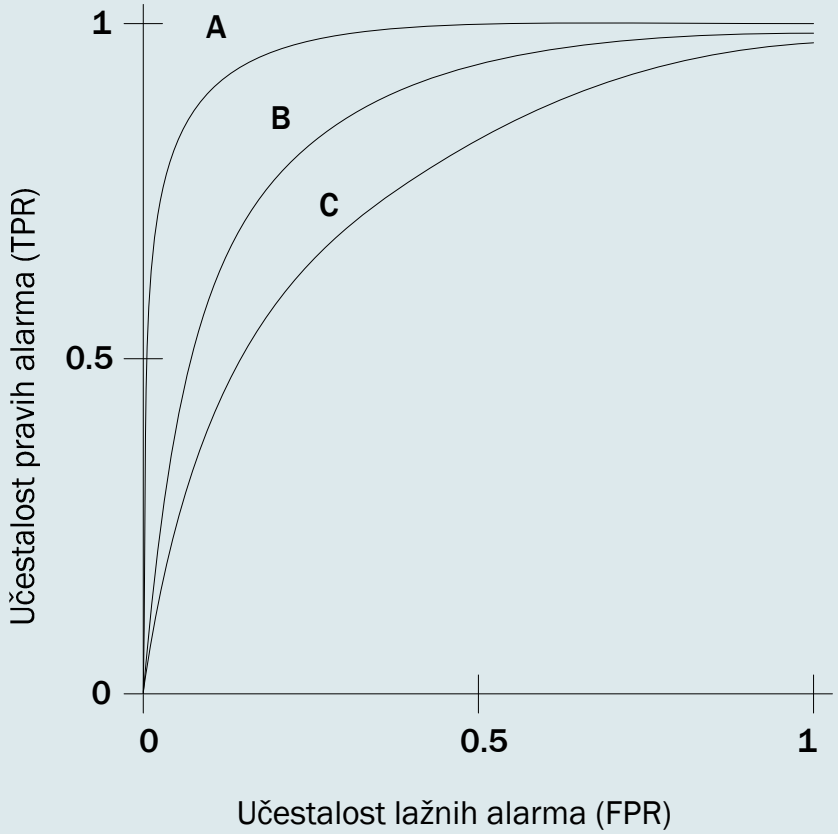
Tačnost (engl. *accuracy*)

- Termin tačnost (engl. *accuracy*) obuhvata i određenost i osetljivost.
- Često treba napraviti kompromis između osetljivosti i određenosti. Granična tačka odstupanja od normalnog ponašanja može biti izabrana liberalno ili konzervativno.
- Tačnost je proporcija, tj. odnos svih IDS rezultata (pozitivnih i negativnih) koji su ispravni, tj. korektni

Kriva operativne karakteristike primaoca

- Operativna karakteristika primaoca (engl. *Receiver Operating Characteristic Curve*, ROC) jeste metoda grafičkog prikazivanja relacije između osetljivosti i određenosti. ROC kriva iscrtava odnos osetljivosti i učestalosti lažno pozitivnih (1 – određenost).

Kriva operativne karakteristike primaoca



Prediktivne vrednosti i odnos mogućnosti

- **Prediktivne vrednosti** (engl. *predictive values*) vode računa o uticaju konkretne mreže, tj. uračunavaju varijacije u ponašanju koje unose konkretne mreže u kojima su IDS-ovi primenjeni, i mnogo su korisnije u praksi.
  - prethodne verovatnoće (engl. *prior probability*)
- Odnos mogućnosti
  - odnos dve verovatnoće (engl. *odds*)
    - odnos = verovatnoća / (1 – verovatnoća),
    - verovatnoća = odnos / (1 + odnos).
  - Mogućnost da se nešto desi (engl. *likelihood ratio*, *LR*) i nemogućnost da se nešto ne desi (engl. *odd ratio*, *OR*) primeri su odnosa verovatnoća.

6.3 Sistemi za sprečavanje upada (IPS)

- IDS sistemi zasnovani na potpisima koncentrisani su na to kako napad "radi", tj. kako se izvodi. Ako napadač unese minorne izmene u napad (pomoću različitih tehnika za izbegavanje IDS-a), prethodno formirani potpisi neće više moći da otkriju napad. IPS se fokusira na to šta napad radi, što je relativno nepromenljivo.
- Osnovne funkcije IPS sistema su sledeće:
  - identifikacija neovlašćenih aktivnosti na osnovu potpisa,
  - identifikacija neovlašćenih aktivnosti na osnovu detektovanih anomalija,
  - vođenje evidencije i/ili slanje upozorenja administratorima zaduženim za sigurnost u realnom vremenu,
  - prikupljanje forenzičkih podataka o detektovanim napadima,
  - sprečavanje napada.

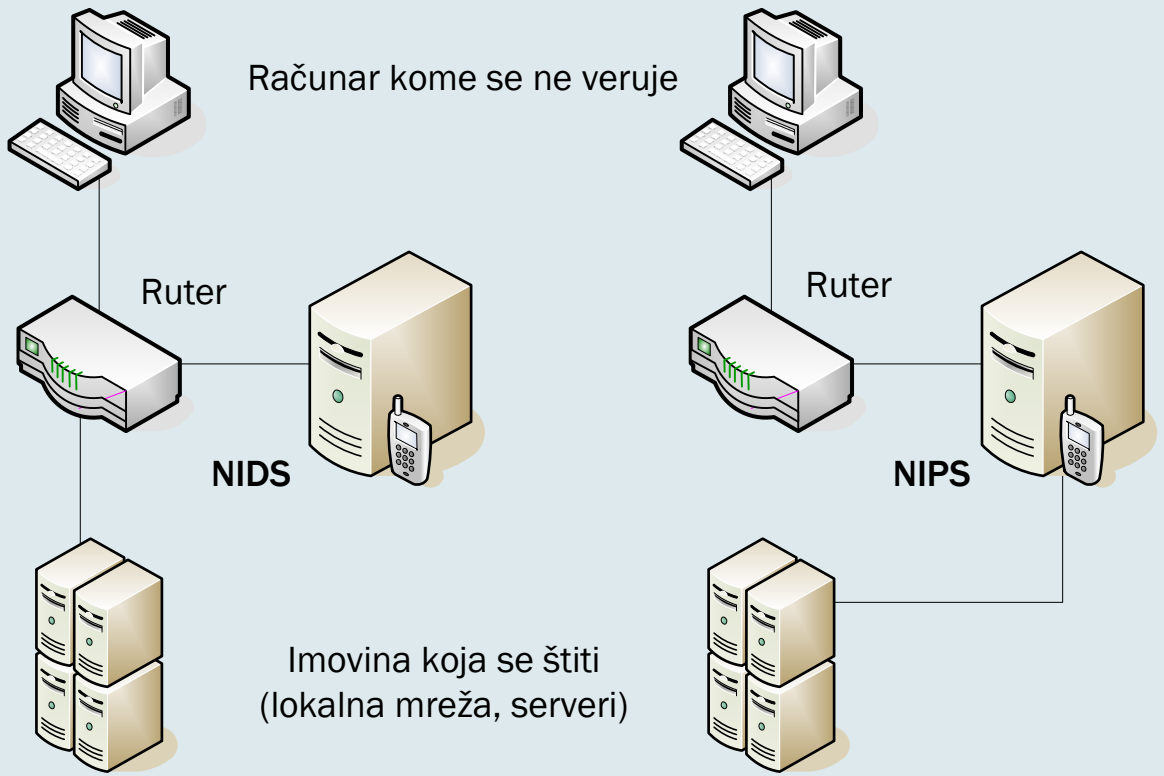
Principi na kojima rade IPS sistemi

- Heuristički pristup zasnovan na softveru (engl. *software based heuristic approach*)
- Sandbox pristup (engl. *sandbox approach*)
- Hibridni pristup (engl. *hybrid approach*)
- Pristup zasnovan na zaštiti pomoću jezgra (engl. *kernel based protection approach*)

Podela IPS sistema

- IPS sistemi smešteni na računaru, koji štite računar (engl. *host based IPS*, *HIPS*)
- Mrežni IPS sistemi (engl. *network based IPS*, *NIPS*)

NIDS i NIPS sistemi



Zahtevi za efikasnu prevenciju

- Nepobitna tačnost detekcije
- Raspoloživost
- Kratko vreme čekanja tj. malo kašnjenje
- Napredno rukovanje alarmima i mogućnost naknadne analize

6.4 Primena sistema sa veštačkom inteligencijom

- Ekspertni sistemi
- Fazi logika (engl. *fuzzy logic*)
- Neuronske mreže

Ekspertni sistemi

- Ekspertni sistemi predstavljaju inteligentne računarske programe koji sadrže "ekspertsko" znanje to jest znanje kakvo bi imao i stručnjak (ekspert) iz te oblasti.
- Ekspertni sistem ima tri komponente:
  - bazu znanja (engl. *knowledge base*),
  - mehanizam izvođenja (engl. *inference engine*),
  - upravljački mehanizam (engl. *control engine*).

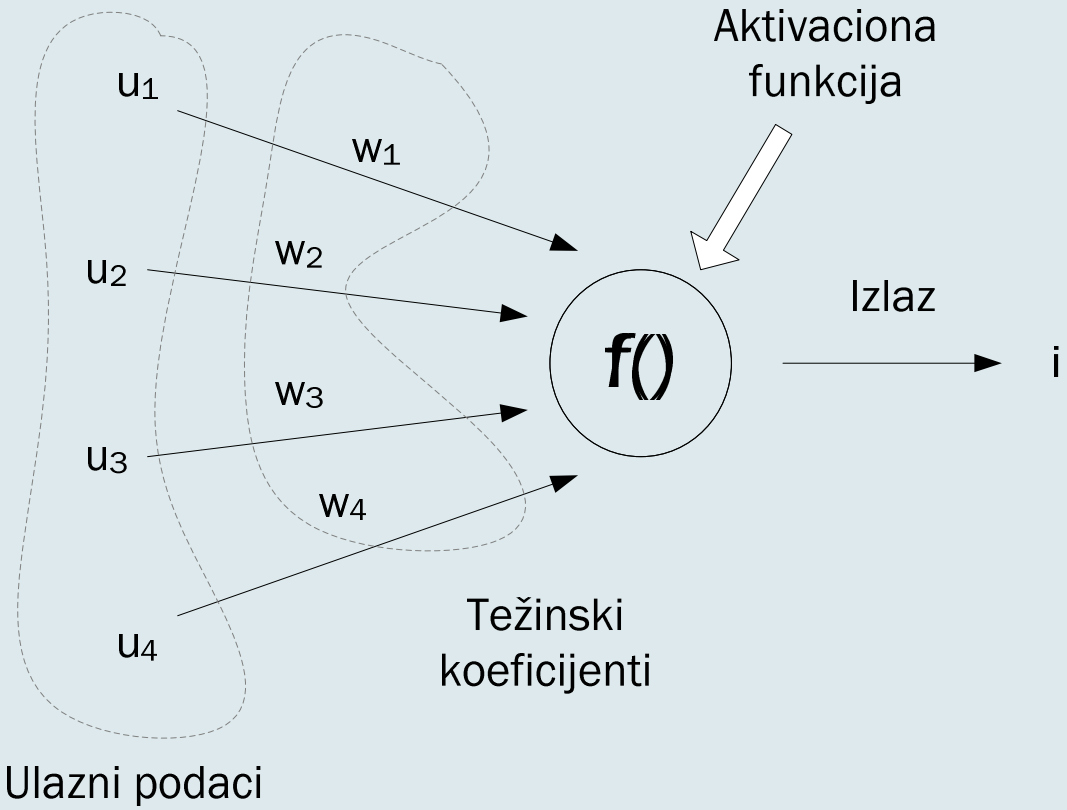
Fazi logika (engl. *fuzzy logic*)

- Za razliku od formalne logike u kojoj se pri rezonovanju koriste dve vrednosti (tačno-netačno, 0-1), fazi logika (engl. *fuzzy logic*) koristi realne brojeve iz intervala [0, 1], što je mnogo bliže realnosti, ljudskom razmišljanju i izražavanju. Mnoge pojave u prirodi teško je opisati pomoću samo dva stanja koja se međusobno isključuju. Fazi logika omogućava opisivanje takvih "nepreciznih" sistema.

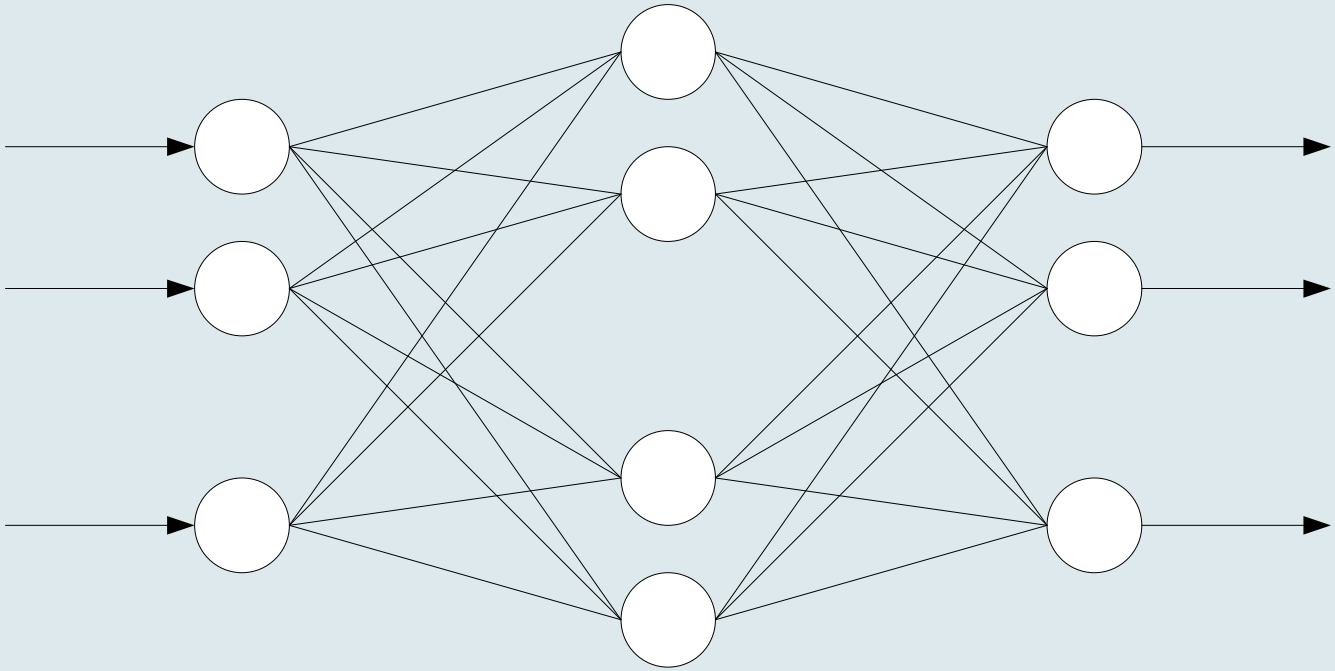
Neuronske mreže

- Postoje dve kategorije neuronskih mreža:
  - veštačke i
  - biološke neuronske mreže.
- Predstavnik bioloških neuronskih mreža je nervni sistem živih bića. Veštačke neuronske mreže su veštačke tvorevine koje oponašaju biološke nervne sisteme u obavljanju funkcija, kao što su učenje na ograničenom skupu primera i prepoznavanje uzoraka.

Model neurona



Model neuronske mreže



Primena veštačke inteligencije u IDS sistemima

- **Jaka veštačka inteligencija** (engl. *strong AI*). Tvrdnja da računari mogu da razmišljaju upravo kao ljudi. Tačnije, tvrdnja da može postojati takva klasa računarskih programa da njihova implementacija zaista razmišlja.

- **Slaba veštačka inteligencija** (engl. *weak AI*). Tvrdnja da su računari važni alati u modelovanju simulacije ljudske aktivnosti.

*Razliku između takozvane "jake" i "slabe veštačke inteligencije", koju je definisao Mark Kantrovic (Mark Kantrowitz) sa univerziteta Carnegie Mellon

Paper

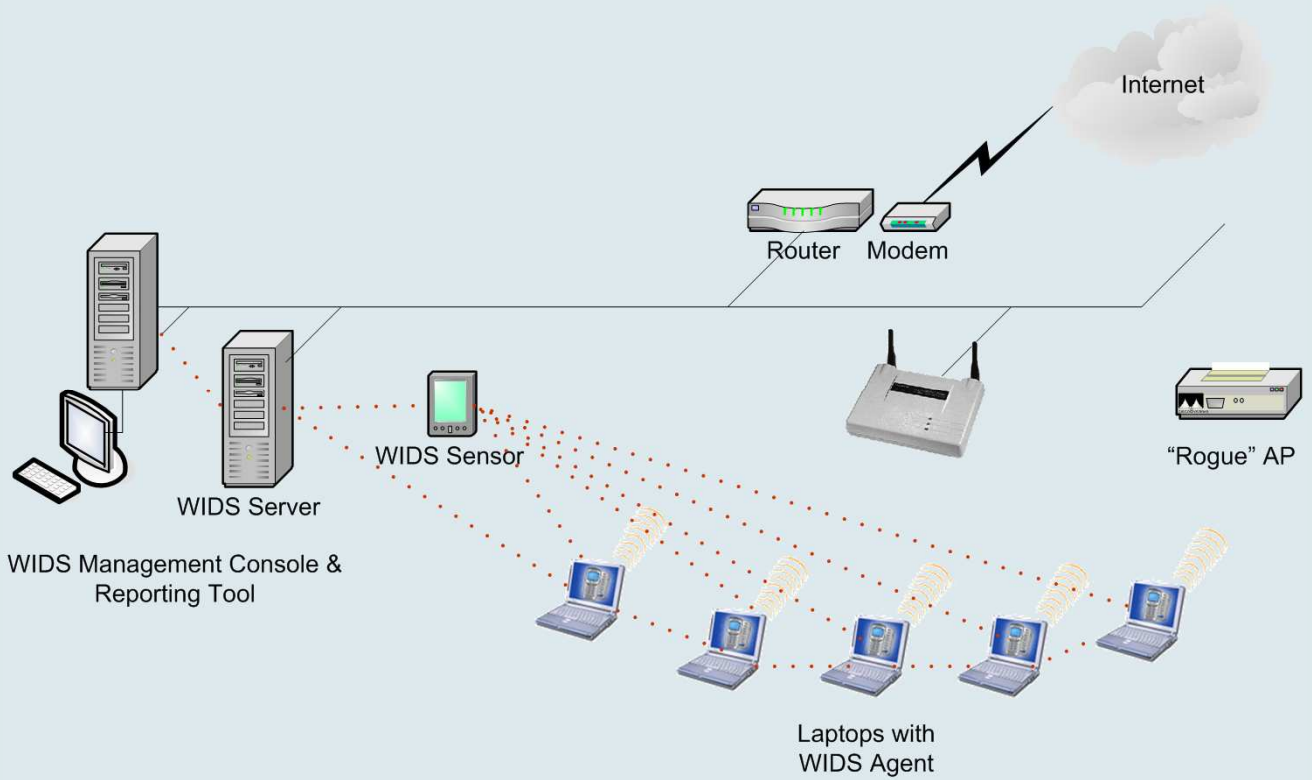
- Dragan Pleskonjić: “Wireless Intrusion Detection Systems (WIDS)”

19th Annual Computer Security Applications Conference
December 8-12, 2003
Las Vegas, Nevada, USA

www.acsac.org/2003/thu.html

www.acsac.org/2003/case/thu-c-1330-Pleskonjic.pdf

WIDS



More papers…

- D. Pleskonjić, D. Kraković, N. Matković, V. Milutinović, S. Omerović, S. Tomažić: "Reduction of False Positive Intrusions by Using Neural Nets", Invited paper, 8th IEEE International Conference - TELSIKS 2007, Serbia, Nis, September 26 - 28, 2007. On page(s): 7-10, ISBN: 978-1-4244-1468-0
  - www.ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=4375902&arnumber=4375925
- Dragan Pleskonjic, Sanida Omerovic, Saso Tomazic, "Network Systems Intrusion: Concept, Detection, Decision, and Prevention", IPSI BgD Transactions on Internet Research, January 2007, Volume 3, Number 1, ISSN 1820-4503
  - http://internetjournals.net/journals/tir/2006/TIRVol3Num1.pdf
- Dragan Pleskonjic, "Wireless Intrusion Detection and Prevention Systems", Invited speaker at IDC IT Security Roadshow 2006, Belgrade, March 16, 2006.
- D. Pleskonjic: “Protecting wireless computer networks by using intrusion detection agents”, IPSI 2005, Venice, Italy, November 10-13, 2005

Literatura

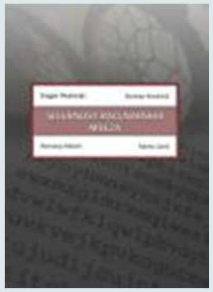
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

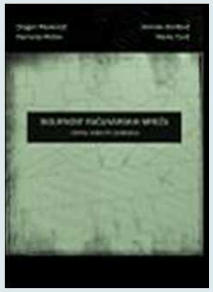
- Za predavanje 6:
  - Poglavlje 6: Sistemi za detekciju i sprečavanje upada

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?