Ofenzivna sigurnost

Kibernetička situacijska svjesnost

Mateo Plavec, 28. 1. 2026.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Definicija situacijske svjesnosti
- Pristup automatiziranom odlučivanju
- Eksperiment: usporedba defenzivnog i ofenzivnog pristupa
- Zaključak

Motivacija

- Kibernetičke prijetnje iziskuju brze i učinkovite reakcije
- Tokom napada želimo što prije odgovore na pitanja: Što se dogodilo? Zašto se dogodilo? [2, p. v]
- Pasivni defenzivni pristup je trom u usporedbi s promjenjivim krajolikom APT napada

Pitanja za ispite

- Definirajte (kibernetičku) situacijsku svjesnost uz pomoć pojmova prošlosti, sadašnjosti i budućnosti.
- Navedite glavnu razliku između aktivne (ofenzivne) i pasivne (defenzivne) obrane.
- Kako aktivna obrana pospješuje situacijsku svjesnost i uspješnost obrane?
- Koji je glavni nedostatak u implementaciji Bayesovih mreža za automatsko donošenje defenzivnih odluka?
- Kako korištenje obmane utječe na situacijsku svjesnost?

Definicija situacijske svjesnosti

- „Situational awareness is the perception of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.” [3, p. 17]
- Kratica: SA

Analiza definicije SA (1/4)

- „Situational awareness is the perception of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.” [3, p. 17]
- Koje su informacije trenutno važne?
- Kako do njih doći?

Analiza definicije SA (2/4)

- „Situational awareness is the perception of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.” [3, p. 17]
- Naučeno – dolazi iz prošlosti
- Skriveno znanje + važne informacije iz okoline → eksplicitno znanje [1]:61

Analiza definicije SA (3/4)

- „Situational awareness is the perception of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.” [3, p. 17]
- Predviđanje budućeg razvoja situacije
- Utjecaj naših radnji na razvoj

Analiza definicije SA (4/4)

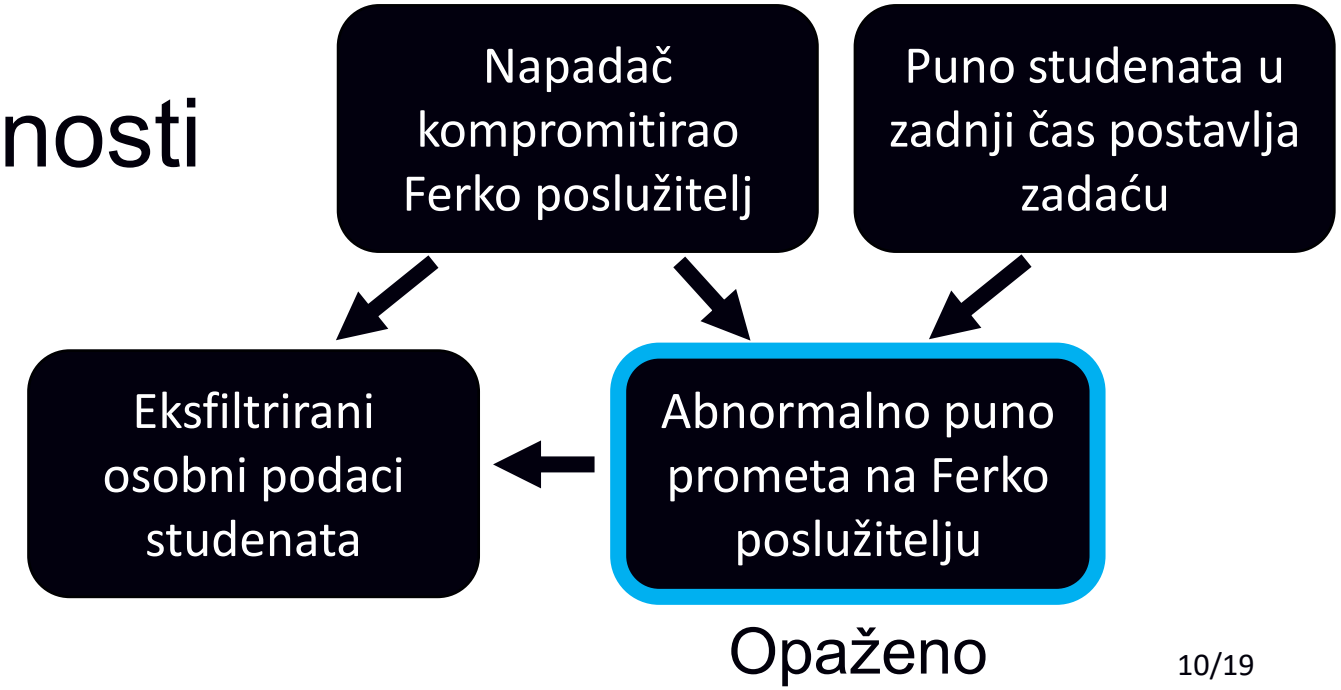
- „Situational awareness is the perception of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.” [3, p. 17]
- Naš najbolji idući korak

Povijest

- „Know thy enemy, know thy self […]” – *Umijeće ratovanja*, Sun Tzu, 5. st. pr. Kr. [1, p. 31]
- Model situacijske svjesnosti proizašao iz ratnog zrakoplovstva, 1998. [6, p. 221]
  - Kasnija primjena na upravljanje zračnim prometom i zapovjedništvom pješačkih vodova
  - Naša definicija je adaptacija

Pristup automatiziranom odlučivanju

- Grafu napada (kombinacija više *kill chaina*) dodamo neizvjesnost [4, p. 56]
- Bayesova mreža
- Tablice uvjetne vjerojatnosti u svakom čvoru
- Izračun najbolje iduće odluke [4, p. 55]



Problemi automatiziranog odlučivanja

- Nema metodologije za određivanje vjerojatnosti
- Teško je dobiti *ground truth* podatke [4, p. 57]
- Postoje ideje da se ovo izbjegne
  - Vjerojatnost → *confidence*
    - 3 razine: moguće, vjerojatno, gotovo sigurno [4, pp. 58–63]
  - Gubimo dobra svojstva Bayesovih mreža?
  - Opet problem određivanja tih razina za pojedine veze između čvorova

Eksperiment: defenzivni i ofenzivni pristup

- Ispitivanje teorije aktivne kibernetičke situacijske svjesnosti (detaljnije u [1, p. 58])
  - Kako aktivno prikupljanje obavještajnih informacija utječe na situacijsku svjesnost?
- Simulirana okolina – ozbiljna igra [1, p. 158]
  - Predefinirani napadi i legitimni korisnici
- Tokom igre pratimo razinu SA igrača
  - Samoprocjena i objektivna procjena stručnjaka

Postava eksperimenta

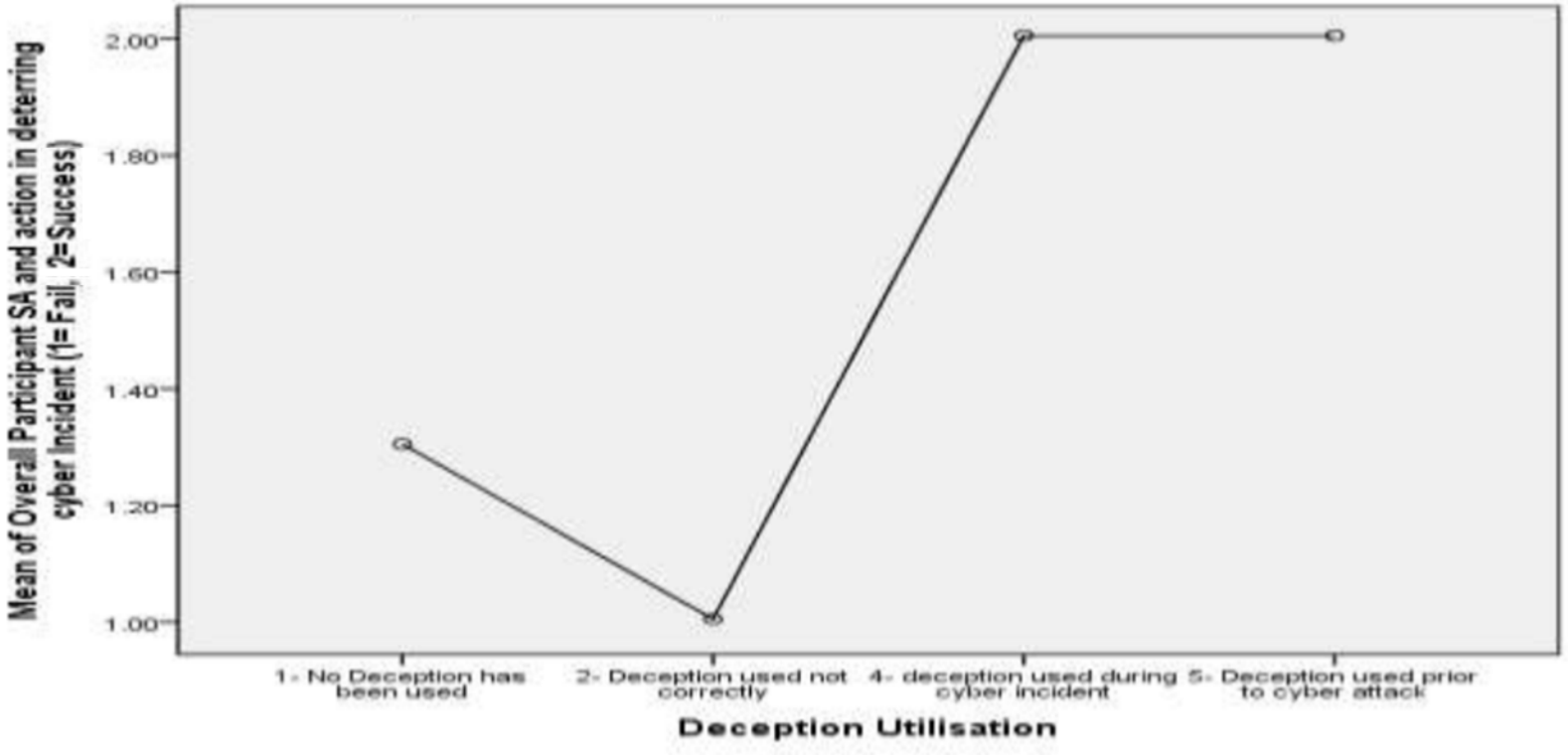
- IDS
- Sigurnosna stijena (engl. *firewall*)
- Razmjena informacija
- „Plavi” (ofenzivni) tim
- Obmana: klonirana mreža
- [1, pp. 115–116]

Defenzivna, pasivna grupa

Ofenzivna, (pro)aktivna grupa

Zaključak eksperimenta (1/2)

- Aktivna grupa uspješnija od pasivne
- Obmana – dvosjekli mač [1, p. 175]



Zaključak eksperimenta (2/2) [1, p. 176]

- Pobjednički stav aktivne grupe
- Poboljšana situacijska svjesnost
  - Percepcija
  - Razumijevanje
  - Predviđanje
- Povećana agilnost i kvaliteta obrane

Ograničenja eksperimenta

- Mali broj ljudi (N = 20)
- Plavi i crveni tim od jedne osobe
- Zanimljivi brojevi, ali
  - u studiji nije opisana konkretna strateška/taktička/tehnička razlika
- Replikacija rezultata?

Zaključak

- Situacijska svjesnost
  - Adekvatan misaoni model
  - Teško pretočiti u računalni model
- Eksperiment pokazuje
  - Ofenzivna sigurnost ima smisla
    - Bolja od pasivne (defenzivne)
- Protunapad – siva zona

Literatura (1/2)

- [1] A. Al-Shamisi, "Active offensive cyber situational awareness: theory and practice", Ph.D. dissertation, Dept. of Comp. Sci., Brunel Univ., London, UK, 2014. Available: https://bura.brunel.ac.uk/bitstream/2438/13427/1/FulltextThesis.pdf
- [2] S. Jajodia, P. Liu, V. Swarup and W. Cliff, *Cyber Situational Awareness: Issues and Research*, New York, USA: Springer-Verlag, 2009, doi: 10.1007/978-1-4419-0140-8
  - [3]: G. P. Tadda, and J. S. Salerno, "Overview of cyber situation awareness", in *Cyber Situational Awareness: Issues and Research*, New York, USA: Springer-Verlag, 2009, pp. 15-35, doi: 10.1007/978-1-4419-0140-8_2.
  - [4]: J. Li, X. Ou and R. Rajagopalan, "Uncertainty and risk management in cyber situational awareness", in *Cyber Situational Awareness: Issues and Research*, New York, USA: Springer-Verlag, 2009, doi: 10.1007/978-1-4419-0140-8_4.

Literatura (2/2)

- [5] S. Groš. "Englesko-hrvatski rječnik". Accessed: Jan. 23, 2026. [Online]. Available: https://www.zemris.fer.hr/~sgros/stuff/rjecnik.shtml
- [6] J. Brynielsson, U. Franke and S. Varga, "Cyber Situational Awareness Testing", in *Combatting Cybercrime and Cyberterrorism*, B. Akhgar and B. Brewster, Eds., Switzerland: Springer, 2016, ch. 12, pp. 209–233, doi: 10.1007/978-3-319-38930-1_12. Available: https://www.foi.se/download/18.7fd35d7f166c56ebe0bfffd/1542623724855/Cyber-situational-awareness_FOI-S--5619--SE.pdf

Hvala!