Инжењеринг знања
2020/2021. година

Пројектни задатак

Дизајнирати, имплементирати и тестирати систем за подршку одељењу информационе безбедности једног предузећа.

Функционалности, које је инжењерима информационе безбедности потребно омогућити су:

1. **Регистрација, преглед и ажурирање безбедносног инцидента (напада) предузећа.**
   - Да би евидентирање безбедносног инцидента било могуће, потребно је формално описати безбедносне концепте, као што су рањивост, напад и претња, затим, домен и последице деловања безбедносних концепата, као и везе између њих.
   - У складу са доменом напада, омогућити складиштење инстанци поменутих безбедносних концепата, увид у складиштене инстанце и њихово ажурирање.
   - Модел концепата информационе безбедности, као и њихове инстанце, складиштити у *RDF* формату, а за упите над овим складиштем користити *SPARQL* језик.
2. **Процена вероватноће припадности регистрованог инцидента одређеној класи напада на информациону безбедност.**
   - На основу годишњег статистичког извештаја о нападима на информациону безбедност (*Internet Security Threat Report*[1]), креирати Бајесове вероватноће за категорије безбедносних инцидената у односу на карактеристике претње и предузећа (број запослених, држава у којој предузеће послује, итд).
   - За евидентирање поменутих категорија безбедносних инцидената референцирати се на регистар *Common Attack Pattern Enumeration and Classification (CAPEC)*[2].
   - Класификовање инцидента врши се на основу највеће Бајесове вероватноће да се одређени инцидент догоди. При томе је инжењеру информационе безбедности предузећа неопходно омогућити специфицирање карактеристика предузећа и тренутне претње.
3. **Идентификација заведеног инцидента (напада), који је најсличнији датом.**
   - За потребе ове тачке имплементирати расуђивање по случајевима.
   - При моделовању случаја водити се атрибутима похрањеним у датотеци: https://capec.mitre.org/data/csv/3000.csv.zip, датој од стране *CAPEC* регистра.
   - Употреба формуле за израчунавање сличности даје се на вољу студентима, при чему мора да постоји конкретан разлог употребе одређене формуле.
4. **Сугерисање метода ублажавања или отклањања последица инцидента.**
   - Након идентификовања најсличнијег напада, расуђивањем по правилима омогућити сугерисање мера, које инжењер информационе безбедности треба да предузме.

1 https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
2 https://capec.mitre.org/data/definitions/3000.html

5. **Процена ризика рањивости.**
   - На основу метрика датих у водичу система *Common Vulnerability Scoring System (CVSS)*[3], имплементирати *fuzzy* систем за одређивање ризика рањивости.
   - Графички кориснички интерфејс, који пружа увид у процењени ризик рањивости, имплементирати по узору на *CVSS* калкулатор процене ризика[4]

Напомене:

1. Израда пројектног задатка предодређена је за четворочлане студентске тимове.
2. Сваки пројектни тим бави се тачно одређеним доменом безбедносних напада дисјунктним у односу на остале (софтверски напади, хардверски напади, социјални инжењеринг, итд).

Корисни ресурси за моделовање рањивости и напада могу се наћи на следећим адресама:

- https://github.com/Ebiquity/Unified-Cybersecurity-Ontology
- https://www.ida.liu.se/divisions/adit/security/projects/secont/
- http://cis.csi.cuny.edu/iSecure/sob.html

3 https://www.first.org/cvss/v1/guide
4 https://www.first.org/cvss/calculator/3.1