Resources on Intrusion Detection: Algorithms

Preparation Lecture 8

- Read an intuitive tutorial on decision trees, emphasize on Chapter 1:
  A Decision Tree Primer, C. Kirkwood
  https://www.public.asu.edu/~kirkwood/DAStuff/refs/decisiontrees/index.html

- Using a cost-based analysis with a decision tree to evaluate an IDS:
  A Decision Analysis Method for Evaluating Computer Intrusion Detection Systems, J. Ulvila, J. Gaffney
  https://tinyurl.com/bdch9zs
  Emphasize on deriving the cost formula in section 2 and finding the optimal operating point. Extensions to this approach (e.g. multiple IDSs) can be found in *Evaluation of Intrusion Detection Systems, J.Ulvila, J.Gaffney*

Literature Lecture 8

- The LODA intrusion detection technique:
  Loda: Lightweight on-line detector of anomalies by T. Pevný
  https://link.springer.com/article/10.1007/s10994-015-5521-0 Emphasize on sections 3.1, 3.2, 3.3 for the training and testing procedures.

- The isolation forest technique:
  Isolation Forest by F.T. Liu et al.
  http://www.lamda.nju.edu.cn/publication/icdm08b.pdf Emphasize on sections 2 and 4 to understand the iTree and iForest structure.

- The LOF technique:
  LOF: Identifying Density-Based Local Outliers by M. Breunig et al.
  https://www.dbs.ifi.lmu.de/Publikationen/Papers/LOF.pdf Emphasize on sections 3 that defines DB outliers and the demonstrates the problem of masking in clusters. Continue to the definitions in section 4 until you reach LOF.