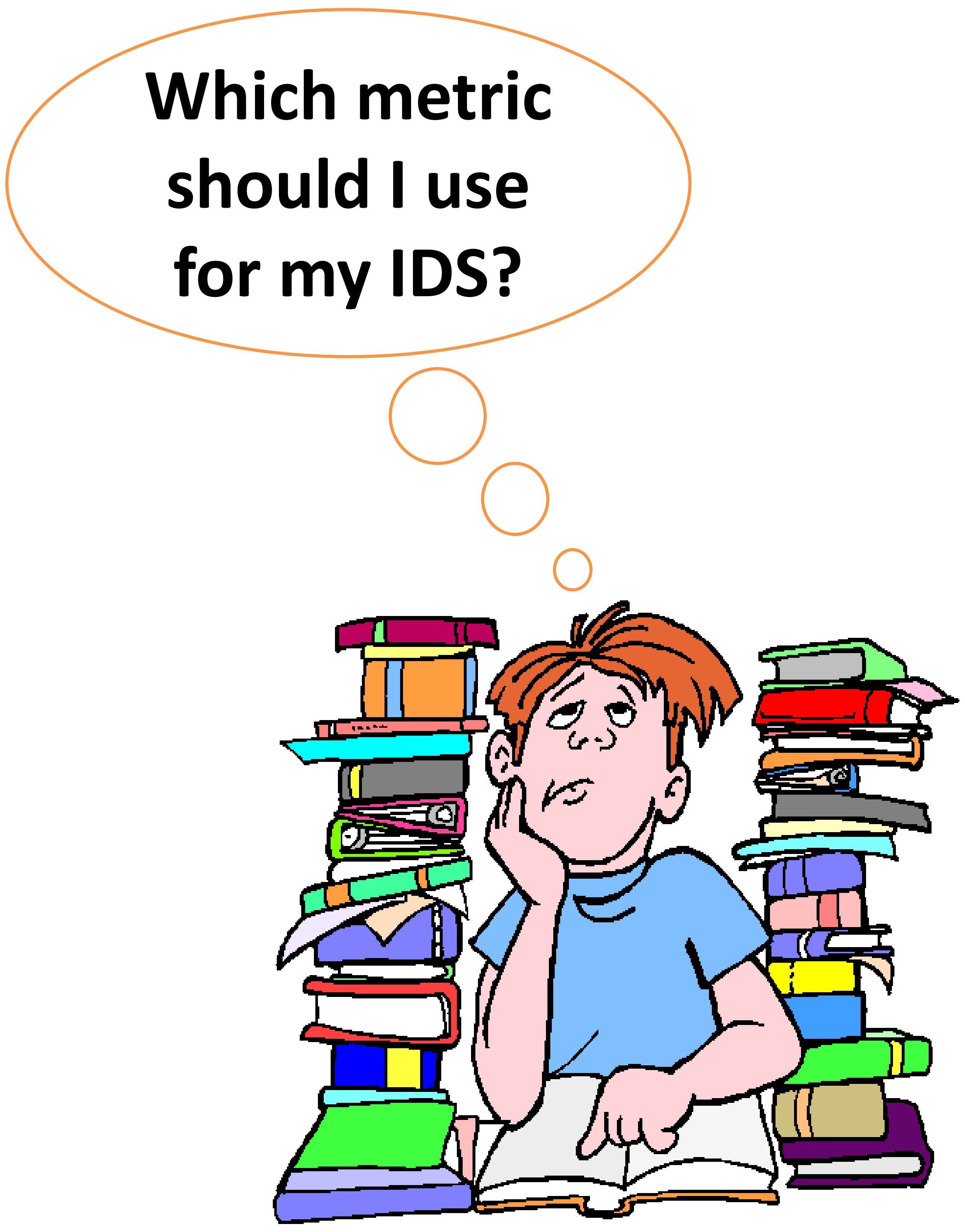
2015 SYMPOSIUM & BOOTCAMP URBANA IL HOTSOS ON THE SCIENCE OF SECURITY

Systematization of Metrics in Intrusion Detection Systems

Yufan Huang, Xiaofan He, and Huaiyu Dai (NCSU)



- Taxonomy of IDS metrics
  - Information theoretical
  - Probabilistic
  - Proximity-based
  - Reliability-based

- Simulation study on KDD’99

	Information Theoretical		Probabilistic		Proximity	
	ID3	C4.5	Naïve Bayes	TAN	K-Mean	Y-Mean
Normal	92.79	96.33	98.13	98.56	97.56	89.89
DoS	96.03	97.02	95.74	97.10	97.31	91.17
R2L	2.24	4.58	0.56	3.15	6.43	5.19
U2R	3.07	1.75	3.51	7.02	29.82	10.96
Probe	86.46	80.82	72.25	78.90	87.54	75.25

- Future plan
  - More metrics in each category
  - Combinations
  - Evaluation metrics for IDS

http://hot-sos.org/

The Science of Security initiative is
funded by the National Security Agency.