An Empirical Study on Current Models for Reasoning about Digital Evidence

Roy Campbell
Department of Computer Science
University of Illinois at Urbana-Champaign

Outline

- Motivation
- Problem Statement
- Analysis of Current Models
  - Differential Analysis
  - Probabilistic Models
  - Event Reconstruction
  - Attack Graphs
- Discussion
- Conclusion

Motivation

- Forensic process relies on the scientific method
- Analysis of digital evidence is highly subjective

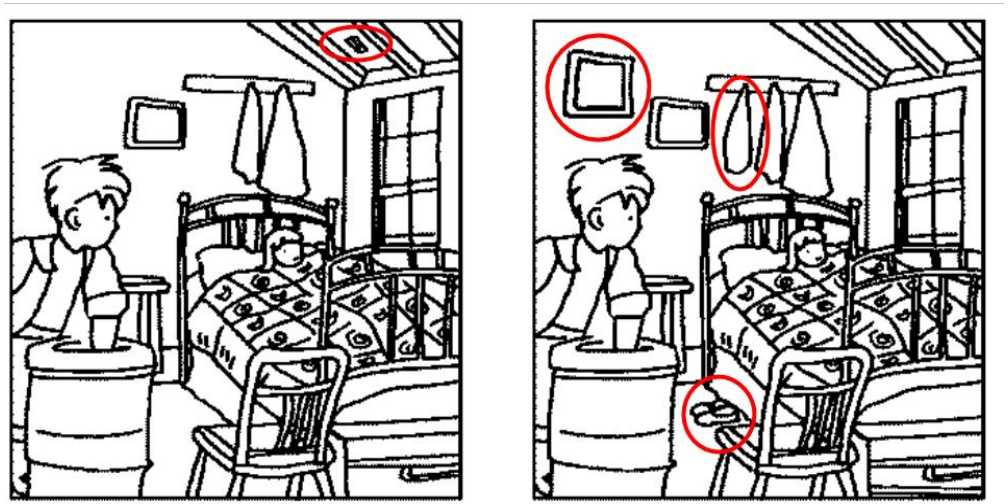
Problem Statement

Digital Forensics is in need of a deterministic approach to obtain the most judicious conclusions from evidence

Differential Analysis

- Method of data comparison used for reporting differences between two digital objects
- Need differential analysis to limit the amount of evidence that is needed

Baseline

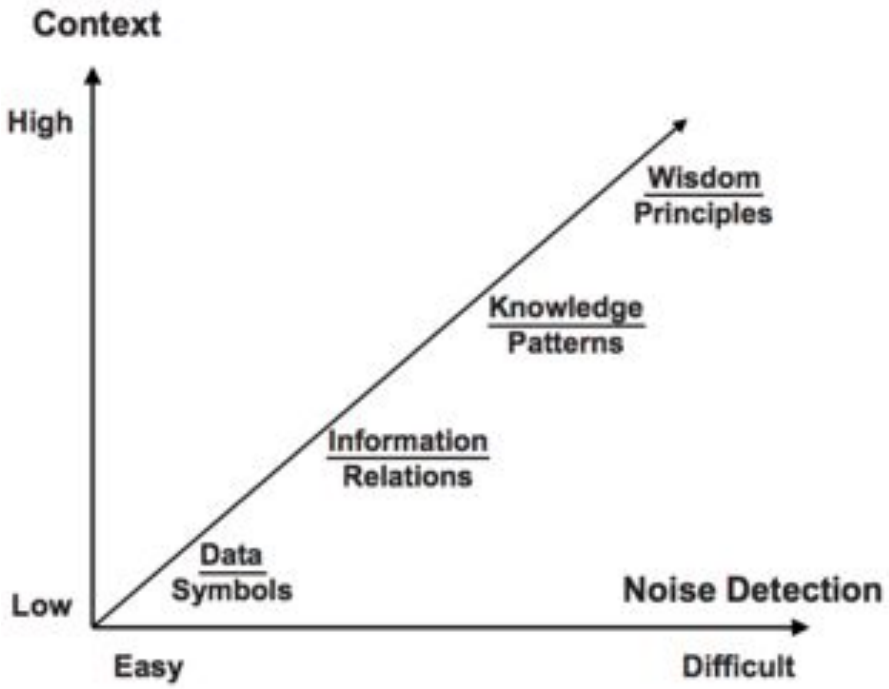


Final

1. http://www.krupukz.com/91152-printable-find-the-difference-fish

Differential Analysis

- Noise
- Hidden Data
- Reducing the noise

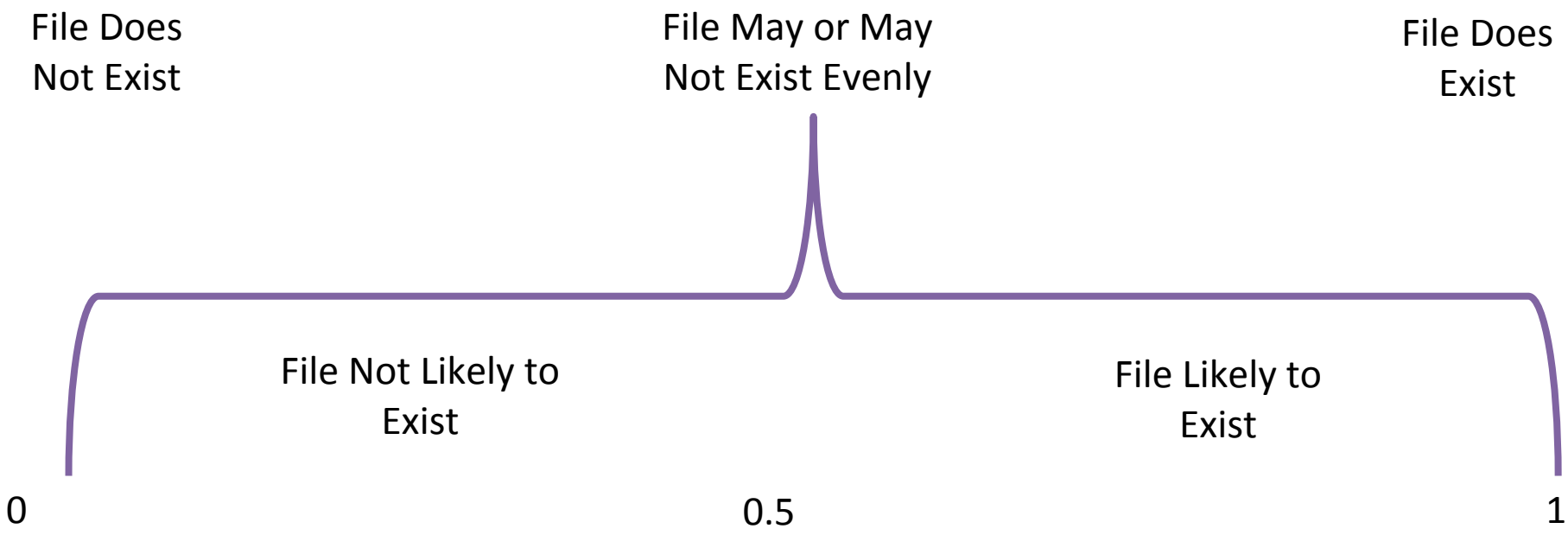


1. Nunamaker, N.J.J., Romano J., Briggs, R. A Framework for Collaboration and Knowledge Management. in Proceedings of the 34th Annual Hawaii International Conference on System Sciences, January 2001.

Probabilistic Models

- Assess the degree of certainty for which hypotheses and evidence can be linked

Classical Probability



Bayesian Network

Poor Password	
T	F
0.2	0.8

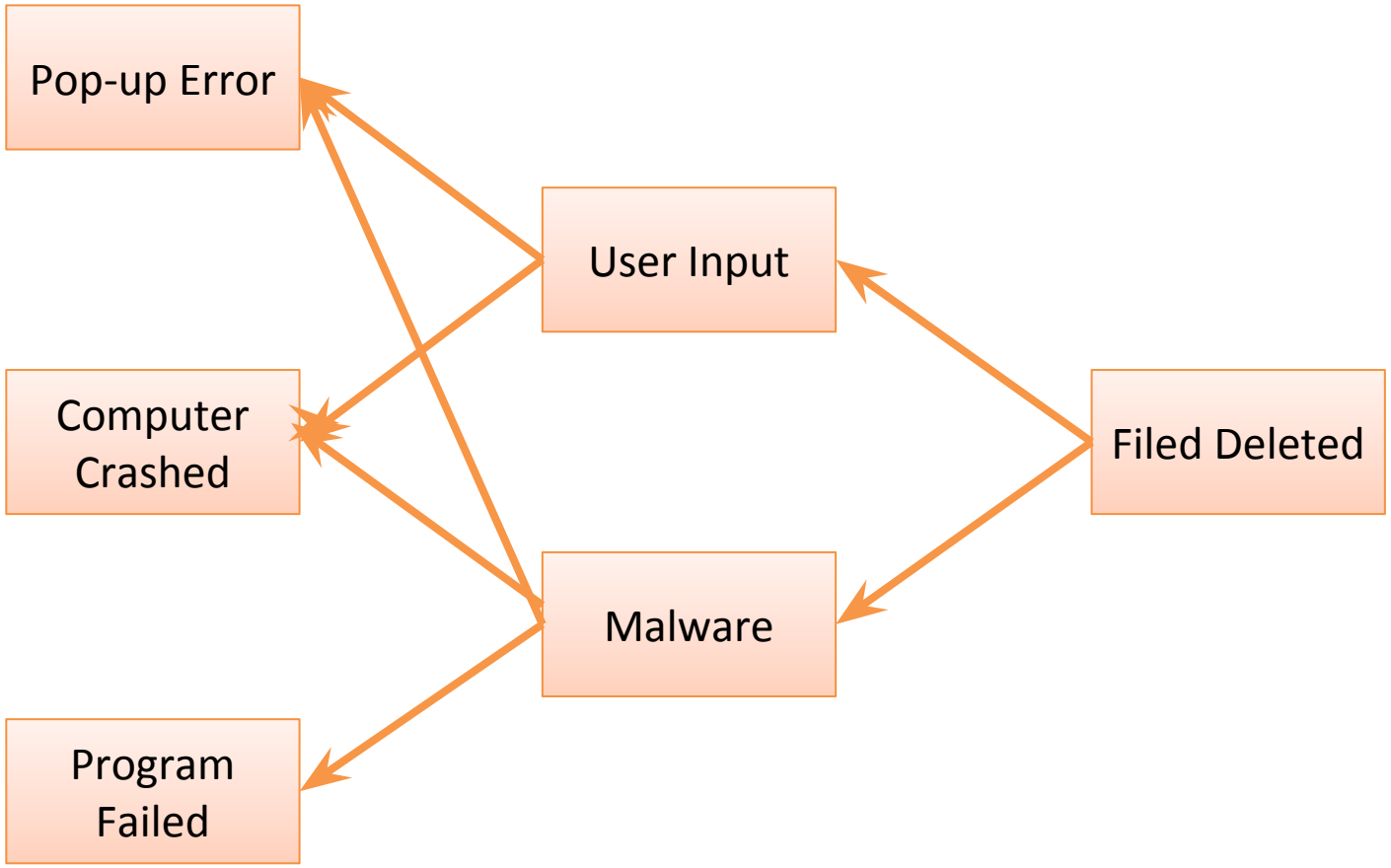
	Intrusion	
Poor Psswrd	T	F
F	0.4	0.6
T	0.01	0.99

		Computer Crashed	
Intrusion	Poor Psswrd	T	F
F	F	0.0	1.0
F	T	0.8	0.2
T	F	0.9	0.1
T	T	0.99	0.01

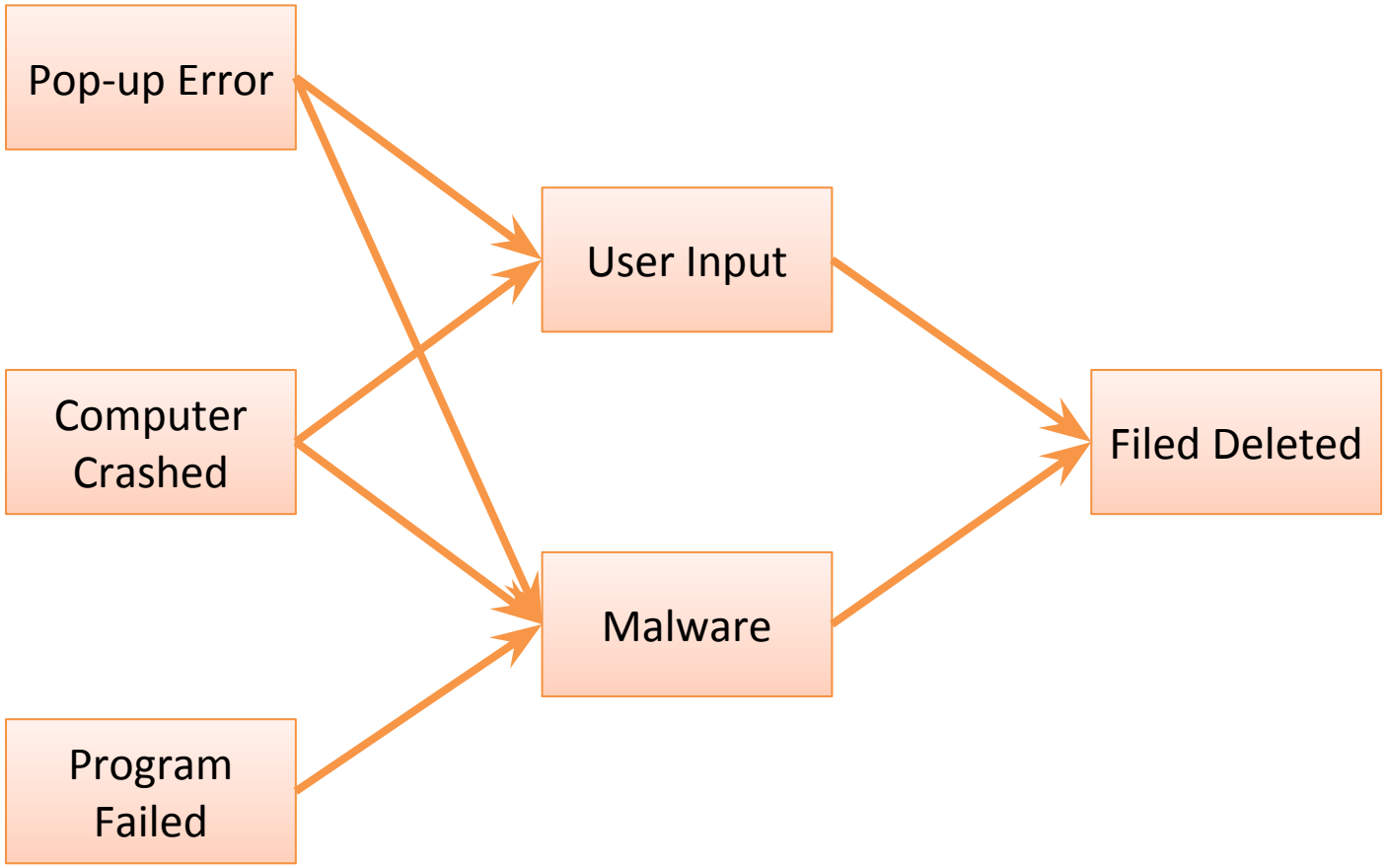
Dempster-Shafer Theory

Possible Forms of Intrusion

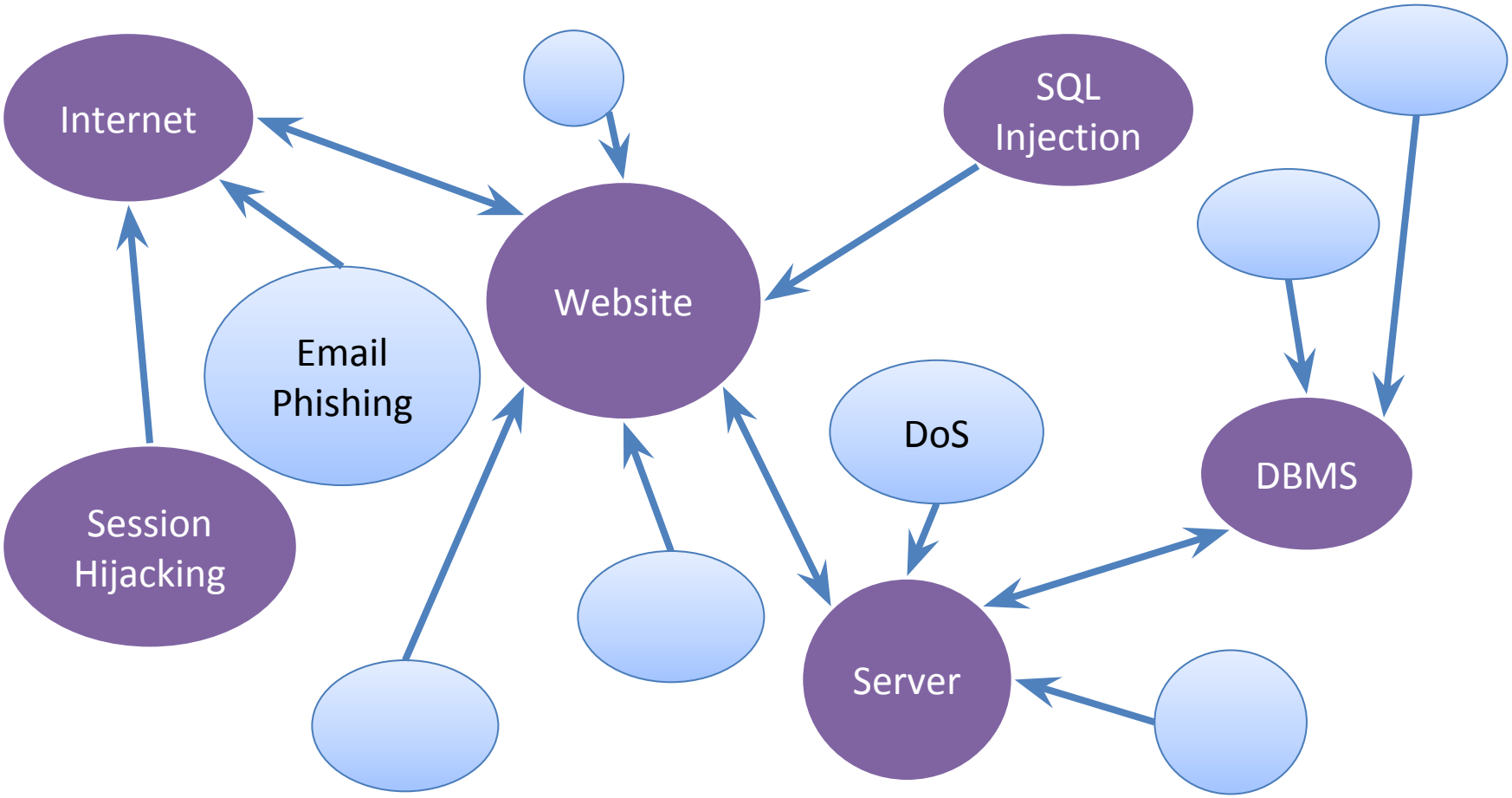
Event Reconstruction Models



Back-Tracing Event States



Attack Graphs



Discussion

- Differential Analysis
  - Noise
- Probabilistic Models
  - Prior probabilities
  - Niche scenarios
- Event Reconstruction
  - Limited attack presentation

Conclusion

Digital Forensics is in need of a deterministic approach to obtain the most judicious conclusions from evidence

- Identification of limitations in current models
- Reasoning analysis architecture
- Prior probability dataset
  - File hashes
  - Machine states
  - Probability metrics
- Admissibility