Using Provenance for Security and Interpretability

Michael Xueyuan Han (2nd year)
Advisor: Dr. Margo Seltzer
Research Areas: Systems, Computer Security, Machine Learning
Harvard University

HARVARD
John A. Paulson
School of Engineering
and Applied Sciences

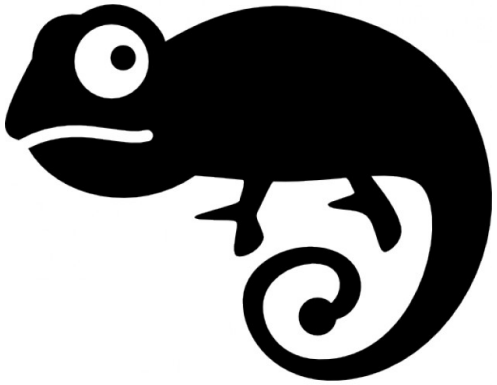
In a Nutshell

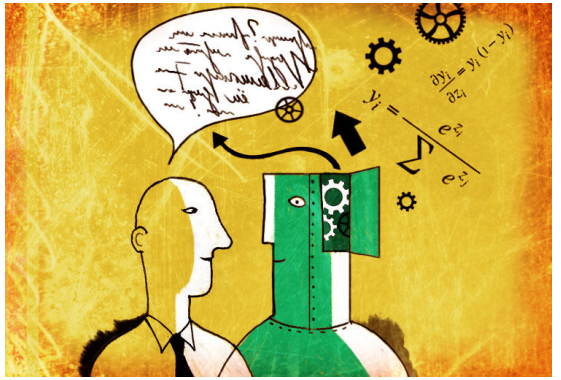
- Host-based intrusion detection is *inaccurate* and *non-interpretable* because our models of system behavior are *incomplete*, *imprecise*, and *hard to reason*.
- Intrusion detection is an important line of defense but it constantly *fails* us.
- *Data provenance* provides a *complete*, *structured*, and *semantic* understanding of system behavior.
- Better information leads to better models with better detection capability and attack attribution.

Host-Based Intrusion Detection

Anomaly Detection

Challenges



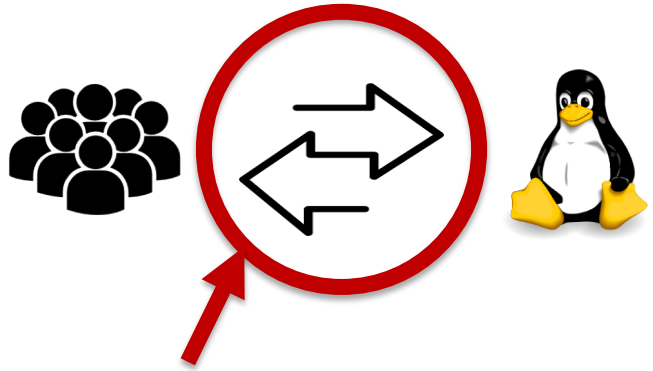


Data, Data, Data

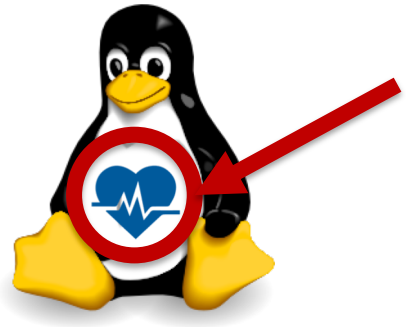
“

… **many** computationally sophisticated methods have been applied to the intrusion-detection problem, yet there are **few** well-accepted solutions … perhaps a **disproportionate** amount of attention has been directed to the data modeling … attention should be paid to considering what are the most effective data streams … [Warrender, 1999]

”



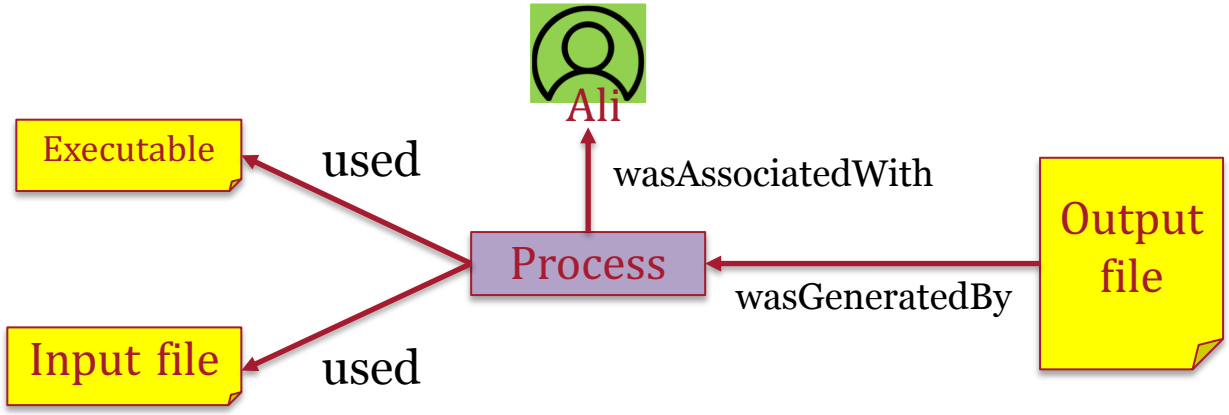
We have been analyzing data a lot here



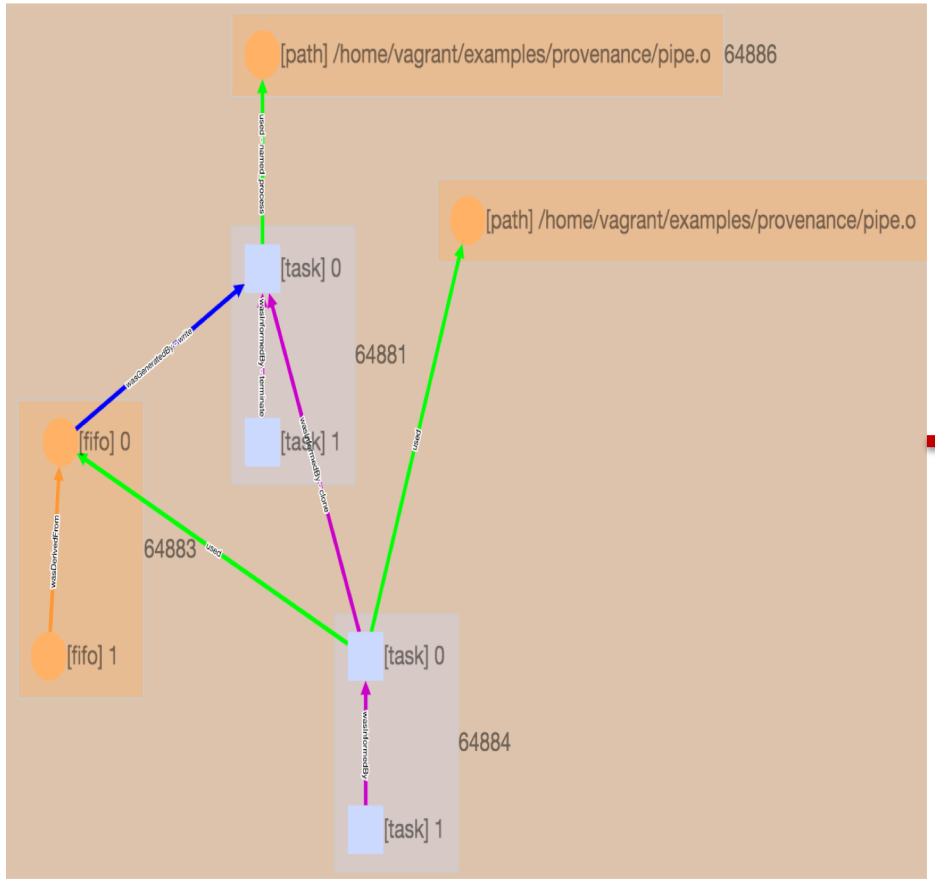
Maybe we should start looking at what’s happening here

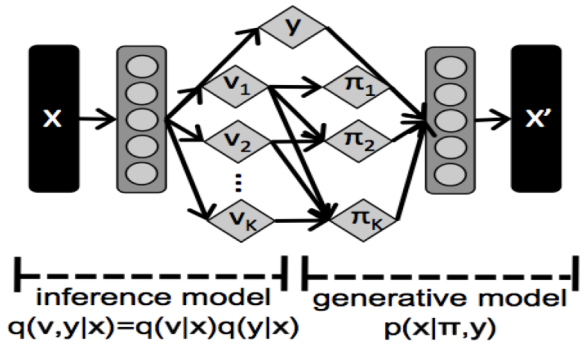
Data, Data, Data **Provenance**

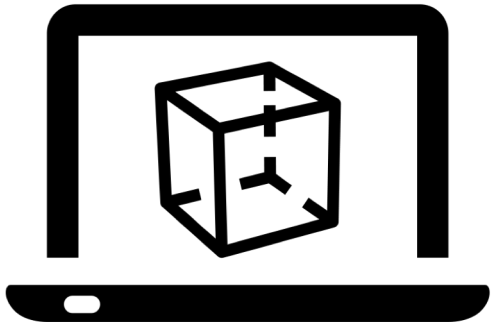
W3C PROV Data Model Type	DAG Representation	Example
Entity/Activity	Node	Kernel data objects (e.g., files, packets) Inode attributes, network addresses, etc.
Relationship	Edge	Processes manipulate entities
Agent	Node	Users and groups that enact activities



From Provenance to Models







Can Provenance Help?