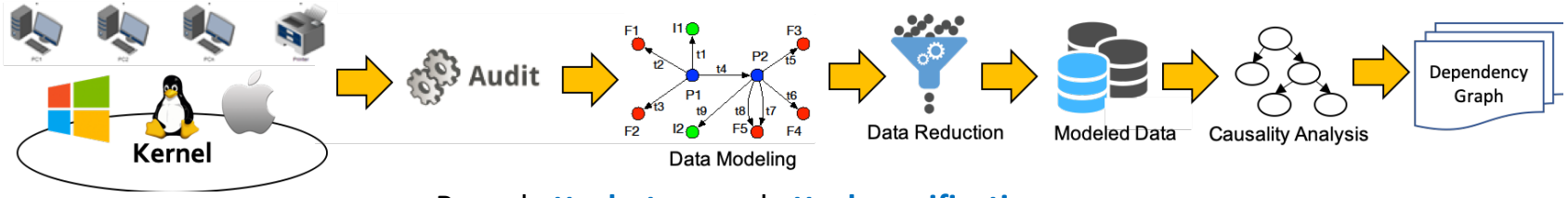
Scalable Cyber Attack Investigation using Declarative Queries and Interrogative Analysis

CASE SCHOOL OF ENGINEERING
CASE WESTERN RESERVE UNIVERSITY
Department of Computer and Data Sciences

Causality analysis based on system auditing models **causality of software behaviors** as a **dependency graph**



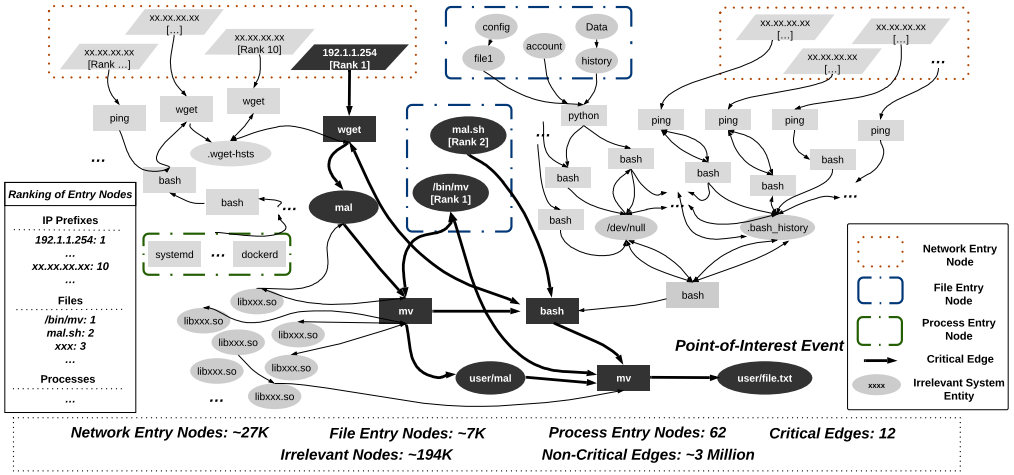
Reveal **attack steps** and **attack ramifications**

Challenge:

- Large dependency graph with irrelevant activities
- Lack of expert knowledge
- Difficult interface to explore software behaviors

Solution:

- Weighted graph to filter irrelevant dependencies
- Domain-Specific Language to incorporate expert knowledge
- Interrogative analysis framework to support behavior exploration



Progress Highlight:

- Subgraph filtered by weights is **234** edges, which is **4611×** smaller than the original dependency graph (1 million edges).
- Subgraphs filtered by weights is **72x** smaller than the state-of-the-art result (Hassan et al. NDSS'19).
- Weighted graph reduction is published in USENIX Security'22.
- New Subgraph Query suggestion algorithms are published for "Why" semantics (ICDE '22, WSDM '22).

Scientic Impact:

- Design of discriminative weights to distinguish attack steps and irrelevant dependencies
- Declarative graph query language for describing causality analysis
- Interrogative analysis using Why and What-if semantics

Broader Impact and Broader Partication:

- Help security analysts better understand complex attacks and assist them in providing cyber-incident response and recovery
- Help intrusion detection systems better prioritize detected alerts, promote database research and visual analysis to assist attack
- Collaborations with industry partners demonstrate promising results and reveal practical insights

SaTC CNS-2028748
PI: Xusheng Xiao, Co-PI: Yinghui Wu
Case Western Reserve University
xusheng.xiao@case.edu, yxw1650@case.edu