HØGSKOLEN I GJØVIK

Process Tracking for Forensic Readiness

Yi-Ching Liao

Norwegian Information Security Laboratory

yi-ching.liao@hig.no

ABSTRACT

- **Summarize the research on process tracking for forensic readiness**
  - the state-changing activities of processes
  - cost-benefit analysis of process tracking
  - the architecture for process tracking
  - privacy implications of process tracking

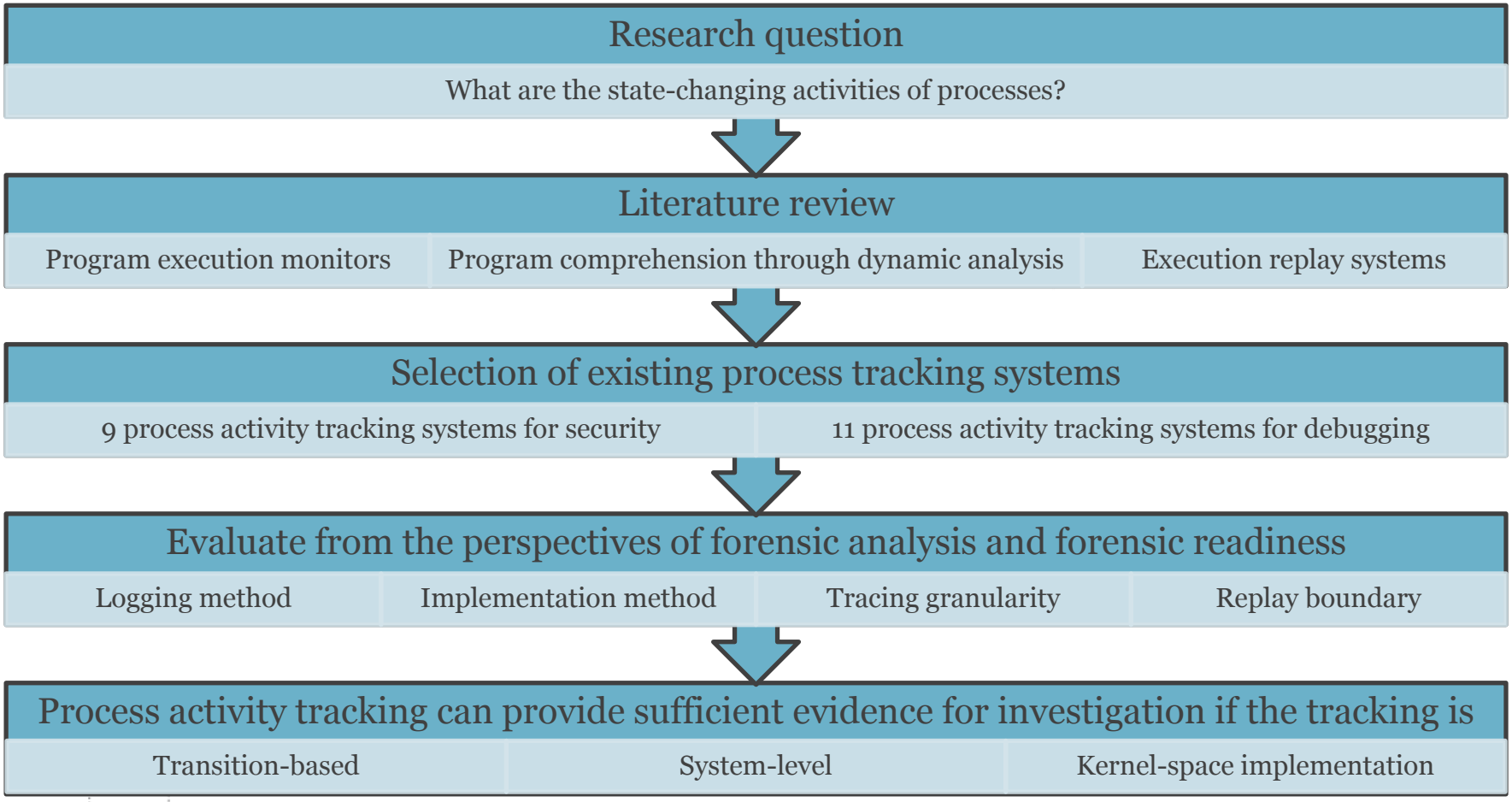
PROBLEM STATEMENT

- **Forensic analysis**
  - suffers from insufficient logging of events
- **Current system loggers**
  - do not record enough information for incident analysis and replay
- **Comprehensive process tracking**
  - provides precise, timely, complete, and dependable information for incident investigation and replay
  - recovers the traceability links between the incident and the person or action accountable for the incident

RESEARCH QUESTIONS

1. What are the state-changing activities of processes?
2. How effective, efficient, and expensive is comprehensive process activity tracking?
3. Which hardware/software architecture facilitates process activity tracking?
4. What are privacy implications for users of systems that support comprehensive traceability?
5. How does comprehensive traceability affect evidence gathering and the legal process?

STATE-CHANGING ACTIVITIES OF PROCESSES
OVERVIEW



STATE-CHANGING ACTIVITIES OF PROCESSES
SUMMARY

System name	Logging method[1]	Tracing granularity[2]	Replay boundary[3]	Design purpose[4]	Implementation method[5]	OS[6]
ReVirt [17]	SB	IL	SL	S	VM	L
ExecRecorder [15]	SB & TB	IL	SL	S	Emulator	Any
AskStrider [50]	TB	PL	N/A	S	U	W
Capture [45]	TB	PL	N/A	S	K	W
XenLR [28]	TB	IL	SL	S	Hypervisor	L
Process Hacker [42]	TB	PL	N/A	S	K	W
Process Monitor [31]	TB	PL	N/A	S	K	W
Carbon Black [10]	TB	PL	N/A	S	N/A	W
FileSure [9]	TB	PL	N/A	S	N/A	W
Tornado [13]	TB	IL	UL	D	K & U	L
Jockey [43]	TB	IL	UL	D	B & U	L
liblog [20]	TB	IL	UL	D	B & U	L
Flashback [46]	SB	IL	UL	D	K	L
iDNA [5]	TB	IL	UL	D	B	W
ODR [1]	TB	IL	UL	D	B & K	L
Respec [26]	SB & TB	IL	UL	D	K	L
DoublePlay [48]	SB & TB	IL	UL	D	K	L
FDR [51]	SB & TB	IL	SL	D	H	Any
BugNet [35]	SB & TB	IL	UL	D	B & H	L
QuickRec [40]	TB	IL	SL	D	H & K	L

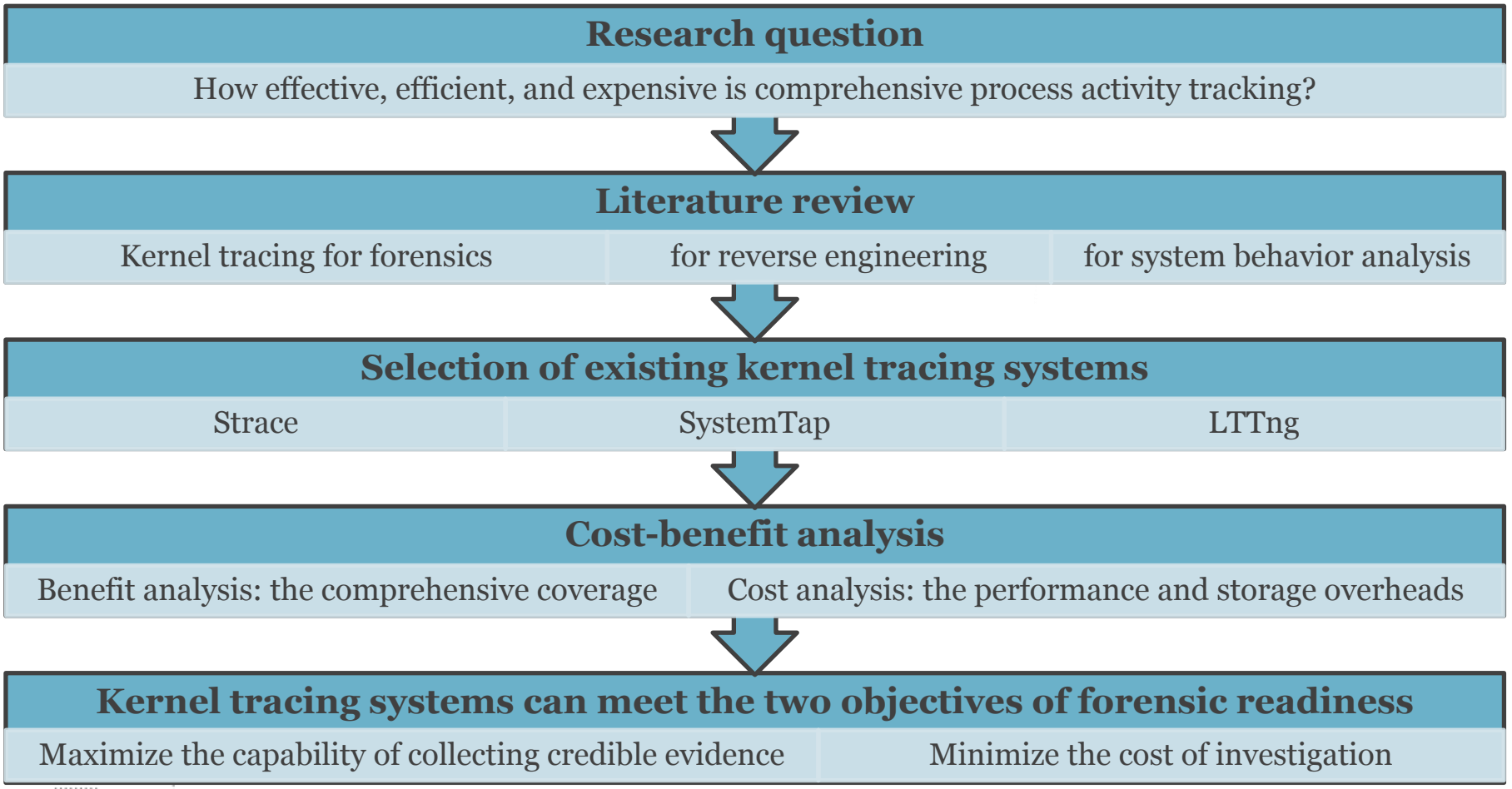
[1] SB=State-based; TB=Transition-based
[2] IL=Instruction-level; PL=Process-level
[3] SL=System-level; UL=User-level
[4] D=Debugging; S=Security
[5] B=Binary patching; H=Hardware; K=Kernel-space; U=User-space
[6] L=Linux; W=Windows

STATE-CHANGING ACTIVITIES OF PROCESSES
CONCLUSION AND QUESTION RAISED

- **Process activity tracking can provide sufficient evidence for investigation if the tracking is**
  - transition-based
  - system-level
  - kernel-space implementation
- **To strike a balance between the forensic effectiveness and efficiency, we need to**
  - evaluate the soundness, completeness, and cost of process activity tracking

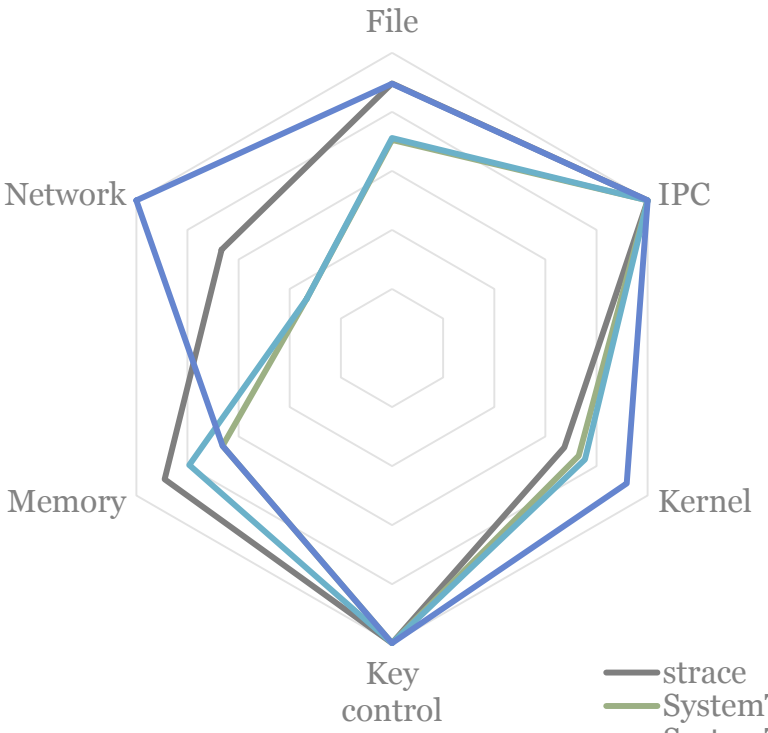
COST-BENEFIT ANALYSIS OF PROCESS TRACKING

OVERVIEW

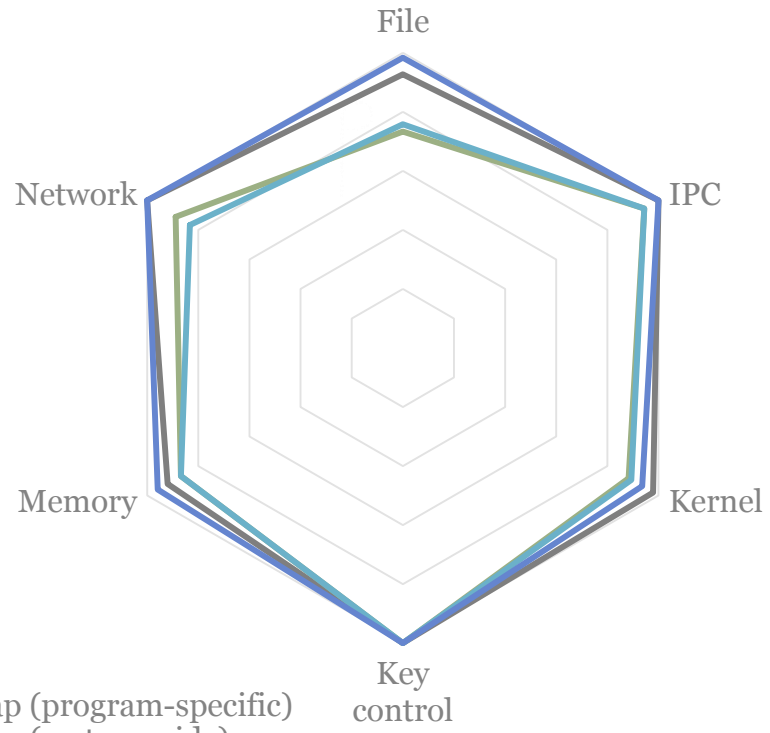


COST-BENEFIT ANALYSIS OF PROCESS TRACKING
BENEFIT ANALYSIS RESULTS

Comprehensive coverage in 32-bit architecture

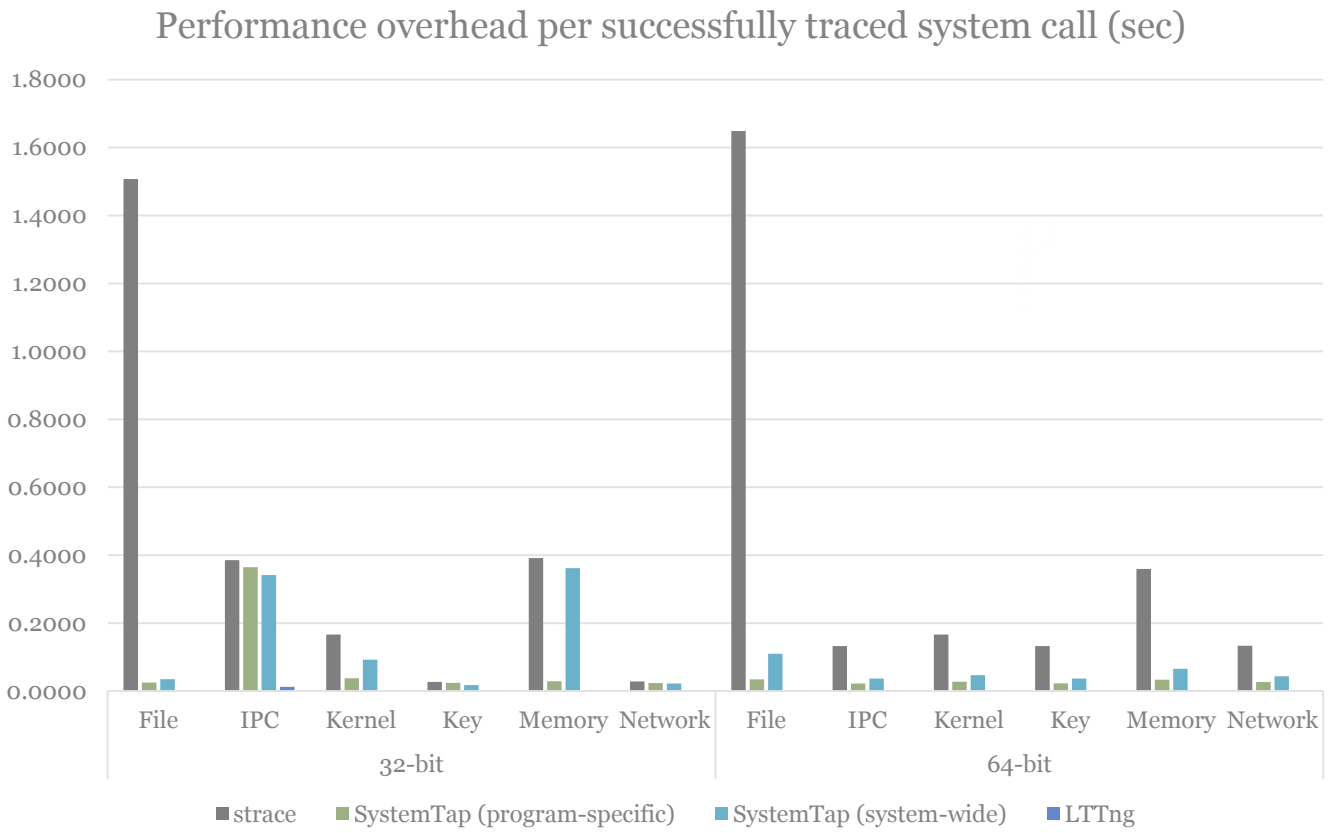


Comprehensive coverage in 64-bit architecture

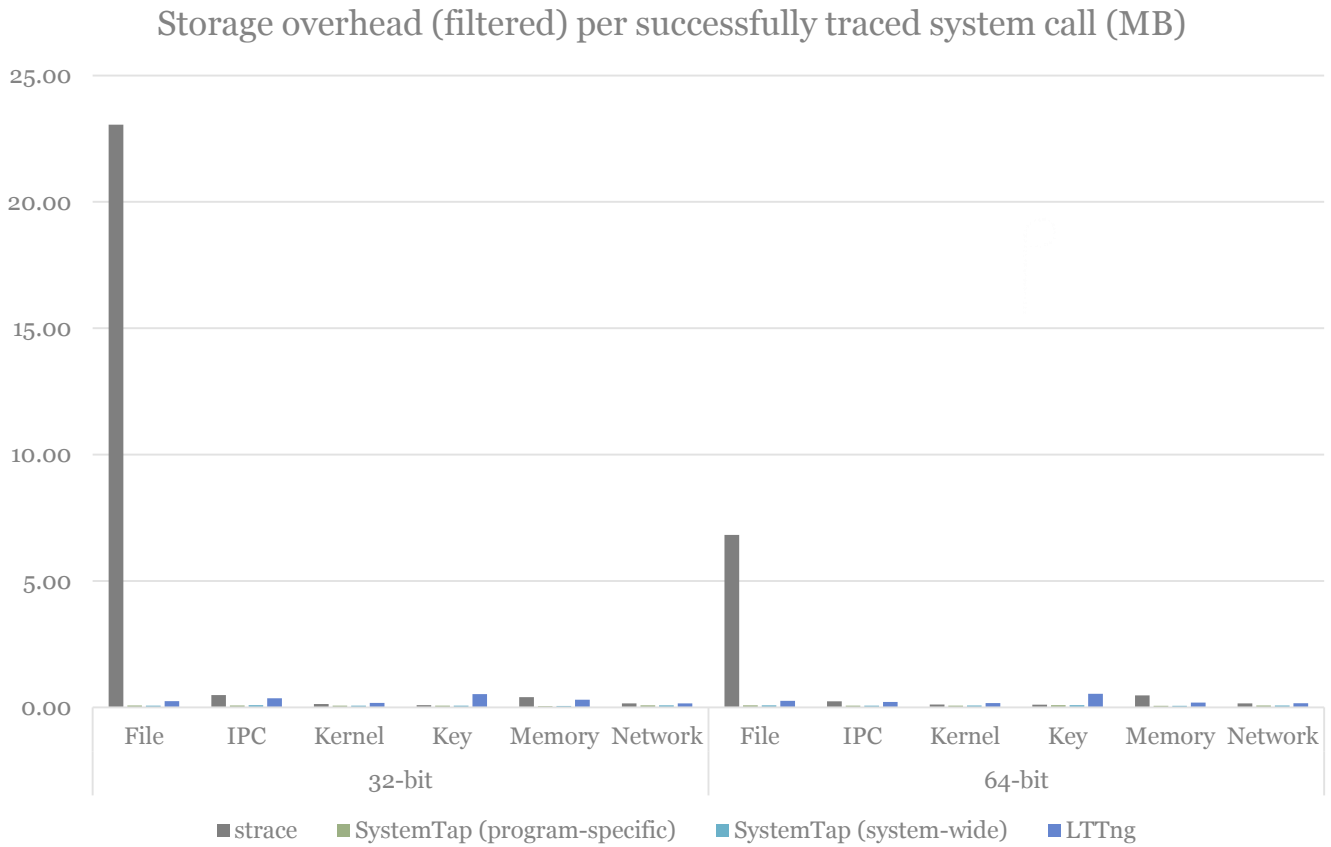


strace
SystemTap (program-specific)
SystemTap (system-wide)
LTTng

COST-BENEFIT ANALYSIS OF PROCESS TRACKING
COST ANALYSIS RESULTS: PERFORMANCE OVERHEAD



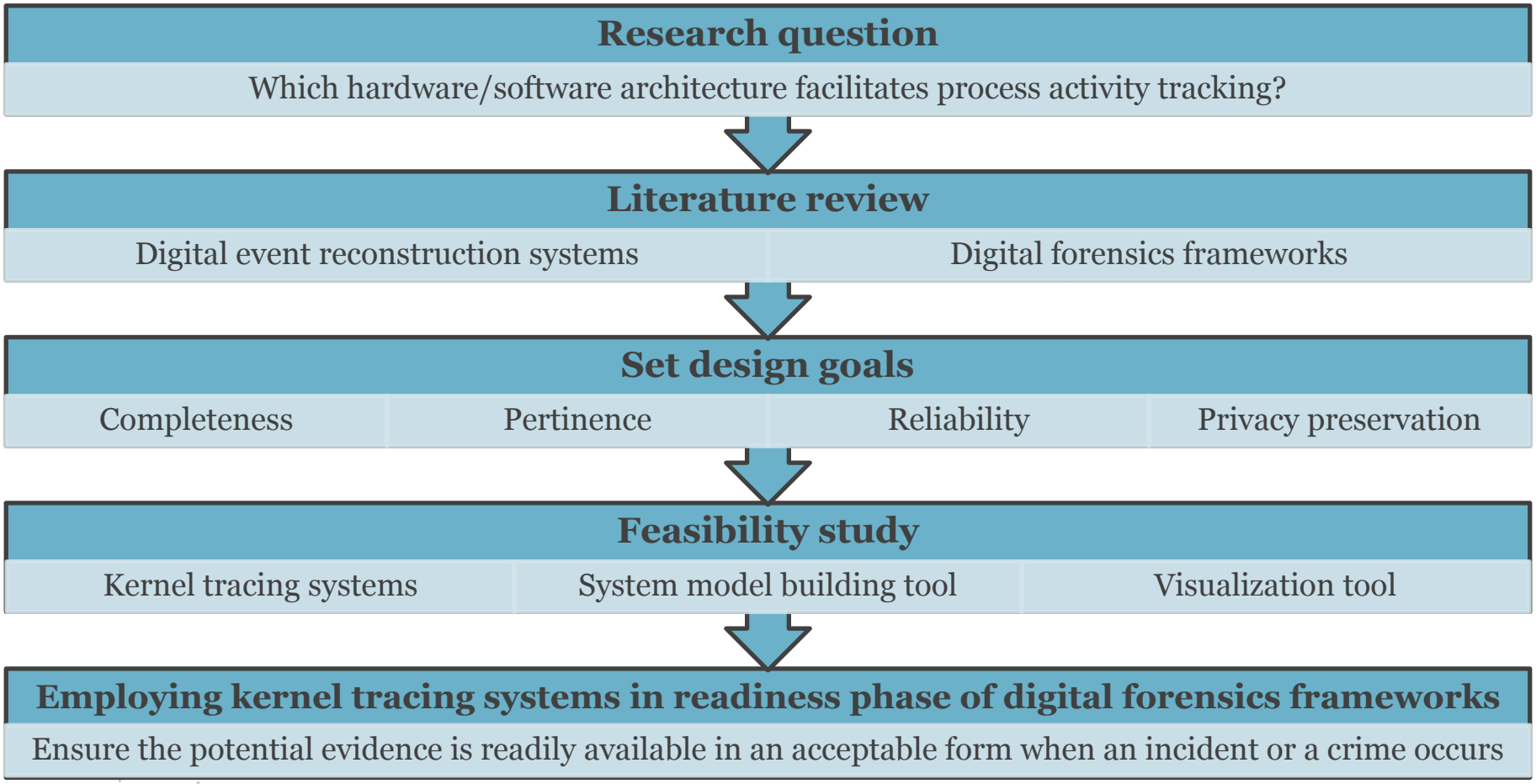
COST-BENEFIT ANALYSIS OF PROCESS TRACKING
COST ANALYSIS RESULTS: STORAGE OVERHEAD



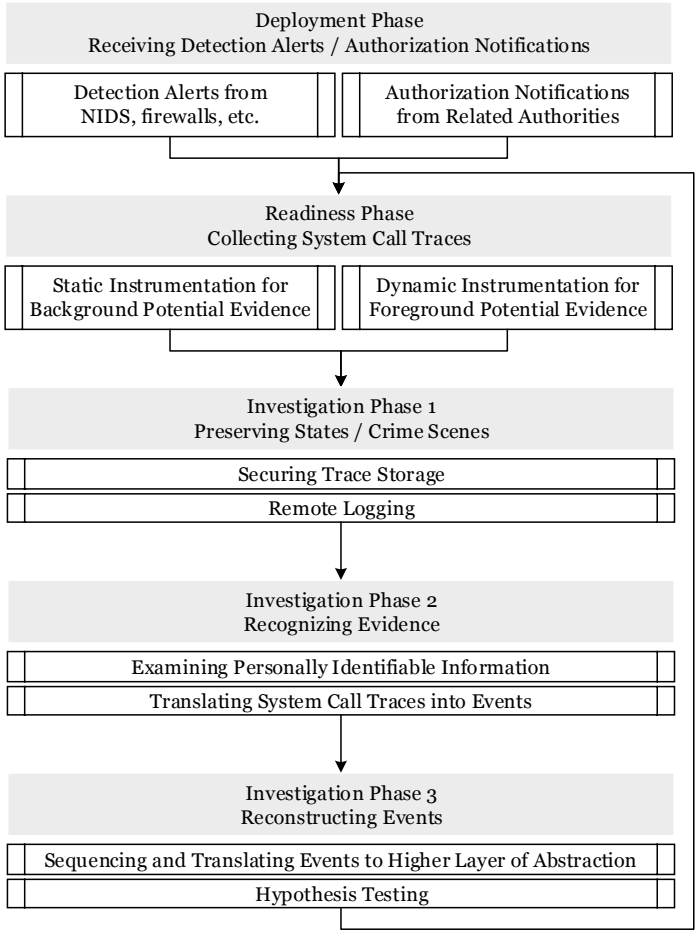
COST-BENEFIT ANALYSIS OF PROCESS TRACKING
CONCLUSION AND QUESTION RAISED

- **Kernel tracing systems can meet the two objectives of forensic readiness (Tan, 2001)**
  - maximize the capability of collecting credible digital evidence
  - minimize the cost of investigation
- **However**
  - high performance and storage overheads caused by dynamic instrumentation
- **For cost-benefit trade-off, we need to**
  - design the architecture for flexible and adjustable process tracking

ARCHITECTURE FOR PROCESS TRACKING
OVERVIEW

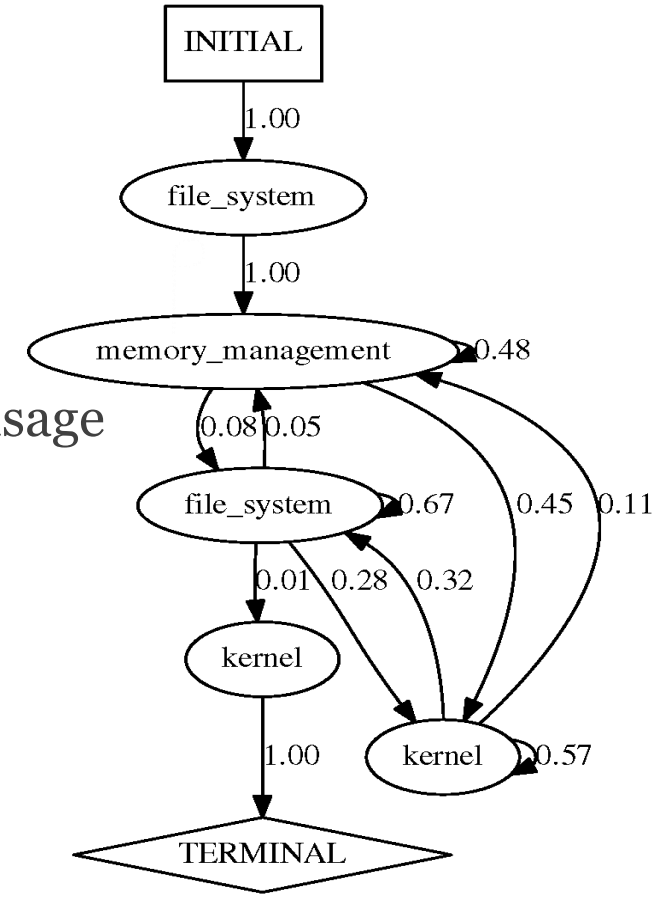


ARCHITECTURE FOR PROCESS TRACKING
PROTOTYPE FRAMEWORK



ARCHITECTURE FOR PROCESS TRACKING
FEASIBILITY STUDY: SYSTEM MODEL

- **Generated System Model**
  - ls command
  - each edge label
    - transition probability
  - the state transitions of resource usage



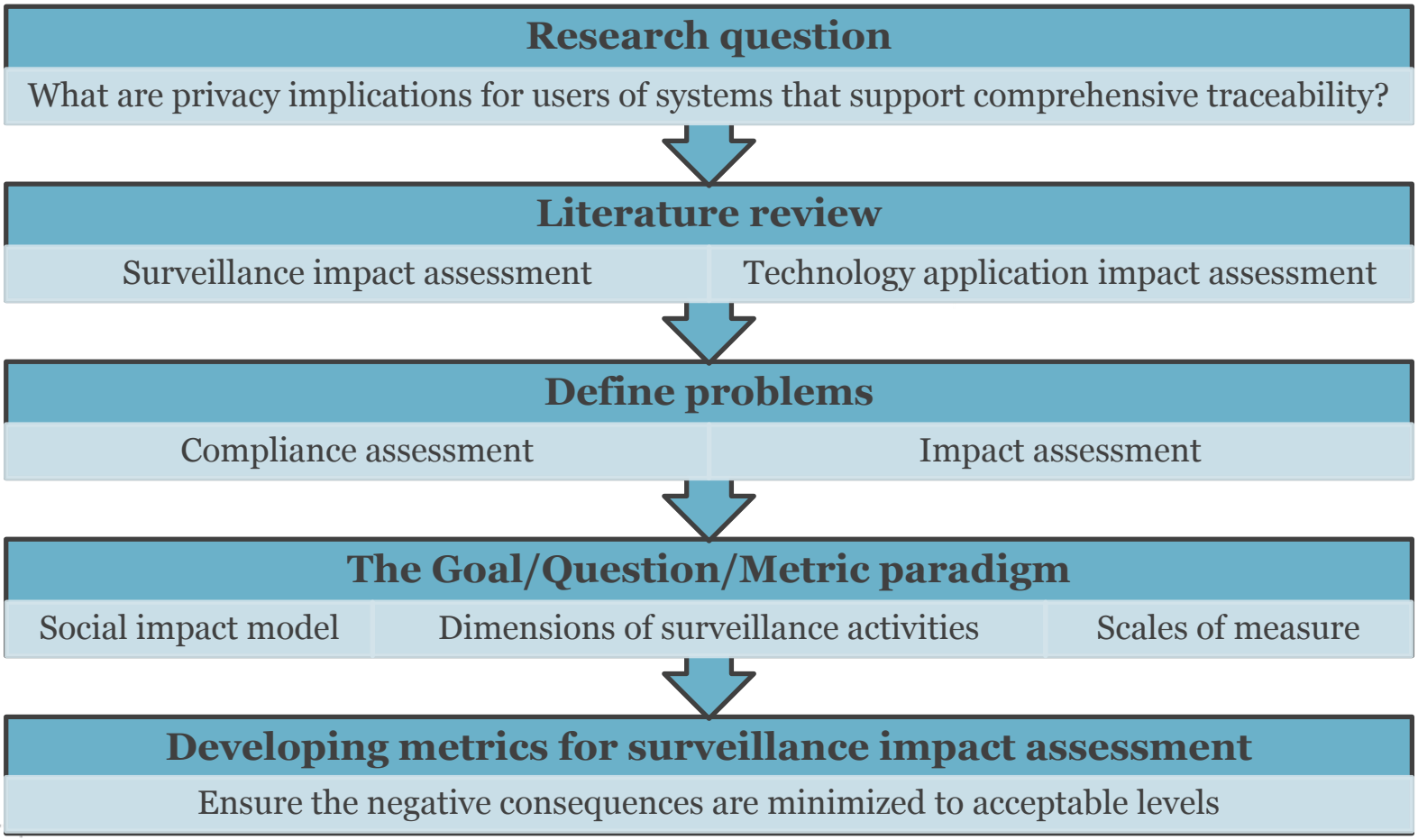
ARCHITECTURE FOR PROCESS TRACKING
FEASIBILITY STUDY: RECONSTRUCTING EVENTS

- **Reconstructing Events**
  - play back the system activity history as an animation
    - Gource
      - » generates a dynamic tree to animate the software development history
      - » user who commits the update floating near the files
      - » color the update actions (add, modify, and delete)
      - » animate the history by the timelines

ARCHITECTURE FOR PROCESS TRACKING
CONCLUSION AND QUESTION RAISED

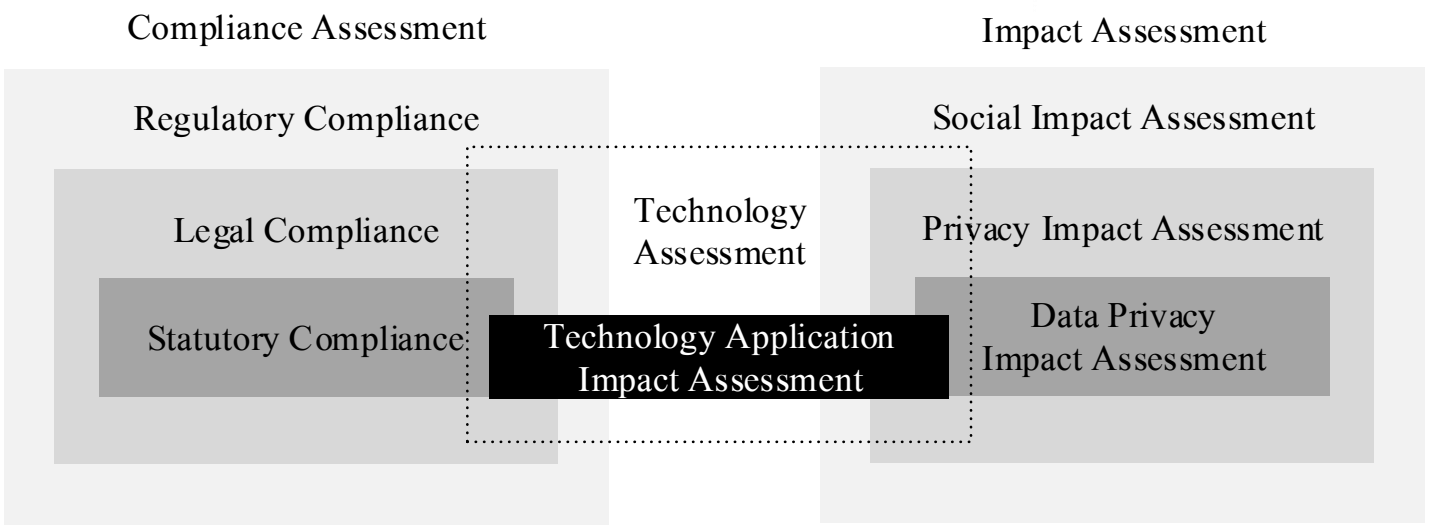
- **Employing kernel tracing systems in readiness phase of digital forensics frameworks can**
  - ensure the potential evidence is readily available in an acceptable form when an incident or a crime occurs
- **Interpret the meaning of digital events**
  - cause and effect analysis
  - layers of abstraction

PRIVACY IMPLICATIONS OF PROCESS TRACKING
OVERVIEW



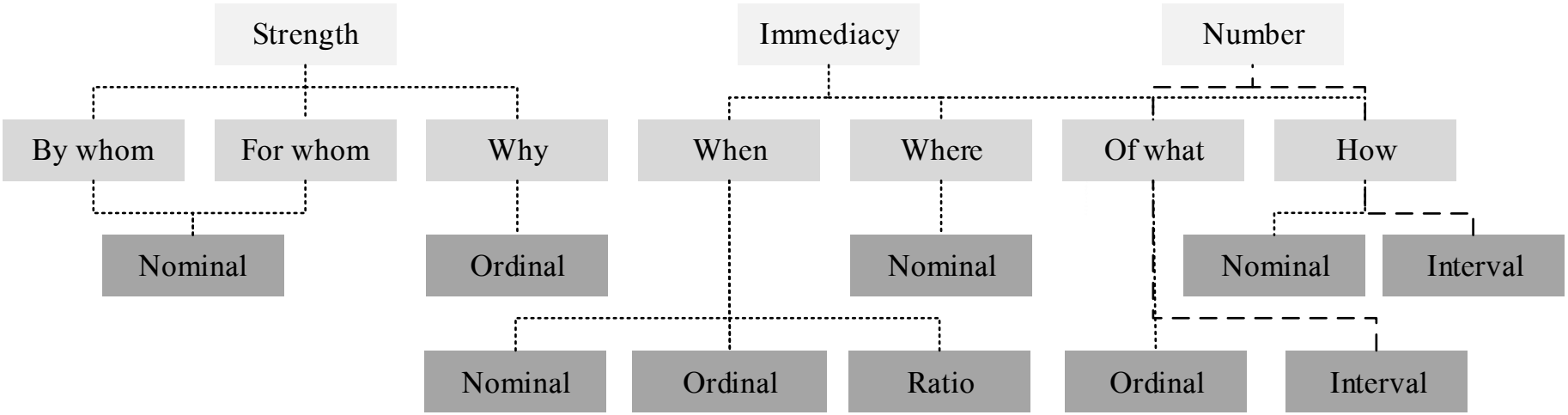
PRIVACY IMPLICATIONS OF PROCESS TRACKING
SURVEILLANCE IMPACT ASSESSMENT

- **Objective**
  - identify and assess the impacts posed by surveillance technologies on different dimensions of privacy



PRIVACY IMPLICATIONS OF PROCESS TRACKING

THE GOAL/QUESTION/METRIC PARADIGM



PRIVACY IMPLICATIONS OF PROCESS TRACKING
CONCLUSION AND QUESTION RAISED

- **Social Impact**
  - an ongoing chain process of continuing influences
- **Developing Metrics for Surveillance Impact Assessment**
  - can ensure the negative consequences are minimized to acceptable levels
- **Metric Validation through a Feasibility Study**
  - utilize the metrics to compare the impacts between
    - kernel tracing systems
    - application-level logging systems
  - provide credible information for decision-making

HØGSKOLEN I GJØVIK

Thank you

Yi-Ching Liao

Norwegian Information Security Laboratory

yi-ching.liao@hig.no