How Good is a Security Policy against Real Breaches?

Özgür Kafali[†], Jasmine Jones[*], Megan Petruso[*], Laurie Williams, and Munindar P. Singh

Security Policies vs Breaches

Goal: To help analysts measure the gaps between security policies and reported breaches by developing a systematic process based on semantic reasoning

Research Questions

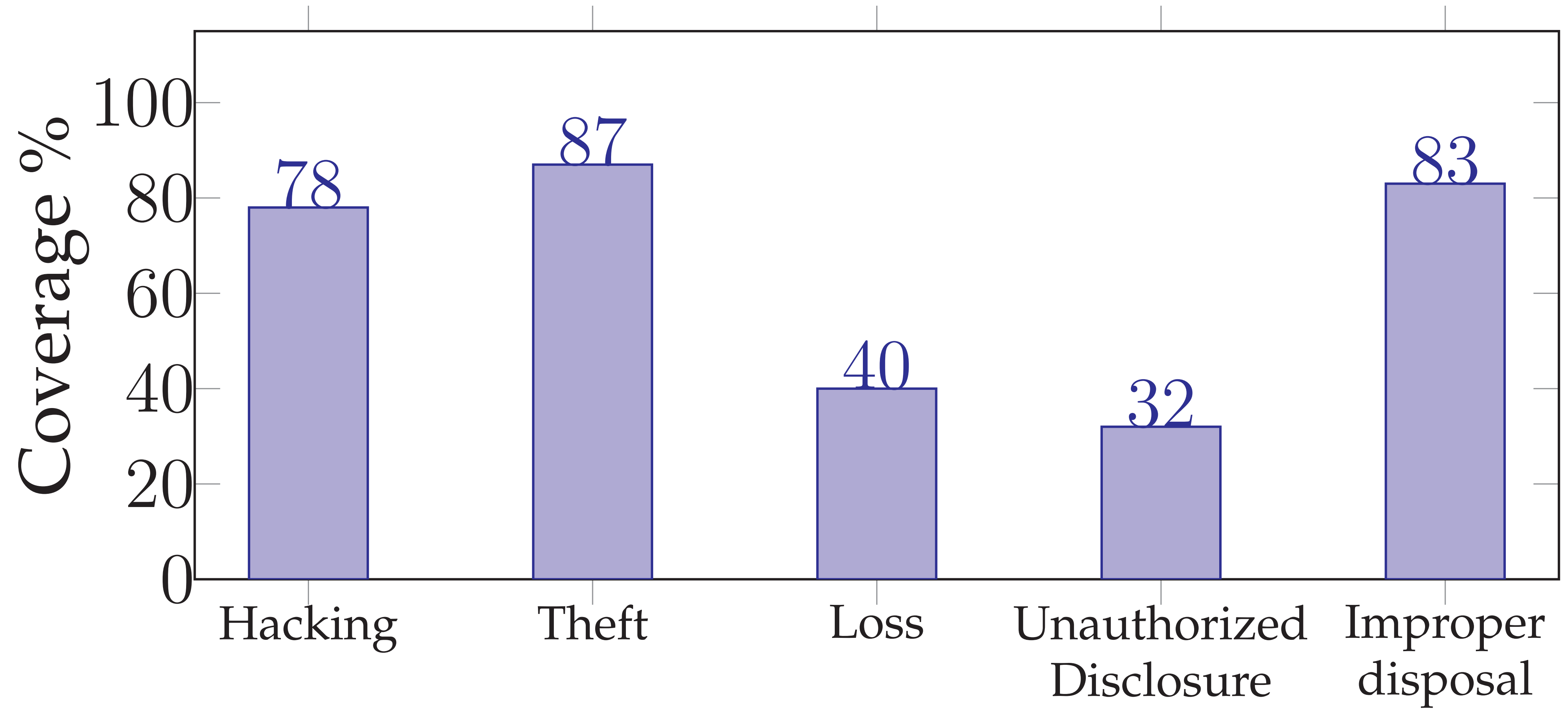
- How can we formalize security policies and breaches to bring out their mutual correspondence?
- What are the commonalities and differences between concepts in security policies and breach descriptions? How do those correspond to gaps in between?
- How prevalent are accidental misuses among reported breaches, and do security policies account for them?

Example

HHS breach incident: In 2010, a failure to erase data contained on disposed photocopiers' hard drives led to the disclosure of patient records.

HIPAA clause 45 CFR 164.310–(d)(2)(i): "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

HIPAA Case Study

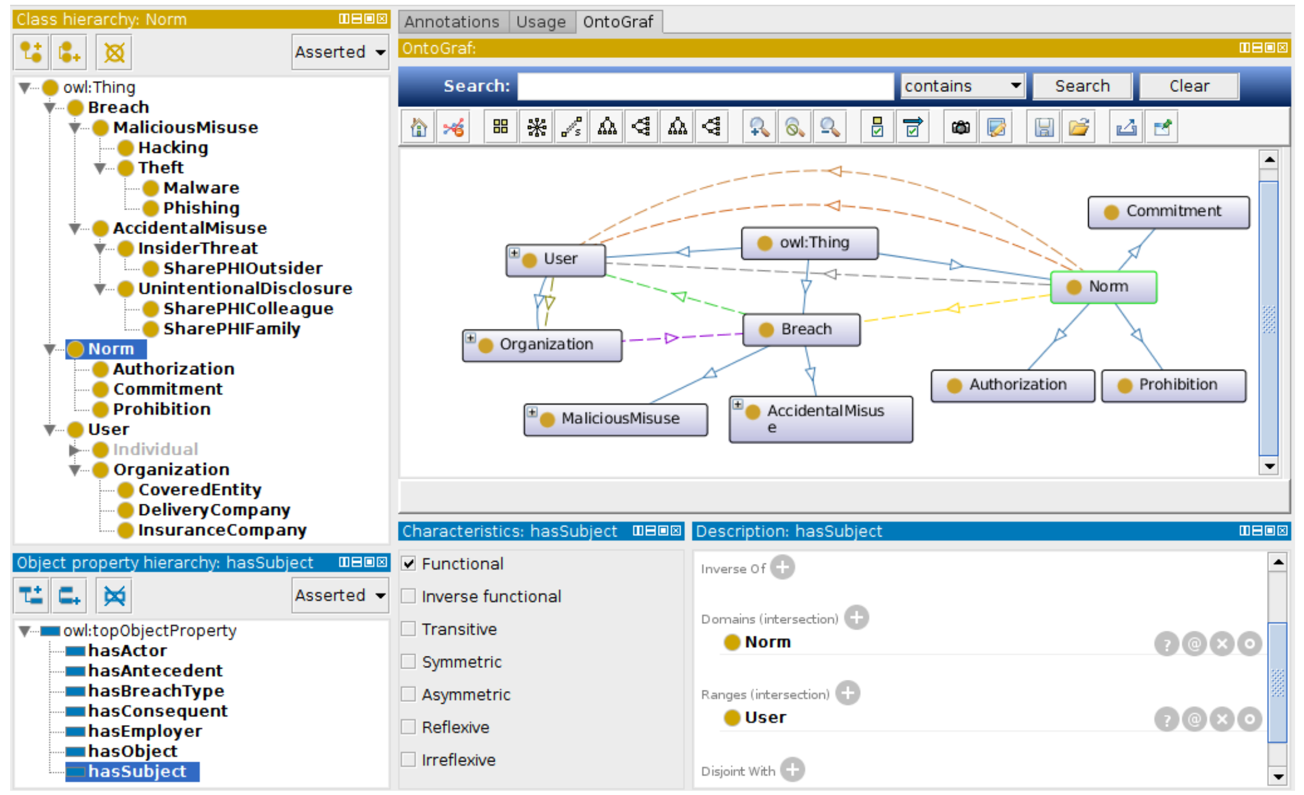


- 1,577 breaches reported by HHS
- 44% accidental misuses and 56% malicious misuses
- 65% overall coverage by HIPAA
- Significantly better coverage for malicious misuses than accidental misuses

Semaver Framework

Fundamental Elements

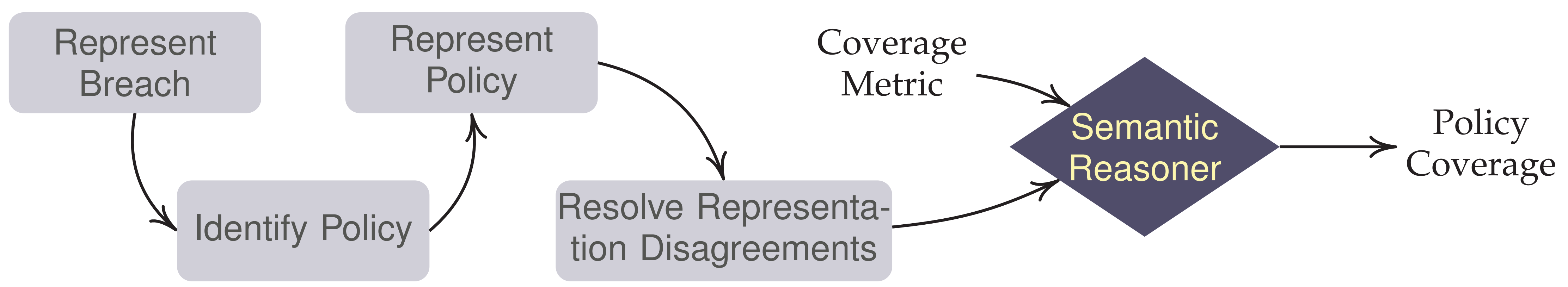
- Norms: Commitments, Authorizations, Prohibitions
  - Represent policy clauses
  - Represent breach incidents
- Breach ontology
- Coverage metric



☑ Functional
☐ Inverse functional
☐ Transitive
☐ Symmetric
☐ Asymmetric
☐ Reflexive
☐ Irreflexive

Domains (intersection): Norm
Ranges (intersection): User

Methodology



Limitations & Future Work

Limitations

- Subjective modeling
- Assumptions on ontology, e.g., single inheritance, no instances
- Incompleteness of breaches
- Only applied to healthcare domain (though HIPAA is a dominant standard)

Future Work

- Guidelines for ontology development
- Automation and crowd for norm gathering
- Validation of coverage metric
- Narrowing the gaps with policy refinement

[†]Contact Özgür Kafali at rkafali@ncsu.edu

[*]Jasmine Jones and Megan Petruso were supported by NSF under the Science of Software REU grant at NCSU