University of Kent

Computing

Reasoning about Security Related Artifacts

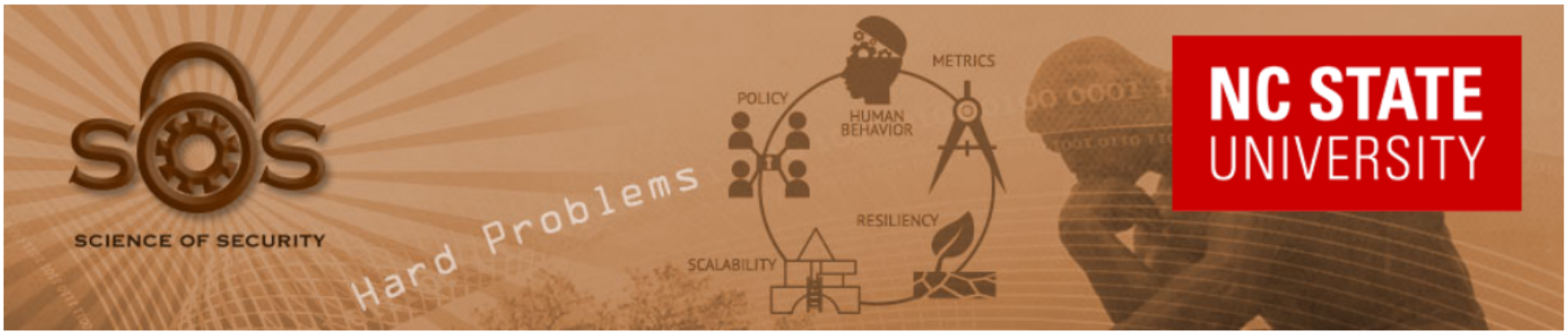
Requirements, Regulations, and Breach Reports

Dr Özgür Kafalı

Lecturer
School of Computing
University of Kent

13 July 2018

Research Background



Science of Security Lablet

North Carolina State University's (NCSU) Science of Security Lablet (SoSL) has embraced and helped build a foundation for NSA's vision of the Science of Security (SoS) and of a SoS community. We have emphasized data-driven discovery and analytics to formulate, validate, evolve, and solidify the theory and practice of security. Efforts in our current lablet have yielded significant findings, providing a deeper understanding of users' susceptibility to deception, developers' adoption of security tools, how trust between people relates to their commitments. These efforts have led to over 50 peer-reviewed publications with more on the way. The lablet has supported 32 faculty and students and engaged more than 30 colleagues from industry.

Motivated by NSA's overarching vision for SoS and building on our experience and accomplishments, we will continue (1) developing a science-based foundation for the five hard problems that we previously helped

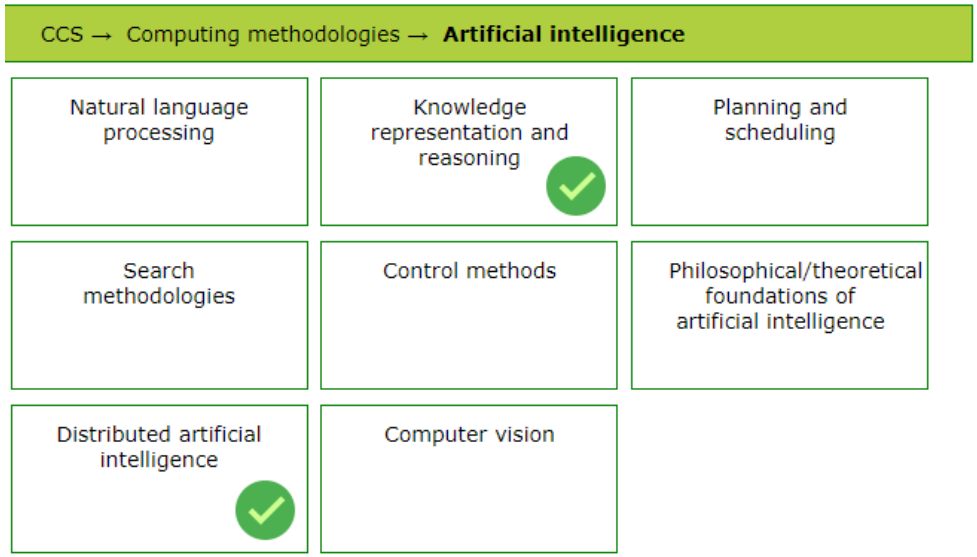
Science of Security Lablet

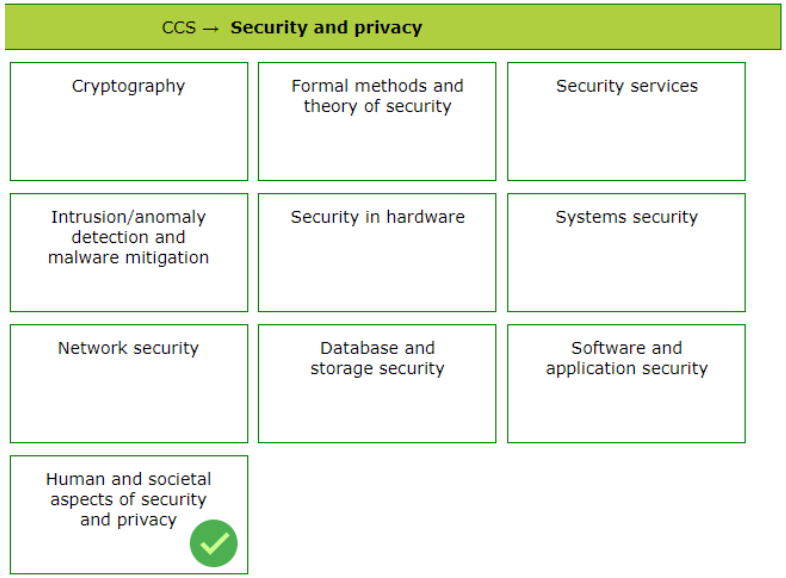
- Home
- Lablet Hard Problems
- Lablet Projects
- Events
- Research Planning and Publication Guidelines
- Security Research Home

Security Hard Problems

- Resilient architectures
- Scalability & composability
- Metrics
- Human behaviour
- Policy and governance

Research Interests



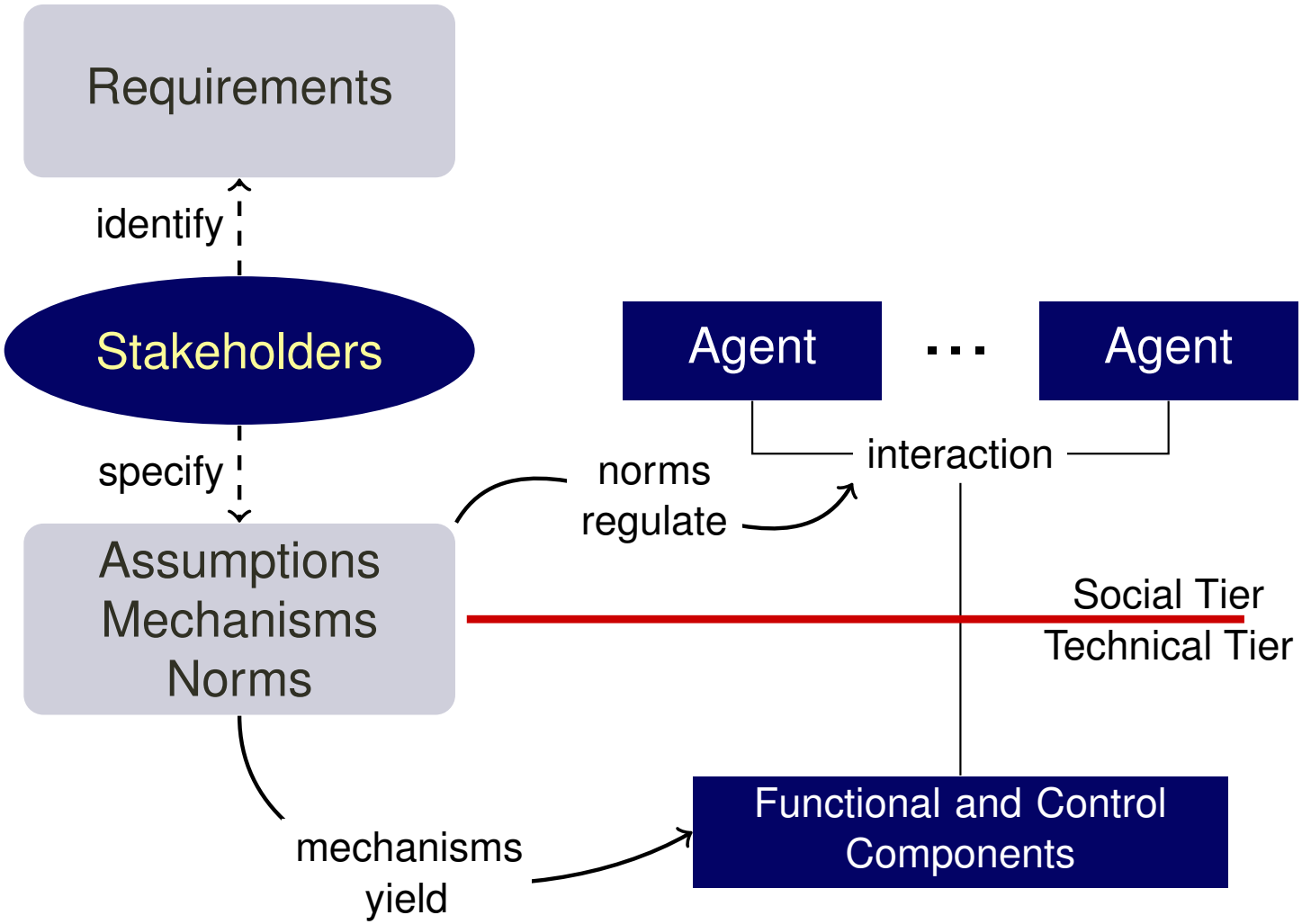


- Distributed AI → Knowledge Representation and Reasoning
- Security and Privacy → Human and Social Factors

Socio-technical Systems (STS)

- STS: Any modern information system
  - Technical: Computers and software components
  - Social: People and interactions
- Example: Hospital environment
  - Technical: Electronic health records (EHR) software
  - People: Doctors, nurses, patients, admin staff
  - Interactions: Doctor consulting a colleague about a patient
- Significance
  - Cause of data breaches: Mostly humans
  - Solutions: Combination of technical and social controls

STS Conception



Regulations

Credit to my colleague Munindar Singh

Ambiguity

- Hard to extract “actionable” requirements for users
  - State the obvious
  - Contradict with themselves or each other
  - Fail to present all possible alternatives

Regulatory Norms

- Describe expected behaviour of users
- Formalise who is accountable to whom and for what
- Normative reasoning
  - Deontic logic concepts
  - AI and law for legal text
  - Requirements engineering

- *norm*(SUBJECT, OBJECT, antecedent, consequent)
- Three norm types:
  - Commitment
  - Authorisation
  - Prohibition

---

von Wright. Deontic logic: A personal view. Ratio Juris, 1999

Commitment

- A physician is committed to the hospital to operating upon patients in an emergency
- C(PHY, HOS, emergency, operate)

- The physician is accountable to the hospital for this commitment
- If the physician fails to operate upon patients, the commitment is violated

Authorisation

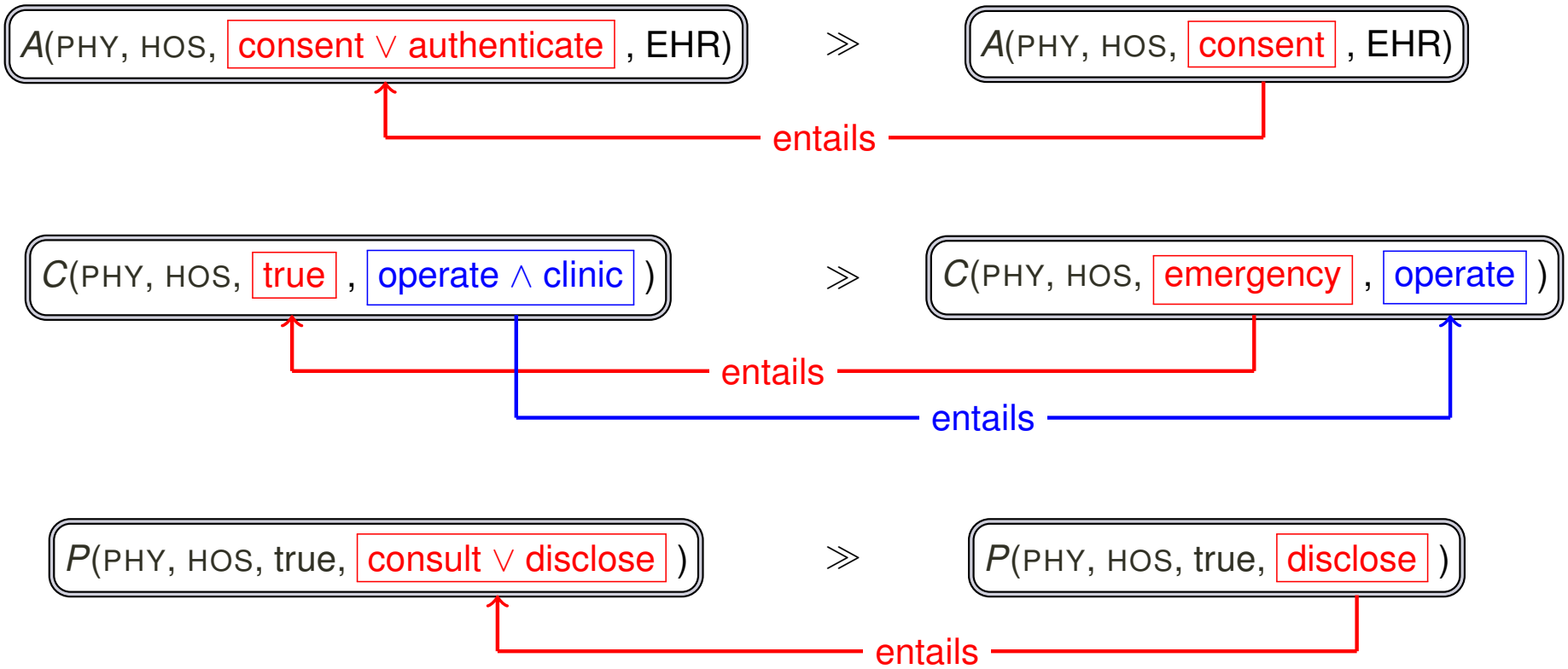
- A physician is authorised by the hospital to access a patient's EHR if the patient gives consent
- *A*(PHY, HOS, consent, EHR)

- Not simply a permission: The object (HOS) is accountable to the subject (PHY)

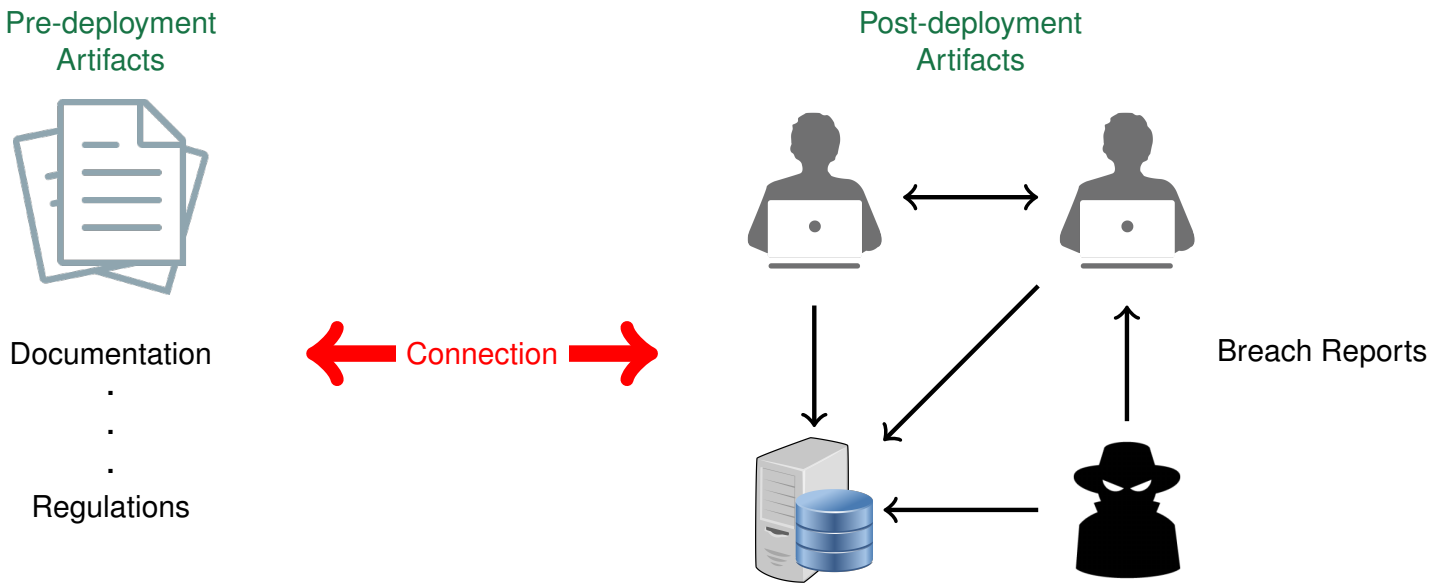
Prohibition

- A physician is prohibited by the hospital from disclosing a patient's protected health information (PHI) to outsiders
- P(PHY, HOS, true, disclose)

Norm Strength



Connecting Regulations and Breaches



- Research question: Where are the gaps between what the regulation states and what happened during the breach?

Kafalı, Jones, Petruso, Williams, and Singh. "How Good is a Security Policy against Real Breaches? A HIPAA Case Study". Proceedings of the 39th International Conference on Software Engineering (ICSE), pages 530-540, 2017

Breach Analysis

- HHS breach incident: In 2010, an employee in a covered entity forgot to erase data contained on disposed photocopiers' hard drives, which led to disclosure of patient records.

- HIPAA clause 45 CFR 164.310–(d)(2)(i): "A covered entity or business associate must implement policies and procedures to address the final disposition of electronic protected health information, and the hardware or electronic media on which it is stored."

HHS: US Department of Health and Human Services
HIPAA: US Health Insurance Portability and Accountability Act

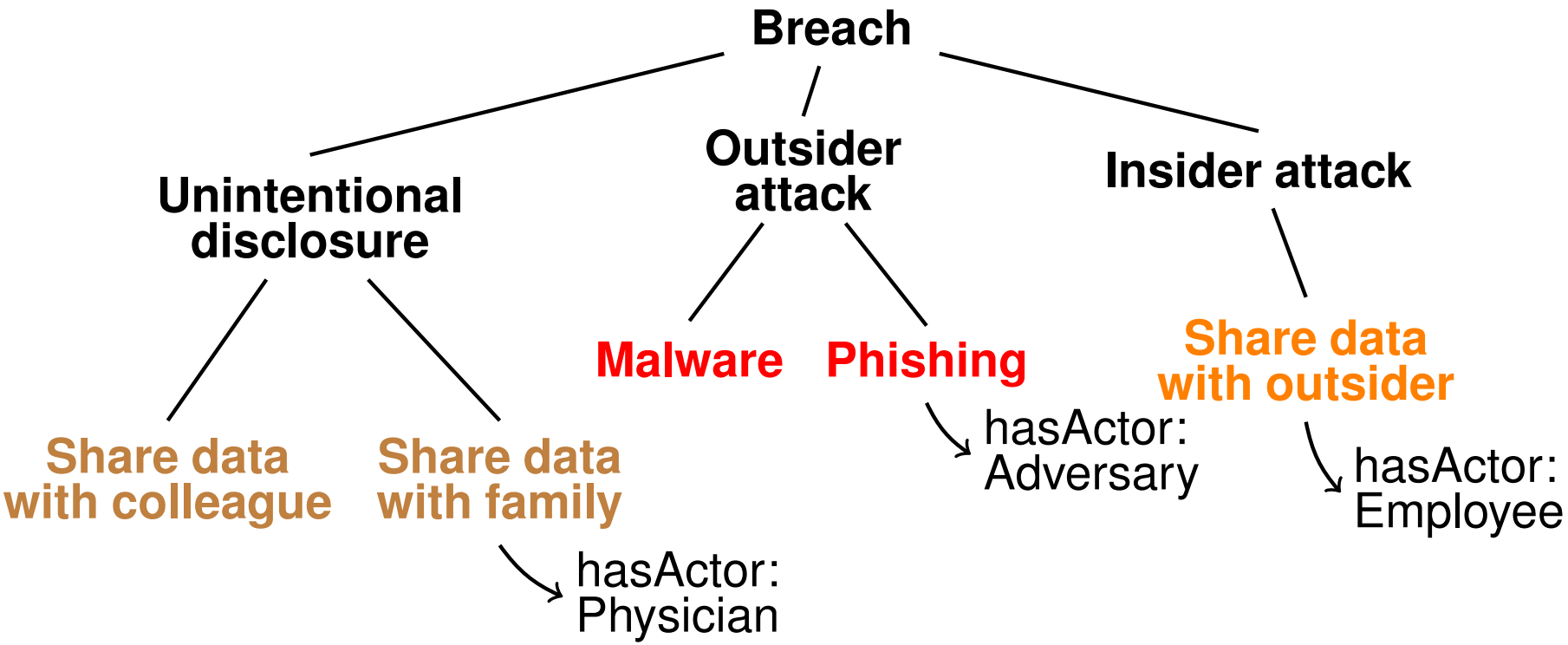
Breach Analysis

- HHS breach incident: In 2010, an employee in a covered entity forgot to erase data contained on disposed photocopiers' hard drives, which led to disclosure of patient records.

- HIPAA clause 45 CFR 164.310–(d)(2)(i): "A covered entity or business associate must implement policies and procedures to address the final disposition of electronic protected health information, and the hardware or electronic media on which it is stored."

HHS: US Department of Health and Human Services
HIPAA: US Health Insurance Portability and Accountability Act

Breach Ontology

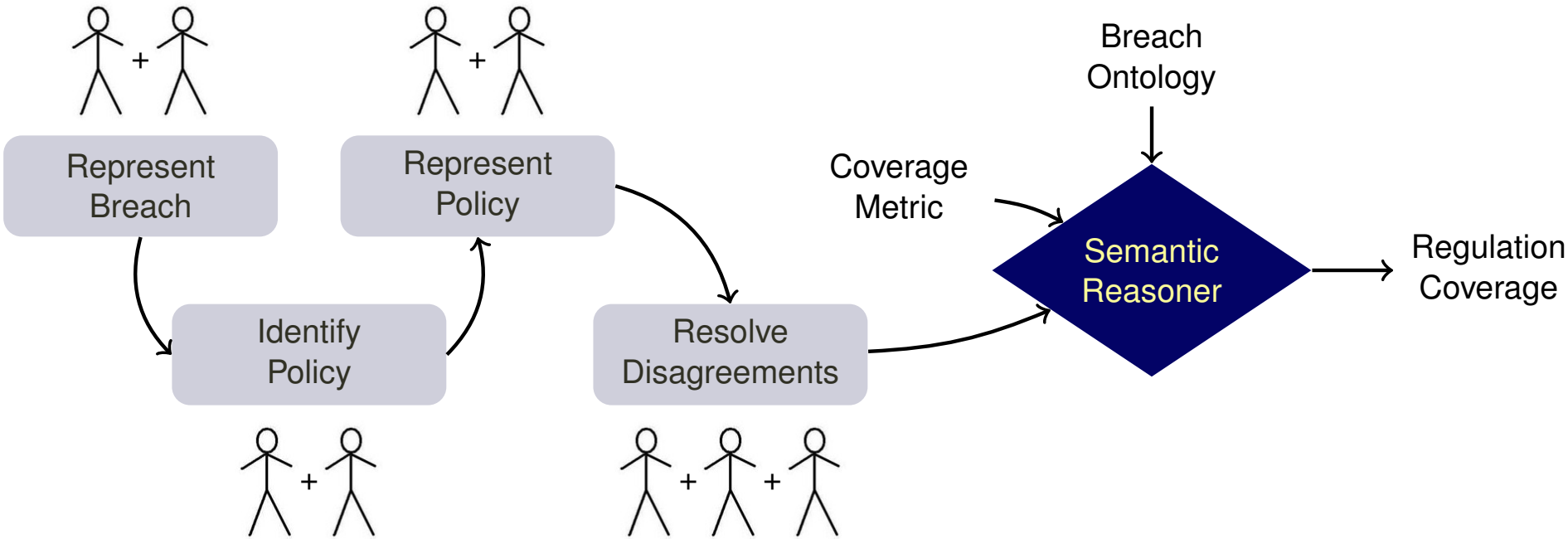


From Norm Similarity to Regulation Coverage

1. Pairwise norm similarity: Compute similarity between individual norm elements
    a. Taxonomic distance between concepts: Count edges in between concepts
    b. Properties of concepts: Compute similarity among common properties

2. Regulation coverage: Compute overall coverage based on the similarity between each breach and the corresponding regulation clause

Methodology



HHS Breach Reports

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

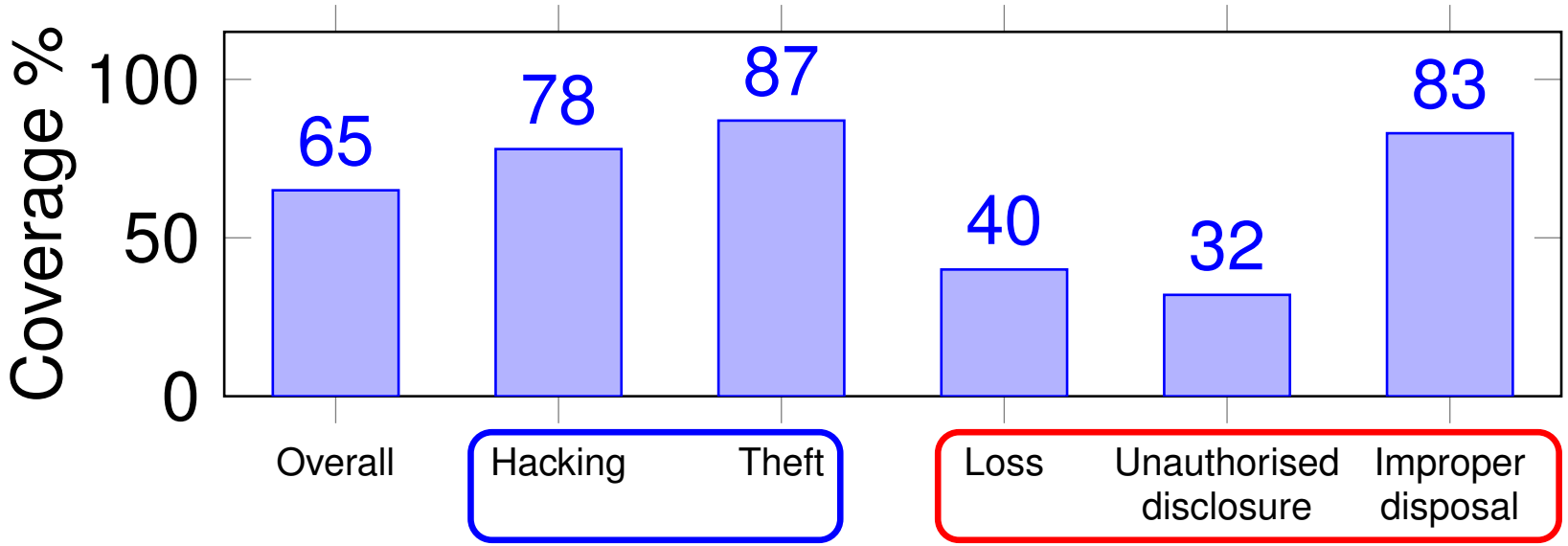
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
Business Associate Present:	No					
Web Description:	Five desktop computers containing unencrypted electronic protected health information (e-PHI) were stolen from the covered entity (CE). Originally, the CE reported that over 500 persons were involved, but subsequent investigation showed that about 260 persons were involved. The ePHI included demographic and financial information. The CE provided breach notification to affected individuals and HHS. Following the breach, the CE improved physical security by installing motion detectors and alarm systems security monitoring. It improved technical safeguards by installing enhanced antivirus and encryption software. As a result of OCR's investigation the CE updated its computer password policy.					
Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
Mark D. Lurie, MD	CA	Healthcare Provider	5166	11/20/2009	Theft	Desktop Computer
L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer
David I. Cohen, MD	CA	Healthcare Provider	857	11/20/2009	Theft	Desktop Computer
Michele Del Vicario, MD	CA	Healthcare Provider	6145	11/20/2009	Theft	Desktop Computer
Joseph F. Lopez, MD	CA	Healthcare Provider	952	11/20/2009	Theft	Desktop Computer
City of Hope National Medical Center	CA	Healthcare Provider	5900	11/23/2009	Theft	Laptop
The Children's Hospital of Philadelphia	PA	Healthcare Provider	943	11/24/2009	Theft	Laptop
Cogent Healthcare, Inc.	TN	Business Associate	6400	11/25/2009	Theft	Laptop
Democracy Data & Communications, LLC (	VA	Business Associate	83000	12/08/2009	Other	Paper/Films

Notice to the Secretary of HHS breach of unsecured protected health information affecting 500 or more individuals: https://ocrportal.hhs.gov/ocr/breach/

Results: Are Accidental Misuses Prevalent?

- Investigated 1,577 breaches reported by HHS
  - *Hacking* (191) and *Theft* (642) contain malicious misuses
  - *Loss* (129), *Unauthorised disclosure* (338), and *Improper disposal* (58) contain accidental misuses
  - *Unclassified* (219): 68% accidental misuses and 13% malicious misuses
- Overall: 44% accidental misuses and 56% malicious misuses

Results: How Good is HIPAA against Real Breaches?



- Investigated a random subset of breaches reflecting the distribution of categories
- Better coverage for malicious misuses than accidental misuses

Ongoing Work: Crowdsourcing

- Follow-up study to extract information from breach reports using the crowd
- Prepared a survey-style online form to extract norm elements
  - Which elements of a norm are harder to extract?
  - What effects worker performance?
  - Breach reporting: Evaluate performance on modified breaches
- Deployed on Amazon Mechanical Turk
- Created a curated dataset of worker responses and evaluations

---

Guo, Kafalı, Jeukeng, Williams, and Singh. “What Can We Learn about Security from Breaches? Connecting Regulations and Breaches for Improved Security and Privacy Requirements”. Empirical Software Engineering journal (In preparation), 2018

Ongoing Work: Natural Language Processing

- Use the curated dataset to train automated methods
- Predict which sentences in a breach description imply norms

- Classify recovery actions in a breach description
  - Technical requirements (for software developers)
  - Regulatory requirements (for end-users)
  - Administrative requirements (e.g. training)

Guo, Kafalı, and Singh. “Extraction and Formal Representation of Natural Language Requirements from Breach Reports”. 5th International Workshop on Artificial Intelligence for Requirements Engineering (Accepted), 2018

Research Plan: Breach Analysis

- Backward responsibility: Which processes are likely to cause a breach and which parties are accountable?
  - What interactions and inter-dependencies are likely to carry risk?
  - Which roles carry complexity in terms of task responsibility?
  - Which regulations need revision?

- Forward responsibility: Which parties are responsible for recovering from a breach?
  - What actions are taken based on the type of the breach?
  - Which roles have the capability to carry out those actions?
  - Is there any correlation between the cause of the breach and the recovery actions?

Research Plan: Training Theme

- Guidelines (NIST, Cyber Essentials)
  - CVSS (vulnerability prioritisation)
  - CMSS (misuse prioritisation)
  - SP 800-16 (role-based training guidelines)
- Breach portal
- Interactive and targeted training
  - Incident-driven
  - Agent-based simulation
  - Game playing

Core Collaborators


Dr Pınar Yolum – Utrecht University, Netherlands


Dr Munindar Singh – North Carolina State University, US


Dr Laurie Williams – North Carolina State University, US


Dr Kostas Stathis – Royal Holloway University of London, UK


Dr Alberto Paccanaro – Royal Holloway University of London, UK


Dr Francesca Toni – Imperial College London, UK


Dr Akın Günay – Lancaster University, UK


Dr Paolo Torroni – University of Bologna, Italy


Dr Bedour Alrayes – King Saud University, Saudi Arabia