University of Kent

Computing

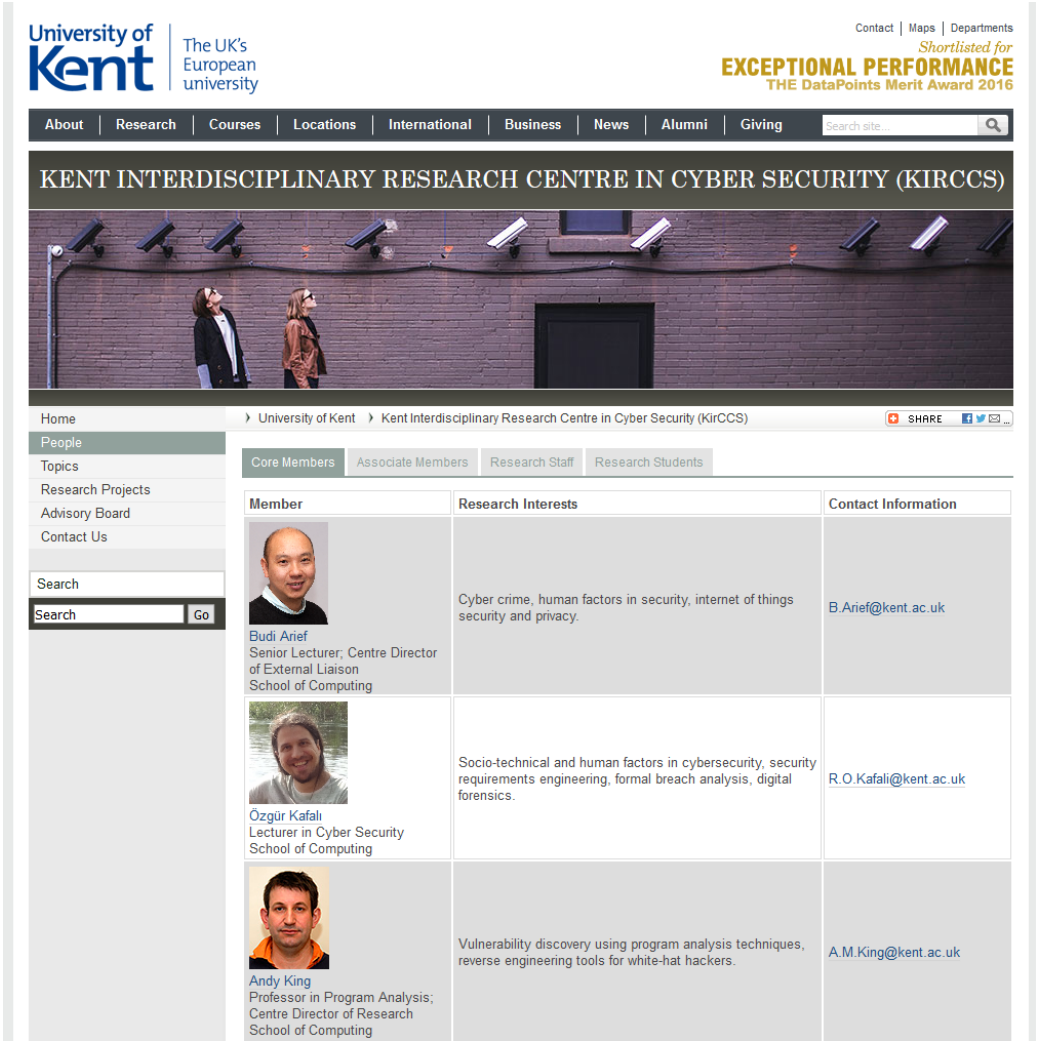
The Social Side of Security Requirements, Regulations, and Breaches

Dr Özgür Kafalı

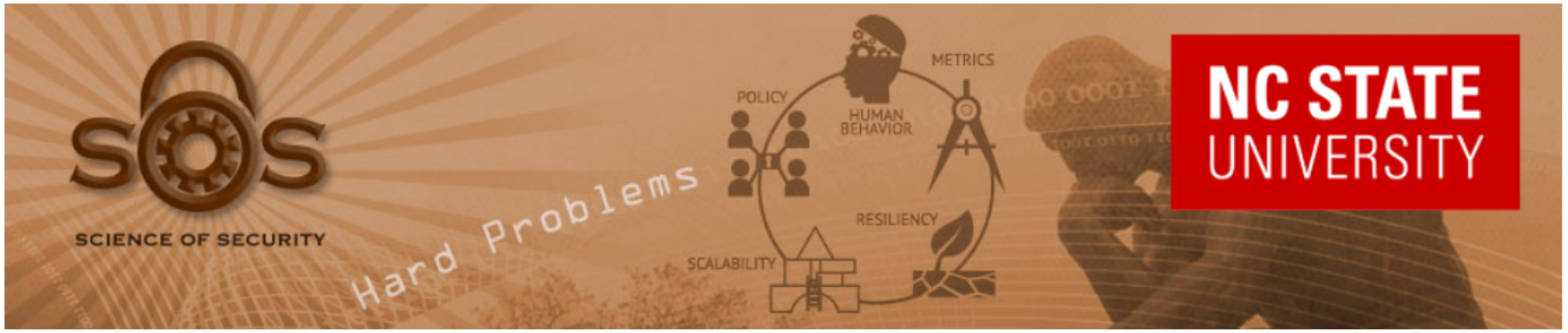
Lecturer
School of Computing
University of Kent

20 March 2018

Research Background



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

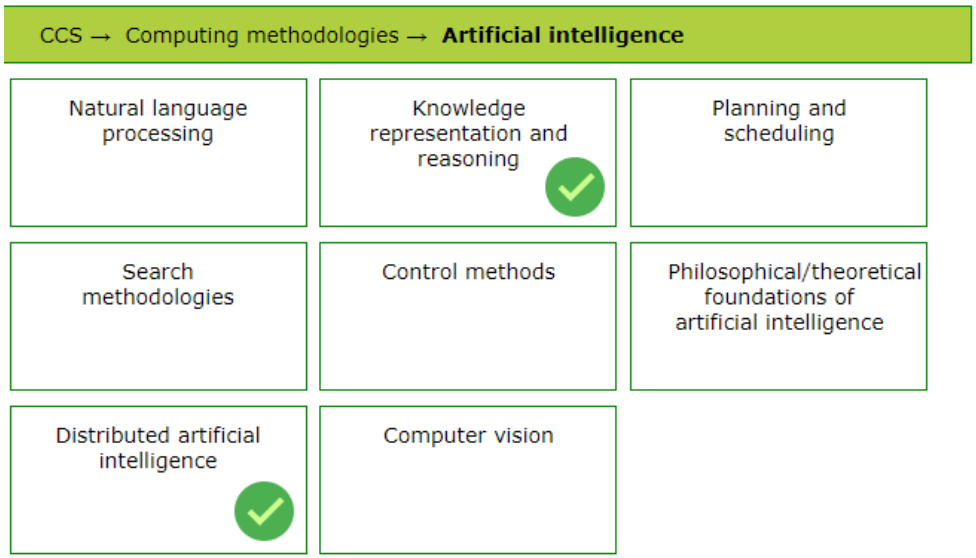
Science of Security Lablet

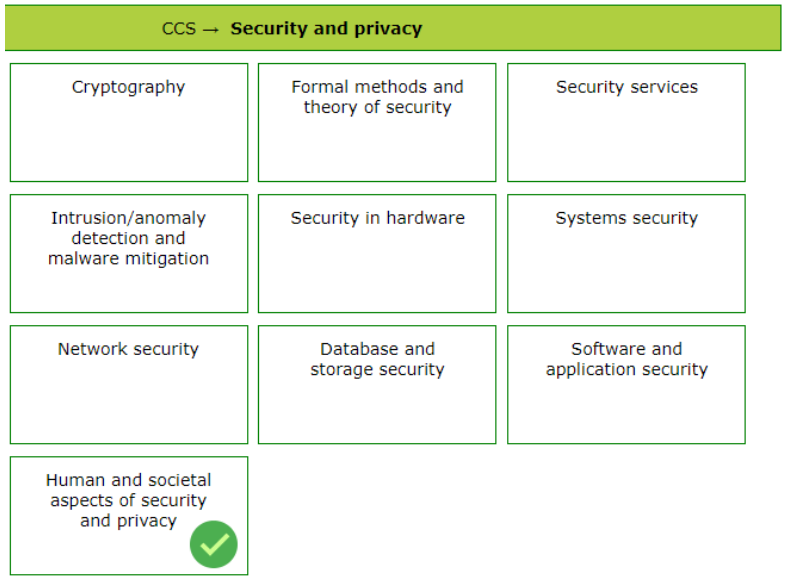
- Home
- Lablet Hard Problems
- Lablet Projects
- Events
- Research Planning and Publication Guidelines
- Security Research Home

Hard Problems

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

Research Interests





Glossary

- Sociotechnical systems
- Regulations and norms
- Accountability
- Role-based access control
- Ontologies

Security-Critical Data

https://techgeek365.com/how-to-protect-your-data-when-shopping-online/

Alternative Ways to Use your Card

Oops, They Did It Again

- Nurses peek celebrity medical records

http://www.avant.org.au/news/20160622-improper-access-of-medical-records/
http://articles.latimes.com/2008/mar/15/local/me-britney15

Common Factor in Breaches

- Mostly humans

Common Factor in Breaches

- Mostly humans
- More broadly: Sociotechnical and human factors

Common Factor in Breaches

- Mostly humans
- More broadly: Sociotechnical and human factors

- Corroborated by reports from
  - Governments
  - Organisations
  - Academic studies

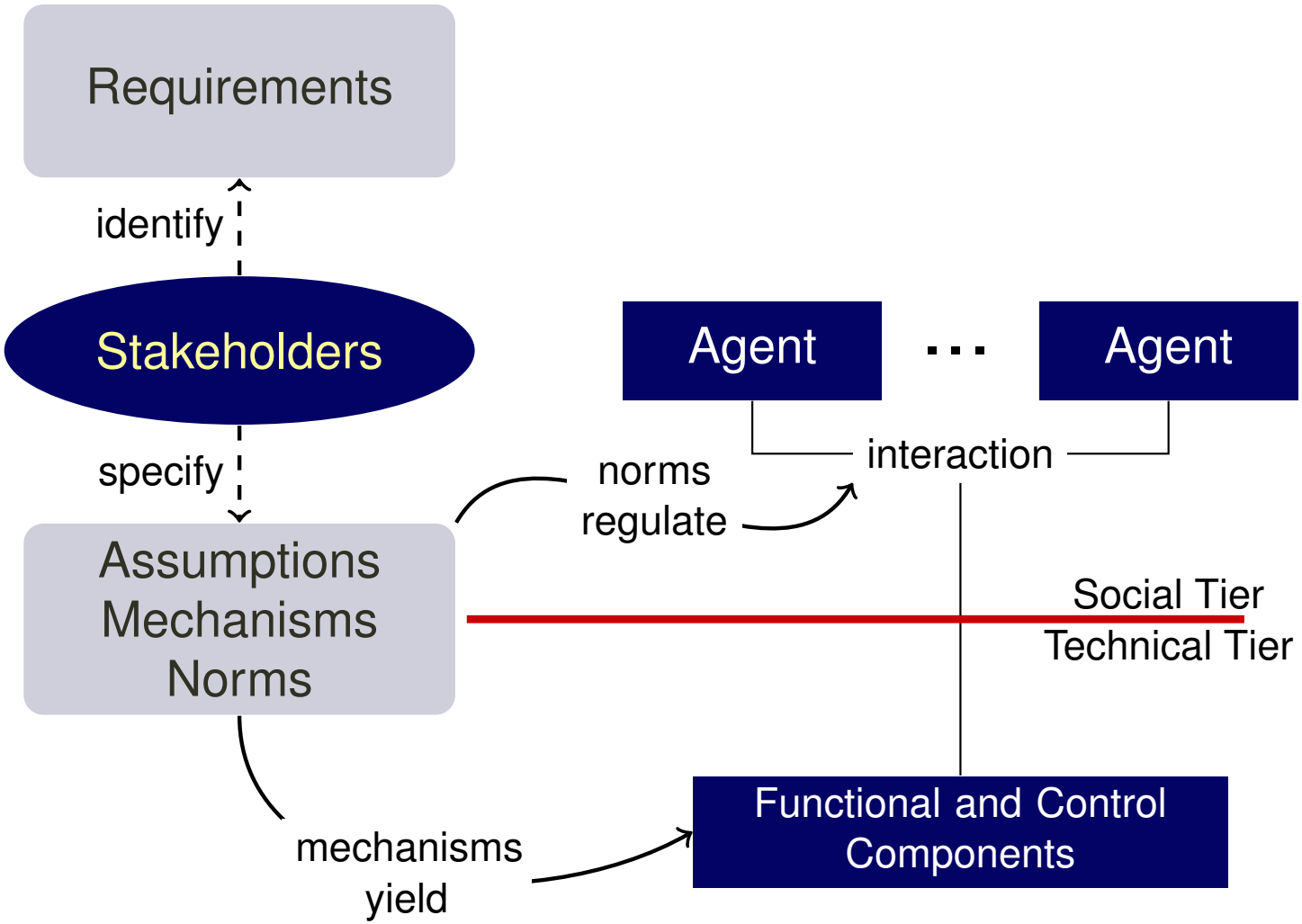
Sociotechnical Systems (STS)

- STS: Any modern ICT system
  - Technical: Computers and software components
  - Social: People and interactions

Sociotechnical Systems (STS)

- STS: Any modern ICT system
  - Technical: Computers and software components
  - Social: People and interactions
- Consider a hospital environment
  - Technical: Electronic health records (EHR) software
  - People: Doctors, nurses, patients
  - Interactions: Doctor consulting a colleague

STS Conception



Regulatory Norms

Credit to my colleague Munindar Singh

Security Requirements and Regulations

- Correspond to “authorizations”, “commitments”, and “prohibitions”
- Authorization: A doctor is authorized to access a patient’s EHR if the patient gives consent
- Commitment: The hospital is committed to keeping patients’ EHR secure
- Prohibition: A doctor is prohibited from disclosing a patient’s protected health information (PHI) to outsiders

Challenges

- Elicitation: Extracting functional requirements is hard, extracting security and privacy requirements is (almost) impossible
- Hybrid approaches for extraction of requirements from regulations and breaches
  - Human intelligence: Crowdsourcing
  - Machine intelligence: Natural language processing (NLP)

Challenges

- Elicitation: Extracting functional requirements is hard, extracting security and privacy requirements is (almost) impossible
- Hybrid approaches for extraction of requirements from regulations and breaches
  - Human intelligence: Crowdsourcing
  - Machine intelligence: Natural language processing (NLP)

- Ambiguity

Need for Intelligence: Breaches vs Bridges

Getty Images

Core Research Questions

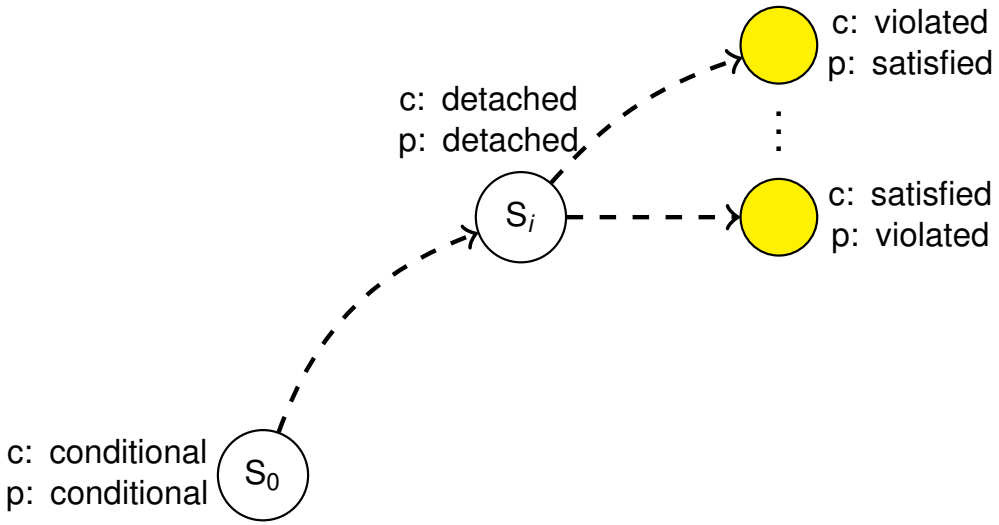
- RQ_1 – Verification: How can we verify an STS specification against the requirements of its stakeholders?
- RQ_2 – Design: How can we design a secure and privacy-aware STS with respect to tradeoffs and conflicts among its requirements?
- RQ_3 – Extraction: How can we identify potential malicious and accidental misuses, and associated requirements of an STS?

RQ_1: Requirements Verification

c: conditional
p: conditional
S_0

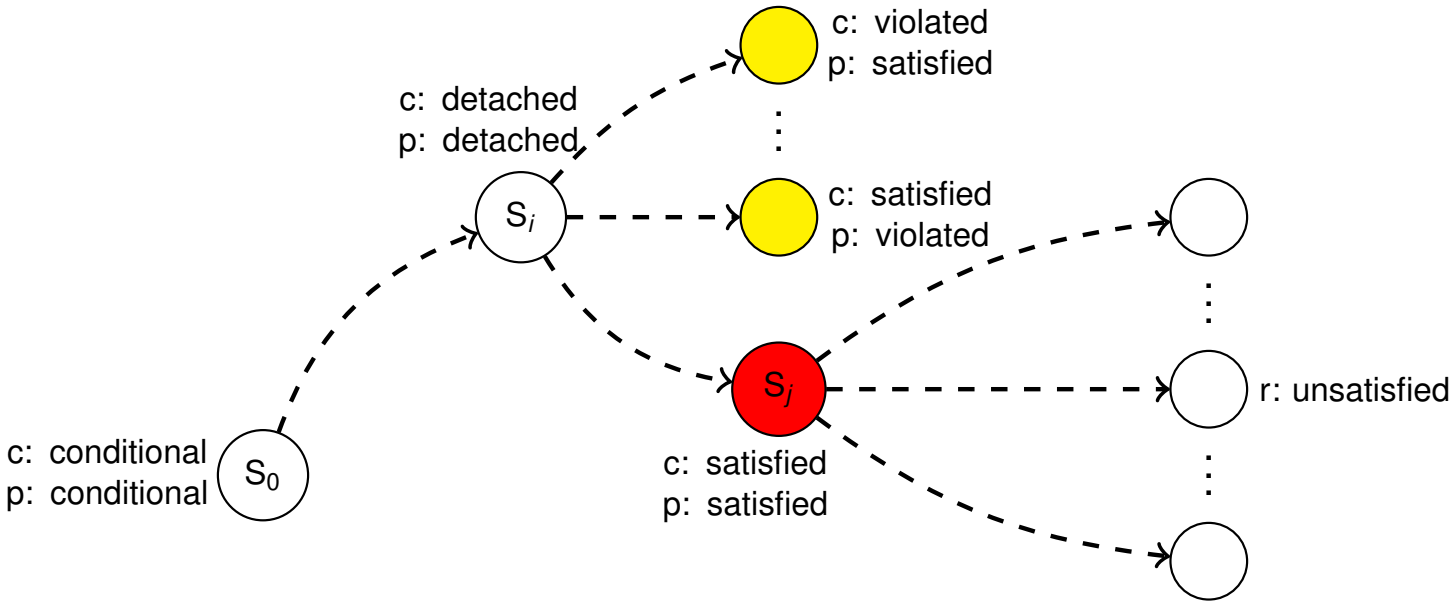
Kafalı et al. Revani: Revising and Verifying Normative Specifications for Privacy. IEEE Intelligent Systems, 31(5):8-15, 2016

RQ_1: Requirements Verification



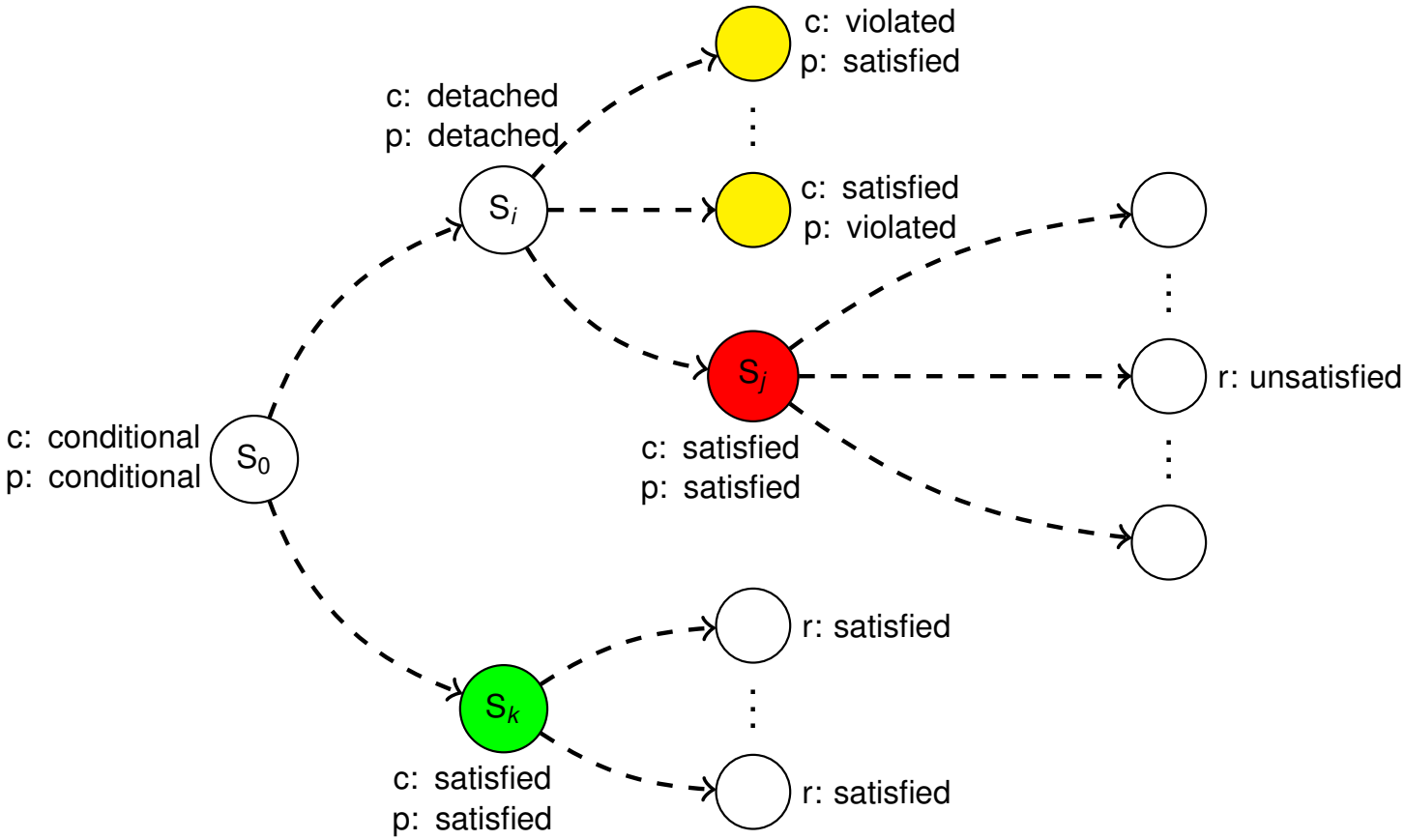
Kafalı et al. Revani: Revising and Verifying Normative Specifications for Privacy. IEEE Intelligent Systems, 31(5):8-15, 2016

RQ_1: Requirements Verification



Kafalı et al. Revani: Revising and Verifying Normative Specifications for Privacy. IEEE Intelligent Systems, 31(5):8-15, 2016

RQ_1: Requirements Verification



Kafalı et al. Revani: Revising and Verifying Normative Specifications for Privacy. IEEE Intelligent Systems, 31(5):8-15, 2016

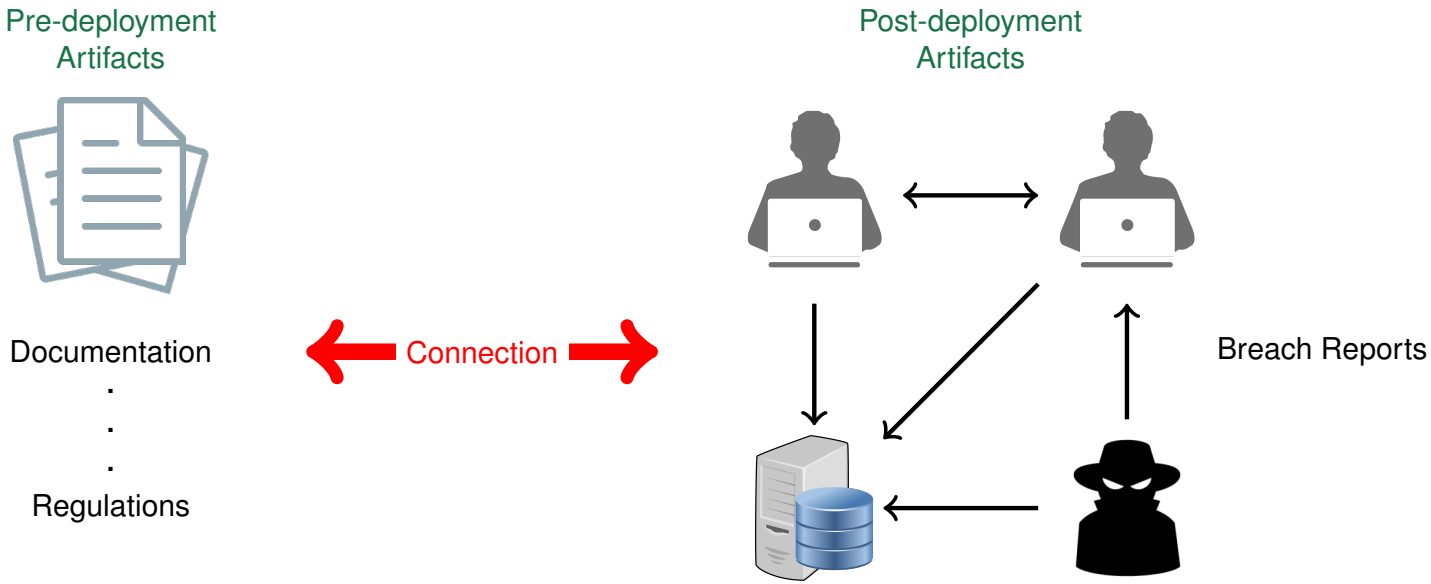
RQ_2: STS Design with Tradeoffs

- Regiment (technical) or regulate (social)?
- Functionality or security?
- Comply with multiple regulations

- Design patterns
- Refinement based on changing requirements

Kafalı et al. Kont: Computing Tradeoffs in Normative Multiagent Systems. AAAI Conference on Artificial Intelligence, pages 3006–3012, 2017

RQ_3: Requirements Extraction



- Normative formalization to connect regulations and breaches
- Ontology of breach concepts
- Semantic similarity metric to identify gaps or holes

Kafalı et al. 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

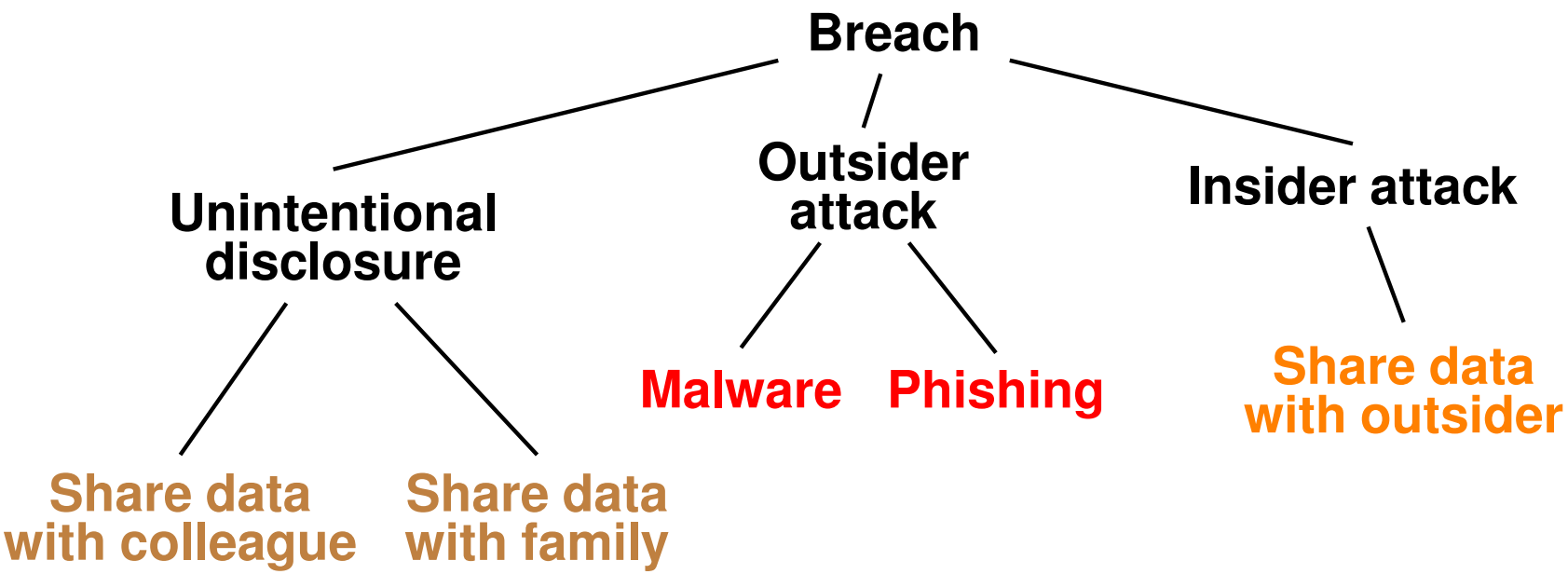
Breach Analysis

- 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.

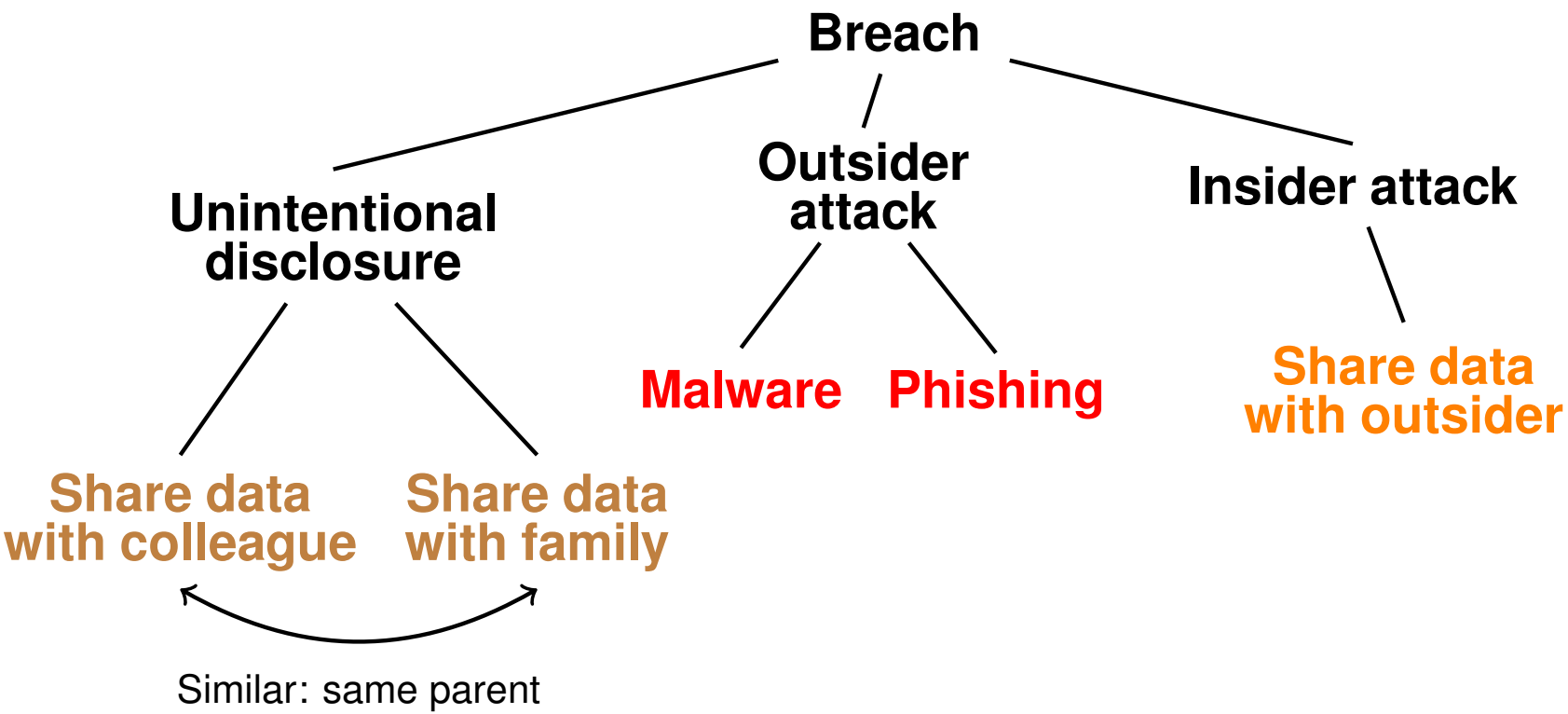
- HIPAA clause 45 CFR 164.310–(d)(2)(i): "A covered entity or business associate must implement policies and procedures to address the final disposition of electronic protected health information, and the hardware or electronic media on which it is stored."

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

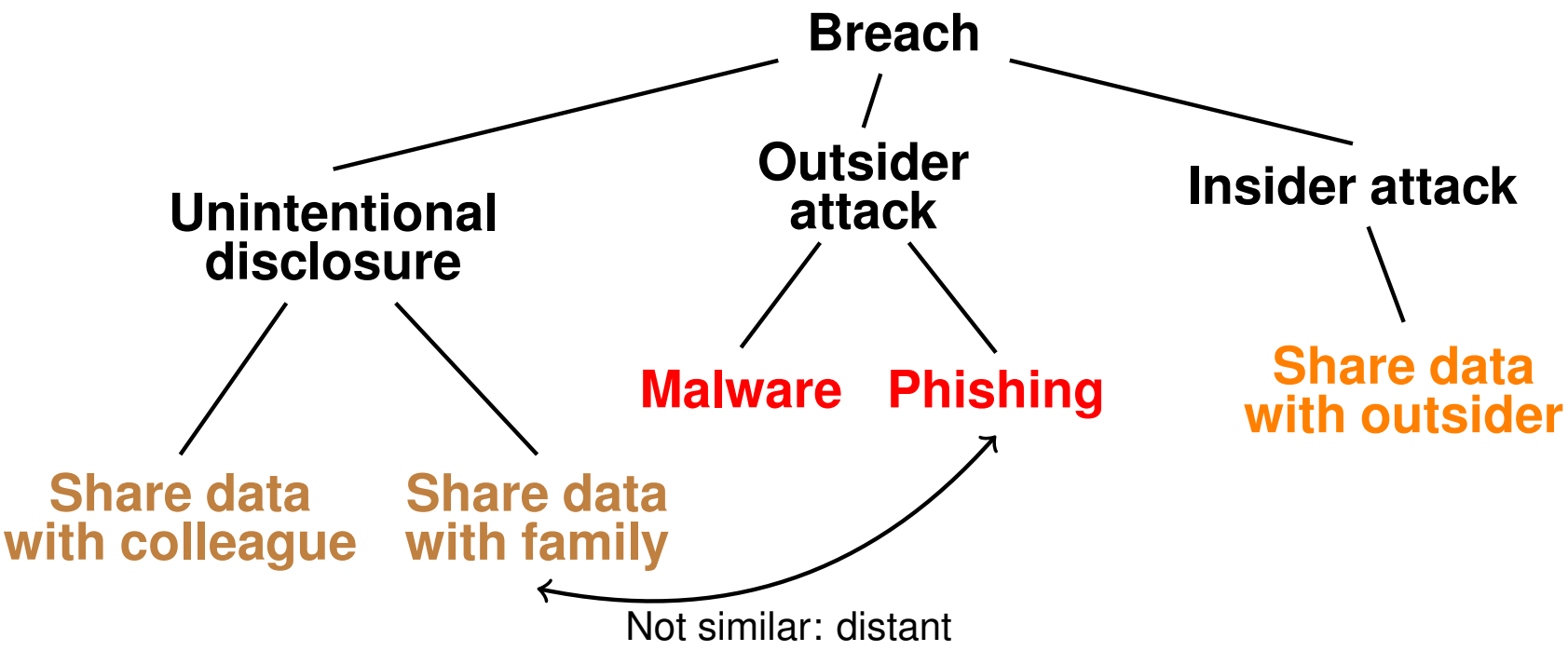
Breach Ontology



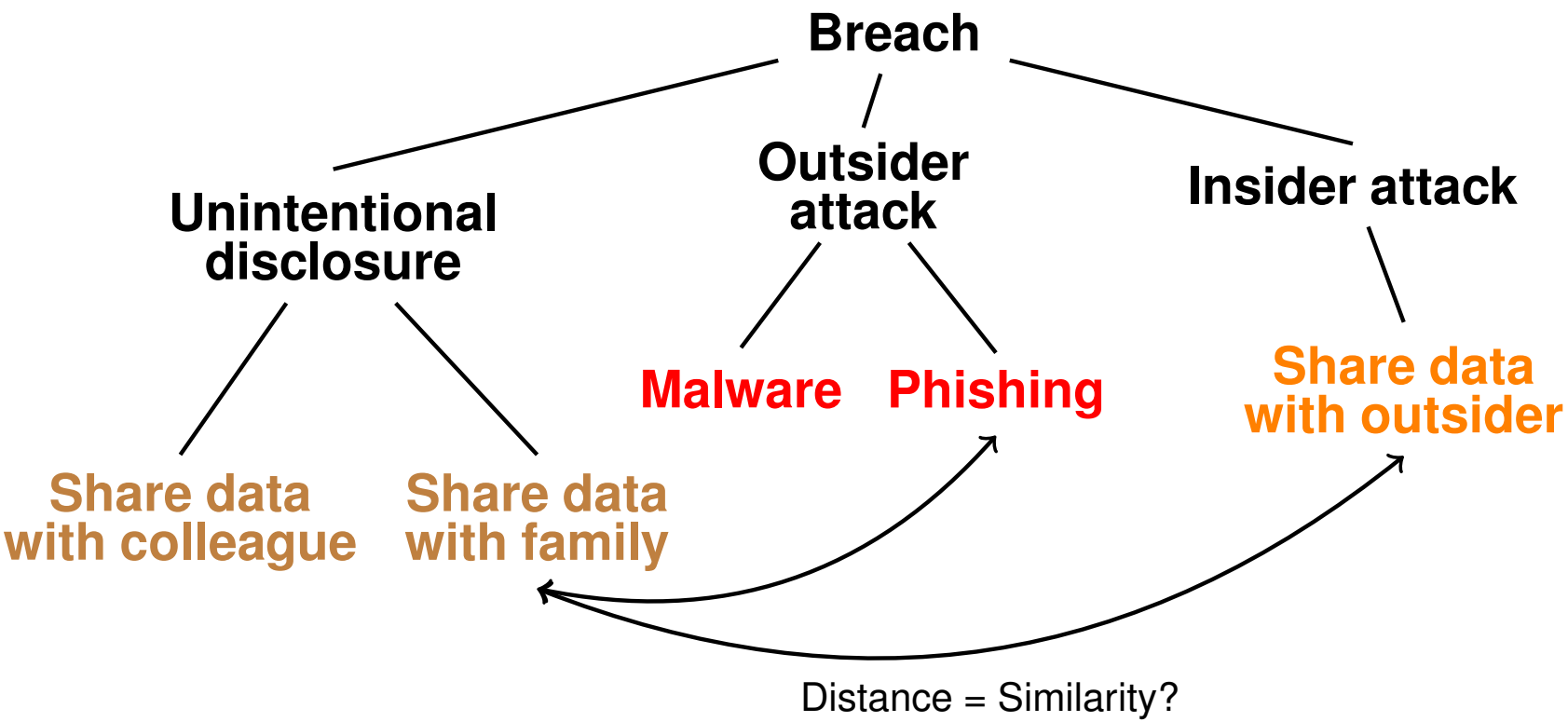
Breach Ontology



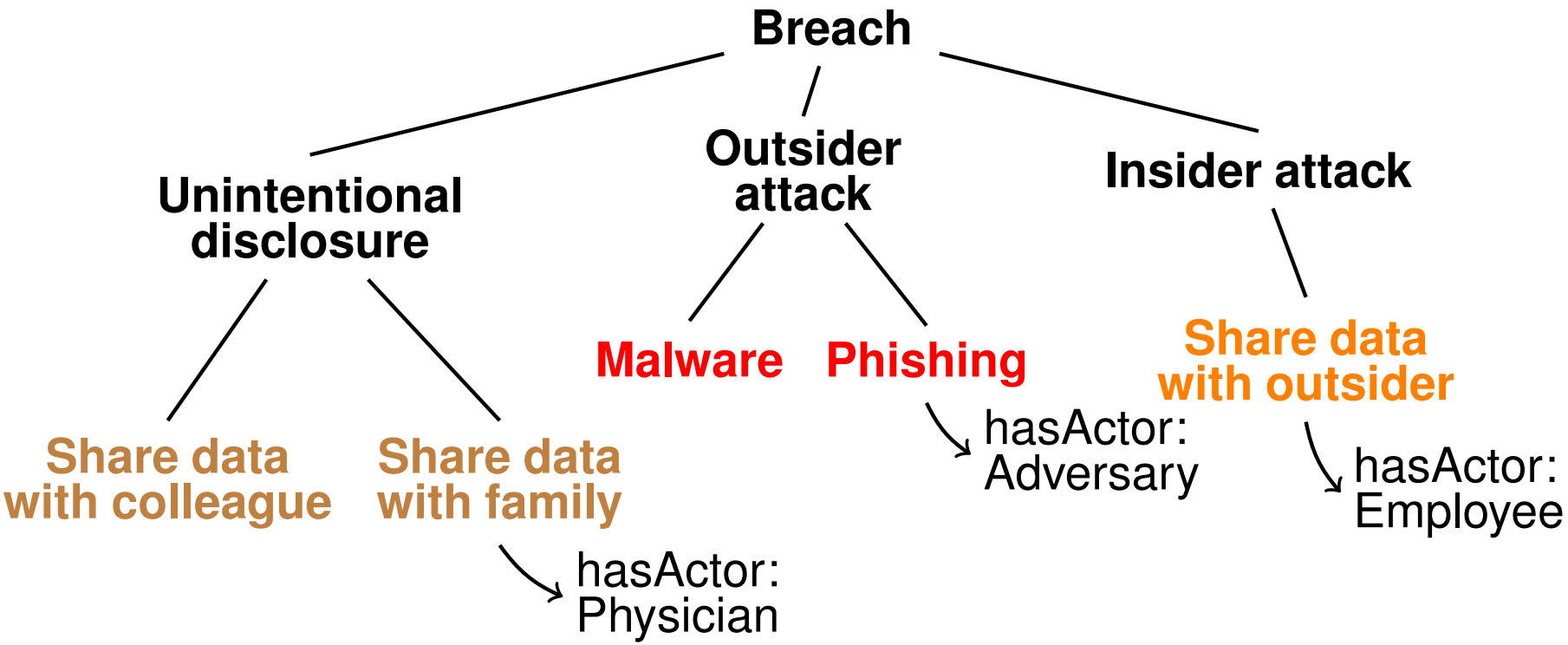
Breach Ontology



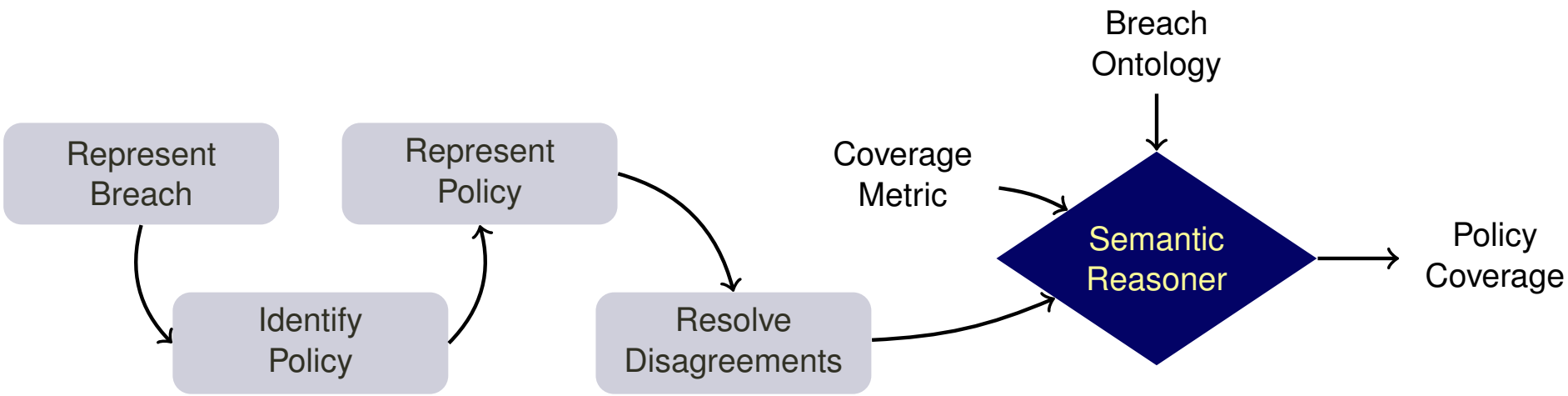
Breach Ontology



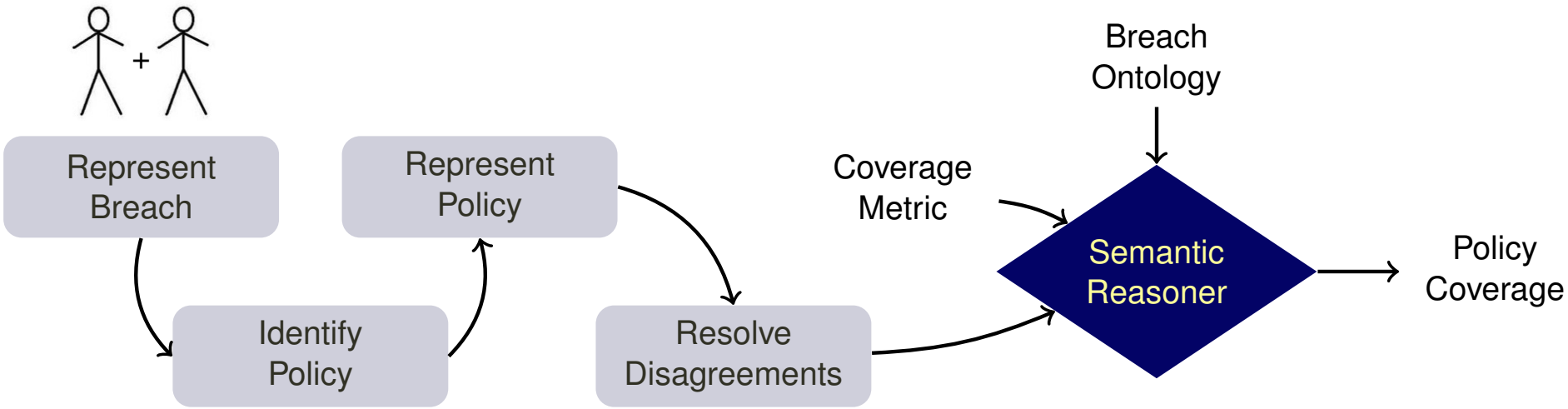
Breach Ontology



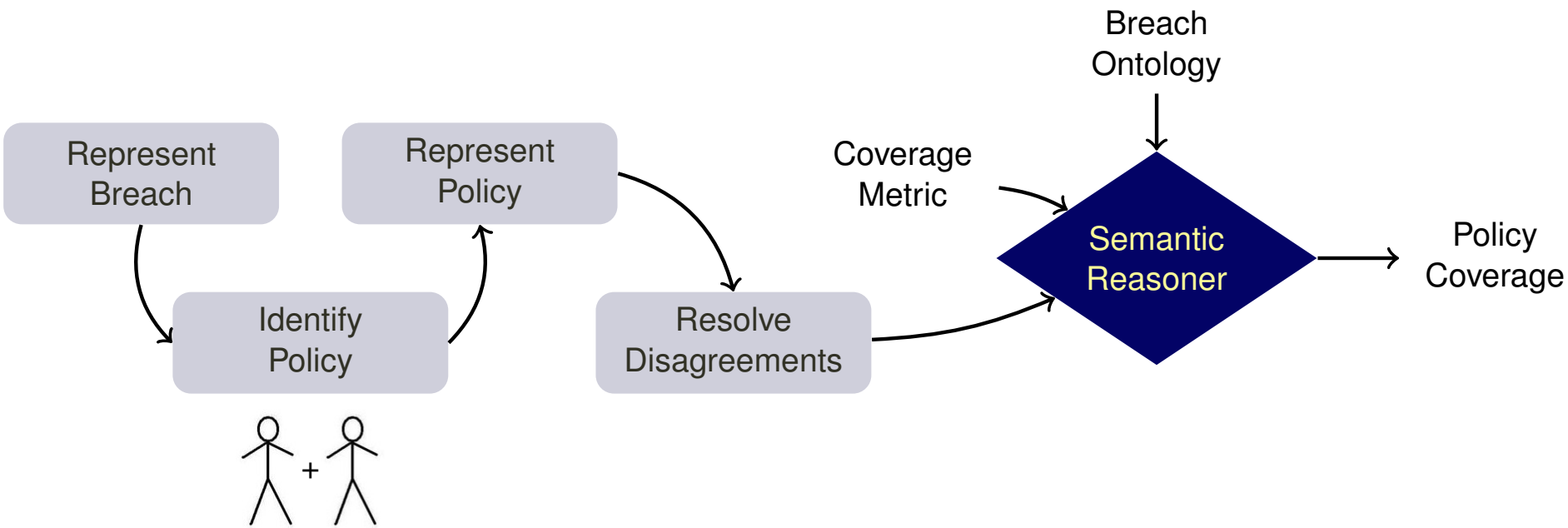
Methodology



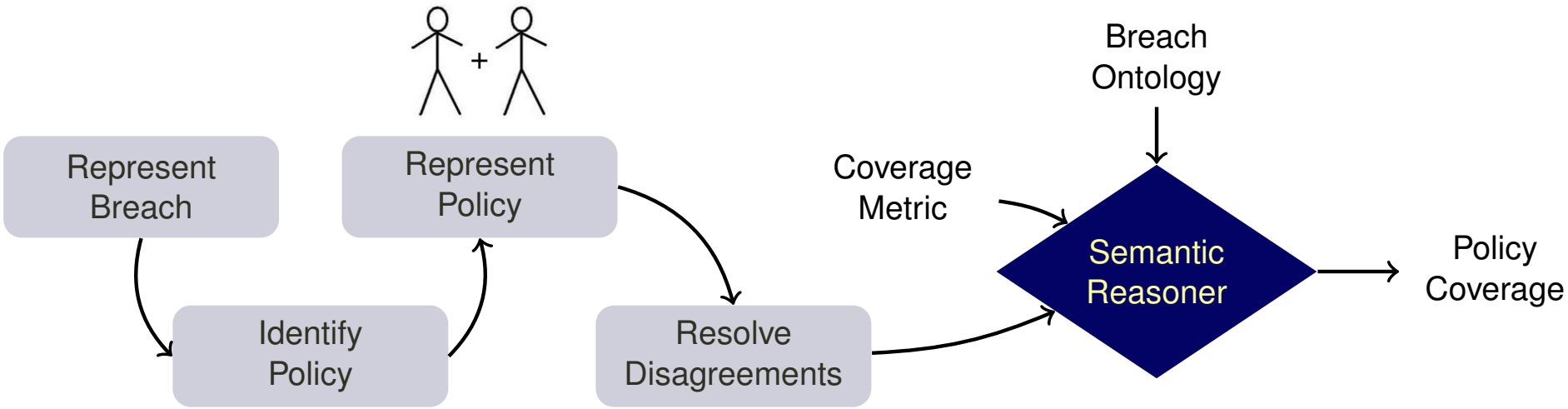
Methodology



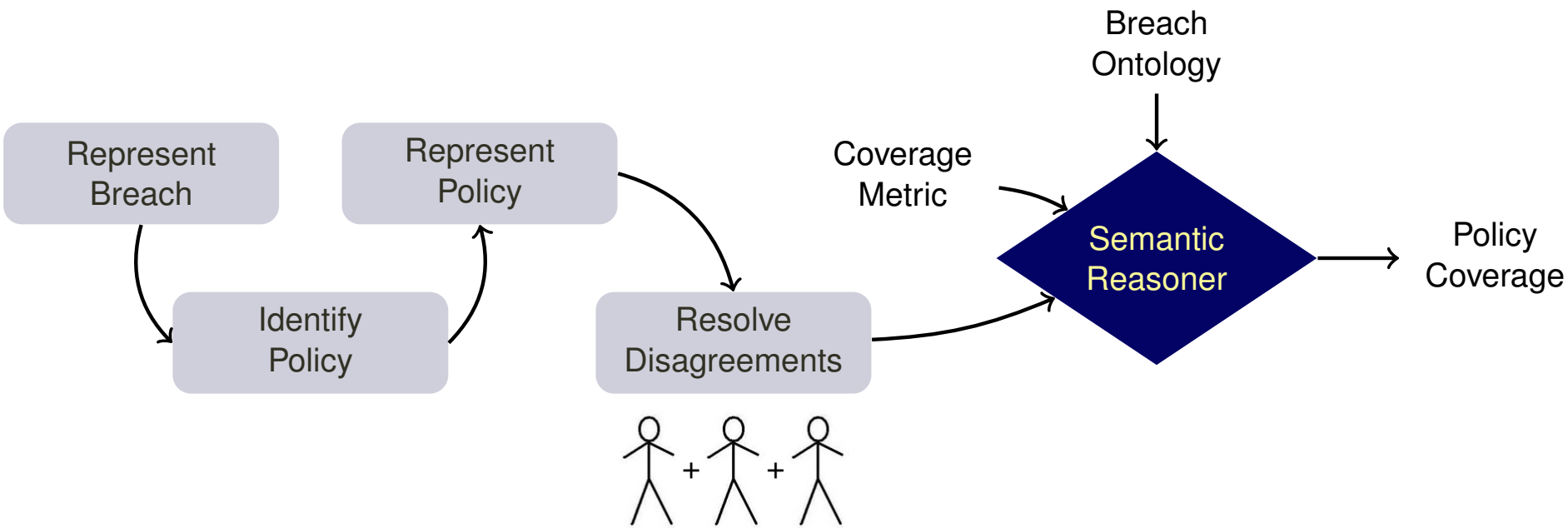
Methodology



Methodology



Methodology



HHS Breach Reports

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:

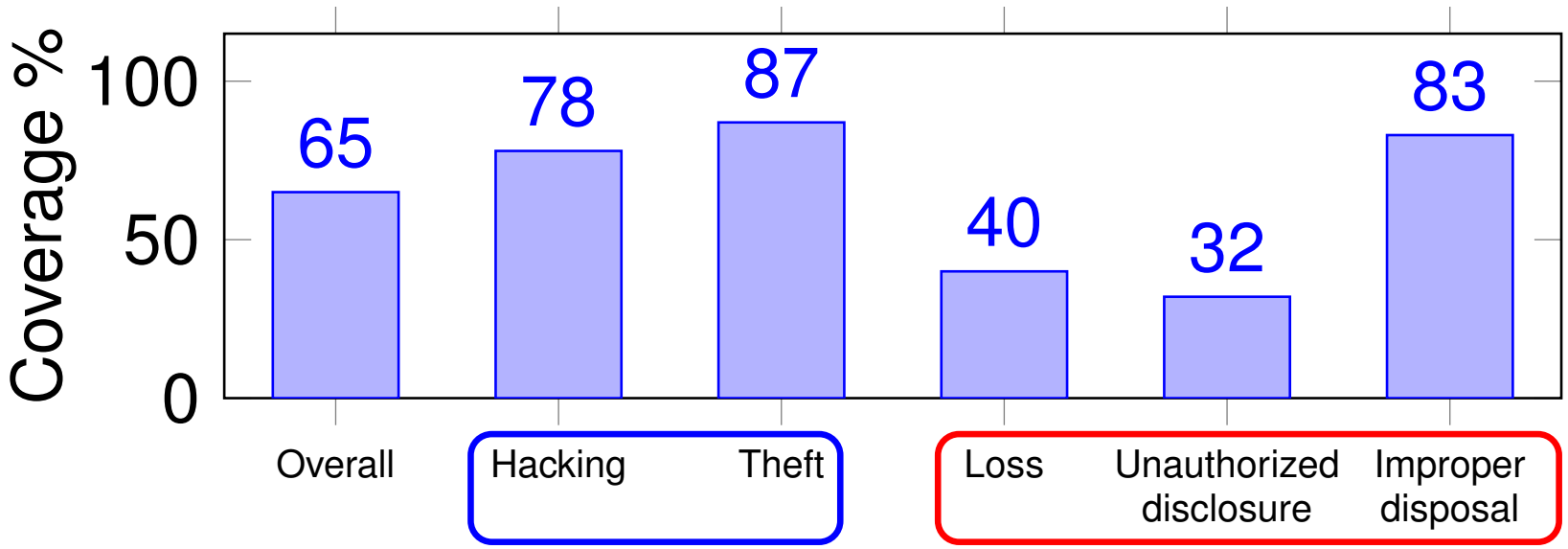
Show Advanced Options

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/

How Good is HIPAA against Real Breaches?



- 56% malicious misuses and 44% accidental misuses
- Better coverage for malicious misuses than accidental misuses

Natural Language Processing

- Breach description: Two laptop computers with questionable encryption were stolen from the Covered Entity (CE)'s premises.

- Follow-up action: The CE reported the theft to law enforcement.
- Follow-up action: The CE worked with the local police to recover the laptops.
- Follow-up action: The CE developed and implemented new policies and procedures to comply with the HIPAA Security Rule.
- Follow-up action: The CE placed an accounting of disclosures in the medical records of all affected individuals.

- Impact to practice: Standards for breach reporting

User Expectations

- Existing design efforts divided between:
  - Secure software design disregards user expectations
  - Usable security and privacy research relies on heuristics about user attitudes (e.g., collected via interviews, surveys)
- Develop unified representations of user expectations and software implementation
- Identify discrepancies between user expectations and software implementation
- Implications to practice: Help IoT device developers, Android app developers

---

Kafalı et al. Nane: Identifying Misuse Cases Using Temporal Norm Enactments. Proceedings of the 20th International Requirements Engineering Conference (RE), pages 136-145, 2016

Digital Forensics and Accountability

- Logging: Adequate vs excessive
- Computational models of accountability
- Improved threat modelling (e.g. attack/defense trees)
  - AI techniques such as intention recognition
  - Prioritisation of misuse via interactive game-playing

Kafalı and Singh. Improving Cybersecurity: User Accountability and Sociotechnical Systems. https://www.computer.org/web/computingnow/archive/improving-cybersecurity-april-2017-introduction

Collaborators


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 Pınar Yolum – Utrecht University, Netherlands


Dr Bedour Alrayes – King Saud University, Saudi Arabia