CSC 495.002 – Lecture 10
AI for Privacy: Privacy Breaches

Dr. Özgür Kafalı

North Carolina State University
Department of Computer Science

Fall 2017

Privacy Norms

- Cannot control everything with software features
- Provide flexibility to users (don't prevent everything)
- Need a social mechanism to regulate the interactions among users
- Hold users accountable for their actions

Problem Definition

- An instance of accidental or unauthorized collection, use or exposure of sensitive information about an individual

  Or,

- An event that creates the perception that unauthorized collection, use or exposure of sensitive information about an individual may happen

Motivation for Breach Analysis

- Security and privacy breaches increase in numbers and variety
- Affect large numbers of people
- Contain clues about vulnerabilities and how to mitigate them
- Tedious and time consuming task for humans

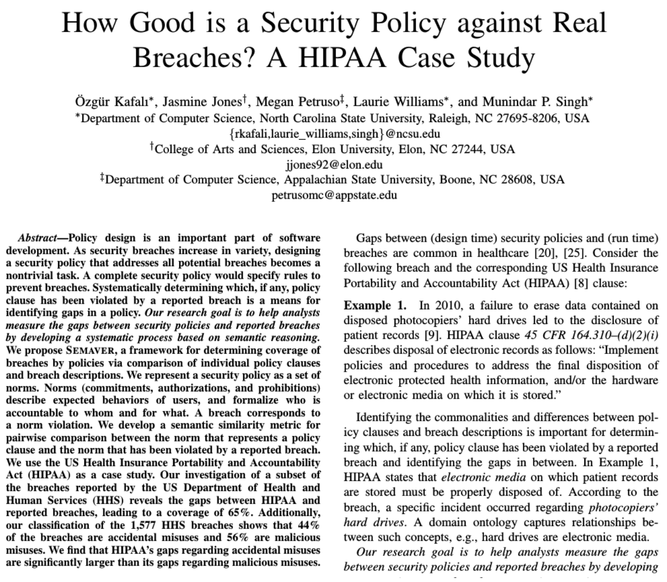
Implications

- Policy and regulation design
- Better breach reporting

Methods

- Semantic reasoning
- Crowdsourcing
- Natural language processing

How Good is a Policy against Breaches?



How Good is a Security Policy against Real Breaches? A HIPAA Case Study

Özgür Kafalı*, Jasmine Jones[†], Megan Petruso[‡], Laurie Williams*, and Munindar P. Singh*
*Department of Computer Science, North Carolina State University, Raleigh, NC 27695-8206, USA
{rkafali,laurie_williams,singh}@ncsu.edu
[†]College of Arts and Sciences, Elon University, Elon, NC 27244, USA
jjones92@elon.edu
[‡]Department of Computer Science, Appalachian State University, Boone, NC 28608, USA
petrusomc@appstate.edu

***Abstract*—Policy design is an important part of software development. As security breaches increase in variety, designing a security policy that addresses all potential breaches becomes a nontrivial task. A complete security policy would specify rules to prevent breaches. Systematically determining which, if any, policy clause has been violated by a reported breach is a means for identifying gaps in a policy. *Our research goal is to help analysts measure the gaps between security policies and reported breaches by developing a systematic process based on semantic reasoning.* We propose SEMAVER, a framework for determining coverage of breaches by policies via comparison of individual policy clauses and breach descriptions. We represent a security policy as a set of norms. Norms (commitments, authorizations, and prohibitions) describe expected behaviors of users, and formalize who is accountable to whom and for what. A breach corresponds to a norm violation. We develop a semantic similarity metric for pairwise comparison between the norm that represents a policy clause and the norm that has been violated by a reported breach. We use the US Health Insurance Portability and Accountability Act (HIPAA) as a case study. Our investigation of a subset of the breaches reported by the US Department of Health and Human Services (HHS) reveals the gaps between HIPAA and reported breaches, leading to a coverage of 65%. Additionally, our classification of the 1,577 HHS breaches shows that 44% of the breaches are accidental misuses and 56% are malicious misuses. We find that HIPAA's gaps regarding accidental misuses are significantly larger than its gaps regarding malicious misuses.**

Gaps between (design time) security policies and (run time) breaches are common in healthcare [20], [25]. Consider the following breach and the corresponding US Health Insurance Portability and Accountability Act (HIPAA) [8] clause:

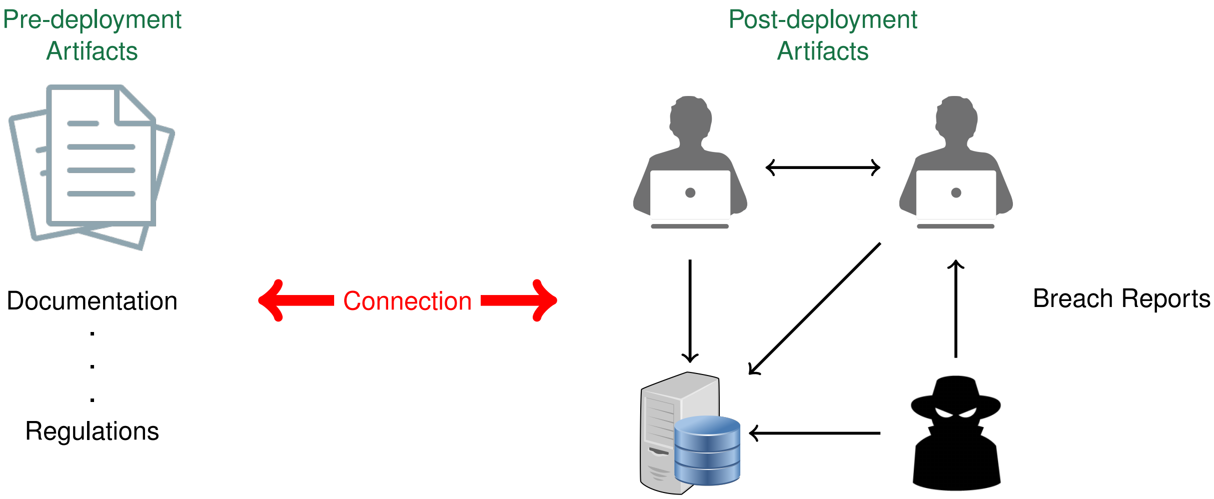
Example 1. In 2010, a failure to erase data contained on disposed photocopiers' hard drives led to the disclosure of patient records [9]. HIPAA clause *45 CFR 164.310–(d)(2)(i)* describes disposal of electronic records as follows: "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

Identifying the commonalities and differences between policy clauses and breach descriptions is important for determining which, if any, policy clause has been violated by a reported breach and identifying the gaps in between. In Example 1, HIPAA states that *electronic media* on which patient records are stored must be properly disposed of. According to the breach, a specific incident occurred regarding *photocopiers' hard drives*. A domain ontology captures relationships between such concepts, e.g., hard drives are electronic media.

Our research goal is to help analysts measure the gaps between security policies and reported breaches by developing

Kafalı et al. How Good is a Security Policy against Real Breaches? A HIPAA Case Study. International Conference on Software Engineering (ICSE), pages 530–540, 2017

Motivation



Pre-deployment Artifacts

Post-deployment Artifacts

Documentation
.
.
.
Regulations

Connection

Breach Reports

Exercise: Identify Common Elements

- 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

Research Questions

- Representation: How can we formalize policies, regulations, and breaches to bring out their mutual correspondence?
- Similarity: What are the commonalities and differences between concepts in policies, regulations, and breach descriptions?
- Analysis: How prevalent are human errors among reported breaches, and do policies account for them?

Exercise: Connect Breaches to Norms

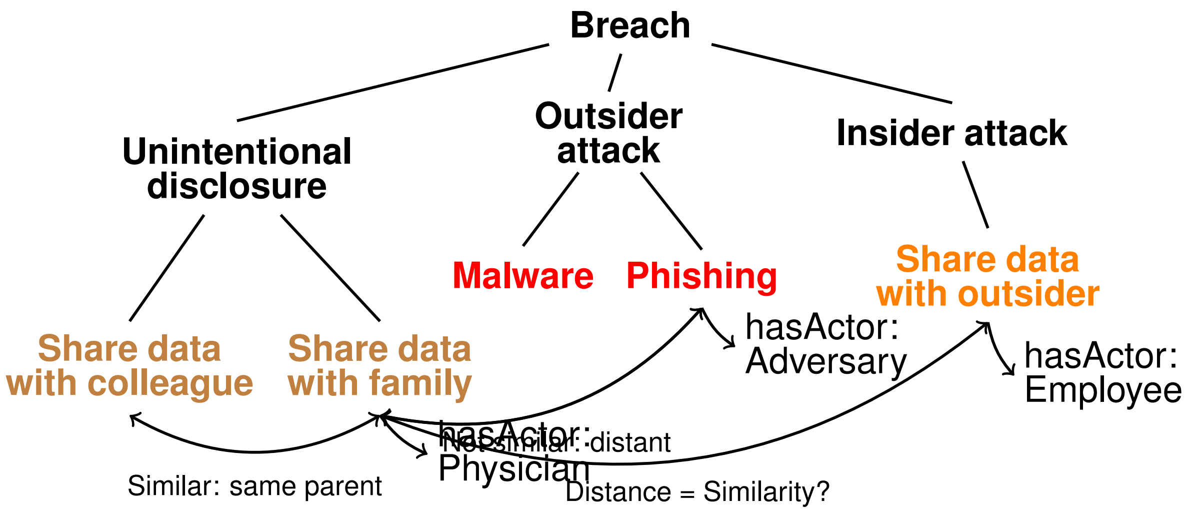
- A breach corresponds to a norm violation
- Specify norm(s) that would help mitigate the breach
- An employee in a covered entity forgot to erase data contained on disposed photocopiers' hard drives

C(EMPLOYEE, COVERED_ENTITY, disposal, erase_drive)

Framework Elements

- Two fundamental elements:
  - Norms to represent breaches and policies
  - Domain ontology to capture breach concepts
- Similarity metric for computing to what extent breaches are covered by a policy

Ontologies: Breach Concepts



Breach

Unintentional disclosure

Outsider attack

Insider attack

Share data with colleague

Share data with family

Malware

Phishing

Share data with outsider

hasActor: Adversary

hasActor: Employee

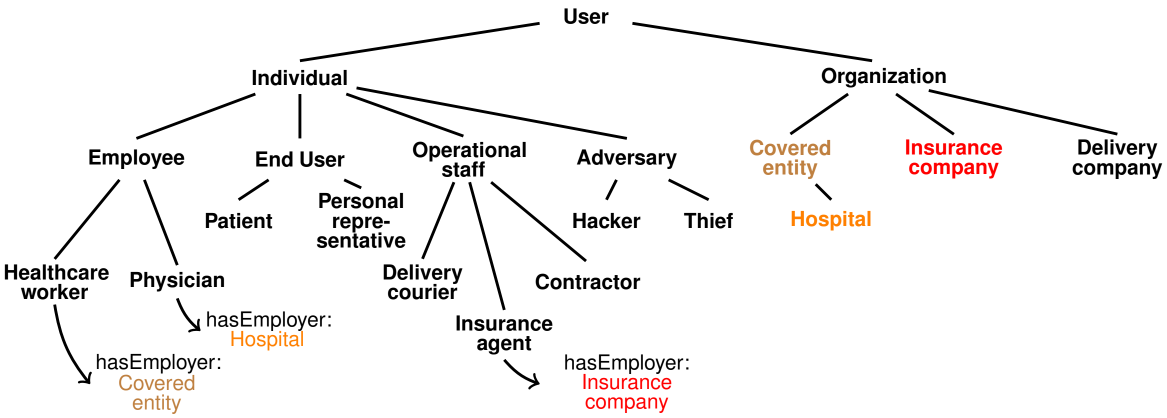
hasActor: Physician

Similar: same parent

Not similar: distant

Distance = Similarity?

Ontologies: Healthcare Users



User

Individual

Organization

Employee

End User

Operational staff

Adversary

Covered entity

Insurance company

Delivery company

Patient

Personal representative

Hacker

Thief

Hospital

Healthcare worker

Physician

Delivery courier

Contractor

Insurance agent

hasEmployer: Hospital

hasEmployer: Covered entity

hasEmployer: Insurance company

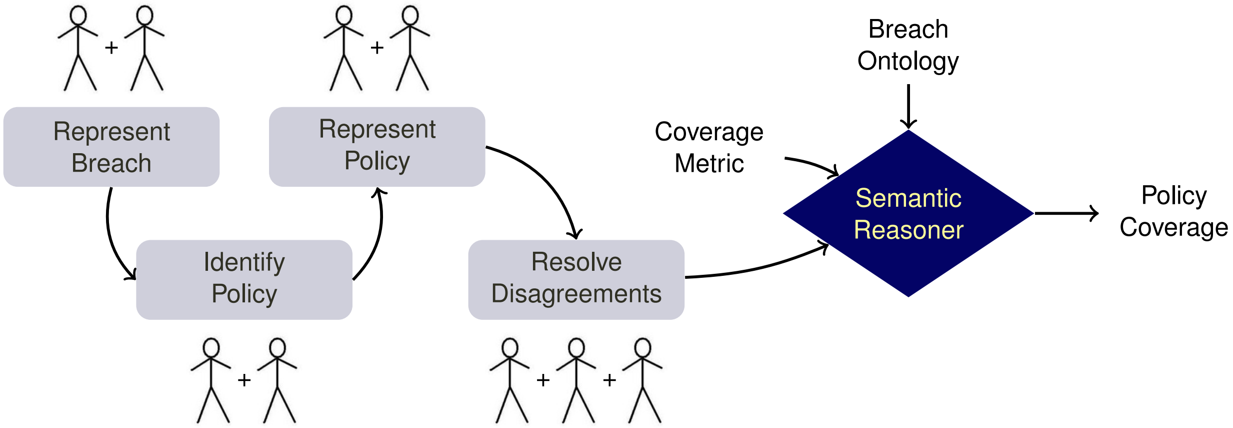
Semantic Reasoning

- Norm similarity:
$\mathit{sim}_{n_1,n_2} = (\mathit{sim}_{\text{SBJ}_1,\text{SBJ}_2} + \mathit{sim}_{\text{OBJ}_1,\text{OBJ}_2} + \mathit{sim}_{\text{ant}_1,\text{ant}_2} + \mathit{sim}_{\text{con}_1,\text{con}_2})\ /\ 4$
- Distance between concepts: $\Delta_{c_1,c_2} = \text{edge\_count}(c_1, c_2)$
- Similarity between concepts: $\mathit{sim}_{c_1,c_2} = \frac{1}{1+\Delta_{c_1,c_2}} \times \mathit{sim}^{prop}_{c_1,c_2}$
- Assumption: $\mathit{sim}_{\phi,\text{true}} = 0.001$
- Property similarity: $\mathit{sim}^{prop}_{c_1,c_2} = \begin{cases} 1 & \text{if P not shown} \\ \prod\limits_{p_i \in \text{P}} \dfrac{1}{1+\Delta_{p_i}} & \text{otherwise} \end{cases}$

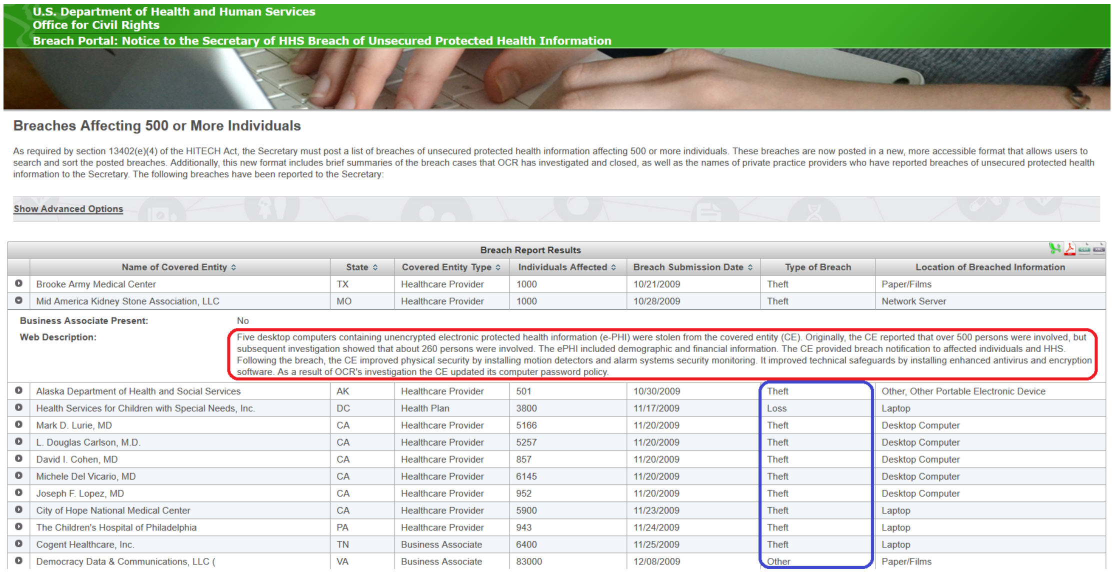
Overall Policy Coverage

- $\mathit{coverage} = \dfrac{\sum\limits_{b_i \in \text{B}} \mathit{sim}_{n_{\text{policy}},n_{b_i}}}{|\text{B}|}$
- B: Set of all breaches
- n_{b_i}: Norm to mitigate breach i
- n_{policy}: Policy clause relevant to breach i

Methodology



HHS Breach Report



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.

	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach	Location of Breached Information
●	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/

Breach Categories

Category	Count	Description
Hacking	191	Adversary exploits vulnerability to access EHR
Theft	642	Employee discloses PHI
Loss	129	Electronic media containing PHI are lost
Unauthorized disclosure	338	PHI is disclosed due to unauthorized access
Improper disposal	58	Employee fails to properly dispose PHI
Unclassified	219	Not classified by HHS

Exercise: Incident I

- “A physician of the CE lost a flash drive which he routinely used for data backup and remote access to patient data. The flash drive contained names, dates of birth and treatment notes for approximately 1,711 patients. Following the breach, the CE notified affected individuals. The CE retrained the physician who lost the flash drive and implemented an organization-wide decision to prohibit storage of protected health information on any removable electronic devices. As a result of OCR’s investigation, the CE notified the media and posting substitute notification on its website.”
- Hacking, theft, loss, unauthorized disclosure, improper disposal?

Exercise: Incident II

- “Two former employees of the covered entity (CE), Sentara Healthcare, accessed protected health information (PHI) outside of their normal job duties and used this information to process fraudulent tax returns. The US Attorney’s office investigated the matter and both individuals received prison sentences. Following this incident, the CE increased safeguards by installing a new software system to help monitor and detect inappropriate access to its electronic medical records system, updated its security policies and procedures, and re-trained employees.”
- Hacking, theft, loss, unauthorized disclosure, improper disposal?

Exercise: Incident III

- “OCR opened an investigation of the covered entity (CE), Mt. Sinai Medical Center, after it reported that a trash vendor placed two garbage bags in an open box containing the protected health information (PHI) of 1,586 patients outside the Mt. Sinai’s Department of Preventive Medicine’s facility with the regular trash. The PHI involved in the breach included names, dates of service, payer information, patients’ clinical information, mental health information and social security numbers. As a result of the breach, the CE retrieved the two trash bags and the box that contained PHI, provided training to its staff regarding appropriate disposal of PHI including paper files, and sanctioned the supervisor for failing to follow its policy regarding confidential waste.”
- Hacking, theft, loss, unauthorized disclosure, improper disposal?

Exercise: Incident IV

- “The covered entity (CE), Carolina’s Medical Center, discovered that a physician had responded to a phishing email and provided her password to a third party, causing all of the physician’s emails to be forwarded to a third party. The forwarded emails included protected health information (PHI) regarding 5,600 individuals, including names, dates of birth, medications, treatment information, social security numbers, admission/discharge dispositions and dates, and internal medical record and account numbers. Following the breach, CE improved technical safeguards by terminating auto-forwarding capabilities and implementing an alert for remote system accesses that originate from a foreign country. The CE also trained employees on identifying social engineering schemes.”
- Hacking, theft, loss, unauthorized disclosure, improper disposal?

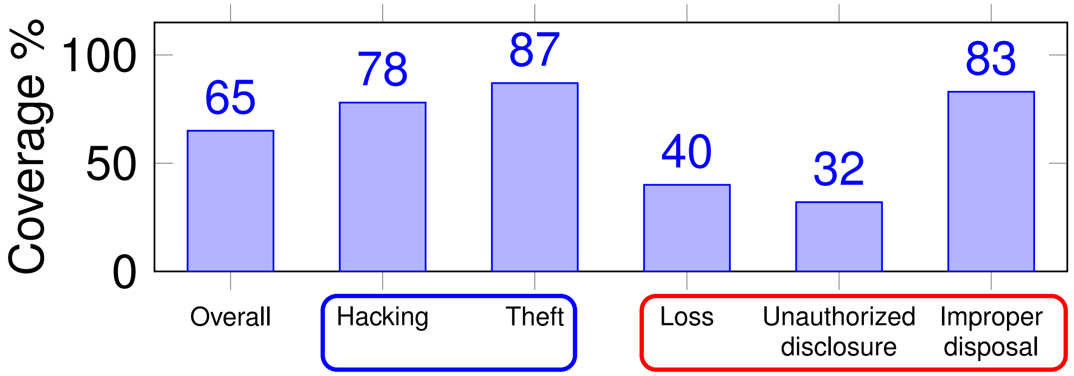
Results: Classification of Breaches

- Investigated 1,577 breaches reported by HHS
  - *Hacking* (191) and *Theft* (642) contain malicious misuses
  - *Loss* (129), *Unauthorized 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
- Implications:
  - Human factors are an important consideration in preventing breaches
  - Results corroborate additional findings in other cybersecurity reports [DoD, HIMMS]

The United States Department of Defense (DoD). Cybersecurity culture and compliance initiative. 2015.

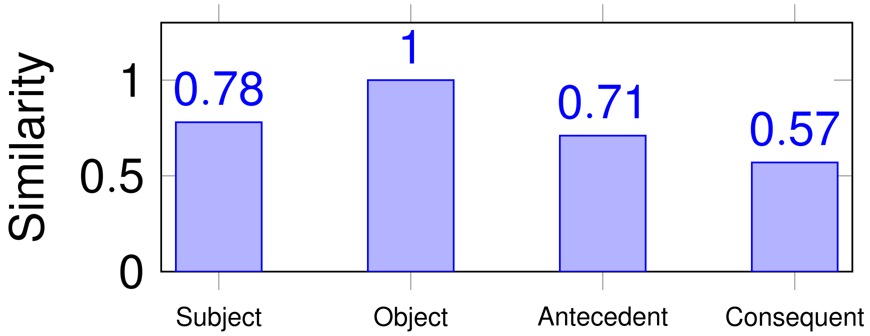
The healthcare information and management systems society (HIMSS) cybersecurity study. 2016.

Results: Coverage by Breach Category



- Better coverage for malicious misuses than accidental misuses
- Implications:
  - Policy clauses for accidental misuses have more gaps/holes
  - Refinement of such clauses would help reduce human errors

Results: Similarity among Norm Elements



- Similarity between actors (subject/object) is higher than assets (antecedent/consequent)
- Consequent may be given a higher weight to provide a more realistic measure of coverage

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)

Accidental or Malicious Disclosure

- NHS news article: https://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds
- WHSmith news article: http://www.businessinsider.com/whsmith-customer-emails-data-privacy-2015-9?r=UK&IR=T
- Links are also on the course website

Things to Look For

- What are the similarities and differences between the two incidents?
- Mitigation (using methods we have seen): Prevention, detection, recovery
- Take 10 minutes to look at the incidents on your own

- Now discuss with your neighbor
- Also take a look at the summary reports
  - NHS: https://drive.google.com/file/d/0B3m-l0YVAv0Ed3NXRDdsWEhDdkk/view
  - WHSmith: https://drive.google.com/file/d/0B3m-l0YVAv0ER1BKY2g3MXpmbmc/view