The Social Side of Security
Requirements, Regulations, and Breaches

Dr Özgür Kafalı

Lecturer
School of Computing
University of Kent

20 March 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
INTRODUCTION

Hard Problems

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

CCS → Computing methodologies → Artificial intelligence
- Natural language processing
- Knowledge representation and reasoning
- Search methodologies
- Control methods
- Planning and scheduling
- Philosophical/theoretical foundations of artificial intelligence
- Distributed artificial intelligence
- Computer vision

CCS → Security and privacy
- Cryptography
- Formal methods and theory of security
- Security services
- Intrusion/anomaly detection and malware mitigation
- Security in hardware
- Systems security
- Network security
- Database and storage security
- Software and application security
- Human and societal aspects of security and privacy
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

Shannon
Dustin’s first credit card. I’m sooo proud!!!! Your growing up so fast :) — with Dustin

Thanks for dinner... and my new car and everything on eBay
2 minutes ago - Like

Did you just post some kids credit card number all over Facebook?
about a minute ago - Like
Oops, They Did It Again

- Nurses peek celebrity 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

- **Requirements**
  - identify
- **Stakeholders**
  - specify
- **Assumptions**
  - Mechanisms
  - Norms
  - mechanisms yield
  - norms regulate interaction
  - Agent ... Agent
  - Social Tier
  - Technical Tier
- **Functional and Control Components**

Dr Özgür Kafalı
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
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?
**RQ₁: Requirements Verification**

\[ c: \text{conditional} \quad S_0 \]

RQ₁: Requirements Verification

RQ₁: Requirements Verification
RQ₁: Requirements Verification

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

RQ₃: Requirements Extraction

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

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.”
Breach Ontology

- Unintentional disclosure
  - Share data with colleague
  - Share data with family
- Outsider attack
  - Malware
  - Phishing
- Insider attack
  - Share data with outsider
Breach Ontology

Breach

Unintentional disclosure

Outsider attack

Malware

Phishing

Insider attack

Share data with outsider

Share data with colleague

Share data with family

Similar: same parent
Breach Ontology

Breach

Outsider attack

Malware

Phishing

Unintentional disclosure

Share data with colleague

Share data with family

Insider attack

Share data with outsider

Not similar: distant
Breach Ontology

- Unintentional disclosure
  - Share data with colleague
  - Share data with family
- Outsider attack
  - Malware
  - Phishing
- Insider attack
  - Share data with outsider

Distance = Similarity?
Breach Ontology

- Breach
  - Outsider attack
    - Malware
    - Phishing
      - hasActor: Physician
  - Insider attack
    - Share data with outsider
      - hasActor: Adversary
      - hasActor: Employee
- Unintentional disclosure
  - Share data with colleague
  - Share data with family
Methodology

- Represent Breach
- Represent Policy
- Identify Policy
- Resolve Disagreements
- Coverage Metric
- Semantic Reasoner
- Breach Ontology
- Policy Coverage
Methodology

1. Represent Breach
2. Represent Policy
3. Identify Policy
4. Resolve Disagreements
5. Coverage Metric
6. Semantic Reasoner
7. Breach Ontology
8. Policy Coverage
Methodology

1. Represent Breach
2. Represent Policy
3. Identify Policy
4. Resolve Disagreements
5. Coverage Metric
6. Semantic Reasoner
7. Breach Ontology
8. Policy Coverage

The Social Side of Security
Methodology

1. Represent Breach
2. Represent Policy
3. Identify Policy
4. Resolve Disagreements
5. Coverage Metric
6. Semantic Reasoner
7. Breach Ontology
8. Policy Coverage
Methodology

- Represent Breach
- Represent Policy
- Identify Policy
- Resolve Disagreements
- Coverage Metric
- Semantic Reasoner
- Breach Ontology
- Policy Coverage
HHS Breach Reports

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:

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brooke Army Medical Center</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>1000</td>
<td>10/21/2009</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Alaska Department of Health and Services</td>
<td>AK</td>
<td>Healthcare Provider</td>
<td>501</td>
<td>10/30/2009</td>
<td>Theft</td>
<td>Other, Other Portable Electronic Device</td>
</tr>
<tr>
<td>Health Services for Children with Special Needs, Inc.</td>
<td>DC</td>
<td>Health Plan</td>
<td>3800</td>
<td>11/17/2009</td>
<td>Loss</td>
<td>Laptop</td>
</tr>
<tr>
<td>Mark D. Lurie, MD</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>5106</td>
<td>11/20/2009</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>L. Douglas Carlson, M.D.</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>5257</td>
<td>11/20/2009</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>David I. Cohen, MD</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>857</td>
<td>11/20/2009</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Michele Del Viciano, MD</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>6146</td>
<td>11/20/2009</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Joseph F. Lopez, MD</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>952</td>
<td>11/20/2009</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>City of Hope National Medical Center</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>5800</td>
<td>11/23/2009</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>The Children’s Hospital of Philadelphia</td>
<td>PA</td>
<td>Healthcare Provider</td>
<td>943</td>
<td>11/24/2009</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Coget Healthcare, Inc.</td>
<td>TN</td>
<td>Business Associate</td>
<td>64000</td>
<td>11/25/2009</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Democracy Data &amp; Communications, LLC</td>
<td>VA</td>
<td>Business Associate</td>
<td>83000</td>
<td>12/08/2009</td>
<td>Other</td>
<td>Paper/Films</td>
</tr>
</tbody>
</table>

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?

- Overall: 65%
- Hacking: 78%
- Theft: 87%
- Loss: 40%
- Unauthorized disclosure: 32%
- Improper disposal: 83%

- 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

Future Work

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

CONCLUSIONS

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