Cybersecurity – How Hard Can It Be? A Sociotechnical View

Dr Özgür Kafalı

Lecturer
School of Computing
University of Kent

IEEE Turkey Computer Society Congress
2 March 2018

Research Background

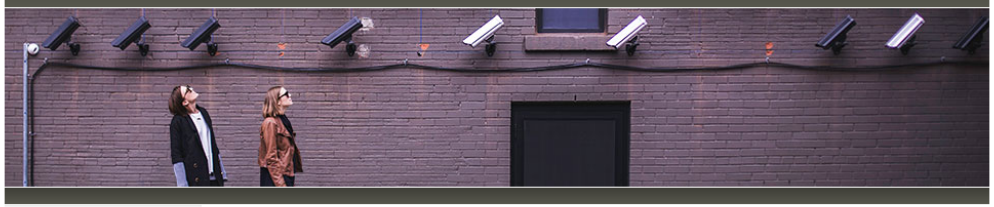
University of Kent | The UK's European university

Contact | Maps | Departments

Shortlisted for EXCEPTIONAL PERFORMANCE THE DataPoints Merit Award 2016

About | Research | Courses | Locations | International | Business | News | Alumni | Giving

KENT INTERDISCIPLINARY RESEARCH CENTRE IN CYBER SECURITY (KIRCCS)



Home
People
Topics
Research Projects
Advisory Board
Contact Us

Search
Search Go

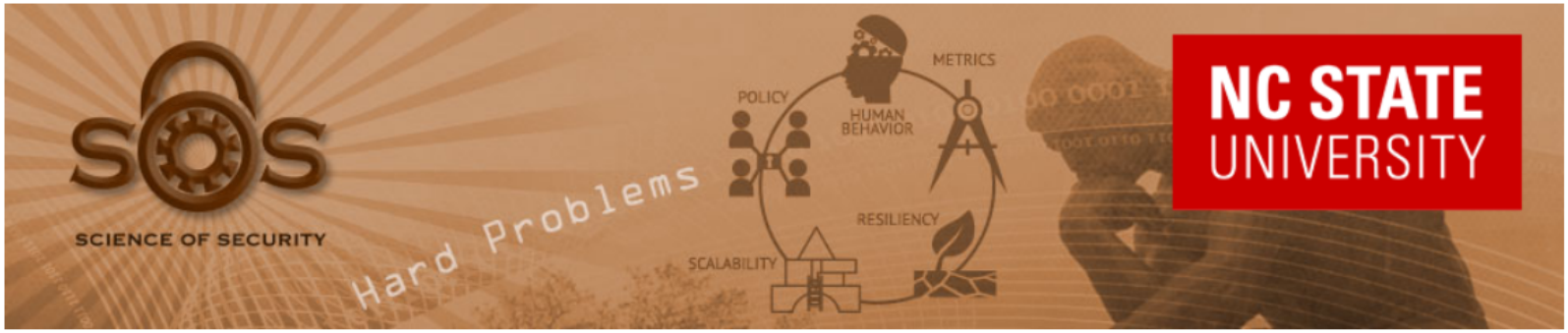
University of Kent › Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

SHARE

Core Members | Associate Members | Research Staff | Research Students

Member	Research Interests	Contact Information
 Budi Arief Senior Lecturer; Centre Director of External Liaison School of Computing	Cyber crime, human factors in security, internet of things security and privacy.	B.Arief@kent.ac.uk
 Özgür Kafalı Lecturer in Cyber Security School of Computing	Socio-technical and human factors in cybersecurity, security requirements engineering, formal breach analysis, digital forensics.	R.O.Kafali@kent.ac.uk
 Andy King Professor in Program Analysis; Centre Director of Research School of Computing	Vulnerability discovery using program analysis techniques, reverse engineering tools for white-hat hackers.	A.M.King@kent.ac.uk

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

Glossary

- Sociotechnical systems
- Norms
- Accountability
- Access control
- Privacy
- Artificial Intelligence

Security-Critical Data

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

Quantum Computing

- To break RSA, a “high specification” computer would take

Credit to my colleague Carlos Perez Delgado

Quantum Computing

- To break RSA, a “high specification” computer would take more than one million times the age of the universe

Credit to my colleague Carlos Perez Delgado

Quantum Computing

- To break RSA, a “high specification” computer would take more than one million times the age of the universe
- A “modest” quantum computer could do it in

Credit to my colleague Carlos Perez Delgado

Quantum Computing

- To break RSA, a “high specification” computer would take more than one million times the age of the universe
- A “modest” quantum computer could do it in 14 minutes

Credit to my colleague Carlos Perez Delgado

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

- US Department of Defense cybersecurity report
- Verizon breach reports
- Academic research studies

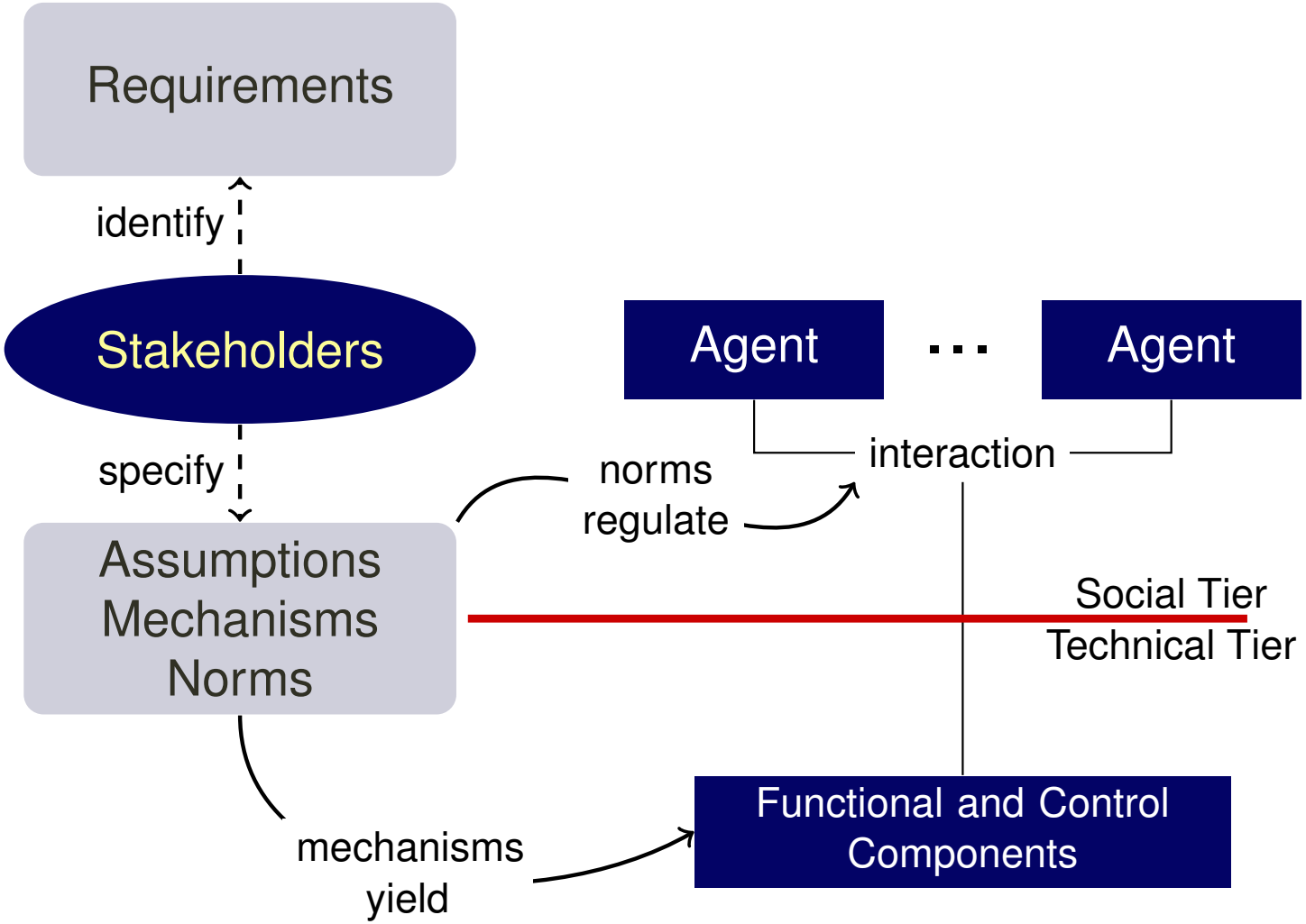
Sociotechnical Systems (STS)

- 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

Design of STS



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

Elicitation

- Extracting functional requirements is hard
- Extracting security and privacy requirements is (almost) impossible

- Rely on hybrid approaches
  - Human intelligence: Crowdsourcing
  - Machine intelligence: Natural language processing (NLP)

Scope of AI

- Big secret:

Scope of AI

- Big secret: AI is not just Machine Learning!

Need for Intelligence

Getty Images

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

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

Breach Analysis

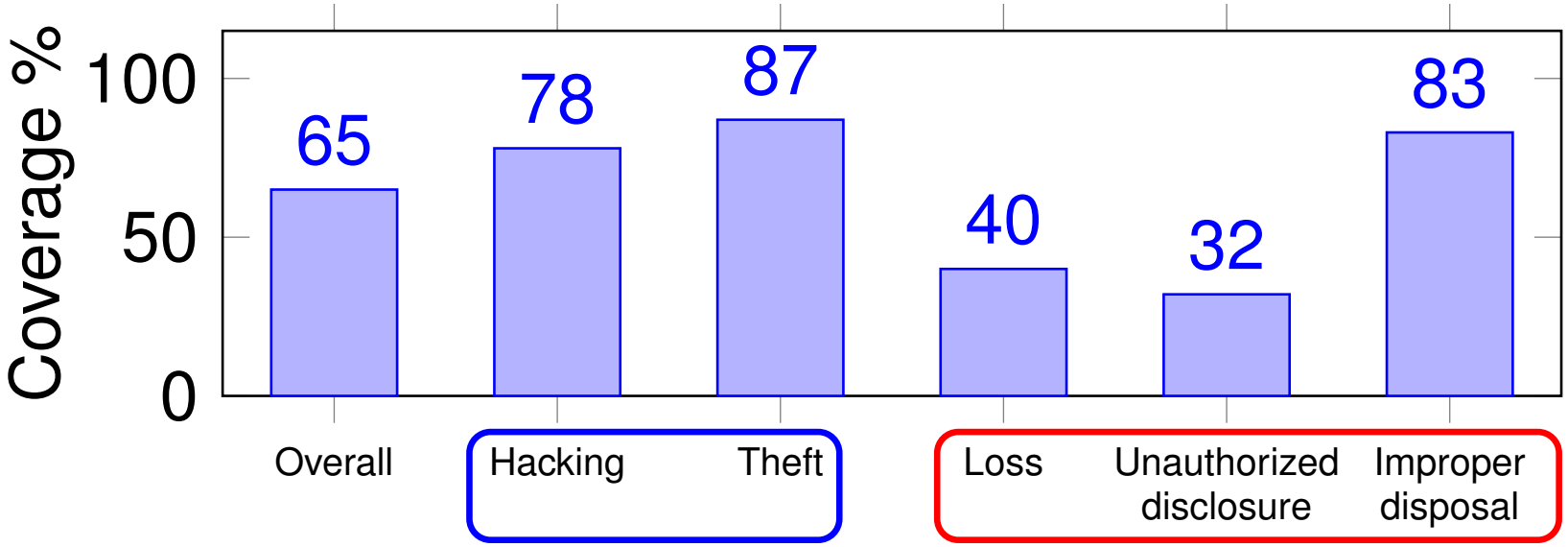
- HHS breach incident: In 2010, an employee in a covered entity forgot to erase data contained on disposed photocopiers' hard drives, which led to disclosure of patient records.

- 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

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

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.

Designing STS

- Regiment (technical) or regulate (social)?
- Design patterns
- Refinement based on changing requirements

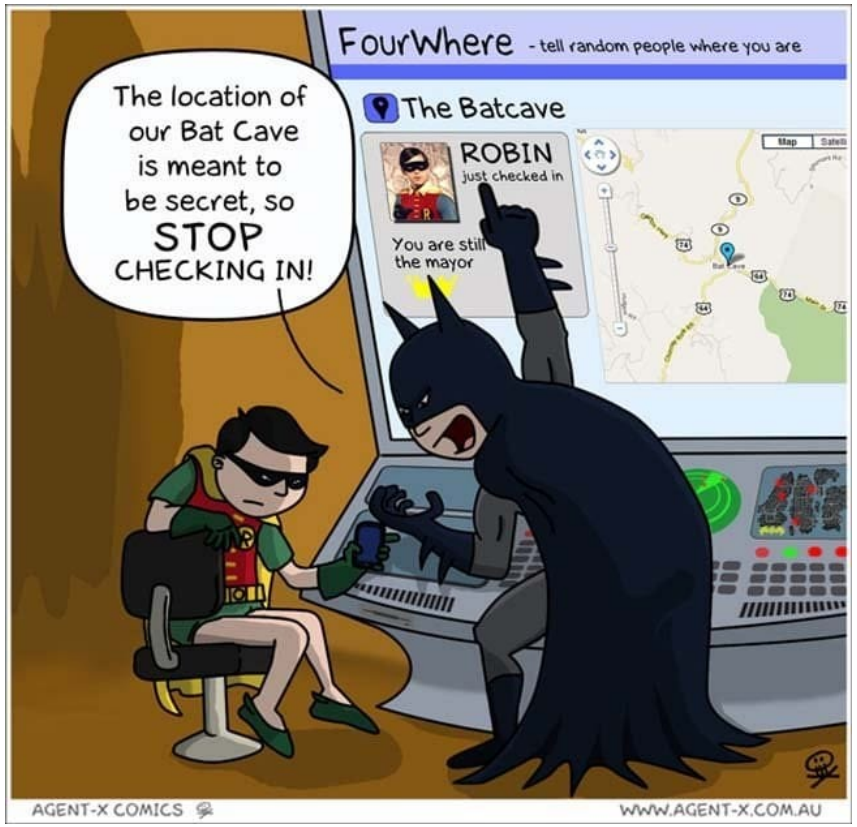
Kafalı et al. Revani: Revising and Verifying Normative Specifications for Privacy. IEEE Intelligent Systems, 31(5):8–15, 2016

Dealing with Tradeoffs

- Functionality or security?
- Security or privacy?
- Comply with multiple regulations
- All of the above

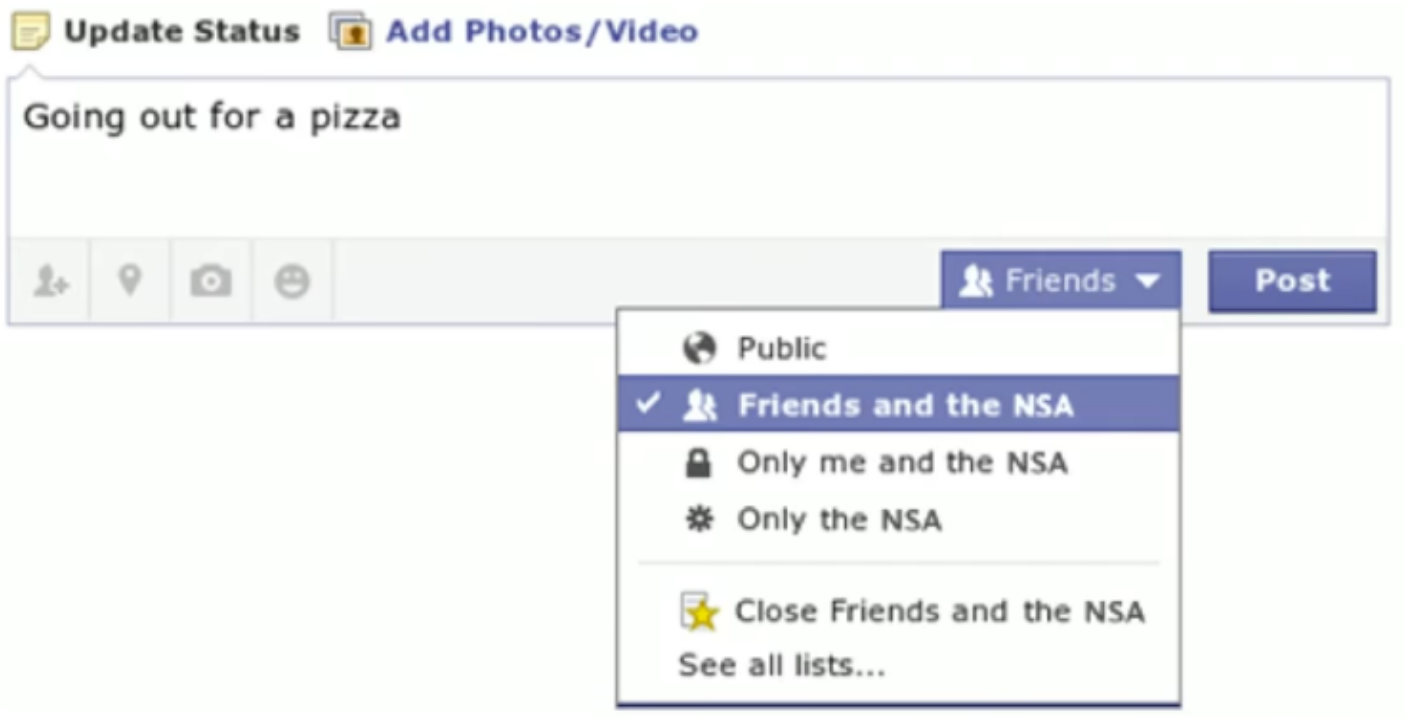
Kafalı et al. Kont: Computing Tradeoffs in Normative Multiagent Systems. AAAI Conference on Artificial Intelligence, pages 3006–3012, 2017

Data Privacy: Location Sharing



Foursquare app: https://www.buzzfeed.com/ashleyperez/creepers-r-us

Data Privacy: Surveillance



https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters#t-53301

Need for Cybersecurity Experts

- At all levels
- Academia
- Security engineers
- Testers
- “Security and privacy aware” software developers

Secure Application Development

- Application developers focus on functional requirements
- Depending on the product, security & privacy considered non-functional requirements
- Requirements elicitation: “Unknown unknowns”

Security vs Usability

- People want cybersecurity and privacy
- Until it disrupts their everyday functionality
- Different needs for novices vs experts

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