Call for Participation:
SPMED - Real-World Security and Privacy for Collaborative Medical Analytics

July 18, 2016, Darmstadtium, Darmstadt, Germany
https://www.securityweek2016.tu-darmstadt.de/spmed-2016/

Workshop Focus:
Medical progress increasingly depends on analyzing large data sets. This is often prevented by data silos and stringent privacy requirements. New technologies are emerging that allow **privacy-preserving collaborative analytics of medical data**, even if the amounts of data are large, the security and privacy requirements remain stringent, and the data origins from multiple silos. In particular fields with highly sensitive data such as genomics or other health domains, the wide range of privacy-preserving analytics technologies promise to enable new and exciting applications and scientific breakthroughs.

Keynote Speakers:
- Kate Black (23andMe): *"Navigating Privacy and Security in Consumer Genetics"*

- Jim Davies (Genomics England Limited and Oxford University):
  "Security and Privacy in the UK: The 100,000 Genomes Project"

- Roland Eils (German Center for Cancer Research (DKFZ) and University of Heidelberg):
  "Curse or Cure: Big Data in Health"

- Michael Steiner (Intel Labs): *"ReliancePoint: A Foundation for Scalable & Secure Computation over Privacy-Sensitive Shared Data"*

- Paul Francis (MPI-SWS and Aircloak): *"A Breakthrough in Anonymity X Utility for Anonymized Analytics"*

Workshop Goals:
- To bring stakeholders from Medicine, Law, and Technology together to get a better understanding of the full range of requirements, capabilities, and constraints.
- To compare and contrast recent advances from a user perspective and to identify promising directions for further research and real-world validation.
- Discuss the current state of technology and to identify remaining technical and non-technical hurdles for public adaption.

Poster Submission, Logistics and Registration:
- **Date and Venue:** July 18, 2016 at the Darmstadtium, Darmstadt, Germany
- **Logistics and Registration:** www.spw2016.de (Register for SPMED; regular 90EUR, Student 60EUR).
- **Call for Posters that discuss related research.** Please submit A0 posters by email before July 1. The workshop will not publish proceedings: The goal is to openly share and summarize progress and insights.

Keynotes

Kate Black - Privacy Officer & Corporate Counsel at 23andMe

Talk: Navigating Privacy and Security in Consumer Genetics

23andMe often sits at the intersection of emerging and dynamic trends, including: providing and empowering individuals through genetics, exploring genetic research for personalized medicine, challenging and conflicting legal requirements, and risks in cyber security and surveillance.I will provide an overview of how we navigate these challenges, the most common privacy and security issues, and some practical approaches to protecting sensitive health information online.

About Kate Black

Kate joined 23andMe in 2015 in the newly created role of privacy officer and corporate counsel. Her responsibilities include: developing, implementing, overseeing, and maintaining comprehensive privacy and data use policies, practices and procedures for the company. Prior to 23andMe, Kate spent two years with the U.S. Department of Health and Human Services' Office of the National Coordinator for Health IT (ONC) where she was responsible for developing and updating national privacy and security requirements. Before ONC, she was staff attorney for the Health Privacy Project at the Center for Democracy and Technology (CDT). Kate holds a Juris Doctorate from The George Washington University and received a bachelor of science degree in health sciences from The Florida International University.

About 23andMe

23andMe, Inc. is the leading personal genetics company. Founded in 2006, the mission of the company is to help people access, understand and benefit from the human genome. 23andMe has over 850,000 customers worldwide with over 80 percent consented to participate in research. 23andMe, Inc. is located in Mountain View, CA. More information

Jim Davies - University of Oxford & Genomics England Limited

Talk: Security and Privacy in the UK 100,000 Genomes Project

The 100,000 Genomes Project is linking whole genome sequences to detailed accounts of diagnosis, treatment, and outcomes.The sequences come from patients with cancer or rare, inherited disorders who have consented to the use of their data to increase our understanding of disease and to accelerate the development of new diagnostics and new therapeutics. The patients are under the care of the National Health Service (NHS) in England, and NHS staff are identifying eligible patients, providing detailed clinical and laboratory data, and receiving reports based upon the interpretation of the sequences.These reports may lead to new diagnoses and - following confirmatory tests - to new treatment decisions. The Project has two objectives: to establish a flow of high-quality data for research, and to facilitate the adoption of genomic medicine in the NHS. In this talk, I will explain some of the social and technical challenges encountered in the delivery of the project, with a particular focus upon privacy and security.

About Jim Davies

Jim Davies is Professor of Software Engineering at the University of Oxford, Director of Informatics for the Oxford NIHR Biomedical Research Centre, and Chief Technology Officer of Genomics England Limited. He leads a team of architects, engineers, and researchers working on model-driven approaches to software engineering and data management, with a particular focus upon semantic interoperability.

About Genomics England Limited

Genomics England is a wholly owned company of the Department of Health. Genomics England was set up to deliver the 100,000 Genomes Project: This flagship project will sequence 100,000 whole genomes from NHS patients and their families. More information here.

Roland Eils - DKFZ and University of Heidelberg

Talk: Curse or Cure: Big Data in Health

Recent developments in DNA sequencing technology now enable human whole-genome sequencing for less than €1,000 facilitating applications in cancer research and care. These cost reductions have spurred initiatives such as the International Cancer Genome Consortium to pursue sequencing and analysis of large numbers of patient genomes. Hundreds of thousands of patient genomes will become sequenced in the next few years. Thus, an unprecedentedly rich set of "big data" will emerge in cancer and other diseases with the promise to improve patient stratification and diagnostics towards personalized medicine. I will discuss in my presentation our ongoing effort to bring next generation sequencing into clinical practice at the National Center for Tumor Diseases (NCT) in Heidelberg and how we address ethical, legal and privacy issues in this process.

About Roland Eils

Roland Eils is trained as a Mathematician and Computer Scientist. He is professor of Bioinformatics and Functional Genomics at the University of Heidelberg, where he co-founded and directs Bioquant, Heidelberg's centre for Quantitative Biology. At the German Cancer Research Center he directs the Theoretical Bioinformatics Division.

About DKFZ (German Cancer Research Center)

DKFZ is the largest biomedical research institute in Germany. In over 90 divisions and research groups, more than 2,700 employees, of which more than 1,200 are scientists, are investigating the mechanisms of cancer, are identifying cancer risk factors and are trying to find strategies to prevent people from getting cancer.They are developing novel approaches to make tumor diagnosis more precise and treatment of cancer patients more successful. More information here.

Michael Steiner - Intel Labs

Talk: ReliancePoint: A Foundation for Scalable & Secure Computation over Privacy-Sensitive Shared Data

Big data is created and accumulated each day in many organizations. Mining and analyzing the big data, especially aggregated data across organizations, has the huge benefit of both business and research values. However, loss of privacy or secret information would be detrimental an inhibit widespread applications of data analytics on joint multi-party datasets. As a result, data are locked in data silos, unavailable for research and business analysis.

In this talk, I will present the Reliance Point (RP) technology that supports hosting big data analytics in an untrusted cloud. RP addresses the problem by providing a secure and scalable "neutral environment" for computation based on hardware-based Trusted Execution Environments (TEE). RP enables analytic workflows (pipeline of analytics jobs) by dynamically forming trusted cluster of TEEs, protect data confidentiality and execution integrity while leaving data providers in full control over their data throughout workflow execution.

About Michael Steiner

Dr. Michael Steiner is a Research Scientist at Intel Labs in Hillsboro, OR, USA. At Intel Labs and in previous positions at IBM Research in India, USA and Switzerland, his work ranged from cryptographic protocol design & analyis, over security architectures & implementations to penetration testing in domains as varied as electronic commerce & payment systems, compliance management, web2.0, cloud and smart grid. Most recently, he is focusing on using hardware-security as foundation to enable scalable multi-party computation.

About Intel Labs

Intel Labs is the research arm of Intel. It fuels Intel's growth and technology leadership by providing leading edge technologies– not only for current roadmaps, two to five years from now, but also disruptive technology for the "next big thing"! More information here.

Paul Francis - Max Planck Institute for Software Systems & Aircloak

Talk: A Breakthrough in Anonymity X Utility for Anonymized Analytics

Working over the past few years in close conjunction with the MPI-SWS spinoff Aircloak, we have developed what we believe is a breakthrough in the anonymity X utility "product". Our system, dubbed the "Cloak", may be installed in front of any existing SQL database (unmodified), with negligible configuration. Untrusted analysts may submit an unlimited number of SQL queries to the database through the Cloak with, so far as we know, virtually no possibility of inferring individual user information from the answers. The noise added by the Cloak is minimal: Gaussian with a typical standard deviation of 2 for counting queries. The SQL queries may be composed of the "aggregate subset" of SQL, which includes most standard math, string, datetime, and aggregate functions, as well as custom functions. This talk will describe cloak operation, present a case study based on a real medical database, and give an overview of the anonymization mechanisms.

 About Paul Franics

Paul Francis is a tenured faculty at the Max Planck Institute for Software Systems in Germany. Paul has held research positions at Cornell University, ACIRI, NTT Software Labs, Bellcore,and MITRE, and was Chief Scientist at two Silicon Valley startups. In the past, Paul's research centered around routing and addressing problems in the Internet and P2P networks. Paul's innovations include NAT, shared-tree multicast, the first P2P multicast system, the first DHT (as part of landmark routing), and Virtual Aggregation. More recently, Paul's research has focused on Internet privacy with a focus on private behavioral advertising systems and anonymized analytics. Paul is cofounder of the startup Aircloak.

About Aircloak

Aircloak is a startup, based in Germany which is building a system that provides rich and accurate analytics over user data while keeping the data anonymous. More information here.