Fraunhofer AISEC

VDE ITG Informationstechnische Gesellschaft

Hochschule Bonn-Rhein-Sieg University of Applied Sciences

TU berlin

USP DAY 2022

Friday, February 11, 2022
Online via MS Teams

Privacy in a Digital World

Program

February 11, 2022
(all times CET)

09.00 am **Welcoming words**
Dr. Maija Poikela, Fraunhofer AISEC

Keynote: Nudging Software Developers Toward Secure Code
Prof. Jens Großklags, TU München

10.00 am Session 1

Chair: Jörg Smykowski, Fraunhofer AISEC

Center for Trustworthy Artificial Intelligence / How can we trust machines?
Verena Till and Michael Puntschuh, iRights.Lab / ZVKI

Trust in Digital Identities
Sandra Kostic, Fraunhofer AISEC

Monetary Valuation of Privacy and Control over Privacy Settings
Vera Schmitt, TU Berlin

How effective are the user rights of the GDPR? Empirical insights into data portability and data erasure practices
Emmanuel Syrmoudis, TU München

Data Cart – Designing a tool for the GDPR-compliant handling of personal data by employees.
Jan Tolsdorf, Hochschule Bonn-Rhein-Sieg

01.00 pm Session 2

Chair: Nikolai Lenski, Fraunhofer AISEC

AnonymPrevent – AI-based Improvement of Anonymity for Remote Assessment, Treatment and Prevention against Child Sexual Abuse
Jun.-Prof. Ingo Siegert, Otto von Guericke Universität Magdeburg

Will Identity Wallets Provide User-centred Privacy?
Dr. Paul Dunphy, OneSpan

Do we know enough to use Online Public Services (OPS) safely?
Anne Jellinghaus, Technische Hochschule Wildau

Service Providers: Crucial Stakeholders for Trustable and Privacy-friendly Digital Identities
Dr. Michael Kubach, Fraunhofer IAO

Usable Security and Privacy of Risk-based Authentication
Stephan Wiefling, Hochschule Bonn-Rhein-Sieg

Passwords are dead - What's next?
Prof. Markus Dürmuth, Leipniz-Universität Hannover

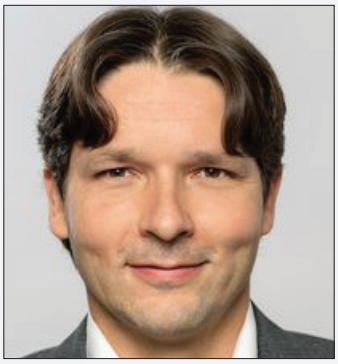
04.00 pm Panel Discussion

How important is trust?

Dr. Maija Poikela, Fraunhofer AISEC (host)
Prof. Angela Sasse, Ruhr University Bochum
Kai Wagner, Jolocom
Prof. Jens Großklags, TU München
Prof. Tom Bäckström, Aalto University

SPEAKER
KEYNOTE AT 9.10 AM

PROF. JENS GROSSKLAGS, TU MÜNCHEN



Jens Grossklags is Professor of Cyber Trust at the Department of Informatics, Technical University of Munich. He received a Ph.D. at the School of Information, University of California at Berkeley, and was a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. He then directed the Security, Privacy and Information Economics Lab, and served as the Haile Family Early Career Professor at the Pennsylvania State University. His research and teaching activities focus on interdisciplinary challenges in the areas of security, privacy and technology policy.

BIO

Keynote:
Nudging Software Developers Toward Secure Code

The prevalence of insecure code is one of the main challenges security experts are trying to solve. We study behavioral patterns among developers which largely contribute to insecure software - googling and reusing code from the web - and apply nudge theory to harness these behaviors and help developers write more secure code.

ABSTRACT

BIO

USP DAY 2022

FEBRUARY 11, 2022

SPEAKERS
SESSION 1 AT 10AM

VERENA TILL
IRIGHTS.LAB & ZVKI

Bio

Verena Till is a member of the Research & Projects team at iRights.Lab, where she coordinates the Center for Trustworthy Artificial Intelligence. She has worked in trend and futurology research for many years and has supervised numerous studies and projects related to the digital taansformation of society. She is particularly interested in how artificial intelligence is shaping our world.

MICHAEL PUNTSCHUH
IRIGHTS.LAB & ZVKI

Bio

Michael Puntschuh is a freelance policy analyst and works on societal, ethical and legal aspects of digital technologies. At the independet Think Tank iRights.Lab he contributes to the Center for Trustworthy AI. His work currently focusses on criteria for the development of algorithmic systems and public innovation. Furthermore, he is involved in projects on digital ethics and algorithmically mediated discrimination.

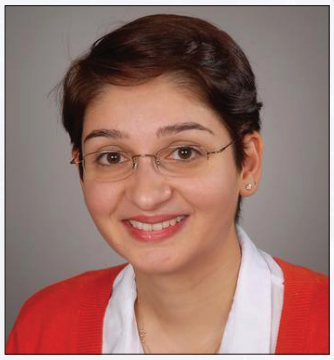
Center for Trustworthy Artificial Intelligence
(Zentrum für vertrauenswürdige Künstliche Intelligenz, ZVKI)

Abstract

As a non-partisan national organization linking the business, industry, political and civil society communities, the Center for Trustworthy Artificial Intelligence informs the public about consumer-relevant issues in AI, fosters public debate on the subject and develops instruments for evaluating and certifying AI. With support from the German Federal Ministry for the Environment, Nature Conservation, Nuclear Saftey and Consumer Protection, iRights.Lab, an independent think tank, has founded the ZVKI in co- operation with the Fraunhofer institutes AISEC and IAIS and the Freie Universität Berlin.

How can we trust machines?

Which criteria determine whether we trust AI systems? Why should machine learning applications be trustworthy? And how can we contribute to the development of trustworthy AI? I a short presentation we summarize current research and projects on the issue to gain insights into answers to these questions. We furthermore present the Center for Trustworthy AI, which was recently launched by the iRights.Lab, FU Berlin and Fraunhofer.



Trust in Digital Identities

Abstract

This talk presents the results of a user study on a high-level concept of a digital identity that is stored on the smartphone and can be used for online identification at various services. Criteria are discussed which factors could be significant for the trust in digital identities and which could influence it in a positive or negative way.

SANDRA KOSTIC
FRAUNHOFER INSTITUTE
FOR APPLIED AND INTEGRATED SECURITY

Bio

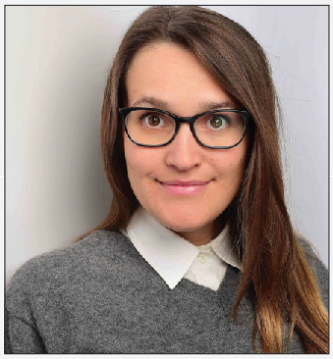
Sandra Kostic studied at Freie Universität Berlin, where she received her master's degree in computer science in the field of usable security. During her studies, she joined the research group of Prof. Dr. Marian Margraf at Freie Universität Berlin. There she took on the role of project lead for Freie Universität Berlin in a project dealing with identities on mobile devices in 2018. Since 2020, she has been working in the Secure Systems Engineering department at Fraunhofer AISEC, where she is part of the Usable Security and Privacy group and works on user-friendliness and acceptance of digital identities, among other topics. In addition, her research interests lie in the area of trust. There, she is working toward her PhD degree, investigating the relationship between privacy and trust.

USP DAY 2022
FEBRUARY 11, 2022

SPEAKERS
SESSION 1 AT 10AM

Monetary Valuation of Privacy and Control over Privacy Settings

VERA SCHMITT
TU BERLIN



ABSTRACT

The standard approach of Notice and Choice does not provide sufficient control over personal privacy preferences. A more granular analysis of privacy preferences is needed where the monetary valuation of different data types can contribute to the understanding of individual privacy concerns and preferences of personal information. The question of how much consumers value their privacy is still underexplored. Therefore, this talk will present experiments conducted to measure monetary valuations of different data types with a focus on location information. Furthermore, findings from experiments about mechanisms to control privacy settings are presented and an outlook about future experiments is given, to combine approaches of monetary valuation and privacy control.

BIO

Vera Schmitt is a PhD candidate at the Quality and Usability Lab TU Berlin. She started her PhD in the beginning of 2020 and her research interests range from usable privacy, fake news detection to ethics of AI. She studied Politics and Public Administration at the University of Konstanz, where she also co-founded CorrelAid, a non-profit network of data science enthusiast, to support the social sector with statistical analysis and machine learning. This motivated her to study Data Science and start a PhD at the Quality and Usability Lab.

EMMANUEL SYRMOUDIS
TU MÜNCHEN

BIO

Emmanuel Syrmoudis is a PhD student at the Technical University of Munich. His research focuses on technological and economic implications of privacy regulation.

How effective are the user rights of the GDPR? Empirical insights into data portability and data erasure practices

ABSTRACT

The GDPR promises to give users more control over their data. In two empirical studies, we find a high heterogeneity and low compliance rates in the execution of user requests. We identify challenges and provide best practices to increase the usability of the rights to data portability and data erasure.

JAN TOLSDORF
HOCHSCHULE BONN-RHEIN-SIEG

BIO

Jan Tolsdorf works as a research assistant in the Data and Application Security Group of Prof. Dr.-Ing. Luigi Lo Iacono at Bonn-Rhein-Sieg University of Applied Sciences. He is also a last year external PhD candidate in the Computer Security and Privacy Research Group of Prof. Dr.-Ing. Delphine Reinhardt at the University of Göttingen. His current research activities are in the area of usable security & privacy, and privacy in employment.

Data Cart – Designing a tool for the GDPR-compliant handling of personal data by employees

ABSTRACT

Employees who process personal data as part of their job have a particular responsibility when it comes to protecting privacy. With the General Data Protection Regulation, the obligations have become even stricter. However, there are few studies that address the needs of these employees for appropriate tools to help them comply with data protection laws. To develop a suitable tool, we applied a human-centered development approach and conducted a series of eight workshops with 19 employees from two public institutions in Germany. The tool is based on the novel metaphor of a data cart and is designed to support employees equally in data management and data protection compliance. Usability evaluations show that Data Cart gives employees a greater sense of security when handling personal data and sharpens their awareness of data protection. Our results also suggest that employee perceptions of privacy may become more positive when Privacy by Design becomes an integral part of digitalization. The presentation covers details on the development process and the core results of our evaluations.

SPEAKERS
SESSION 2 AT 1PM

AnonymPrevent – AI-based Improvement of Anonymity for Remote Assessment, Treatment and Prevention against Child Sexual Abuse

ABSTRACT

AnonymPrevent investigates both the use and improvement of innovative AI-based anonymization techniques for initial counseling and preventive remote treatment of people who are sexually attracted to children. The goal of AnonymPrevent is speech anonymization that anonymizes a patient's identity (voice, manner of speaking) while retaining the emotion and personality expression content relevant for clinical diagnostic assessment. The trustworthiness of such an AI system is crucial for the utilization of the preventive therapy offer by those seeking help, since participation is associated with shame and fear of social exclusion. The team also investigates whether anonymization of the verbal communication channel leads to more acceptance for preventive treatment against child abuse and promotes an open exchange without unfavorably influencing the communication in the therapy.

JUN.-PROF. INGO SIEGERT
OTTO VON GUERICKE
UNIVERSITÄT MAGDEBURG

BIO

Ingo Siegert is Juniorprofessor for Mobile Dialog Systems at the Otto von Guericke University Magdeburg since 2018. He received his Doktoringenieur (equivalent to PhD) in Electrical Engineering in 2015 from the Otto von Guericke University Magdeburg Germany. His research interests and publications focus on signal-based analyses and interdisciplinary investigations of (human-) human-computer interaction in terms of addressee detection and the utilization of further interaction patterns, such as filled pauses or discourse particles. A further recent focus is on privacy and security of speech-based interactions, where currently two research projects "Emonymous" and "AnonymPrevent" are settled. Ingo Siegert has published 100+ peer reviewed papers on several conferences and various journals and is an active organizer of several workshops and conferences in the area of speech privacy, voice assistants and HCI.

ANNE JELLINGHAUS
TECHNISCHE HOCHSCHULE WILDAU

BIO

Anne Jellinghaus completed her Diploma in Psychology at the University of Bremen. Anne has research experience in areas such as Neuropsychology, Robotics, Gender Studies, Usability and Gaming. Currently, she is conducting research about usable privacy and security of digital public services funded by the German Federal Ministry of Justice and Consumer Protection.

Do we know enough to use Online Public Services (OPS) safely?

ABSTRACT

In this presentation we discuss which usability aspects could contribute to compensate asymmetries related to knowledge about digital privacy and security for using online public services. What kinds of usability interventions could compensate digital asymmetries about data privacy and security knowledge while keeping digital sovereignty and trust in the use of online public services? How much and in which form information about data privacy and security should be shared? As empirical example we focus on the context of single contact point solutions based upon the "Online access act; Onlinezugangsgesetz" (OZG) in Germany. We discuss the challenges of developing intervention usability tools in relation to digital skills and trust in electronic government and implementing participatory usability methods to design data safe and secure online public services.

DR. PAUL DUNPHY
ONESPAN

BIO

Paul is a Principal Researcher at OneSpan based at their Innovation Centre in Cambridge, UK. His expertise is at the intersection of human-computer interaction and information privacy and security. Before joining OneSpan, he spent time as a User Experience Analyst at Atom Bank during its early days as a startup and the first successful release of its mobile banking app. In addition, he has spent time at Microsoft Research and Nokia Research and gained his PhD in computing science from Newcastle University.

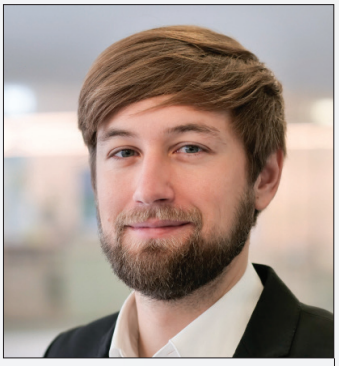
Will Identity Wallets Provide User-centred Privacy?

ABSTRACT

Digital Identity is a topic that is has re-emerged as a topic of significant interest in the technology community. In this talk, I will introduce the emerging digital identity landscape and zoom in on one technology in particular: the identity wallet. Then I will briefly introduce preliminary results from a study where we aimed to learn about the user-centred properties of a prototype identity wallet set in the context of self-sovereign identity.

SPEAKERS
SESSION 2 AT 1PM

Service Providers: Crucial Stakeholder for Trustable and Privacy-friendly Digital Identities



ABSTRACT

It is rightly emphasized that the user must be placed at the center of the development of digital identities. However, to achieve the goal of widely usable trustable and privacy friendly identities, we cannot neglect the role of and requirements of service providers as crucial stakeholders. My talk aims to substantiate this claim and to give related insights from our current research.

DR. MICHAEL KUBACH
FRAUNHOFER INSTITUTE FOR INDUSTRIAL ENGINEERING IAO

BIO

Since 2013, Michael Kubach is researching issues around digital identity and trust, where he takes a socioeconomic, user-oriented perspective, at the Fraunhofer IAO Team Identity Management. Michael has worked in several European and national cooperative research projects such as the EC-funded projects ESSIF-TRAIN and LIGHTest (on trust infrastructures) and FutureID (federated identity management) as well as in national projects such as ONCE (combining self-sovereign identities and other eIDs in a wallet to build an ecosystem for secure identities), ENTOURAGE (ecosystems for smart assistants), and SkIDentity (cloud identity management). Moreover, he is consulting international corporations and NGOs on identity management and blockchain/DLT topics. His research interests are in the areas of socioeconomic aspects of identity management, IT-security, privacy, and blockchain/DLT and their importance for building trustable ecosystems, e.g., for self-sovereign identities.

Michael studied politics and administrative science as well as management in Konstanz, Göttingen and Lille. He received a PhD in economics at the Georg-August-University Göttingen.

Usable Security and Privacy of Risk-based Authentication

ABSTRACT

Risk-based Authentication (RBA) is recommended by NIST (USA) and NCSC (UK) to strengthen password-based authentication against attacks involving stolen passwords, like credential stuffing or password spraying. Large online services already deployed RBA to protect their user base. Beyond that, users find RBA more usable than 2FA, and equally secure. But what about its usability, security, and privacy in practice? We studied RBA on a real-world online service for almost two years to find out more. And yes, we can create a strong, usable, and still more privacy-friendly RBA that complies with the GDPR and CCPA.

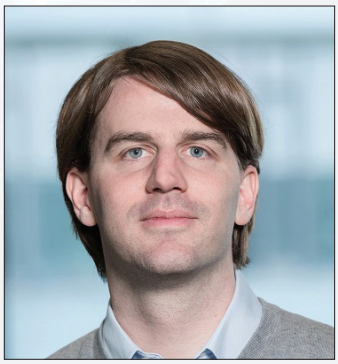
STEPHAN WIEFLING
HOCHSCHULE BONN-RHEIN-SIEG

BIO

Stephan Wiefling is a PhD student in Sankt Augustin, Germany (Data and Application Security Group, H-BRS). His current research spans areas of Authentication and Usability.
Twitter: @SWiefling

PROF. MARKUS DÜRMUTH
LEIBNIZ UNIVERSITY HANNOVER

BIO



Prof. Dr. Markus Dürmuth is associate professor at the Leibniz University Hannover. Previous stations include Ruhr University Bochum, Saarland University, McKinsey & Company, IBM Research, and Stanford University. His research areas are in the field of usable security, specifically usability and technical aspects of user authentication, privacy from an end-user perspective, and the "right to be forgotten". He is author of more than 55 scientific papers, involved in various interdisciplinary teaching and research projects, and member of several program committees including IEEE S&P and PETS.

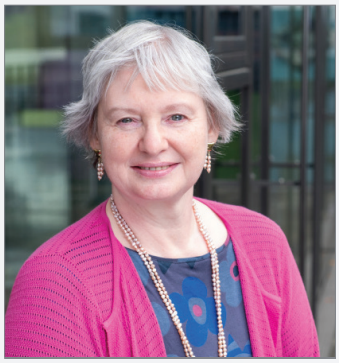
Passwords are dead - What's next?

ABSTRACT

There is growing discomfort about password-based authentication, and passwords are declared "dead" on a regular basis. However, passwords are still the most widely used tool for user authentication on the Internet. In this talk we will have a closer look on the current state of user authentication, and will discuss several variants to strengthen user authentication. One specifically interesting approach is to use additional signals such as source IP, geo-location, or browser configuration. These allow a service to estimate the risk of a malicious login and to take appropriate countermeasures. This requires minimal changes to the user experience, and is used in practice by several services.

USP DAY 2022
FEBRUARY 11, 2022

SPEAKERS
Panel Discussion at 4pm

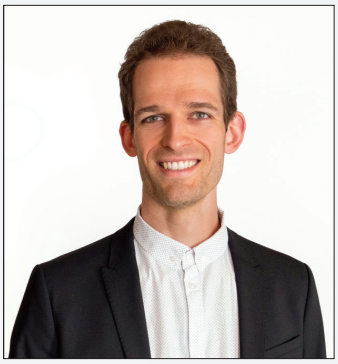


PROF. ANGELA SASSE
Ruhr University Bochum

Bio

M. Angela Sasse is the Professor of Human-Centred Security at Ruhr University Bochum. She obtained an M.Sc. in Occupational Psychology from Sheffield University and a PhD in Computer Science from Birmingham University. From 1990-2018 she was a faculty member in the Department of Computer Science at UCL. She started researching usability issues in IT security in the late nineties, and her 1999 paper with Anne Adams, Users are Not the Enemy, is the most cited paper on the topic. She is one of the pioneers of interdisciplinary security research and led the UK Reseach Institute in Socio-Technical Security from 2012-2018. In 2018, she moved to Ruhr University Bochum to establish the Chair in Human-Centred Security. She is a Speaker of the Exzellenzclusterprojekt CASA and of the interdisciplinary Graduate School SecHuman. She was elected Fellow of the Royal Academy of Engineering in the UK in 2015, and to the NRW Akademie in 2021.

KAI WAGNER
JOLOCOM

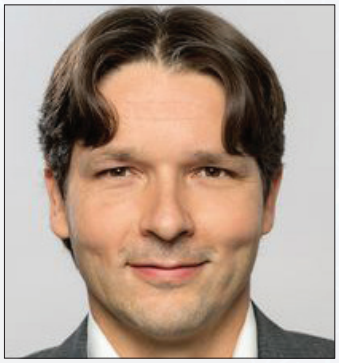


Bio

Kai Wagner works at the self-sovereign identity company Jolocom in Berlin on strategic business development and collaborations. In addition, he regularly represents Jolocom and the topic of digital identity at presentations and panel discussions worldwide. Kai is convinced that decentralized and collaborative approaches offer enormous potential for a future-oriented, fair and sustainable society. Driven by the goal of enabling individual data sovereignty, he is also active on the board of the international association INATBA, where he leads the working group on digital identity.

PROF. JENS GROSSKLAGS
TU MÜNCHEN

Bio



Jens Grossklags is Professor of Cyber Trust at the Department of Informatics, Technical University of Munich. He received a Ph.D. at the School of Information, University of California at Berkeley, and was a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. He then directed the Security, Privacy and Information Economics Lab, and served as the Haile Family Early Career Professor at the Pennsylvania State University. His research and teaching activities focus on interdisciplinary challenges in the areas of security, privacy and technology policy.

PROF. TOM BÄCKSTRÖM
AALTO UNIVERSITY

Bio

Tom Bäckström received the master's and doctor of science degrees from Aalto University, in 2001 and 2004, respectively, which was then known as the Helsinki University of Technology. He has been an Associate Professor with the Department of Signal Processing and Acoustics, Aalto University, Finland, since 2016. He was a Professor at the International Audio Laboratory Erlangen, Friedrich-Alexander University (FAU), from 2013 to 2016, and a Researcher at Fraunhofer IIS from 2008 to 2013. He has contributed to several international speech and audio coding standards and is the chair and co-founder of the ISCA Special Interest Group "Security and Privacy in Speech Communication". His research interests include technologies for spoken interaction, emphasizing efficiency and privacy, and in particular in multi-device and multi-user environments.

USP Day 2022

February 11, 2022