9. Usable Security und Privacy Workshop

Luigi Lo Iacono
luigi.lo_iacono@h-brs.de
Hochschule Bonn-Rhein-Sieg

Hartmut Schmitt
hartmut.schmitt@hk-bs.de
HK Business Solutions GmbH

Denis Feth
denis.feth@iese.fraunhofer.de
Fraunhofer IESE

Andreas Heinemann
andreas.heinemann@h-da.de
Hochschule Darmstadt, ATHENE

ZUSAMMENFASSUNG

Ziel der neunten Ausgabe des wissenschaftlichen Workshops "Usable Security und Privacy" auf der Mensch und Computer 2023 ist es, aktuelle Forschungs- und Praxisbeiträge auf diesem Gebiet zu präsentieren und mit den Teilnehmer:innen zu diskutieren. Getreu des Konferenzmottos "Building Bridges" soll mit dem Workshop ein etabliertes Forum fortgeführt und weiterentwickelt werden, in dem sich Expert:innen, Forscher:innen und Praktiker:innen aus unterschiedlichen Domänen transdisziplinär zum Thema Usable Security und Privacy austauschen können. Das Thema betrifft neben dem Usability- und Security-Engineering unterschiedliche Forschungsgebiete und Berufsfelder, z. B. Informatik, Ingenieurwissenschaften, Mediengestaltung und Psychologie. Der Workshop richtet sich an interessierte Wissenschaftler:innen aus all diesen Bereichen, aber auch ausdrücklich an Vertreter:innen der Wirtschaft, Industrie und öffentlichen Verwaltung.

KEYWORDS

Usable Security, Usable Privacy

1 THEMA

Digitale Technologien haben unser Leben rasant verändert. Immer mehr Menschen, Gegenstände und Orte sind digital miteinander verbunden und kommunizieren miteinander. Bereits heute durchdringt die digitale Vernetzung nahezu alle Interaktionsformen unserer Gesellschaft. Dieser Trend – auch Hyperkonnektivität genannt [2] – bringt ständig neue Technologien, Produkte, Dienstleistungen und Geschäftsmodelle hervor. Dies ermöglicht Fortschritt, gleichzeitig ergeben sich jedoch auch Risiken – vom Diebstahl geistigen Eigentums über den Verlust digitaler Identitäten bis hin zu Cyberangriffen, die die Sicherheit von Staaten, Unternehmen und Menschen bedrohen. In einer von Hyperkonnektivität geprägten Zukunft müssen digitale Anwendungen daher höchsten Ansprüchen an Cybersicherheit und Cyberprivatheit gerecht werden, die bei der Ausgestaltung alle angedachten Nutzendengruppen angemessen adressieren müssen.

Angemessene Sicherheits- und Datenschutztechnologien, die von den Benutzer:innen verstanden und effektiv, effizient und zufriedenstellend genutzt werden können, sind grundlegende Faktoren für einen effektiven Schutz von Privat- und Unternehmensdaten [6]. Die Usability von sicherheits- bzw. privatheitsfördernden Verfahren ist somit eine Schlüsseleigenschaft, die die individuellen Anforderungen aller beteiligter Gruppen von Benutzer:innen sowohl in Entwicklungsprozessen als auch im produktiven Einsatz berücksichtigen muss.

Der Ansatz, diese drei wichtigen Grundlagen der Digitalisierung – Sicherheit, Datenschutz und Usability – zusammen zu denken und miteinander in Einklang zu bringen, wird als Usable Security bzw. Usable Privacy bezeichnet. *Usable Security* bezeichnet den inter- und transdisziplinären Ansatz, sicherheitsfördernde Verfahren für digitale Produkte und Dienstleistungen so auszugestalten, dass Benutzer:innen bei ihren sicherheitsrelevanten Zielen und Vorhaben bestmöglich unterstützt werden. Hierdurch werden z. B. auch Lai:innen und technikferne Anwender:innen in die Lage versetzt, Sicherheitselemente und deren Notwendigkeit zumindest grundlegend zu verstehen und die Elemente in der dafür vorgesehenen Weise zu verwenden. *Usable Privacy* verfolgt äquivalente Ziele und fokussiert dabei auf Technologien zur Förderung der Privatheit in digitalen Systemen und Plattformen.

Sowohl technische als auch organisatorische Maßnahmen können beeinflussen, wie die Nutzer:innen informationstechnischer Systeme die darin integrierten Funktionen zur Erhöhung der Sicherheit und der Privatheit wahrnehmen und nutzen. Ein Beispiel, das wie fast kein anderes für das Leitthema "Building Bridges" der diesjährigen Mensch und Computer steht, sind sogenannte Datentreuhänder. Ein Datentreuhänder ist eine spezielle Form des Datenmittlers und eine Vertrauensinstanz, die schützenswerte Daten zwischen Datengebenden und Datennutzenden unter Wahrung der Interessen beider Seiten digital vermittelt [5]. Insbesondere das Schaffen von Vertrauen und das Vertreten der Interessen aller Parteien bedingen hier eine benutzerfreundliche Umsetzung der IT-Sicherheit und des Datenschutzes. Neben personenbezogenen Daten werden bei Datentreuhandmodellen auch viele unternehmensbezogene Daten vermittelt. Diese fallen nicht notwendigerweise unter den Datenschutz, aber häufig unter den Geschäftsgeheimnisschutz. Daher ist es eine spannende Frage, wie man neben "Usable Security and Privacy" auch "Usable Data Sovereignty" angeht, welche es Datengebern ermöglicht - unabhängig von der Art der Daten - informiert und selbstbestimmt an Datentreuhandmodellen teilzunehmen.

Viele Lösungen zur Ausübung der Souveränität im digitalen Raum erreichen geltende Usability-Standards bislang nicht [8]. Häufige Ursache dafür ist eine unzureichende Ausgestaltung von Sicherheits- und Datenschutzmechanismen, die den Bedürfnissen, Fähigkeiten und Zielen der Nutzer:innen nicht gerecht wird. Die hohe und stetig steigende Komplexität informationstechnischer Systeme – auch bedingt durch deren Hyperkonnektivität – sorgt für immer neue Herausforderungen. Beispielsweise können dezentrale Systemarchitekturen, die ohne eine zentrale Entität auskommen, technisch ein hohes Schutzniveau bieten –

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in P. Fröhlich & V. Cobus (Hrsg.):
Mensch und Computer 2023 – Workshopband, 03.-06. September 2023, Rapperswil (SG)

https://doi.org/10.18420/muc2023-mci-ws11-114

im Anwendungssegment Instant Messaging wäre hier z. B. das Matrix-Protokoll zu nennen. Durch die für Nutzende dabei noch benötigte technische Expertise für die Installation und den Betrieb eines Home-Servers [3] werden derartige Ansätze in der Praxis aber bisher kaum verwendet. Zentralisierte Systeme wie WhatsApp oder Signal werden stattdessen vorgezogen. Twitter vs. Mastodon ist ein weiteres Beispiel dafür, dass zentrale Systeme trotz ihrer Nachteile gegenüber dezentralen Systemarchitekturen – z. B. datengetriebenes Geschäftsmodell – aufgrund von Usability-Vorteilen präferiert werden.

Der Workshop fokussiert dieses Themenspannungsfeld und diskutiert in thematischer Breite aktuelle Herausforderungen, Erkenntnisse und Ansätze aus Wissenschaft und Praxis.

2 ZIELE UND INHALTE DES WORKSHOPS

Der Workshop "Usable Security und Privacy" ist seit 2015 Teil der Konferenz "Mensch und Computer". Ziel der neunten Auflage ist es, dieses etablierte Forum, in dem sich Expert:innen aus Wissenschaft und Praxis zum Thema nutzerfreundliche Technologien zur Gewährleistung von Informationssicherheit und Privatsphäre austauschen können, zu festigen und weiterzuentwickeln. Zugleich soll der Workshop die Diskussion für ein breiteres Fachpublikum öffnen.

Interessent:innen können Forschungs- und Entwicklungsarbeiten - auch in noch frühen Stadien - in deutscher oder englischer Sprache einreichen. Mögliche Beitragstypen sind:

- neue Vorgehensweisen oder Werkzeuge,
- gestalterische Studien, z. B. UI-Gestaltung, Persuasive Design,
- Berichte praktischer Umsetzung (erfolgreiche Beispiele, untaugliche Ansätze),
- Systemdemonstrationen,
- praxiserprobte Methoden, Best Practices,
- kritische Reflexionen (Herausforderungen, Fallstricke),
- Replikationsstudien,
- theoretische/zukunftsweisende Arbeiten,
- laufende Forschungs- und Entwicklungsprojekte,
- Betrachtungen besonderer Benutzergruppen (z. B. Kinder, Senior:innen, Arbeitnehmer:innen, Softwareentwickler:innen, Administrator:innen) und Anwendungsdomänen (z. B. Behörden).

Thematisch möchte der Workshop ein möglichst breites Spektrum abdecken. Einige aktuelle Beispiele sind:

- neuartige Interaktionsformen und Benutzeroberflächen, z. B. Voice User Interfaces,
- konkrete UI-Gestaltung, z. B. bei Video-Konferenzsystemen,
- konkrete Anwendungen/Erfahrungen aus der Praxis,
- Erfahrungen aus den ersten Jahren DSGVO,
- Security Awareness vs. Usable Security.

Die angenommenen Beiträge werden in Vorträgen vorgestellt und mit dem gesamten Auditorium diskutiert. Zudem wird angeboten, die schriftlichen Einreichungen zu publizieren.

Neben Publikationen können für den Usable Security und Privacy Workshop auch interaktive Beiträge eingereicht werden. Die Art eines interaktiven Beitrages ist relativ offen, soll sich aber deutlich von einem Vortrag unterscheiden. Denkbar sind kurze, moderierte Gruppenarbeitsphasen, aber auch Übungen mit neuartigen Werkzeugen. Für diese Beitragsart wird eine kurze Beschreibung des Themas und des geplanten Formats eingereicht. Die Vorschläge für interaktive Beiträge werden von den Workshoporganisator:innen gesichtet, bewertet und dahingehend ausgewählt, dass möglichst abwechslungsreiche Interaktionsformate und unterschiedliche Themen bedient werden.

Zusätzlich zu den Vorträgen und interaktiven Beiträgen wird das Workshop-Programm durch eine eingeladene Keynote abgerundet. Als Keynote Speaker:in wird eine namhafte Persönlichkeit aus der Usable Security und Privacy Forschung oder aus der Industrie akquiriert.

Das Ergebnis des Workshops ist eine dokumentierte Sammlung von neuen Entwicklungen und Forschungsergebnissen im Bereich Usable Security und Privacy im Workshopband der Mensch und Computer.

Der Usable Security und Privacy Workshop findet in enger Abstimmung mit der Fachgruppe "Usable Safety & Security" im Fachbereich Mensch-Computer-Interaktion (MCI) der Gesellschaft für Informatik (GI) statt, die federführend den "Workshop Mensch-Maschine-Interaktion in sicherheitskritischen Systemen" organisiert. Einreichungen aus dem Umfeld von Usable Safety verweisen wir auch auf diesen Workshop.

3 PROGRAMMKOMITEE

Das Programmkomitee des Workshops übernimmt die fachliche und inhaltliche Begutachtung der Einreichungen und unterstützt die Verbreitung des Call for Papers zum Workshop. Die Mitglieder des Programmkomitees sind anerkannte Expert:innen auf dem Gebiet der Usable Security und Privacy aus Wissenschaft und Praxis (Stand: Mai 2023):

- Florian Alt (Universität der Bundeswehr München, DE)
- Zinaida Benenson (FAU Erlangen-Nürnberg, DE)
- Florian Dehling (Hochschule Bonn-Rhein-Sieg, DE)
- Markus Dürmuth (Ruhr-Universität Bochum, DE)
- Sascha Fahl (CISPA, DE)
- Peter Gorski (infodas, DE)
- Marc-André Kaufhold (TU Darmstadt, DE)
- Patrick Kühtreiber (Universität Göttingen, DE)
- Marian Magraf (FU Berlin, DE)
- Tilo Mentler (Hochschule Trier, DE)
- Sebastian Möller (TU Berlin, DE)
- Anna-Marie Ortloff (Universität Bonn, DE)
- Christian Reuter (TU Darmstadt, DE)
- Gunnar Stevens (Universität Siegen, DE)
- Jan Tolsdorf (Hochschule Bonn-Rhein-Sieg, DE)
- Stephan Wiefling (Hochschule Bonn-Rhein-Sieg, DE)

Die Mitglieder des Programmkomitees begutachten alle eingereichten Beiträge in einem Double-Blind-Peer-Review-Verfahren. Jede Einreichung wird hierbei von drei Gutachtern bewertet. Auswahlkriterien für die Annahme sind die Relevanz, Originalität und wissenschaftliche Qualität des Beitrags, eine klare Beschreibung des Lösungsansatzes und ein überzeugender Beleg für dessen Nützlichkeit. Die Autor:innen werden mit einem Shepherding-Prozess unterstützt, in dem den Autor:innen jeweils ein Mitglied des Organisationsteams für Rückfragen zu den Reviewkommentaren zur Verfügung steht.

4 AKZEPTIERTE BEITRÄGE UND KEYNOTE

Das Workshop-Programm besteht im Wesentlichen aus einer eingeladenen Keynote und den angenommenen Beiträgen.

In seiner Keynote zeigt Sascha Fahl (CISPA) wie eine ganzheitliche Betrachtung menschlicher Faktoren in der Cybersicherheitsforschung dazu beiträgt, die Lücke zwischen theoretischer

Sicherheit, Datenschutz und realen Einsätzen zu schließen. Auf Basis früherer und aktueller Arbeiten zur Unterstützung von Experten und zum Schutz von Endnutzern möchte er Ziele und Strategien für die zukünftige Forschung erläutern. Sascha Fahl vertritt hier die These, dass durch eine Kombination aus technischer Innovation und der Berücksichtigung menschlicher Faktoren der unfreiwillige Verlust der Kontrolle über Daten erfolgreich verhindert und den Nutzern die Möglichkeit gegeben werden kann, die Kontrolle über ihre Sicherheit und Privatsphäre zu behalten.

Von den eingereichten Beiträgen wurden vier Arbeiten für das Programm des Workshops akzeptiert, die im Folgenden kurz vorgestellt werden. Die vollständigen Papiere sind im Workshopband der Mensch und Computer 2023 enthalten.

In der Arbeit "Let's Write Privacy: Vision for an Experiment Design on Textual Privacy in Conversation" [1] gehen die Autoren Beyer et. al auf das Thema Datenschutz in Konversationen mit virtuellen Assistenten ein. Neben Methoden zur Identifikation und Maskierung von personenbezogenen Daten und Quasi-Identifikatoren stellen die Autoren eine Benutzerschnittstelle zur Konfiguration von Sprachmodellen zur Generierung von Konversationsdaten vor und beschreiben ein geplantes Card-Sorting-Experiment zur empirischen Evaluation ihres Ansatzes.

In der Arbeit "Towards informed choices: A decision model for adaptive warnings in self-sovereign identity" [4] diskutieren die Autoren Ebert et. al im Kontext souveräner Identitäten (Self-Sovereign Identity, SSI) ein auf der DSGVO basierendes Entscheidungsmodell, welches die Bedrohungsstufe bei Anfragen zur Übermittlung und Weitergabe von personenbezogenen Daten ermittelt und dem Nutzer dabei unterstützt, eine informierte und fundierte Entscheidung hinsichtlich der Weitergabe seiner Daten zu treffen.

In der Arbeit "Legal Requirements and Technical Metrics for Controlling Privacy of Employees' Location Data" [9] gehen die Autoren Waldmann et. al auf die Besonderheiten des Beschäftigtendatenschutzes ein. Sie empfehlen die Verwendung geeigneter Metriken, mit denen Unternehmen in der Lage sind, die DSGVO-Anforderungen hinsichtlich Datenminimierung und Speicherbegrenzung automatisiert zu überprüfen. Dies wird anhand eines Anwendungsbeispiels aus der Logistik erläutert, bei dem Echtzeit-Standortdaten der Beschäftigten in der agilen Personaleinsatzplanung verarbeitet werden.

In der Arbeit "Is Privacy a Trait or a State? Examining Hangriness and its Influence on Individual's Privacy Perception" [7] untersuchen die Autoren Schmitt et. al, ob der Stoffwechselzustand Hunger einen Einfluss auf das Konstrukt Privatsphäre bei einem Nutzer hat. Hintergrund ist hier die Debatte der Privatsphärenforschung, ob der Wunsch nach Privatheit eher ein Zustand oder eine Eigenschaft einer Person ist. Die Studienergebnisse der Autoren weisen darauf hin, Privatheit als Zustand zu begreifen. Hunger bei den Probanden zeigt hier keinen Einfluss. Allerdings beeinflusst der Sättigungszustand der Probanden deren Privatheitskompetenz.

5 ORGANISATION UND DURCHFÜHRUNG

Die Durchführung des Workshops erfolgt durch Luigi Lo Iacono (Hochschule Bonn-Rhein-Sieg), Hartmut Schmitt (HK Business Solutions GmbH), Denis Feth (Fraunhofer IESE) und Andreas Heinemann (Hochschule Darmstadt).

Luigi Lo Iacono ist Professor für Informationssicherheit am Fachbereich Informatik der Hochschule Bonn-Rhein-Sieg. Dort leitet er das Institut für Cyber Security & Privacy und die Arbeitsgruppe für *Daten- und Anwendungssicherheit*

Hartmut Schmitt (HK Business Solution GmbH) ist seit 2006 in Verbundvorhaben auf den Gebieten Mensch-Computer-Interaktion, Usability/User Experience, IT-Security & Datenschutz tätig, u. a. als Projektkoordinator in den Verbundvorhaben USecureD, TrUSD und D'accord.

Denis Feth ist Expert »Data Sovereignty« am Fraunhofer IESE. Er leitet dort den Forschungsbereich Datensouveränität und Projekte rund um die Themen Datennutzungskontrolle, Datentreuhänder und Usable Security and Privacy.

Andreas Heinemann ist Professor für IT-Sicherheit und Computernetzwerke am Fachbereich Informatik der Hochschule Darmstadt. Dort leitet er die Arbeitsgruppe *User-Centered Security*. Er ist Repräsentant der Hochschule Darmstadt im Board des Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENEund Mitglied im Vorstand des Competence Center for Applied Security Technology, CAST e.V.

Die neunte Auflage des Usable Security und Privacy Workshops wird in Zusammenarbeit mit dem GI Fachbereich Mensch-Computer-Interaktion (MCI), dem ITG-Fachbereich Dienste und Anwendungen, dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE und dem Projekt "D'accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen" durchgeführt.

DANKSAGUNG

Die Organisatoren möchten nochmals allen Autor:innen danken, die den Workshop mit ihren Einreichungen bereichern. Außerdem gebührt den Mitgliedern des Programmkomitees ein herzlicher Dank, die die Einreichungen mit konstruktiven und ausführlichen Gutachten bewerten.

Diese Arbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projekts "D'accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen" unterstützt.

LITERATUR

[1] Franka Beyer, Zahra Kolagar, and Darina Gold. 2023. Let's write Privacy: Vision for an Experiment Design on Textual Privacy in Conversation. In *Mensch und Computer 2023 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2023-mci-ws11-260

[2] Bundesministerium für Bildung und Forschung. 2022. Hyperkonnektivität: Chancen der digitalen Vernetzung. https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/hyperkonnektivitaet/digitale-vernetzung.html

[3] Matrix.org Foundation C.I.C and Matrix Community. 2022. Synapse – Installation Instructions. https://matrix-org.github.io/synapse/latest/setup/installation.html

[4] Sarah Ebert, Anna-Magdalena Krauß, and Jürgen Anke. 2023. Towards informed choices: A decision model for adaptive warnings in self-sovereign identity. In *Mensch und Computer 2023 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2023-mci-ws11-322

[5] Denis Feth, Bernd Rauch, Daniel Krohmer, Jannis von Albedyll, and Karina Barreto Villela. 2023. Datentreuhänder – Begriffliche Einordnung und Definition. https://www.iese.fraunhofer.de/blog/datentreuhaender-definition/

[6] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security*. Springer Nature Switzerland AG, Gewerbestrasse 11, 6330 Cham, Switzerland. https://doi.org/10.1007/978-3-031-02343-9

[7] Vera Schmitt, Robert P. Spang, Wafaa Wardah, and Sebastian Möller. 2023. Is Privacy a Trait or a State? Examining Hangriness and its Influence on Individual's Privacy Perception. In *Mensch und Computer 2023 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2023-mci-ws11-377

[8] Jan Tolsdorf, Florian Dehling, and Denis Feth. 2021. Benutzerfreundlicher Datenschutz in Cloud-basierten Office-Paketen. *Datenschutz und Datensicherheit - DuD* 45, 1 (Jan. 2021), 33–39. https://doi.org/10.1007/s11623-020-1386-x

[9] Ulrich Waldmann, Thomas Kunz, Janine Schleper, Matthias Kohn, and Paulina Jo Pesch. 2023. Legal Requirements and Technical Metrics for Controlling Privacy of Employees' Location Data. In *Mensch und Computer 2023 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2023-mci-ws11-364