

10. Usable Security und Privacy Workshop

Luigi Lo Iacono
Hochschule Bonn-Rhein-Sieg
Germany

Denis Feth
Fraunhofer IESE
Germany

Hartmut Schmitt
HK Business Solutions GmbH
Germany

Andreas Heinemann
Hochschule Darmstadt
Germany

Zusammenfassung

Ziel der zehnten Ausgabe des wissenschaftlichen Workshops "Usable Security und Privacy" auf der Mensch und Computer 2024 ist es, aktuelle Forschungs- und Praxisbeiträge auf diesem Gebiet zu präsentieren und mit den Teilnehmer:innen zu diskutieren. Getreu dem Konferenzmotto "Hybrid Worlds" 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.

CCS Concepts

• Security and privacy → Social aspects of security and privacy.

Keywords

Usable Security, Usable Privacy

1 Thema

In hybriden Welten, in denen die Grenzen zwischen physischer und virtueller Welt immer mehr verschwimmen, sind die Themen IT-Security und Datenschutz so relevant wie noch nie. Die zunehmende Digitalisierung, künstliche Intelligenz und ähnliche Megatrends eröffnen in allen Lebensbereichen neue Chancen – beispielsweise helfen verbesserte Flexibilität und Handlungsfähigkeit den Unternehmen dabei, resilienter und krisenfester zu werden. Gleichzeitig kommen an der Schnittstelle zwischen Realität und digital-virtuellem Raum immer ausgefeiltere Techniken für Ransomwareangriffe, Social Engineering oder Identitätsdiebstahl zum Einsatz.

Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) [3] als auch die Europäische Agentur für Netz- und Informationssicherheit ENISA [6] kommen in ihren aktuellen Lageberichten zu dem Schluss, dass die Bedrohung im Cyberraum so hoch ist wie nie zuvor. Ein wichtiger Baustein bei der verantwortungsvollen Entwicklung digitaler Technologien, so

das BSI, ist die einfache, barrierefreie und intuitive Gestaltung von Sicherheitsfunktionen in Geräten und Onlineanwendungen. Der US-Marktforscher Gartner [8] hat in einer Studie festgestellt, dass über 90 Prozent der Mitarbeiter, die während ihrer Arbeit unsichere Handlungen vornehmen, dies tun, obwohl sie wissen, dass ihre Handlungen das Risiko für das Unternehmen erhöhen. Damit sich die Akzeptanz entsprechender Bedienelemente erhöht, findet bei den Herstellern aktuell ein Umdenken statt: Beim Design sollen nicht mehr Technologie oder Bedrohungen im Zentrum stehen, sondern das Individuum. Der Anteil der Unternehmen, die Sicherheitstechnologien menschenzentriert entwickeln, werde bis 2027 auf 50 Prozent steigen.

Gleichzeitig wird auch das Thema Datenschutz immer relevanter – nicht nur aus Sicht der Betroffenen, deren Daten verarbeitet werden, sondern auch für Unternehmen. Gartner [8] empfiehlt internationalen Unternehmen, Datenschutzprogramme aufzulegen, die sich am umfassenden Datenschutzstandard der Europäischen Datenschutzgrundverordnung orientieren. Dadurch könnten sie sich in einem zunehmend wettbewerbsintensiven Markt differenzieren, Vertrauen bei den Kunden aufzubauen – und gleichzeitig Daten umfassender nutzen.

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 [7]. 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. Viele Lösungen zur Ausübung der Souveränität im digitalen Raum erreichen geltende Usability-Standards bislang nicht [11]. Häufige Ursachen dafür sind eine unzureichende Ausgestaltung von



This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Mensch und Computer 2024 – Workshopband, Gesellschaft für Informatik e.V., 01.-04. September 2024, Karlsruhe, Germany

© 2024 Copyright held by the owner/author(s). Publication rights licensed to GI.

<https://doi.org/10.18420/muc2024-mci-ws17-105>

Sicherheits- und Datenschutzmechanismen, die den Bedürfnissen, Fähigkeiten und Zielen der Nutzer:innen nicht gerecht werden. Die hohe und stetig steigende Komplexität informationstechnischer Systeme – auch bedingt durch deren Hyperkonnektivität – sorgt für immer neue Herausforderungen. 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 wird seit 2015 als MuC-Workshop durchgeführt. Ziel der zehnten Auflage ist es, dieses etablierte Forum, in dem sich Expert:innen aus Wissenschaft und Praxis zum Thema benutzerfreundlicher Technologien zur Gewährleistung der Informationssicherheit und Privatheit austauschen können, zu festigen und weiterzuentwickeln. Zugleich soll die Diskussion für ein breites Fachpublikum geöffnet werden.

Interessent:innen können Forschungs- und Entwicklungsarbeiten in deutscher oder englischer Sprache einreichen. Die akzeptierten Beiträge werden in Vorträgen vorgestellt und in der Digitalen Bibliothek der Gesellschaft für Informatik publiziert. Mögliche Beitragstypen sind

- neue Vorgehensweisen oder Werkzeuge,
- gestalterische Studien,
- Berichte praktischer Umsetzung,
- Systemdemonstrationen,
- praxiserprobte Methoden/Best Practices,
- kritische Reflexionen,
- Replikationsstudien,
- theoretische/zukunftsweisende Arbeiten,
- laufende Forschungs- und Entwicklungsprojekte sowie
- Betrachtungen besonderer Benutzergruppen und Anwendungsdomänen.

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

- neuartige Interaktionsformen und Benutzeroberflächen,
- konkrete UI-Gestaltung,
- Anwendungen/Erfahrungen aus der Praxis,
- Erfahrungen aus den ersten Jahren DSGVO sowie
- Security Awareness vs. Usable Security.

Die angenommenen Beiträge werden in Vorträgen vorgestellt und mit dem gesamten Auditorium diskutiert. Zudem wird wie in den vergangenen Jahren angeboten, die schriftlichen Einreichungen zu publizieren. Die Autor:innen arbeiten dafür das Feedback aus den Gutachten in die finale Versionen ein.

Neben Publikationen können für den 10. Usable Security und Privacy Workshop auch interaktive Beiträge eingereicht werden. Die Art des Beitrages ist relativ offen, soll sich aber deutlich von einem Vortrag unterscheiden. Denkbar sind kurze, moderierte Gruppenarbeitsphasen, aber auch Übungen mit neuartigen Werkzeugen. Die Vorschläge für interaktive Beiträge werden von den Workshoporganisatoren gesichtet, bewertet und dahingehend ausgewählt, dass möglichst abwechslungsreiche Interaktionsformate und unterschiedliche Themen bedient werden.

Das Ergebnis des Workshops ist eine dokumentierte Sammlung von neuen Entwicklungen und Forschungsergebnissen im Bereich Usable Security und Privacy in den Proceedings der "Mensch und Computer 2024" sowie – für den zweiten Teil – ein intensiver Wissensaustausch zwischen den Teilnehmer:innen auf Basis der Interaktion am Workshoptag, der ebenfalls in geeigneter Form dokumentiert wird.

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:

- Yasemin Acar (Universität Paderborn, DE)
- Florian Alt (Universität der Bundeswehr München, DE)
- Zinaida Benenson (FAU Erlangen-Nürnberg, DE)
- Florian Dehling (Hochschule Bonn-Rhein-Sieg, DE)
- Markus Dürmuth (Leibniz Universität Hannover, DE)
- Sascha Fahl (CISPA, DE)
- Peter Leo Gorski (infodas, DE)
- Timo Jakobi (Technische Hochschule Nürnberg, DE)
- Marc-André Kaufhold (TU Darmstadt, DE)
- Patrick Kühtreiber (Georg-August-Universität Göttingen, DE)
- David Langer (Hochschule Bonn-Rhein-Sieg, DE)
- Marian Margraf (FU Berlin, DE)
- Tilo Mentler (Hochschule Trier, DE)
- Sebastian Möller (TU Berlin, DE)
- Anna-Marie Orloff (Universität Bonn, DE)
- Christian Reuter (TU Darmstadt, DE)
- Angela Sasse (Ruhr Universität Bochum, DE)
- Vera Schmitt (TU Berlin, DE)
- Gunnar Stevens (Universität Siegen, DE)
- Jan Tolsdorf (George Washington University, US)
- Stephan Wiefeling (swiefeling.de & Vodafone, DE)

Mitglieder des Programmkomitees begutachten die eingereichten Beiträge in einem Double-Blind-Peer-Review-Verfahren. Jede Einreichung wird von zwei bis drei Gutachtern bewertet. Bewertungskriterien sind Relevanz, Originalität und wissenschaftliche Qualität des Beitrags, eine klare Beschreibung des Lösungsansatzes und Belege für dessen Nützlichkeit.

4 Wissenschaftliche und interaktive Beiträge

Von den eingereichten Beiträgen wurden sechs Arbeiten für das Programm des Workshops akzeptiert. Diese werden im Folgenden kurz vorgestellt. Die vollständigen Papiere sind im Workshopband der Mensch und Computer 2024 enthalten.

Im Beitrag "Usability and Understanding of Individual Verifiability in the 2023 GI-Election" [9] stellen Hilt et al. eine Online-Nutzerstudie zur individuellen Verifizierbarkeit vor, die mit einem Teil der Wählerschaft der Gesellschaft für Informatik e.V. durchgeführt wurde. Die Ergebnisse deuten auf ein unzureichendes Verständnis von Funktionsweise und Zweck entsprechender Mechanismen hin und werfen die Frage auf, wie dieses verbessert werden kann.

Drescher et al. decken in ihrer Arbeit "Data Protection Can Sometimes Be a Nuisance: A Notification Study on Data Sharing Practices in City Apps" [5] Datenschutzmängel bei städtischen

Apps auf: Über die Hälfte der Apps kommuniziert ohne Nutzereinwilligung mit Dritten außerhalb der EU. In ihrer Benachrichtigungsstudie beobachteten sie jedoch relativ hohe Behebungs- und Reaktionsraten der App-Anbieter.

Köpferl et al. stellen im Beitrag "Ich sehe das, was Du nicht siehst: Spuren einfacher Sensordaten im smarten Zuhause erleben und reflektieren" [10] ihren partizipativen Ansatz "Privacy by Co-Design" vor und präsentieren Ergebnisse einer Feldstudie. Die Arbeit soll einen Beitrag dazu leisten, dass Nutzende die Implikationen smarter Geräte besser verstehen und befähigt werden, informierte Entscheidungen zu treffen.

In "Towards Privacy-friendly Telepresence Robots for Schoolchildren with Long-term Illnesses: User Needs of Relevant User Groups" [4] diskutieren Büttner et al. Datenschutzanforderungen und -implikationen bei der Gestaltung von Telepräsenzrobotern für Schulkinder. Sie stellen Ergebnisse aus drei Workshops mit unterschiedlichen Nutzergruppen wie Kindern, Eltern, Pädagogen und Betreuungspersonal vor.

Im Beitrag "Pass auf! – Child-Oriented Cyber Safety & Security Educational Content" [2] gleichen Bopp et al. aktuelle Cyber-Risiken mit dem Stand der Forschung, offiziellen Empfehlungen und vorhandenem Lernmaterial ab. Dies soll ein erster Schritt sein, um Kindern, Eltern und Lehrer:innen kohärente, aktuelle und leicht verständliche Empfehlungen zu Online-Sicherheitsrisiken und passenden Abhilfemaßnahmen zu liefern.

Ballreich & Volkamer schildern in ihrem Beitrag die "Erstellung eines Erklärvideos zur Verwendung von S/MIME" [1] entsprechende Erfahrungen an einer deutschen Universität. Sie gehen auf die Grundlagen, die getroffenen Entwurfsentscheidungen, die Videoinhalte, den iterativen Entwicklungsprozess sowie die Evaluation des Videos ein.

Abgerundet wird das Programm durch zwei interaktive Beiträge: Im Kurzworkshop "Crafting Usable Security: Enhancing Public Understanding of Security and Privacy" identifizieren und priorisieren Mandy Balthasar, Nina Gerber und Timo Jakobi gemeinsam mit den Teilnehmern relevante Inhalte und Medien für die Bereitstellung nutzbarer Sicherheits- und Datenschutzmaterialien. Ziel ist es, das verfügbare Wissen zu Usable Security und Privacy für Nutzende besser zugänglich zu machen.

Zum Abschluss lädt die SECUSO Forschungsgruppe ins "KASTEL Engineering Secure Systems - HSF Lab". Hier erwarten die Teilnehmer:innen insgesamt sechs Stationen, die einerseits veranschaulichen, wie Forschung im Bereich Human Factors in Security und Privacy aussieht, und andererseits demonstrieren, welche Inhalte bereits in früheren Studien evaluiert wurden.

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*¹.

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 leitet die Abteilung »Security Engineering« am Fraunhofer IESE. In seiner Forschung beschäftigt er sich mit den Themen Datensouveränität, Datennutzungskontrolle, Datentreuehandmodelle sowie Usable Security und Privacy.

Andreas Heinemann ist Professor für IT-Sicherheit und Computernetzwerke am Fachbereich Informatik der Hochschule Darmstadt. Dort leitet er die Arbeitsgruppe *User-Centered Security*². Er ist Repräsentant der Hochschule Darmstadt im Board des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE³ und Mitglied im Vorstand des Competence Center for Applied Security Technology, CAST e.V.⁴.

Der Workshop wird in Zusammenarbeit mit dem GI Fachbereich Mensch-Computer-Interaktion, 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

Unser Dank gilt allen Autor:innen, die den Workshop mit ihren Einreichungen bereichern, sowie den Mitgliedern des Programmkomitees, 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] Fabian Lucas Ballreich and Melanie Volkamer. 2024. Erstellung eines Erklärvideos zur Verwendung von S/MIME (WIP). In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-152>
- [2] Karen Bopp, Andreas Heinemann, and Karen Renaud. 2024. Pass auf! - Child-Oriented Cyber Safety & Security Educational Content. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-163>
- [3] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2023. Die Lage der IT-Sicherheit in Deutschland 2023. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html>
- [4] Sebastian Thomas Büttner, Paul Neumann, Luca Hernández Acosta, Delphine Reinhardt, and Michael Prilla. 2024. Towards Privacy-friendly Telepresence Robots for Schoolchildren with Long-term Illnesses – User Needs of Relevant User Groups. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-162>
- [5] Jan Niklas Drescher, Jakob Moser, Nicolas Strangmann, Jonas Spinner, Dominik Herrmann, and Melanie Volkamer. 2024. Data Protection Can Sometimes Be a Nuisance: A Notification Study on Data Sharing Practices in City Apps. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-159>
- [6] European Union Agency for Cybersecurity. 2023. ENISA Threat Landscape 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [7] 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>
- [8] Gartner, Inc. 2023. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024. <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>
- [9] Tobias Hilt, Philipp Matheis, and Melanie Volkamer. 2024. Usability and Understanding of Individual Verifiability in the 2023 GI-Election. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-151>
- [10] Karola Köpferl, Tanja Lehmann, Andy Börner, Alexa Becker, Arne Berger, Andreas Bischof, and Albrecht Kurze. 2024. Ich sehe das, was Du nicht siehst: Spuren einfacher Sensordaten im smarten Zuhause erleben und reflektieren. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., Bonn. <https://doi.org/10.18420/muc2024-mci-ws17-153>
- [11] J. Tolsdorf, F. Dehling, and D. 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>

²<https://ucs.h-da.io>

³<https://www.athene-center.de>

⁴<https://www.cast-forum.de>

¹<https://das.h-brs.de>