5. Usable Security und Privacy Workshop

Luigi Lo Iacono
TH Köln
Köln, Germany
luigi.lo_iacono@th-koeln.de

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

Svenja Polst
Fraunhofer IESE
Kaiserslautern, Germany
svenja.polst@iese.fraunhofer.de

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

ZUSAMMENFASSUNG

In Fortführung zu den erfolgreichen „Usable Security und Privacy“ Workshops der vergangenen vier Jahre werden in einem fünften ganztätigen wissenschaftlichen Workshop auf der Mensch und Computer 2019 fünf aktuelle Arbeiten auf dem Gebiet Usable Security und Privacy in Kurzpräsentationen vorgestellt und diskutiert. Das Themenspektrum umfasst Beiträge aus Forschung und Praxis, die neue Ansätze, aber auch praxisrelevante Lösungen zur nutzerzentrierten Entwicklung und Ausgestaltung von digitalen Schutzmechanismen thematisieren. Mit dem Workshop wird ein etabliertes Forum fortgeführt und weiterentwickelt, in dem sich Experten aus unterschiedlichen Domänen, z. B. dem Usability- und Security-Engineering, transdisziplinär austauschen können.

SCHLAGWORTE

Usable Security, Usable Privacy

1 Motivation

Unser Leben hat sich durch die fortschreitende Entwicklung von Informations- und Kommunikationstechnologien entscheidend verändert. Kaum ein Produkt, eine Dienstleistung oder eine private wie berufliche Aktivität bleibt von der digitalen Transformation ausgenommen. Das hieraus hervorgegangene digitale Leben stellt viele neue und herausfordernde Anforderungen. Dem adäquaten Schutz digitaler Güter und Informationen kommt dabei ein besonders hoher Stellenwert zu. Dies liegt unter anderem an den erheblichen Erfassungs-, Kommunikations-, Verarbeitungs-, und Speicherkapazitäten digitaler Systeme, die immense Menge an Daten verwalten können. Das Verschwinden von Systemgrenzen durch die ubiquitäre Vernetzung über das Internet bzw. im Internet of Things verstärkt diese Kapazitäten zudem. Die Verfügbarkeit der Daten weckt nicht zuletzt Begehrlichkeiten, etwa zweckentkoppelte Verwertungen, die sowohl durch kommerzielle als auch kriminelle Beweggründe motiviert sein können.

Kritisch ist diese Verwendung von Daten gegen den Willen von Nutzern vor allem, wenn es sich dabei um personenbeziehbare Daten der Nutzer eines Systems handelt. Auf diese Weise kann die Privatsphäre der Nutzer massiv verletzt werden als auch finanzieller Schaden verursacht werden. Das Risiko der zweckfremden Verwendung kann durch den Einsatz von digitalen Sicherheitslösungen und privatheitsfördernden Technologien minimiert werden.

Digitale Mechanismen zum Schutz sensibler Daten sind allerdings nur dann effektiv, wenn sie von den Anwendern möglichst intuitiv verstanden und mit geringem Aufwand richtig eingesetzt werden können. Ein klassisches Beispiel für unzureichende Sicherheitslösungen sind die auch im Jahr 2019 noch fehlende Möglichkeit der leicht zugänglichen vertraulichen Ende-zu-Ende-E-Mail-Kommunikation für den Anwender.

Auch viele Lösungen zum Schutz der Privatsphäre erreichen geltende Usability-Standards nicht. Zum Beispiel erfordern Sprachassistenten, wie Amazons Alexa, den Wechsel zu einem anderen Interface, um Privatsphäreeinstellungen vornehmen zu können. Somit wird Nutzern mit geringem technischem Verständnis oder eingeschränkten Sehfähigkeiten der Zugang dazu erschwert.

Die Usability von sicherheits- bzw. privatheitsfördernden Verfahren ist somit eine Schlüsseleigenschaft, die die individuellen Anforderungen aller beteiligten Benutzergruppen sowohl in Entwicklungsprozessen als auch im produktiven Einsatz berücksichtigen muss.

Usable Security bezeichnet den inter- und transdisziplinären Ansatz, sicherheitsfördernde Verfahren für digitale Produkte und Dienstleistungen so auszugestalten, dass Benutzer bei ihren sicherheitsrelevanten Zielen und Vorhaben bestmöglich unterstützt werden. Hierdurch werden z. B. auch Laien und technikferne Anwender in die Lage versetzt, Sicherheitselemente und

MuC'19 Workshops, Hamburg, Deutschland

https://doi.org/10.18420/muc2019-ws-302

deren Notwendigkeit zumindest grundlegend zu verstehen und die Elemente in der dafür vorgesehenen Weise zu verwenden. Usable Privacy verfolgt äquivalente Ziele, fokussiert dabei auf Technologien zur Förderung der Privatheit in digitalen Systemen und Plattformen.

2 Ziele und Inhalte des Workshops

Ziel des 5. Usable Security und Privacy Workshops ist es, das etablierte Forum zu festigen und weiterzuentwickeln, in dem sich Experten aus Wissenschaft und Praxis zum Thema benutzerfreundlicher Technologien zur Gewährleistung der Informationssicherheit und Privatheit austauschen können. Zugleich soll durch den Workshop die Diskussion für ein breiteres Fachpublikum geöffnet werden. Ergebnis des Workshops ist eine dokumentierte Sammlung von neuen Entwicklungen und Forschungsergebnissen im Bereich Usable Security und Privacy.

Interessenten konnten Studien sowie Forschungs- und Entwicklungsarbeiten in deutscher oder englischer Sprache zu dem oben beschriebenen Themengebiet einreichen. Exemplarisch vorgegebene Themenfelder für wissenschaftliche oder praxisorientierte Beiträge beinhalteten:

- neue Vorgehensweisen oder Werkzeuge,
- gestalterische Studien, z. B. UI-Gestaltung, Persuasive Design,
- Berichte praktischer Umsetzung (erfolgreiche sowie fehlgeschlagene Beispiele),
- Systemdemonstrationen,
- praxiserprobte Methoden und Best Practices,
- kritische Reflexionen (Herausforderungen, Fallstricke),
- Replikationsstudien,
- theoretische/zukunftsweisende Arbeiten,
- laufende Forschungs- und Entwicklungsprojekte sowie
- Betrachtungen besonderer Benutzergruppen (z. B. Kinder, Senioren, Arbeitnehmer, Softwareentwickler, Administratoren).

3 Programmkomitee

Das Programmkomitee des Workshops übernahm die fachliche und inhaltliche Begutachtung der Einreichungen und unterstützte die Verbreitung des Call for Papers zum Workshop. Die Mitglieder des Programmkomitees sind anerkannte Experten auf dem Gebiet der Usable Security und Privacy aus Wissenschaft und Praxis:

- Yasemin Acar (Leibniz Universität Hannover, DE)
- Florian Alt (Universität der Bundeswehr München, DE)
- Mandy Balthasar (Universität der Bundeswehr München, DE)
- Jens Bender (BSI, DE)
- Zinaida Benenson (FAU Erlangen-Nürnberg, DE)
- Alexander De Luca (Google, CH)
- Markus Dürmuth (Ruhr-Universität Bochum, DE)
- Denis Feth (Fraunhofer IESE, DE)
- Nina Gerber (KIT, DE)
- Peter Gorski (TH Köln, DE)
- Marit Hansen (ULD Schleswig-Holstein, DE)
- Tobias Hirsch (TU Berlin, DE)
- Timo Jakobi (Universität Siegen, DE)
- Sebastian Möller (TU Berlin und DFKI Berlin, DE)
- Günter Müller (Universität Freiburg, DE)
- Delphine Reinhardt (Universität Göttingen, DE)
- Emanuel von Zezschwitz (Universität Bonn & Fraunhofer FKIE, DE)

Alle eingereichten Beiträge wurden durch die Mitglieder des Programmkomitees in einem Double-Blind-Peer-Review-Verfahren begutachtet. Jede Einreichung wurde von drei Gutachtern bewertet. Auswahlkriterien für die Annahme waren die Relevanz, Originalität und wissenschaftliche Qualität des Beitrags, eine klare Beschreibung des Lösungsansatzes und ein überzeugender Beleg für dessen Nützlichkeit.

4 Akzeptierte Einreichungen

Von den eingereichten Beiträgen wurden fünf Arbeiten für das Programm des Workshops akzeptiert, die im Folgenden kurz vorgestellt werden. Die vollständigen Papiere sind in den Tagungsbänden der Mensch und Computer 2019 enthalten.

Die Arbeiten „Mitigating Cryptographic Mistakes by Design“ und „Eigenschaften optimierter API-Dokumentationen im Entwicklungsprozess sicherer Software“ behandeln mit unterschiedlichen Ansätzen Herausforderungen, denen sich Entwickler bei der Erstellung sicherer Software stellen müssen. Die erste Arbeit von Blochberger et al. [1] schlägt eine einfach zu benutzende Krypto-API für die Programmiersprache *Swift* vor, deren Design unerfahrene Programmierer davor bewahren soll, häufige, aus der Literatur bekannte Programmierfehler zu begehen. Die zweite Arbeit von Huesmann et al. [2] geht der Frage nach, warum Entwickler im Entwicklungsprozess sicherer Software nicht vorrangig die offiziellen Herstellerdokumentation von Krypto-APIs im Alltagsgeschäft konsultieren, sondern stattdessen auf Internetquellen ausweichen, die wiederum potentiell unsichere Implementierungen vorschlagen. Mithilfe von Fokusgruppen wurden hier Eigenschaften erarbeitet, die eine optimale API-Dokumentation mit sich bringen sollte.

Die Arbeit von Fietkau und Balthasar mit dem Titel „Using Hash Visualization for Real-time User-governed Password Validation“ [3] schlägt ein Verfahren zur Visualisierung von Bit-Strings vor. Das mit MosaicHash benannte Verfahren ist in Anwendungsfällen verwendbar, in denen visuelle Repräsentationen von komplexen Zeichenketten vom Endnutzer verarbeitet werden müssen, z. B. beim Vergleich zweier Hashwerte. Die Autoren gehen speziell auf die Passworteingabe und die Validierung des maskierten Passworts durch MosaicHash ein. Es werden Empfehlungen gegeben und diskutiert, welche Aspekte bei der Verwendung in diesem Kontext zu berücksichtigen sind.

In der Arbeit „Usable Specification of Security and Privacy Demands" von Rudolph et al. [4] wird evaluiert, welche Spezifikationsparadigmen für Datenschutzeinstellungen zu welchen Benutzertypen passen. Es wurde in einem Pretest untersucht, mit welchem Spezifikationsparadigma ein bestimmter Nutzertyp die besten Ergebnisse hinsichtlich objektiver und wahrgenommener Korrektheit, Effizienz und Zufriedenheit erzielte. Die gegebenen Empfehlungen sollen in weiteren Studien validiert werden.

Der letzte Workshopbeitrag „Ein Kampf gegen Windmühlen: qualitative Studie über Informatikabsolvent_innen und ihre Datenprivatheit" von Schmidbauer-Wolf et al. [5] fokussiert auf Privacy. Die Autoren gehen mit dieser Arbeit der Frage nach, wie eigene private Daten geschützt werden können. Dazu wurde eine qualitative Studie mit sechs Informatikabsolventen durchgeführt. In semistrukturierten Interviews haben die Teilnehmer ein Bewusstsein für die Brisanz ihrer privaten Daten gezeigt. Erhebliche Unterschiede sind bei der Definition ebendieser „privater Daten", sowie beim Verhalten, um diese zu schützen, geäußert worden. Obwohl viele Zusammenhänge und angelehnte Fragestellungen offenbleiben, gibt die Arbeit die paradoxe Situation wieder, in der sich die Privatheit im digitalen Zeitalter aktuell befindet.

5 Organisation und Durchführung

Die Durchführung des Workshops erfolgt durch die vier folgenden Organisatoren:

- Luigi Lo Iacono (Technische Hochschule Köln),
- Hartmut Schmitt (HK Business Solutions GmbH),
- Svenja Polst (Fraunhofer IESE) und
- Andreas Heinemann (Hochschule Darmstadt)

in Zusammenarbeit mit der Fachgruppe E-Commerce und E-Government (FG ECOM) der Gesellschaft für Informatik, dem Arbeitskreis Usable Security & Security der German UPA und dem Projekt „TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen".

Danksagung

Die Organisatoren möchten nochmals allen Autoren danken, die den Workshop mit ihren Einreichungen bereichert haben. Außerdem gebührt den Mitgliedern des Programmkomitees ein herzlicher Dank, die die Einreichungen mit konstruktiven und ausführlichen Gutachten bewertet haben.

Diese Arbeit wurde unterstützt vom Bundesministerium für Bildung und Forschung (BMBF) im Projekt „TrUSD – Transparente und selbstbestimme Ausgestaltung der Datennutzug im Unternehmen" (FKZ: 16KIS0896K, 16KIS0897, 16KIS0898, 16KIS0899, 16KIS0900).

Literatur

[1] Maximilian Blochberger, Tom Petersen, and Hannes Federrath. Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy. Mitigating Cryptographic Mistakes by Design. In Proceedings of (MuC'19 Workshops). ACM, New York, NY, USA. https://doi.org/10.18420/ muc2019-ws-302-02

[2] Rolf Huesmann, Alexander Zeier, and Andreas Heinemann. Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy. Eigenschaften optimierter API-Dokumentationen im Entwicklungsprozess sicherer Software. In Proceedings of (MuC'19 Workshops). ACM, New York, NY, USA. https://doi.org/10.18420/muc2019-ws-302-03

[3] Julian Fietkau and Mandy Balthasar. Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy. Using hash visualization for real-time user-governed password validation. In Proceedings of (MuC'19 Workshops). ACM, New York, NY, USA. https://doi.org/10.18420/muc2019-ws-302-04

[4] Manuel Rudolph, Svenja Polst, and Denis Feth. Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy. Usable Specification of Security and Privacy Demands: Matching User Types to Specification Paradigms. In Proceedings of (MuC'19 Workshops). ACM, New York, NY, USA. https://doi.org/10.18420/muc2019-ws-302-05

[5] Gina Maria Schmidbauer-Wolf, Franziska Herbert, and Christian Reuter. Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy. Ein Kampf gegen Windmühlen: Qualitative Studie über Informatikabsolvent_innen und ihre Datenprivatheit. In Proceedings of (MuC'19 Workshops). ACM, New York, NY, USA. https://doi.org/10.18420/muc2019-ws-302-06