WASP Software Engineering assignment

Piero Romare

August 2023

My educational background: Bachelor's degree in Cognitive Psychology, Master's degree in Data Science, and experiences in cybersecurity and human-computer interaction research groups. I'm currently a PhD student at Chalmers University, department of Computer Science and Engineering, unit of information security.

1 My Research: Usable Privacy and Security

My project's primary objective is to develop user-friendly permission settings for IoT automation applications that respect users' privacy choices while ensuring security. We aim to employ a human-centered design methodology to conduct user research and gather data on users' privacy expectations and concerns to inform the creation of a usable permission management system. This research wants to support the permission settings for IoT automation applications with the purpose of being GDPR compliant.

The context is the Trigger-Action application platforms where the users can set the rules that indicate when specific connected activities will be performed. These rules follow the if-else statement and can broadly be defined as "IF This Then That" (IFTTT) or Event-Condition-Action (ECA). The applications can be employed in the IoT between at least two connected entities that can be devices and/or services. The connection between the two entities exists through the Trigger-Action Platforms (TAPs) (e,g., IFTTT, Microsoft Power Automate, Zapier) that host the applications.

We will adopt a mixed-methods approach comprising qualitative data such as interviews, focus groups, and usability testing. We will also use quantitative data such as surveys and behavioural data to segment users' privacy profiles based on behaviour patterns and preferences. We will use machine learning techniques to analyze and predict users' privacy preferences to support privacy-enhancing decisions in the permission management system of TAPs.

We will integrate GDPR principles such as privacy by design and data minimization to ensure compliance with GDPR regulations. To achieve the project's objectives, we will engage end-users throughout the design process to ensure that the final product is user-friendly, legally compliant, and effective in addressing security and privacy end-users' concerns. The development of the UI prototypes for on-the-fly permission management and informed consent will also be enforced for accessibility and transparency by informing and explaining data collection purposes and the consequences of adopting/revoking permissions.

To summarize, the main contributions of my PhD journey:

1. exploratory work on TAPs [1] and literature review on traditional IoT and comparison with IoT TAPs (dealing with the reviews);
2. survey / questionnaire and privacy profiles segmentation (study(ies) design phase);
3. implementation and evaluation of the interface and the protocols for the "on-the-fly" usable permission management GDPR compliant.

2 Robert's lectures

In this section the discussion is about the intersection and which topics of this course may be used during these years of PhD.
The software testing during the verification and validation can be done using *static techniques* such as code inspections and analysis with a human as reviewer and *dynamic techniques* that require executable artefacts as been discussed during the second lecture. In my first work in Chalmers - RQ: what are the privacy preferences and concerns that play a role in the usage of IoT TAP? - the thematic analysis after the focus groups include the trust theme and the certifications as a particular code that somehow can be related to the software testing. The end-users (i.e., our FGs' participants), since the complexity of the IoT systems and different level and field of education, ask for assurance and certainty of use and safety through certifications for instance. The software testing techniques in question do not constitute certifications, but rather represent a set of methodologies employed to ascertain the quality, reliability of software products. Even so, it would be linked to the usable privacy needs that might be achieved during those testing, since they can be automatically communicated to the authorities and mostly to the users, in a understandable way (i.e. through nudges), to improve the trust on their digital environments.

A second topic is about the *cognitive biases and heuristics*. I believe that the cognitive heuristics and biases are the human's side and covert channels. Both involve often unnoticed pathways or in other words unusual behaviour, potentially

leading to security breaches or errors in judgment. Closely, social engineering attacks like phishing and all those kind of scams are associated to side channels because the ”sender” can be identified as the innocent party who is unaware of the impending attack, ~~while the ”receiver” is the individual who is perpetrating~~[1]. Indeed, the list of the cognitive biases in case of replying to the phishing email is huge: authority bias, urgency, social compliance, scarcity and so on. I may have made too strong assumption / parallelism in this paragraph, but I've planned to work on cognitive biases and heuristics related to IoT wearables to investigate easier usage of them, with the human natural shortcuts, or detect potential vulnerabilities due to human involuntary mistakes.

3 Linda's lectures

In her lecture, Linda discussed about SPACE framework and DevBots. In the *SPACE framework* it's clear that the developer productivity cannot be reduced to a single dimension and the importance of communication and collaboration. In usable privacy involves not only complying with GDPR regulations but also considering user perceptions, preferences, concerns, expectations in the context of IoT devices. Many experts should interact such as computer scientists, lawyers, data protection officers, designers, and psychologist among the other.

4 List of topics

The topics *human factors (e.g. what human needs, prefers, expects), HCI (e.g. how human can use technologies in a pleasant way), security and privacy (e.g., how technically preserve human integrity) and regulations and compliance (e.g., what are the requirements that law asks)* are a big part of my research as can be noticed in Sec 1. From explainable AI to industry 5.0, recently the end-users have been started to be considered even more in the technology development. There is an increasing recognition of the fact that technology ought to be in line with the requirements and principles of the people it caters to is being reflected, in other words, the ”human-centered approach”. As afromentioned in 2, my first work in Chalmers was an exploratory study on human concerns and preferences on IoT privacy, as it is the second and will be the third ones. The fourth one will be more related to the design of an usable permission management system [5], where we will use usability testing [4], and to the GDPR for the on-the-fly permissions settings. We will leave the possibilities (we would encourage an active participation) to the

[1] https://caslab.csl.yale.edu/tutorials/acaces2019/acaces2019_proc_arch_sec_part-2.pdf

users if they want to change their privacy settings at times when they anyhow need to ask for possible revising their privacy settings, since the current context make the personal data involved sensitive and thus explicit consent by the user is needed. For example, the users were granted authorization settings to employ their location information. However, from the present location, it was inferred that the individual frequents an abortion clinic. Consequently, the location data has become part of the special categories of data. According to the GDPR, explicit consent must be obtained. In this scenario, if the individual opts to withdraw their permission, they should also be requested whether they would like to withdraw their permission in general. This is particularly relevant if the ML privacy assistant has identified that this coincides with the individual's privacy segment derived from the third study.

The notion of explainable AI has the potential to be implemented within the realm of privacy configurations. Create AI models with the ability to articulate to users in comprehensible language the rationale behind certain data access requests, the feasible repercussions of such requests, and the alternatives available to them. Recently, a direction is machine UNlearning [2] that has a strong link with the GDPR article 17 "Right to be forgotten" [3]. Here, the mechanisms facilitate AI/ML models in deleting particular data points or features upon request from the user or in accordance with data privacy regulations. This techniques could be useful also in terms of retention time, even if in the GDPR there is just the "guideline" in art. 5; "only data can be retained for as long as it is needed for the stated purpose". In consideration of the contextual circumstances and specific characteristics of the user data, it may be necessary for models to selectively delete certain elements while preserving others.

5 Future trends

In general, I believe that one of the first metrics to consider when a new technological tool is launched on the market should be effectiveness instead of efficiency. In terms of AI and ML, for example, we can train a model on data that are not updated. This would make the model already outdated and without real effectiveness, while it could have good accuracy. We need to discover novel approaches to guarantee that the advantages of technological progress are within reach and substantial for a wider range of individuals in society, as opposed to being limited to only a privileged few who have access to the latest data.

We should be more careful in terms of security, safety and privacy - I may be biased on this. Before a new food product or a drug would be reachable by people it is tested and validated, several times. Nowadays, we are not properly considering the consequences, especially for mental health that is still stigmatized in many

societies, when a tech tool is inserted on the market. The addictive nature of some apps and the constant connectivity promoted by smartphones are examples of issues that warrant careful consideration and we shouldn't make the same errors with IoT and future devices and services (i.e., visors) when we distribute them to the large population.

References

[1] Romare, P., Morel, V., Karegar, F., & Fischer-Hübner, S.. (2023). Tapping into Privacy: A Study of User Preferences and Concerns on Trigger-Action Platforms. https://doi.org/10.48550/arXiv.2308.06148 1

[2] Qu, Y., Yuan, X., Ding, M., Ni, W., Rakotoarivelo, T., & Smith, D.. (2023). Learn to Unlearn: A Survey on Machine Unlearning. https://doi.org/10.48550/arXiv.2305.07512 4

[3] Zhang, D., Finckenberg-Broman, P., Hoang, T., Pan, S., Xing, Z., Staples, M., & Xu, X.. (2023). Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions. https://doi.org/10.48550/arXiv.2307.03941 4

[4] Veale, Michael and Binns, Reuben and Van Kleek, Max, Some HCI Priorities for GDPR-Compliant Machine Learning (2018). Paper presented at The General Data Protection Regulation: An Opportunity for the CHI Community? (CHI-GDPR 2018), Workshop at ACM CHI'18 4

[5] B Liu, MS Andersen, F Schaub, H Al- muhimedi, SA Zhang, N Sadeh, Y Agarwal, and A Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In Symp. on Usable Privacy and Security (SOUPS), 2016 4