Analysing Privacy Conflicts in Web-Based Systems

Peter Inglis
School of Computer Science
University of Glasgow
Email: peter.inglis@glasgow.ac.uk

Inah Omoronyia
School of Computer Science
University of Glasgow
Email: inah.omoronyia@glasgow.ac.uk

***Abstract*—Data protection Impact Assessments (DPIA) are used to assess how well a series of design choices safeguard the privacy concerns of data subjects, but they don't address how to analyse privacy conflicts. The challenge with current work on privacy conflict is the necessity to understand the perceived levels of sensitivity to facilitate negotiations. It is unclear how this can be achieved in DPIA procedure. In this work we introduce our model checking tool along with our method to address privacy conflict. We present our evaluation plan before concluding with our research roadmap.**

I. Problem Statement

Several web services use consent elicitation modules to authorise the dissemination of information between 1st and 3rd parties when data subjects visit 1st parties online. Data Protection Impact Assessments (DPIAs) are used to evaluate the effectiveness of such approaches against perceived privacy risks [1] [2]. However, the implementation of different consent modules between independent web services may generate conflicting consent options involving data subjects and 3rd parties. It is unclear whether DPIA procedure can be used to resolve such conflict between subjects and web services owed largely to the disconnect between run-time and design time analysis of software systems.

In this work we propose an approach to represent privacy conflict with an awareness model early during design, the benefit of which is two-fold. Firstly, it allows stakeholders to unambiguously represent the mutually exclusive needs of data subjects and web services that may interact on a system model. Secondly it allows stakeholders to directly relate the privacy management features of a software system to the satisfaction of privacy requirements computationally. In this manner, insights on the effectiveness of privacy management features at run-time can be gained at design time. This in turn allows stakeholders to evaluate the suitability of a given system implementation wrt a series of computational privacy needs between data subjects and web services. The intended stakeholders of the tool are Data Protection Officers (DPOs). It is envisioned that our technique can support DPOs in evaluating the privacy management features of a web service they are responsible for.

II. Related Work

Privacy conflict analysis is commonly discussed in multi-agent negotiation scenarios [3][4]. In such approaches the aim is to have software agents evaluate proposed concessions to their local privacy requirements through a cost/benefit utility function [5] [6]. The challenge with negotiation techniques is the requirement to understand how individual agents perceive the information sensitivity of the information that informs their privacy requirements. When enacting DPIA on a software design early in the development lifecycle of an artefact, it will be challenging to make meaningful inferences on information sensitivity levels, making the application of negotiation approaches difficult.

III. Methodology

Our methodology is as follows. Firstly, we elicit an information flow network where an information flow is defined as a series of dissemination actions between two online entities. Once we have identified an information flow network, we input this representation into our model checker and identify a series of design alternatives. A design alternative is defined as an enumerated path of sequential interactions between multiple entities for the purpose of disseminating user information. Finally, we perform privacy conflict analysis on the design alternatives to support DPOs as a decision support tool. We assume that the client is controlled by a data subject who is someone who can be identified (directly or indirectly) by web services they interact with.

We prepared an arbitrary search query q =*"beats headphone reviews"* for the purpose of eliciting a collection of first parties from the Google search engine. We selected the top 3 results when executing q. These were (1) https://bit.ly/2NnFigh (domain =techradar), (2) https://bit.ly/2NilDhU (domain = whathifi) and (3) https://bit.ly/3fa9XZN (domain = pocket-lint). Next, to identify 3rd parties, we reviewed the consent modules provided by each 1st party to data subjects. We elicited a network of three 1st parties and 46 unique 3rd parties. The network contained 86 edges with 57% of 3rd parties connected to more than one 1st party. We validated this network by cross referencing the elicited 3rd parties with Lightbeam [7] to prune all entities that are excluded in communications. Next, we cross referenced the list generated from step 1 with an external database of known 3rd party tracking domains to prune 3rd parties that perform benign functions. Conflict arises when the subject specifies their privacy requirements on two different 1st parties in a manner that is mutually exclusive when combined by the 3rd party. Furthermore, in an interdependent setting, consent toggles may be offered independently by either the 1st party, 3rd party or both thereby increasing the potential for privacy conflicts.

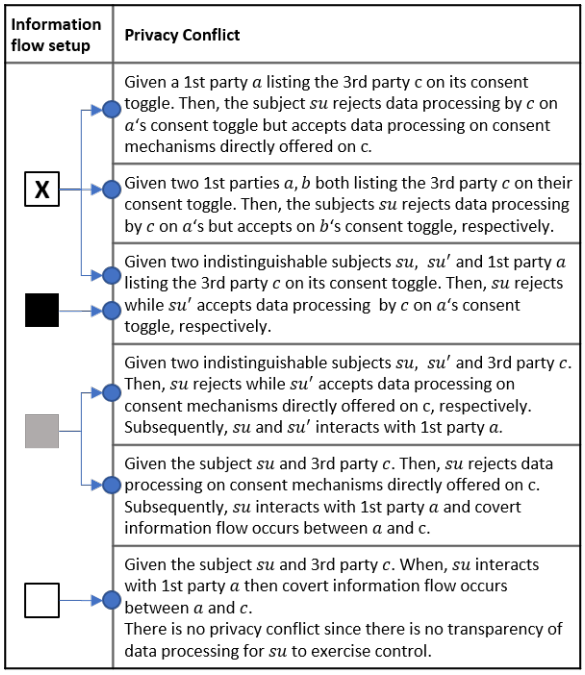

Fig. 1: Mapping information flow setup in web based interaction to privacy conflicts.

We articulate 6 different privacy conflict patterns in this work which are illustrated in figure 1.

Each icon in column 1 represents an instrumentation of a 1st party consent module. Each of these instrumentations are mapped to specific privacy conflict patterns that indicate how conflicts can arise at run-time when data subjects interact with the inter-dependant consent toggles. Each pattern in turn can be mapped to a formalism which is supported by an awareness logic, allowing for a network model to be analysed computationally to determine whether conflicts manifest. The challenge is whether such privacy conflicts can be identified and mitigated during DPIA. Assuming the DPO can identify 3rd parties that the 1st party needs to interact with to achieve such goals; Then at design time, sets of design alternatives can be compared. Each alternative contains information flows between the 1st and 3rd parties that, when executed achieves a business goal. The outcome of such comparisons can be used to identify design configurations that minimises privacy conflict and maximises the satisfaction of the business goal.

IV. Evaluation Roadmap

The intended use case for this work is illustrated in the method plan for our evaluation. A requirements analyst will firstly elicit an information flow network by crawling the results of the Google API with a structured query q. The output of executing q will be a list of distinct 1st parties FP such that $|FP|$ can be specified by the analyst. The analyst will iterate over each first party to generate an information flow network G such that each 3rd party node within G can be verified as a tracker. The evaluation will involve systematically investigating the privacy conflict patterns specified in column 2 of figure 1 on the elicited information network G. We instantiate the network encapsulating the privacy requirements of actors before executing information flows between the different actors on the network. The objective is to identify design alternatives from the elicited network model where privacy conflicts do not occur. Such information flows represent a possible instrumentation of consent modules that do not result in identifiable conflict patterns as per figure 1. We then look to identify the design alternatives such that conflict occurs. In such instances we apply our approach to conflict resolution which investigates the different methods by which consent may be managed by the 1st and 3rd parties involved. In this approach there are three possible outcomes. (1) The subject is given control over how to resolve the conflict. (2) The resolution decision is up to the 1st party. (3) The resolution decision is up to the 3rd party after being informed of the conflict from the 1st party. We aim to benchmark such analysis by investigating time complexity associated with non-trivial sizes of G.

V. Discussion and Future Efforts

We position this work to be of benefit to the requirements engineering process by allowing DPOs and other requirements analyst stakeholders to evaluate the privacy preserving capabilities of 1st party web services that operate interdependently with 3rd parties. This in turn allows us to inform both the conceptualisation and development of solutions. Future work on this project will involve determining whether we can effectively augment the conflict resolution process with perceivable information sensitivity values as currently such information is omitted in the analysis. Further, in previous work we have illustrated that design alternative state-spaces associated with complete artefacts from other technical domains can be restrictive. Therefore, we will look to improve our approach when working with less flexible solution spaces.

References

[1] T. Bisztray and N. Gruschka, "Privacy impact assessment: Comparing methodologies with a focus on practicality," in *Secure IT Systems*, A. Askarov, R. R. Hansen, and W. Rafnsson, Eds. Cham: Springer International Publishing, 2019, pp. 3–19.

[2] J. M. Such and M. Rovatsos, "Privacy policy negotiation in social media," *ACM Trans. Auton. Adapt. Syst.*, vol. 11, no. 1, Feb. 2016. [Online]. Available: https://doi.org/10.1145/2821512

[3] J. M. Such and N. Criado, "Multiparty privacy in social media," *Communications of the ACM*, vol. 61, no. 8, pp. 74–81, 2018.

[4] D. Keküllüoğlu, N. Kökciyan, and P. Yolum, "Strategies for privacy negotiation in online social networks," in *Proceedings of the 1st International Workshop on AI for Privacy and Security*, ser. PrAISe '16. New York, NY, USA: Association for Computing Machinery, 2016. [Online]. Available: https://doi.org/10.1145/2970030.2970035

[5] M. Jozani, E. Ayaburi, M. Ko, and K.-K. R. Choo, "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," *Computers in Human Behavior*, vol. 107, p. 106260, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563220300169

[6] K. Plangger and M. Montecchi, "Thinking beyond privacy calculus: Investigating reactions to customer surveillance," *Journal of Interactive Marketing*, vol. 50, pp. 32–44, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1094996819301124

[7] T. Mandl, W. Thode, and J. Griesbaum, ""i would have never allowed it": User perception of third-party tracking and implications for display advertising," 05 2015.