Fair Context-Aware Privacy Threat Modelling

Saswat Das*
*National Institute of Science Education and Research,
An OCC of Homi Bhabha National Institute, India*

Rakshit Naidu*
Carnegie Mellon University

Abstract

Given the progressive nature of the world today, fairness is a very important social aspect in various areas, and it has long been studied with the advent of technology. To the best of our knowledge, methods of quantifying fairness errors and fairness in privacy threat models have been absent. To this end, in this short paper, we examine notions of fairness in privacy threat modelling due to different causes of privacy threats within a particular situation/context and that across contexts.

1 Introduction

Fairness and Privacy Threat Modelling (PTM) have long been studied in isolation. The reader is referred to these works [3,6] and [4, 5] respectively.

Privacy threat modelling involves thinking of mitigation strategies and solutions against privacy threats in various contexts. For example, let us consider the privacy threat as the loss of the secret password of the victim. This incident would have different implications if the victim's password was lost within an office setting than that in a park/café with public WiFi. That is, it is more obvious for the victim to lose his password in public scenarios due to shoulder surfing than in private, work or office settings. Hence, we believe it is also important

---

*Equal Contribution

to fairly consider contexts in which the privacy threat occurs and assign probabilities to each cause that affects the threat fairly, based on the context in which the threat occurs. In this work, we formally define notions of fairness for context-aware privacy threat modelling.

We consider privacy threats in various situations/contexts given a set of possible causes, based upon which the outcomes may vary[†]. In a privacy threat model, the causes can be weighted in terms of how likely they are to lead to a given outcome. Given a set of causes from a universe of possible causes and a context, we have a particular outcome, which is the real-word privacy threat we are modelling for.

It is possible that in a particular context, we may have a particular cause being given more weightage than it should be, owing to either suboptimal formulation of the context's conditions with respect to the set of all possible causes or the contribution of certain causes to the privacy risk may have been diminished or exaggerated [1]. Therefore, to perform fair privacy threat modelling, methods to quantify fairness errors owing to these factors would be beneficial, and we provide formal definitions in section 2.

2 Formal Definitions

Suppose we want to study a privacy threat model in a context X from a set of contexts $\mathcal{C}$ using causes from a universe of all possible causes χ that affect that particular privacy threat. Then a threat model within a particular context X can be seen as an assignment of probabilities to different causes in χ according to their contribution to the resulting outcome O within that context.

More precisely, given χ and X, we can assign a probability

[†]Hence, we consider a set of contexts that is separate from the set of all outcomes; this allows us to study contexts based on different universes of possible causes. The reason for this will become apparent in section 2.
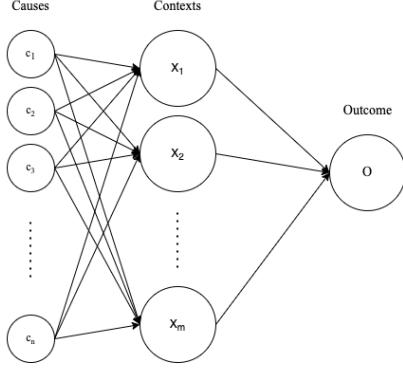
Figure 1: The set of all causes ($\{c_1, c_2, \cdots, c_n\} \subseteq \chi$) and the set of contexts ($\{X_1, X_2, \cdots, X_m\} \subseteq C$) for a particular privacy threat outcome (O).

$p_c^\chi := \Pr[O|X, c, \chi]$ for every cause $c \in \chi$, yielding the probability vector $(p_c^\chi)_{c \in \chi}$.

Now unfairness can arise in these models with respect to each cause and across various contexts; we thus provide a way to mathematically quantify these fairness errors.

Definition 2.1. *Fairness Error due to a Cause $c \in \chi$*
The fairness error due to a cause $c \in \chi$, for an outcome O amd for every $X \in C$, can be defined as

$$\mathcal{E}_{(\chi \setminus \{c\})} \stackrel{\Delta}{=} \sum_{X \in C} \sum_{c' \in \chi \setminus \{c\}} \left| \Pr[O|X, c', \chi] - \Pr[O|X, c', \chi \setminus \{c\}] \right|.$$

Here the fairness error for a cause $c \in \chi$ is given by the sum over all contexts $X \in C$ of the ℓ_1 norm distance between the probability vectors with the entry corresponding to c omitted.

Definition 2.2. *Fairness Error due to a Context $X \in C$*
For an outcome O and each context $X \in C$, we define the fairness error for a context $X \in C$ as

$$\mathcal{E}_X \stackrel{\Delta}{=} \sum_{c \in \chi} \sum_{c' \in \chi \setminus \{c\}} \left| \Pr[O|X, c', \chi] - \Pr[O|X, c', \chi \setminus \{c\}] \right|.$$

That is, here the fairness error for the context X is the sum over all $c \in \chi$ of ℓ_1 norm distances between the probability vectors with only those entries *not corresponding to c* of the probability vectors with respect to the set of causes being χ and $\chi \setminus \{c\}$ respectively.

2.1 Notions of Fairness for Threat Models

The aforementioned errors can serve as quantities to study and rank causes and contexts based on fairness, and can serve as a starting point for trying to mitigate substantial fairness errors with respect to a defined threshold, if any. In this vein, it would also help to define a way to quantify fairness error bounds.

Definition 2.3. λ-*Causal Fairness*
Given a universe χ of all possible causes, and a set C of all possible contexts within which privacy threats may occur, a privacy threat model is said to be λ-causally fair (for $\lambda \geq 0$) if $\sup_{c \in \chi} \mathcal{E}_{\chi \setminus \{c\}} \leq \lambda$.[‡]

Definition 2.4. γ-*Contextual Fairness*
Given a universe χ of all possible causes, and a set C of all possible contexts within which privacy threats may occur, a privacy threat model is said to be γ-contextually fair (for $\gamma \geq 0$) if $\sup_{X \in C} \mathcal{E}_X \leq \gamma$.

3 Discussion

Based on the causal and contextual error bounds for a certain cause or context respectively, a diagnosis of the unfairness incurred can be done, and subsequent steps for mitigation of the same can be taken. If the causal fairness error bound is substantially high, then one can look at the fairness error due to various causes individually and try to make changes to the most unfair causes in χ or add/subtract causes from χ to reduce this error. Similarly, one can improve the contextual fairness error bound on C.

4 Conclusion and Future Directions

We have thus attempted to provide certain methods of quantifying the fairness errors present in privacy threat models and some notions of fairness in that regard. This is but the first step in studying the fairness of privacy threat modelling. Some further directions to extend this can include deducing further mathematical properties based on the provided definitions, or designing diagnosis and mitigation strategies based on these concepts/notions. This can overall make for better and more reasonable threat modelling across various contexts. FAIR [2] provides a way to quantify privacy risk as *(threat_frequency * harm_magnitude)*. We believe our work can also influence the FAIR framework making threat modelling more context-aware by quantifying privacy risk as *[(threat_frequency * harm_magnitude) | context]*.

[‡]Here sup refers to the supremum/least upper bound of the set of values obtained in question.

References

[1] Suchitra Abel, Yenchih Tang, Jake Singh, and Ethan Paek. Applications of Causal Modeling in Cybersecurity : An Exploratory Approach. *Advances in Science, Technology and Engineering Systems Journal*, 5(3):380–387, 2020.

[2] R. Jason Cronk and Stuart S. Shapiro. Quantitative privacy risk analysis. In *2021 IEEE European Symposium on Security and Privacy Workshops*, pages 340–350, 2021.

[3] Sorelle A. Friedler, Carlos Eduardo Scheidegger, and Suresh Venkatasubramanian. The (im)possibility of fairness. *Communications of the ACM*, 64:136 – 143, 2021.

[4] Ali Gholami, Anna-Sara Lind, Jane Reichel, Jan-Eric Litton, Åke Edlund, and Erwin Laure. Privacy threat modeling for emerging biobankclouds. In *EUSPN/ICTH*, 2014.

[5] Shafiq Hussain, Asif Kamal, Shabir Ahmad, Ghulam Rasool, and Sajid Iqbal. Threat modelling methodologies: A survey. 2014.

[6] Abigail Z. Jacobs and Hanna M. Wallach. Measurement and fairness. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 2021.