Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations

Naipeng Dong
FSTC, University of Luxembourg
naipeng.dong@uni.lu

Hugo Jonker
FSTC, University of Luxembourg
hugo.jonker@uni.lu

Jun Pang
FSTC, University of Luxembourg
jun.pang@uni.lu

Classical data privacy assumes that users want to keep their privacy. However, a user may want to reveal information to the adversary due to bribery or coercion. Systems providing electronic services need to protect against such threats. Ddomain-specific formalisations of privacy properties against bribery and coercion were proposed in the literature e.g., receipt-freeness and coercion-resistance in voting, e-auction and e-health. In order to address these privacy concerns domain-independently, we propose a generic notion of *enforced privacy*: a user's privacy is preserved even if the user collaborates with the adversary.

The notions of data privacy and enforced privacy focus on a target user and ignore the impact that other users can have on his privacy. However, a third party may help the adversary break privacy of the target user (*collaboration*), e.g., revealing his vote may enable the adversary to deduce another voter's vote. To capture this negative influence of third parties, domain-specific notions were proposed in e-health and e-voting. We generalise these properties as *independency of privacy*: the help of a set of third parties does not enable the adversary to break a target user's privacy. On the other hand, a third party may help the target user to maintain his privacy (*coalition*), e.g., a non-coerced voter (who happens to vote as the adversary desires) can swap receipts with a coerced voter, providing the coerced voter "proof" of compliance while being free to vote as he pleases. This positive influence of third parties has not been well studied. To capture privacy in this situation, we propose the notion of *coalition privacy*: a target user's privacy is preserved with the help of a set of third parties sharing information with the target user. In particular, we use this notion to also capture the situation where third parties are involved but no information is shared between the target user and third parties, i.e., the mere *existence* of the third parties can help to create a situation where privacy is preserved.

Notions. We distinguish between two classes of privacy-affecting behaviour: the target user (collaborating with the adversary or not), and the behaviour of third parties (*neutral*, collaborating with the adversary (*attacking*), or collaborating with the target user (*defending*) – thus we also consider the situation where some are attacking, some others are defending and the rest are neutral). This gives rise to eight privacy properties with respect to Dolev-Yao adversary (see Tab. I). These properties hold if the adversary cannot link the target user to his data:

Table I
PRIVACY NOTIONS

target user collaborates with adversary	**third parties**			
	all neutral	*some attacking*	*some defending*	*some defending some attacking*
no	priv	ipriv	cpriv	cipriv
yes	epriv	iepriv	cepriv	ciepriv

1) data-privacy (priv): when the target user is honest.
   E.g., the adversary cannot link the contents of an encrypted email to the user.
2) enforced-privacy (epriv): when the target user seems to collaborate with the adversary.
   E.g., a voter should not be able to prove to a vote-buyer how he voted.
3) independency-of-privacy (ipriv): when (some) third parties collaborate with the adversary.
   E.g., in e-health the adversary cannot link a doctor to his prescriptions, despite the help of a pharmacist.
4) independency-of-enforced-privacy (iepriv): even when the target user seems to, and some third parties actually do collaborate with the adversary.
   E.g., the adversary should not be able to link a doctor to his prescriptions (to prevent bribes), even when both the pharmacist and the doctor are helping him.
5) coalition-privacy (cpriv): when (some) third parties collaborate with the target user.
   E.g., in location-based services, the user's real location is hidden amongst the locations of the helping users.
6) coalition-enforced-privacy (cepriv): even when the target user seemingly collaborates with the adversary, provided (some) third parties help to defend the user.
   E.g., in anonymous routing, a sender remains anonymous if he synchronises with a group of senders, even if he seems to collaborate.
7) coalition-independency-of-privacy (cipriv): even when some (attacking) third parties collaborate with the adversary, provided some other (defending) third parties collaborate with the target user.
   E.g., the adversary cannot link an RFID chip to its identity, even though some malicious readers are helping the adversary, provided other RFID tags behave

exactly as the target one.

8) coalition-independency-of-enforced-privacy (ciepriv): even when the target user seems to, and some third parties actually do collaborate with the adversary, provided that other third parties work to defend the target user.
   E.g., in electronic road pricing, other users may hide a user's route from the adversary, even if the user seems to collaborate and malicious routers relay information on passing cars to the adversary.

The examples above illustrate that similar privacy concerns arise in many different domains – e-voting, e-health, location-based services, RFID, electronic road pricing, etc. So far, attempts at formalising privacy have usually been domain-specific. We advocate a domain-independent approach to privacy, and develop a formal framework to achieve this.

Formalisations. Inspired by the frameworks in the applied pi calculus by Arapinis et al. and Delaune et al., our framework allows us to give domain-independent formalisations of all of the identified (enforced) privacy notions. We define a standard form of protocols which is able to represent any protocol. To formally define enforced privacy properties and independency of privacy properties, we model *collaboration* between users and the adversary. A collaboration specifies a set of terms sent to the adversary Ψ, a set of terms replaced by the adversary Φ, a channel from a collaborating user to the adversary c_{out} and a channel from the adversary to the user c_{in}. A collaboration of a user process R is denoted as $R^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}$ which is defined in a similar way as coercion in voting. This formalisation allows us to specify which information is shared (Ψ, Φ) and how it is shared. Thus, our framework provides the necessary flexibility for modelling various types of collaboration. Bribery and coercion can be considered as collaboration between the target user and the adversary, and their formalisations as proposed by Delaune et al. are essentially instances of our collaboration specification. To model coalition privacy properties, we propose the notion of *coalition* in our framework to formally capture the behaviour and shared information among a target user and a set of defending third parties. Coalition is formalised as an extension of collaboration. A coalition specifies a set of communications Θ. In addition, we allow a coalition to specify a set of substitutions Δ and a set of assignments for conditional evaluations Π. A coalition of a set of users R (denoted as $R^{\langle \Theta, \Delta, \Pi \rangle}$) is defined similarly to collaboration.

In our framework, the foundational property priv, is formalised in a classical way as strong secrecy: equivalence of two processes where a variable is instantiated differently, $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}]$. Based on this property, we formalise epriv, ipriv and their combination iepriv by counting for collaboration. epriv is defined similar to coercion-resistance in voting. ipriv adds third parties collaboration $R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}$ to the priv equivalence: $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}] \approx_\ell C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}]$. iepriv combines the formalisations of epriv and iepriv. Using the formalisation of coalition, four corresponding coalition privacy properties are formalised. cpriv is formalised by adding coalition $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}$ to the formalisation of priv, $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D] \approx_\ell C_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}]$. Similarly, cepriv, cipriv and ciepriv are formalised by adding coalition to epriv, ipriv and iepriv, respectively. In particular, we can show that various domain-specific privacy formalisations such as vote-privacy in e-voting, bidding-privacy in e-auction, and prescribing-privacy in e-health, are instances of cpriv, receipt-freeness and coercion-resistance in e-voting are instances of the property cepriv, and independency-of-prescribing-privacy in e-health and vote-independence in e-voting are instances of cipriv.

Relations. We show the relations between the privacy properties in Fig. 1: we use ρ to denote the specification of a target user's collaboration with the adversary, θ to denote the specification of a set of attacking third parties and their collaboration with the adversary, and δ to denote the specification of a set of defending third parties and their coalition with the target user. In the left diamond, epriv_ρ and ipriv_θ are stronger than priv, meaning that if a protocol satisfies epriv_ρ or ipriv_θ, then the protocol satisfies priv, and the reverse does not hold. Similarly, $\mathsf{iepriv}_{\rho,\theta}$ is stronger than both epriv_ρ and ipriv_θ. The right diamond shows the corresponding relations between privacy properties, when taking defending third parties into account. Each privacy property in the left diamond has a weaker corresponding property in the right diamond, meaning that if a protocol satisfies a privacy property in the left diamond, there exists a coalition such that the property satisfies the corresponding coalition privacy property. (Details can be found in a technical report available at http://satoss.uni.lu/projects/epriv/.)

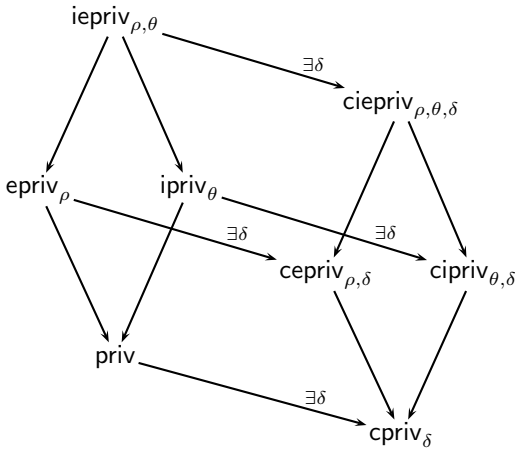

Figure 1. Relations of the privacy notions