GDPR Purpose-Aware Privacy-Enhanced System Design with Multiparty Session Types - Annexes

Evangelia Vanezi, Dimitrios Kouzapas, and Anna Philippou

Department of Computer Science, University of Cyprus, Nicosia, Cyprus
{vanezi.evangelia,kouzapas.dimitrios,philippou.anna}@ucy.ac.cy

A Use Case Typing

System Implementation:

$$B = \mathsf{p}!\langle \text{checkout}\rangle.\mathsf{p}!\langle r_1\rangle.\mathsf{p}!\langle r_2\rangle.\mathbf{0}$$

$$P = \mathsf{b}?(w).\mathsf{b}?(z_1).\mathsf{b}?(z_2).\mathsf{c}!\langle \text{payment}\rangle.\mathsf{c}!\langle z_1\rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle$$

$$C = \mathsf{p}?(w).\mathsf{p}?(z).z?(\_ \otimes x).\mathsf{p} \triangleleft \mathsf{auth}.\mathbf{0}$$

$$M = \mathsf{b} \blacktriangleright [B] \mid \mathsf{p} \blacktriangleright [P] \mid \mathsf{c} \blacktriangleright [C] \mid r_1 \blacktriangleright [\mathsf{id}_1 \otimes \text{cc\_num}] \mid r_2 \blacktriangleright [\mathsf{id}_1 \otimes \text{addr}]$$

We will be typing the Purchases Service process, p. We assume the following environments:

$$\begin{aligned} \Gamma' &= \text{checkout} : \mathtt{checkout\_request}, \text{payment} : \mathtt{payment\_request} \\ \Gamma &= \Gamma', r_1 : [\mathsf{id} \otimes \mathtt{cc\_num}]^{\mathsf{card\_store}}, r_2 : [\mathsf{id} \otimes \mathtt{address}]^{\mathsf{addr\_store}} \end{aligned}$$

We begin with typing the last term of the process, namely the branch term. By the [TBranch] typing rule precondition $\forall i \in I, \Gamma \vdash P_i \triangleright T_i$, we first need to type individually the two branches to obtain $\Gamma \vdash P_1 \triangleright T_1$ and $\Gamma \vdash P_2 \triangleright T_2$ as follows:

- Typing P_2=$\mathbf{0}$ using the [TInact] typing rule:

$$\Gamma \vdash \mathbf{0} \triangleright \mathsf{end}$$

- Typing P_1=$z_2?(x).\mathbf{0}$, using first the [TInact] typing rule exactly as in the other branch, obtaining $\Gamma \vdash \mathbf{0} \triangleright \mathsf{end}$. Then we continue by typing $z_2?(x).\mathbf{0}$ by using the [TInpPD] rule as follows:

$$\frac{\Gamma \vdash z_2 : [\mathsf{id} \otimes \mathtt{address}]^{\mathsf{addr\_store}} \quad \Gamma, x : \iota \otimes \mathsf{g} \vdash \mathbf{0} \triangleright \mathsf{end} \quad \iota = \mathsf{id}}{\Gamma \vdash z_2?(x).\mathbf{0} \triangleright \mathsf{addr\_store}?[\mathsf{id} \otimes \mathtt{address}].\mathsf{end}}$$

Therefore, using the [TBranch] rule:

$$\frac{\Gamma \vdash z_2?(x).\mathbf{0} \triangleright \mathsf{addr\_store}?[\mathsf{id} \otimes \mathtt{address}].\mathsf{end} \qquad \Gamma \vdash \mathbf{0} \triangleright \mathsf{end}}{\Gamma \vdash \mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle}$$

We continue by using the [TOut] rule, twice:
(a)

$$\frac{\begin{array}{l} \Gamma \vdash z_1 : [\mathsf{id} \otimes \mathtt{cc\_num}]^{\mathsf{card\_store}} \\ \Gamma \vdash \mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \mathsf{c}\&\langle \mathsf{auth} : \mathsf{addr\_store}?[\mathsf{id} \otimes \mathtt{address}].\mathsf{end}, \mathsf{deny} : \mathsf{end} \rangle \end{array}}{\begin{array}{l} \Gamma \vdash \mathsf{c}!\langle z_1 \rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \\ \mathsf{c}!\mathsf{card\_store}.\mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle \end{array}}$$

(b)

$$\frac{\begin{array}{l} \Gamma \vdash \mathrm{payment} : \mathtt{payment\_request} \\ \Gamma \vdash \mathsf{c}!\langle z_1 \rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \\ \mathsf{c}!\mathsf{card\_store}.\mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle \end{array}}{\begin{array}{l} \Gamma \vdash \mathsf{c}!\langle \mathrm{payment} \rangle.\mathsf{c}!\langle z_1 \rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \\ \mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}.\mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle \end{array}}$$

Then we use the [TInp] rule three times:
(a)

$$\frac{\begin{array}{l} \Gamma, z_2 : [\mathsf{id} \otimes \mathtt{address}]^{\mathsf{addr\_store}} \vdash \\ \mathsf{c}!\langle \mathrm{payment} \rangle.\mathsf{c}!\langle z_1 \rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \\ \mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}.\mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle \end{array}}{\begin{array}{l} \Gamma \vdash \mathsf{b}?(z_2).\mathsf{c}!\langle \mathrm{payment} \rangle.\mathsf{c}!\langle z_1 \rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l} \mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0} \end{array} \right\rangle \triangleright \\ \mathsf{b}?\mathsf{addr\_store}.\mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}. \\ \mathsf{c}\& \left\langle \begin{array}{l} \mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end} \end{array} \right\rangle \end{array}}$$

(b)

$$\dfrac{\begin{array}{l}\Gamma, z_1 : [\mathsf{id} \otimes \mathtt{cc\_num}]^{\mathsf{card\_store}} \vdash \\ \mathsf{b}?(z_2).\mathsf{c}!\langle \text{payment}\rangle.\mathsf{c}!\langle z_1\rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l}\mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0}\end{array}\right\rangle \triangleright \\ \mathsf{b}?\mathsf{addr\_store}.\mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}. \\ \mathsf{c}\& \left\langle \begin{array}{l}\mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end}\end{array}\right\rangle\end{array}}{\begin{array}{l}\Gamma \vdash \mathsf{b}?(z_1).\mathsf{b}?(z_2).\mathsf{c}!\langle \text{payment}\rangle.\mathsf{c}!\langle z_1\rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l}\mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0}\end{array}\right\rangle \triangleright \\ \mathsf{b}?\mathsf{card\_store}.\mathsf{b}?\mathsf{addr\_store}.\mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}. \\ \mathsf{c}\& \left\langle \begin{array}{l}\mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end}\end{array}\right\rangle\end{array}}$$

(c)

$$\dfrac{\begin{array}{l}\Gamma, w : \mathtt{checkout\_request} \vdash \\ \mathsf{b}?(z_1).\mathsf{b}?(z_2).\mathsf{c}!\langle \text{payment}\rangle.\mathsf{c}!\langle z_1\rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l}\mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0}\end{array}\right\rangle \triangleright \\ \mathsf{b}?\mathsf{card\_store}.\mathsf{b}?\mathsf{addr\_store}.\mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}. \\ \mathsf{c}\& \left\langle \begin{array}{l}\mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end}\end{array}\right\rangle\end{array}}{\begin{array}{l}\Gamma \vdash \mathsf{b}?(w).\mathsf{b}?(z_1).\mathsf{b}?(z_2).\mathsf{c}!\langle \text{payment}\rangle.\mathsf{c}!\langle z_1\rangle.\mathsf{c} \triangleright \left\langle \begin{array}{l}\mathsf{auth} : z_2?(y \otimes x).\mathbf{0}, \\ \mathsf{deny} : \mathbf{0}\end{array}\right\rangle \triangleright \\ \mathsf{b}?\mathtt{checkout\_request}.\mathsf{b}?\mathsf{card\_store}.\mathsf{b}?\mathsf{addr\_store}. \\ \mathsf{c}!\mathtt{payment\_request}.\mathsf{c}!\mathsf{card\_store}. \\ \mathsf{c}\& \left\langle \begin{array}{l}\mathsf{auth} : \mathsf{addr\_store}?(\mathsf{id} \otimes \mathtt{address}).\,\mathsf{end}, \\ \mathsf{deny} : \mathsf{end}\end{array}\right\rangle\end{array}}$$

Therefore, we obtain that $\Gamma \vdash \mathsf{p} \blacktriangleright [P] \triangleright \mathsf{G}\rceil\mathsf{p}$

B Proofs

We present the proof for the Type Preservation Lemma/Theorem.

Proof (Type Preservation).

1. Base Cases

– **Case 1:**

$$\boxed{[\mathsf{Comm}] \quad \mathsf{p} \blacktriangleright [\mathsf{q}!\langle t\rangle.P_1] \mid \mathsf{q} \blacktriangleright [\mathsf{p}?(x).P_2] \longrightarrow \mathsf{p} \blacktriangleright [P_1] \mid \mathsf{q} \blacktriangleright [P_2\{^t/_x\}]}$$

Premises:
- $\Gamma \vdash \mathsf{p}!\langle t\rangle.\ P1 \triangleright \mathsf{p}!\mathsf{U}.\ T$
- $\Gamma \vdash \mathsf{p}?(x).\ P2 \triangleright \mathsf{p}?\mathsf{U}.\ T$'
- $\Gamma \vdash$ t: U (from [TOut] typing rule)

P_2 $\{^t/_x\}$ remains well-typed by the substitution property of types.
By the preconditions of the typing rules [TOut] and [TInp], we get that $\Gamma \vdash \mathsf{p} \blacktriangleright [P_1] \triangleright T$ and $\Gamma \vdash \mathsf{q} \blacktriangleright [P_2\{^t/_x\}] \triangleright T$' hold. Typing is preserved.

– **Case 2:**

$$\boxed{[\mathsf{BranchSel}] \quad \mathsf{p} \blacktriangleright [\mathsf{q} \triangleleft \ell_\mathsf{j}.P] \mid \mathsf{q} \blacktriangleright [\mathsf{p} \triangleright \langle \ell_\mathsf{i} : P_i\rangle_{i\in I}] \longrightarrow \mathsf{p} \blacktriangleright [P] \mid \mathsf{q} \blacktriangleright [P_j] \quad j \in I}$$

Premises:
- $\Gamma \vdash \mathsf{p} \triangleleft \ell : P. \triangleright \mathsf{p} \oplus \langle \ell_\mathsf{i} : T_i\rangle_{i\in I}$
- $\Gamma \vdash \mathsf{p} \triangleright \langle \ell_\mathsf{i} : P_i\rangle_{i\in I} \triangleright \mathsf{p}\&\langle \ell_\mathsf{i} : T_i\rangle_{i\in I}$
- $j \in I$

By the preconditions of the typing rule [TSel] and [$\mathsf{TBranch}$], we get that $\Gamma \vdash \mathsf{p} \blacktriangleright [P] \triangleright T_j$ and $\Gamma \vdash \mathsf{q} \blacktriangleright [P_j] \triangleright T_j$ hold. Typing is preserved.

– **Case 3:**

$$\boxed{[\mathsf{SOut}] \quad \mathsf{p} \blacktriangleright [r!\langle \mathsf{id} \otimes \mathsf{c}\rangle.P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}'] \longrightarrow \mathsf{p} \blacktriangleright [P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]}$$

Premises:
- $\Gamma \vdash u!\langle \mathsf{id} \otimes \mathsf{c}\rangle.\ P \triangleright \alpha![\mathsf{pd}]\mathsf{id} \otimes \mathsf{g}.\ T$
- $\Gamma \vdash r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}']$

By the preconditions of the typing rule [TOutPD], we get that $\Gamma \vdash P \triangleright T$ holds. Typing is preserved.

– **Case 4:**

$$\boxed{[\mathsf{SInp}] \quad \mathsf{p} \blacktriangleright [r?(k).P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}] \longrightarrow \mathsf{p} \blacktriangleright \left[P\{^{\mathsf{id}\otimes\mathsf{c}}/_k\}\right] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]}$$

Premises:
- $\mathsf{\Gamma} \vdash u?(x).P \triangleright \alpha?[\mathsf{pd}]\mathsf{id} \otimes \mathsf{g}.T$
- $\mathsf{\Gamma} \vdash r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]$

By the preconditions of the typing rule [TInpPD], we get that
$\mathsf{\Gamma}$,x: $\mathsf{id} \otimes \mathsf{g} \vdash P \triangleright T$.
$P\ \{^{\mathsf{id}\otimes\mathsf{c}}/_k\}$ remains well-typed by the substitution property of types, $\mathsf{\Gamma} \vdash P$ $\{^{\mathsf{id}\otimes\mathsf{c}}/_k\} \triangleright T$. Typing is preserved.

2. Inductive Step

- **For parallel composition:** $\boxed{[\mathsf{Par}]\ M_1 \mid M_2 \longrightarrow M_1' \mid M_2}$
  If $\mathsf{\Gamma} \vdash M_1 \triangleright \Delta$ and $M_1 \longrightarrow M_1'$, then by induction:
  M_1' remains well-typed ($\mathsf{\Gamma} \vdash M_1' \triangleright \Delta$'), so $M_1' \mid M_2$ is well-typed ($\mathsf{\Gamma} \vdash M_1' \mid M_2 \triangleright \Delta$1', Δ2).
- **For restriction:** $\boxed{[\mathsf{Res}]\ (\nu\ s)\ M}$
  If $M \longrightarrow M'$, then $(\nu\ s)\ M \longrightarrow (\nu\ s)\ M'$
  Since s is private, it does not affect well-typedness. Typing is preserved.
- **For Structural Congruence:**

Since all cases preserve typing, the type preservation theorem holds. The proof is complete. □

We present the proof for the Progress Lemma.

Proof (Progress Lemma).

Case 1: Communication Progress

$\boxed{[\mathsf{Comm}]\quad \mathsf{p} \blacktriangleright [\mathsf{q}!\langle t\rangle.P_1] \mid \mathsf{q} \blacktriangleright [\mathsf{p}?(x).P_2]}$

- By the [TOut] rule: $\mathsf{\Gamma} \vdash \mathsf{p}!\langle t\rangle.\ P \triangleright \mathsf{p}!\mathsf{U}.\ T$
- By the [TInp] rule: $\mathsf{\Gamma} \vdash \mathsf{q}?(x).\ Q \triangleright \mathsf{q}?\mathsf{U}.\ T$'
- Since t: U, a matching input and output are present.

Therefore, the communication can proceed:
$\mathsf{p} \blacktriangleright [\mathsf{q}!\langle t\rangle.P_1] \mid \mathsf{q} \blacktriangleright [\mathsf{p}?(x).P_2] \longrightarrow \mathsf{p} \blacktriangleright [P_1] \mid \mathsf{q} \blacktriangleright [P_2\{^t/_x\}]$
Progress is ensured.

Case 2: Branch Selection Progress

$\boxed{[\mathsf{BranchSel}]\quad \mathsf{p} \blacktriangleright [\mathsf{q} \triangleleft \ell_\mathsf{j}.P] \mid \mathsf{q} \blacktriangleright [\mathsf{p} \triangleright \langle \ell_\mathsf{i} : P_i\rangle_{i\in I}]}$

- By the [TSel] rule: $\Gamma \vdash \mathsf{q} \triangleleft \ell : P. \triangleright \mathsf{q} \oplus \langle \ell_\mathsf{i} : T_i \rangle_{i \in I}$
- By the [$\mathsf{TBranch}$] rule: $\Gamma \vdash \mathsf{p} \triangleright \langle \ell_\mathsf{i} : P_i \rangle_{i \in I} \triangleright \mathsf{p} \& \langle \ell_\mathsf{i} : T_i \rangle_{i \in I}$
- Since $i \in I$, a matching branch is present.

Therefore, the communication can proceed:
$\mathsf{p} \blacktriangleright [\mathsf{q} \triangleleft \ell_\mathsf{j}.P] \mid \mathsf{q} \blacktriangleright [\mathsf{p} \triangleright \langle \ell_\mathsf{i} : P_i \rangle_{i \in I}] \longrightarrow \mathsf{p} \blacktriangleright [P] \mid \mathsf{q} \blacktriangleright [P_j] \quad j \in I$
Progress is ensured.

Case 3: Personal Data Store Progress

- Personal Data Read Progress

  $\boxed{\mathsf{p} \blacktriangleright [r?(k).P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]}$

  - By [TInpPD] rule, r is authorized for id

  Therefore, the read operation proceeds:
  $\mathsf{p} \blacktriangleright [r?(k).P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}] \longrightarrow \mathsf{p} \blacktriangleright \left[P\{^{\mathsf{id} \otimes \mathsf{c}}/_{k}\}\right] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]$

- Personal Data Write Progress

  $\boxed{\mathsf{p} \blacktriangleright [r!\langle \mathsf{id} \otimes \mathsf{c} \rangle.P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}']}$

  - By [TOutPD] rule, r is authorized for id

  Therefore, the write operation proceeds:
  $\mathsf{p} \blacktriangleright [r!\langle \mathsf{id} \otimes \mathsf{c} \rangle.P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}'] \longrightarrow \mathsf{p} \blacktriangleright [P] \mid r \blacktriangleright [\mathsf{id} \otimes \mathsf{c}]$
  Progress is ensured.

A well-typed process always has a valid next step. Progress is proved. $\square$