

Anonymity with Identity Escrow

Aybek Mukhamedov
joint work with Mark Ryan

University of Birmingham

Identity Escrow

- **Context:** online service provider and a user
- **Properties:** user anonymity and identity recoverability
- **Idea:** escrow identity with a trusted party
- **Crypto solutions:** Kilian and Petrank (Crypto'98), and later other schemes:
 - security relies on non-standard assumptions Strong RSA, LRSW, etc.
 - identity escrow authority can be realized by several parties using “threshold crypto” (Desmedt *et al.*), but no security proofs

Identity Escrow: protocol approach

- Based on standard public and symmetric key encryptions
- Marshall *et al.* (FAST'03) protocol distributing trust among several TPs:
 - fails to provide anonymity and no countermeasures against impersonation attacks by TPs
- Our scheme:
 - if at least one of the TPs is honest user's identity will not be revealed
 - TP accountability in recovering dishonest user's identity
- We analyse user anonymity in the applied π calculus

Our protocol

- All communication is via anonymous channels
- Comprises two protocols: sign-up and recovery
- **Sign-up:**
 - User A generates a fresh service key.
 - A chooses a sequence of token issuers T_{a_1}, \dots, T_{a_n} of which at least one is honest Th
 - A constructs a service token $\tilde{\Phi}_A$ by interacting with the token issuers, which she presents to service provider S
- **Recovery:**
 - In the event of a misuse, S recovers identity from $\tilde{\Phi}_A$ by contacting all token issuers from A 's sequence
- S does not learn A 's sequence of service issuers when presented with the service token

Sign-up protocol

- 1 User A constructs a “layered” term Φ_{n-1} :

$$\{ \dots$$
$$\{ \text{serv}K_{[A]}, \text{sym}K_{a_1} \}_{pK_{T_{a_1}}}, \text{sym}K_{a_2} \}_{pK_{T_{a_2}}}$$
$$\dots \}_{pK_{T_{a_{n-2}}}, \text{sym}K_{a_{n-1}} \}_{pK_{T_{a_{n-1}}}}$$

- 2 A signs Φ_{n-1} , sends it to T_{a_n} , and receives $\tilde{\Phi}_1$:

$$[\{ [\Phi_{n-1}, A]_{\text{sign}K_A} \}_{pK_{T_{a_n}}}, \Phi_{n-1}]_{\text{sign}K_{T_{a_n}}}$$

- 3 A sends $\tilde{\Phi}_1$ to $T_{a_{n-1}}$ and receives $\tilde{\Phi}_2$:

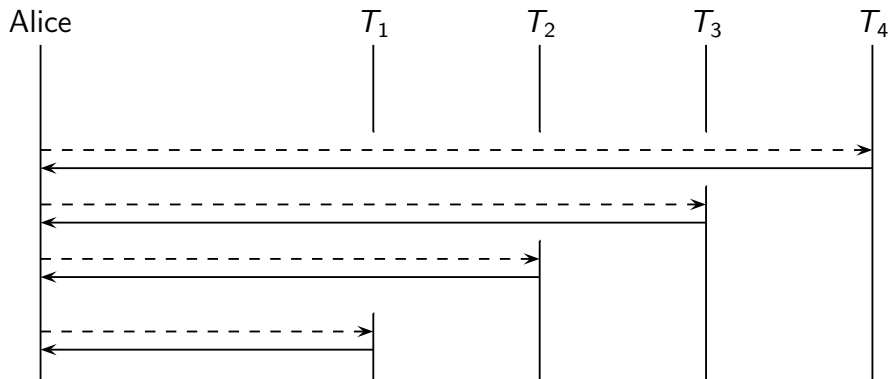
$$[\{ \tilde{\Phi}_1, \text{sym}K_{a_{n-1}} \}_{pK_{T_{a_{n-1}}}}, \Phi_{n-2}]_{\text{sign}K_{T_{a_{n-1}}}}$$

Sign-up protocol

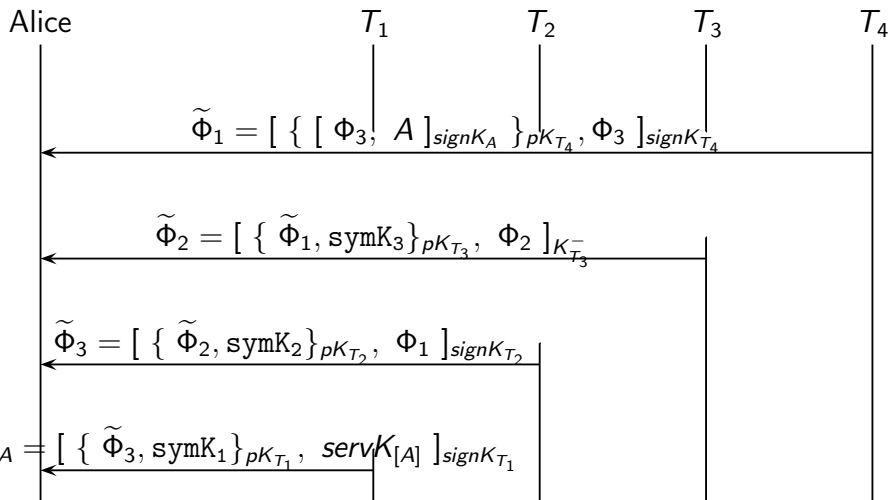
- 4 A repeats the previous step with $T_{a_{n-2}}, \dots, T_{a_1}$
- 5 The resulting service token $\tilde{\Phi}_A$ is of the form:

$$[\{ \dots [\{ \tilde{\Phi}_1, \text{symK}_{a_{n-1}} \}_{\rho K_{T_{a_{n-1}}}}, \Phi_{n-2}]_{\text{signK}_{T_{a_{n-1}}}} \dots \text{symK}_{a_1} \}_{\rho K_{T_{a_1}}}, \text{servK}_{[A]}]_{\text{signK}_{T_{a_1}}}$$

Sign-up (n=4)



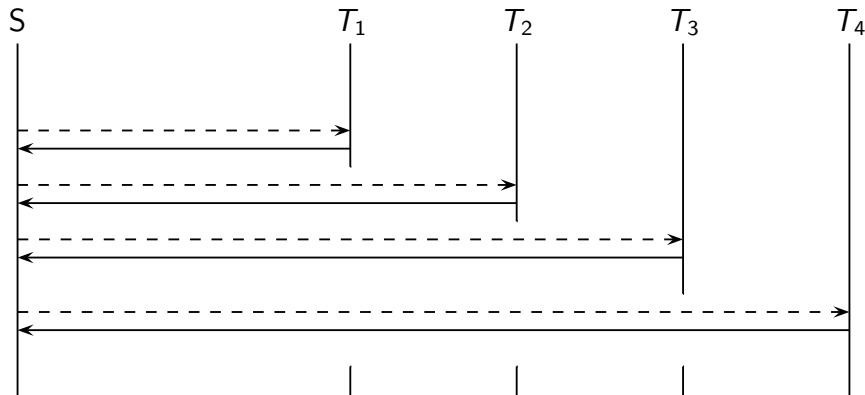
Sign-up messages received (n=4)



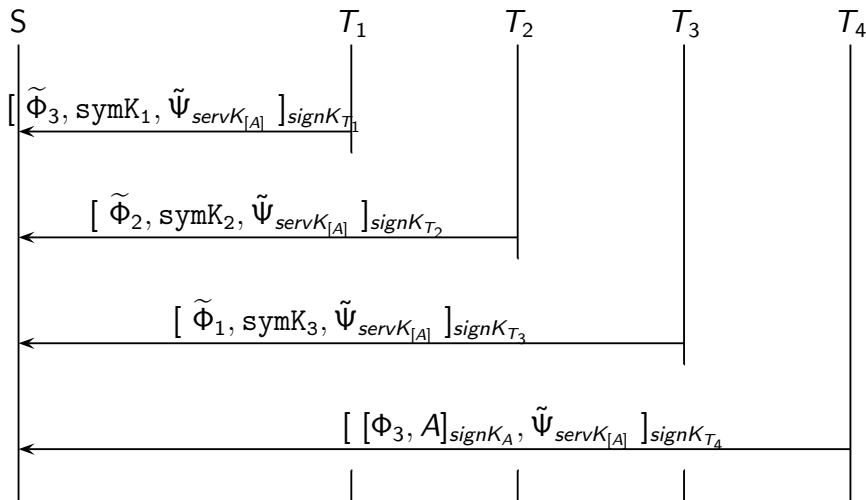
Recovery protocol

- Service provider S has a misuse evidence $\Psi_{servK_{[A]}}$
 - such as a set of requests signed by service key $servK_{[A]}$
- S with the help of T_{a_1}, \dots, T_{a_n} “delayers” the service token $\tilde{\Phi}_A$ to reveal the identity of the user

Recovery (n=4)



Recovery messages received (n=4)



Formal Analysis

- Using the applied π -calculus by Abadi and Fournet
- Equivalence-based specification of anonymity
- The active (Dolev-Yao) attacker is implicit in the model
- Syntax:
 - **Terms:** names, variables, application of functions to other terms.
 - **Equational theory:** $\text{dec}(\text{enc}(x, \text{pk}(y)), y) = x$
 - **Processes:** $Q = \nu n.(\text{out}(c, \text{enc}(M, \text{pk}(n))); \text{in}(d, z); P')$

- Operational semantics: structural equivalence (\equiv), internal reduction (\rightarrow)
- Operational labeled semantics ($\xrightarrow{\alpha}$):

$$Q \xrightarrow{\nu z.out(c,z)} \nu n.(in(d,z); P' \mid \{enc(M, pk(n)) / z\})$$
$$\xrightarrow{in(d,z)} \nu n.P' \{enc(M, pk(n)) / z\}$$

- A frame φ is a process of the form:

$$\nu \tilde{n}. (\{M_1/x_1\} \mid \dots \mid \{M_n/x_n\})$$

Definition (Static equivalence)

For closed frames φ_1, φ_2 , we have $\varphi_1 \approx_s \varphi_2$ if:

- $\text{dom}(\varphi_1) = \text{dom}(\varphi_2)$
- for all terms M, N , $(M = N)_{\varphi_1}$ iff $(M = N)_{\varphi_2}$

Definition (labeled bisimilarity)

Labeled bisimilarity (\approx_l) is the largest symmetric relation \mathcal{R} on closed extended processes, where $A\mathcal{R}B$ implies:

- $\varphi(A) \approx_s \varphi(B)$
 - if $A \rightarrow A'$ then $B \rightarrow^* B'$ and $A'\mathcal{R}B'$ for some B'
 - if $A \xrightarrow{\alpha} A'$ then $B \rightarrow^* \xrightarrow{\alpha} \rightarrow^* B'$ and $A'\mathcal{R}B'$ for some B'
-
- Labeled bisimilarity is equivalent to observational equivalence (Abadi, Fournet)

Analysis of the protocol

- User anonymity:
 - user's service token cannot be **linked** to his real identity
- Expressed via observational equivalence:
 - a system containing at least two honest users A, B and an honest token issuer Th is indistinguishable from the same system where A and B swap their tokens.
 - *alternative formulation*: a system with a user A and an honest token issuer Th is indistinguishable from the same system where A constructs an empty token with the help of an oracle.

Theorem (User anonymity)

$$\nu K_{Th}, \tilde{n}_A, \tilde{n}_B. (A; \text{out}(ch, \tilde{\Phi}(A)) \mid B; \text{out}(ch, \tilde{\Phi}(B)) \mid !Th)$$

\approx

$$\nu K_{Th}, \tilde{n}_A, \tilde{n}_B. (A'; \text{out}(ch, \tilde{\Phi}(A')) \mid B'; \text{out}(ch, \tilde{\Phi}(B')) \mid !Th)$$

- Main effort is in proving static equivalence
- Proved by reducing frames on both sides to α -equivalent form:
 - via lemmas expressing sufficient conditions for replacing ciphertexts with fresh names

Auxilliary lemmas

Given a closed term L in normal form and a frame $\nu\tilde{n}.\sigma$ in normal form, and $k \in \tilde{n}$ if:

Lemma (sk)

- k occurs in σ only as an encryption key argument.
- L does not occur in σ and $s \notin \text{fn}(\sigma)$.

Then: $\nu\tilde{n}.\left(\left\{\left\{L\right\}_k/x\right\}\middle|\sigma\right) \approx_s \nu\tilde{n},s.\left(\left\{s/x\right\}\middle|\sigma\right)$.

Lemma (pk)

- $\nu\tilde{n}.\sigma \not\vdash k$, $\nu\tilde{n}.\sigma \not\vdash \{L\}_{pk(k)}$ and $m \notin \text{fn}(\sigma)$
- $\{L\}_{pk(k)}$ and $\text{dec}(x, k)$ do not occur in σ .

Then $\nu\tilde{n}.\left(\left\{\left\{L\right\}_{pk(k)}/x\right\}\middle|\sigma\right) \approx_s \nu\tilde{n},m.\left(\left\{m/x\right\}\middle|\sigma\right)$.