The SEMPER Framework for Fair Exchange

Matthias Schunter
University of Saarbrücken
Germany

- Introduction
- A Fair Exchange Protocol
- Exchange-Enabling Properties of Transfers
- The SEMPER Framework for Fair Exchange
- Conclusion
Fair Exchange in SEMPER

The SEMPER Model:

- Buyer
- Seller

This Talk

The SEMPER Framework:

Transfer and Fair Exchange Layer

- Fair Exchange Transactions
- Secure Transfer Transactions
  - Payments
  - ... Documents

Payment
Payment Receipt
Fair Exchange: Definition and Goals

Buyer

I give: $\text{sign}_B(C)$
I want: Signature of Seller under contract $C$

If "give=want":

Fair Exchange Transaction

$\text{sign}_S(C)$ $\text{sign}_B(C)$

OR

Else:

failed $\quad$ failed

Who is the Buyer?

Who is the Seller?

Why not use two Transfers?

💡 "Instant" Fairness.
💡 Costs of "legal fairness" higher.
Examples & Goals

- **More Instances of Fair Exchange**
  - Delivery of valueable data: signature for data.
  - Fair purchase: data for payment.
  - Payment for receipt: payment for data.
  - Contract signing: signature for signature.

- **Fair Exchange outside SEMPER:**
  - Protocols for particular instances, i.e., dependent from goods to be exchanged
  - Inline TP: Limited efficiency and unlimited trust in TP

- **Goals**
  - Transfer-based Fair Exchange, i.e., independence from goods
  - Optimistic TP: Efficient and limited trust
Example Protocol: Optimistic Contract Signing

Agreement

Buyer

```
m_1 = sign_B("Let's sign": C)
```

Seller

```
m_2 = sign_S("I agree", m_1)
```

Exchange

Buyer

```
sign_B(C)
```

Seller

```
sign_S(C)
```

continue?

continue?

ok?

ok?
Example: Recovery with TP

**Agreement**

1. $m_1 = \text{sign}_B(\text{"Let's sign": } C)$
2. $m_2 = \text{sign}_S(m_1)$

**Exchange**

3. $\text{sign}_B(C)$

**Recovery**

4. $A := (m_1, m_2)$
5. $\text{sign}_B(C)$
6. $\text{sign}_T(A)$

$A := (m_1, m_2)$
Exchange-Enabling Properties of Signatures

Transfer

Buyer → \text{sign}_{B}(C) \rightarrow \text{Seller}

Recovery:

Observable Transfer
- TP can \textit{observe} status of Transfer

Generateable Transfer
- TP can \textit{redo} the Transfer

Revocable Transfer
- TP can \textit{undo} the Transfer
Exchange-Enabling Properties: More Examples

- **Observability**
  - Messages: Forward.
  - e-cash: Verify and forward.
  - Signatures: Verify and forward.

- **Generatibility**
  - Signatures: Agreement authorizes TP to signs on behalf.
  - e-cash: Agreement contains encrypted coin "verifiable encryption"

- **Revocability**
  - Credit-card payments: Enable TP to revoke payment.
The Fair Exchange Framework – Overview

- Transfer Layer provides Transfers with Exchange-enabling Properties
- Fair Exchange protocols use the properties to guarantee fairness

Secure Transfer Services
- Generatable Transfer
- Observable Transfer
- Revocable Transfer

Fair Exchange Services
The Fair Exchange Framework – Transfers of Goods

Transfer Transactions:

- Any transfer may provide any subset of the properties.
- If a transfer does not provide any property, it cannot be exchanged.
- Properties of transfers may depend on the goods to be transferred: dynamic negotiation.
Using Transfers

Sender

Transfer Transaction (sending)

Recipient

Transfer Transaction (receiving)

protocol

User's Point of View

Sender:
1. Ask the item to be sent for an appropriate transfer transaction.
2. Start it.

Recipient:
1. Instantiate a generic receiver.
2. Start it.
3. Retrieve received item.
The Fair Exchange Framework – Exchanges

**Fair Exchange Layer:**

- Fair Exchange Transaction

- Protocol Plug-In: "observable + generatable"

- Protocol Plug-In: "observable + revocable"

  - obs
  - rev

**Secure Transfer Layer:**

- Transfer Transaction

  - gen
  - obs
  - rev
Using Fair Exchanges

Buyer

Exchange Transaction

exchange protocol

Seller

Exchange Transaction

User's Point of View

Both:

1. Instantiate fair exchange transaction
2. Input item to be sent
3. Input description of item to be expected
4. Start it
5. Retrieve the result ("failed" or received items)
The Fair Exchange Framework in Action

Activities for Fair Exchange:

1. Exchange Transaction instantiates transfers (sender+receiver)
2. Transfer Transactions negotiate enabled properties
3. Exchange Transactions negotiate protocol
4. Selected protocol runs.

Fair Exchange Transaction

Exchange Protocol Plug-in

gen
obs

Transfer Transaction (sending)

genobsrev

Transfer Transaction (receiving)

genobsrev
Conclusion

The SEMPER Framework for Fair Exchange

- Guaranteed Fairness
- Open and Extensible
- Enables Efficient Optimistic Protocols: TP only needed in case of failure