Approaching a Formal Definition of Fairness in Electronic Commerce

Felix Gärtner *Henning Pagnia* *Holger Vogt*

Darmstadt University of Technology, Germany

Overview

- What is *fair exchange* and how does it relate to e-commerce?

Overview

- What is *fair exchange* and how does it relate to e-commerce?
- What are the problems with the usual definition of *fair exchange*?

Overview

- What is *fair exchange* and how does it relate to e-commerce?
- What are the problems with the usual definition of *fair exchange*?
- How can theory help improve the definitions?

Overview

- What is *fair exchange* and how does it relate to e-commerce?
- What are the problems with the usual definition of *fair exchange*?
- How can theory help improve the definitions?
- What are the benefits of the refined definitions in practice?

What is *fair exchange*?

- Orders, goods and payment will be shipped electronically.
- The exchange of such items must be *fair*.
- *fair exchange problem* = How exchange two items between parties A and B over an electronic network without either party suffering a disadvantage?
- Assumption: items can be fully validated.

Strong and Weak Fairness [Asokan 1998]

- *strong fairness*: "When the protocol has completed, A has B's item, or B has gained no additional information about A's item, and vice versa.

Strong and Weak Fairness [Asokan 1998]

- *strong fairness*: "When the protocol has completed, A has B's item, or B has gained no additional information about A's item, and vice versa.

- *weak fairness*: "Either strong fairness is achieved, or a correctly behaving node can prove to an arbiter that an unfair situation has occured."

Strong and Weak Fairness [Asokan 1998]

- *strong fairness*: "When the protocol has completed, A has B's item, or B has gained no additional information about A's item, and vice versa.

- *weak fairness*: "Either strong fairness is achieved, or a correctly behaving node can prove to an arbiter that an unfair situation has occured."

Distinction: inside/outside the exchange system

Some Theory. . .

- *Properties* of systems are sets of traces.

Some Theory. . .

- *Properties* of systems are sets of traces.
- Two main classes of properties [Lamport 1977]:

Some Theory. . .

- *Properties* of systems are sets of traces.
- Two main classes of properties [Lamport 1977]:
  - ⋆ *safety*: "something bad will never happen"

Some Theory. . .

- *Properties* of systems are sets of traces.
- Two main classes of properties [Lamport 1977]:
  - ⋆ *safety*: "something bad will never happen"
  - ⋆ *liveness*: "something good will eventually happen"

Some Theory. . .

- *Properties* of systems are sets of traces.
- Two main classes of properties [Lamport 1977]:
  - ⋆ *safety*: "something bad will never happen"
  - ⋆ *liveness*: "something good will eventually happen"
- Rule of thumb: finitely refutable $\Rightarrow$ safety.

Revisiting *fairness*

- *Strong fairness* is a safety property [Pagnia and Gärtner 1999; Shmatikov and Mitchell 1999].
- What about *weak fairness*?

Revisiting *fairness*

- *Strong fairness* is a safety property [Pagnia and Gärtner 1999; Shmatikov and Mitchell 1999].
- What about *weak fairness*?
  Is there a point in time where
  1. strong fairness is violated, and
  2. a party loses its ability to prove that it has been treated unfair?

Revisiting *fairness*

- *Strong fairness* is a safety property [Pagnia and Gärtner 1999; Shmatikov and Mitchell 1999].
- What about *weak fairness*?
  Is there a point in time where
  1. strong fairness is violated, and
  2. a party loses its ability to prove that it has been treated unfair?
- Answer "No" $\Rightarrow$ weak fairness is liveness
- Answer "Yes" $\Rightarrow$ weak fairness is safety

Eventually Strong Fairness

- Asokan's "weak fairness" as a liveness property.

Eventually Strong Fairness

- Asokan's "weak fairness" as a liveness property.
- Eventually an unfair situation is resolved within the system.

Eventually Strong Fairness

- Asokan's "weak fairness" as a liveness property.
- Eventually an unfair situation is resolved within the system.
- Necessary: additional assumptions about the parties.

Eventually Strong Fairness

- Asokan's "weak fairness" as a liveness property.
- Eventually an unfair situation is resolved within the system.
- Necessary: additional assumptions about the parties.
- In general: "eventual cooperation", achievable e.g. by
  - ⋆ Trusted Computing Environment [Wilhelm 1997],
  - ⋆ Security Kernel [Schneider 1998],
  - ⋆ Smartcards, . . .

New Fairness Definitions

Fairness	property	resolvable	remark
strong	safety	automatically	
eventually strong	liveness	automatically	additional assumptions
weak fairness	safety	outside of the System	

Consequences in Practice

- Use standard formal methods to verify fair exchange protocols.

Consequences in Practice

- Use standard formal methods to verify fair exchange protocols.
  - ⋆ E.g., strong fairness $\Rightarrow$ safety property $\Rightarrow$ invariance argument.

Consequences in Practice

- Use standard formal methods to verify fair exchange protocols.
  - ⋆ E.g., strong fairness $\Rightarrow$ safety property $\Rightarrow$ invariance argument.
- Strong fairness sometimes impossible:
  - ⋆ Identify additional assumptions and prove eventually strong fairness.

Consequences in Practice

- Use standard formal methods to verify fair exchange protocols.
  - ⋆ E.g., strong fairness $\Rightarrow$ safety property $\Rightarrow$ invariance argument.
- Strong fairness sometimes impossible:
  - ⋆ Identify additional assumptions and prove eventually strong fairness.
- Weak fairness: identify "sufficient evidence"

Consequences in Practice

- Use standard formal methods to verify fair exchange protocols.
  - ⋆ E.g., strong fairness $\Rightarrow$ safety property $\Rightarrow$ invariance argument.
- Strong fairness sometimes impossible:
  - ⋆ Identify additional assumptions and prove eventually strong fairness.
- Weak fairness: identify "sufficient evidence"
- Better: stay inside the system!

Conclusions

- *Fair exchange* plays an important role in e-commerce.

Conclusions

- *Fair exchange* plays an important role in e-commerce.
- Need formal definition of fairness to reach assurance on fair exchange protocols.

Conclusions

- *Fair exchange* plays an important role in e-commerce.
- Need formal definition of fairness to reach assurance on fair exchange protocols.
- New formal variants of Asokan's strong and weak fairness definitions.

Conclusions

- *Fair exchange* plays an important role in e-commerce.
- Need formal definition of fairness to reach assurance on fair exchange protocols.
- New formal variants of Asokan's strong and weak fairness definitions.
- Use theory to help clarify concepts in practice.
- Can use new definitions and standard formal methods to reach assurance on correctness of fair exchange protocols.

Acknowledgements

Slides produced using LaTeX and Klaus Guntermann's PPower4:
http://www-sp.iti.informatik.tu-darmstadt.de/software/ppower4/

References

Asokan, N. 1998. *Fairness in electronic commerce*. Ph. D. thesis, University of Waterloo.

Lamport, L. 1977. Proving the correctness of multiprocess programs. *IEEE Trans. Softw. Eng. 3*, 2 (March), 125–143.

Pagnia, H. and Gärtner, F. C. 1999. On the impossibility of fair exchange without a trusted third party. Tech. Rep. TUD-BS-1999-02 (March), Darmstadt University of Technology, Department of Computer Science, Darmstadt, Germany.

Schneider, F. B. 1998. Enforceable security policies. Technical Report TR98-1664 (Jan.), Cornell University, Department of Computer Science, Ithaca, New York.

Shmatikov, V. and Mitchell, J. C. 1999. Analysis of a fair exchange protocol. In *Proc. FLoC Workshop on Formal Methods and Sec. Protocols* (Italy, July 1999).

Wilhelm, U. G. 1997. Cryptographically protected objects. A french version appeared in the Proceedings of RenPar'9, Lausanne, Switzerland, http://lsewww.epfl.ch/~wilhelm/CryPO.html.