On the Security of Fair Non-repudiation Protocols

Sigrid Gürgens[1], Carsten Rudolph[1], and Holger Vogt[2]

[1] Fraunhofer – Institute for Secure Telecooperation SIT,
Rheinstrasse 75, 64295 Darmstadt, Germany
{guergens,rudolphc}@sit.fraunhofer.de
[2] SRC Security Research & Consulting GmbH,*
Graurheindorfer Str. 149a, 53117 Bonn, Germany
Holger.Vogt@src-gmbh.de

Abstract. We analyzed two non-repudiation protocols and found some new attacks on the fairness and termination property of these protocols. Our attacks are enabled by several inherent design weaknesses, which also apply to other non-repudiation protocols. To prevent these attacks, we propose generic countermeasures that considerably strengthen the design and implementation of non-repudiation protocols. The application of these countermeasures is finally shown by our construction of a new fair non-repudiation protocol.

* This research was performed while the last author was at Darmstadt University of Technology.