Verifiability in e-Auction Protocols & Brandt's Protocol Revisited

Jannik Dreier
Université Grenoble 1, CNRS, VERIMAG
jannik.dreier@imag.fr

Jean-Guillaume Dumas
Université Grenoble 1, CNRS, Laboratoire Jean Kuntzmann (LJK)
jean-guillaume.dumas@imag.fr

Hugo Jonker
University of Luxembourg
hugo.jonker@uni.lu

Pascal Lafourcade
Université Grenoble 1, CNRS, VERIMAG
pascal.lafourcade@imag.fr

February 22, 2013

Abstract

An electronic auction protocol will only be used by those who trust that it operates correctly. Therefore, e-auction protocols must be verifiable: seller, buyer and losing bidders must all be able to determine that the result was correct. We pose that the importance of verifiability for e-auctions necessitates a formal analysis. Consequently, in the first part of the talk, we identify notions of verifiability for each stakeholder. We formalize these and then use the developed framework to study the verifiability of several examples. We provide an analysis of the protocol by Sako in the applied pi-calculus with help of ProVerif, finding it to be correct. Additionally we identify issues with the protocols due to Curtis et al. and Brandt.

In the second part, we will analyze the protocol by Brandt in more detail. We show first that this protocol – when using malleable interactive zero-knowledge proofs – is vulnerable to attacks by dishonest bidders. Such bidders can manipulate the publicly available data in a way that allows the seller to deduce all participants' bids. Additionally we discuss attacks on non-repudiation, fairness and the privacy of individual bidders exploiting authentication problems.