COMPUTERS & SECURITY ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Formal modelling and analysis of receipt-free auction protocols in applied pi

Naipeng Dong [a,*], *Hugo Jonker* [b,c], *Jun Pang* [d]

[a] *School of Computing, National University of Singapore, 21 Lower Kent Ridge Rd, 119077 Singapore*
[b] *School of Computer Science, Open University of the Netherlands, Valkenburgerweg 177, 6419 AT Heerlen, The Netherlands*
[c] *Institute for Computing and Information Sciences, Faculty of Science, Radboud University, 6500 GL Nijmegen, The Netherlands*
[d] *Faculty of Science, Technology and Communication, Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 6 rue Richard Coudenhove-Kalergi, L-1359, Luxembourg*

ARTICLE INFO

Article history:
Received 26 June 2015
Received in revised form 28 April 2016
Accepted 8 September 2016
Available online

Keywords:
E-auction
Security protocol
Formal verification
Bidding-price-secrecy
Receipt-freeness

ABSTRACT

We formally study two privacy-type properties for e-auction protocols: bidding-price-secrecy and receipt-freeness. These properties are formalised as observational equivalences in the applied pi calculus. We analyse two receipt-free auction protocols: one proposed by Abe and Suzuki in 2002 (AS02) and the other by Howlader et al. in 2014 (HRM14). Bidding-price-secrecy of the AS02 protocol is verified using the automatic verifier ProVerif, whereas receipt-freeness of the two protocols, as well as bidding-price-secrecy of the HRM14 protocol, are proved manually.

1. Introduction

Auctions are ways to negotiate exchange of goods and services. We use *e-auctions* to refer to auctions over the Internet. A typical (e-)auction works as follows: a seller offers items to bid, then bidders submit bids, finally auctioneers decide the winner. In a traditional auction, bidders attend the auction in person. Compared to the traditional auctions, e-auctions attract more participants, as users with the Internet can join an auction. Real-life examples are well-known websites like *eBay*, *eBid*, *Yahoo!auctions* and so on. E-auction protocols are also the subject of an active field of research (Abe and Suzuki, 2002; Abubaker et al., 2015; Cachin, 1999; Chen et al., 2003; Dreier et al., 2014; Harkavy et al., 1998; Ksiezopolski and Kotulski, 2004; Lipmaa et al., 2003; Micali and Rabin, 2014; Naor et al., 1999).

There are different types of (e-)auctions. For instance, depending on whether the bids are public, there are sealed-bid auctions and open-bid auctions.

- *Sealed-bid auctions*: There are two phases in an auction: the bidding phase and the opening phase. Bidders can only submit bids in the bidding phase. All bids are sealed in the bidding phase and opened in the opening phase.
- *Open-bid auctions*: Bids are broadcast to all participants.

Other criteria to classify (e-)auctions exist as well. For example, depending on the bidding price increases or

* *Corresponding author.*
Email addresses: dcsdn@nus.edu.sg (N. Dong), hugo.jonker@ou.nl (H. Jonker), jun.pang@uni.lu (J. Pang).
http://dx.doi.org/10.1016/j.cose.2016.09.002
0167-4048/

Please cite this article in press as: Naipeng Dong, Hugo Jonker, Jun Pang, Formal modelling and analysis of receipt-free auction protocols in applied pi, computers & security (2016), doi: 10.1016/j.cose.2016.09.002

decreases, there are English auctions (a bid needs to be higher than the previous one; the winning bid is the final bid) and Dutch auctions (the bidding price decreases until a bid is submitted); depending on the calculation of payment, there are first-price auctions (the winner pays for the price he bid (highest price)) and Vickrey auctions (the winner pays for the second highest price). Different auctions are suitable for different types of negotiations, e.g., English auctions are often used in real estate, Dutch auctions are often used in flower selling, and Vickrey auctions are favoured by economists as they are better at encouraging bidders to express their real estimation on the value of the items to bid on (Trevathan, 2007).

Many security issues have been identified in e-auctions, such as a bidder may falsely claim or forge bids, the auctioneer may corrupt with other bidders (Trevathan, 2005). Beside security issues, an important problem with existing e-auction systems is privacy. The link between a bidder and his bids needs to be protected as such information can be used to target a bidder with unsolicited junk mails or other malicious purposes, e.g., *bid shielding*.[1] A major challenge of designing a protocol is to ensure the functionality of the protocol. In addition to that, a challenge for designing a privacy preserving e-auction protocol is that too much anonymity may allow bidders to repudiate bids, whereas insufficient anonymity allows bidders to be profiled.

Depending on different types of auctions, privacy may have varying levels. For instance, in sealed-bid auctions, all bids are sealed until the winner is determined. Therefore, if auctioneers can decide the winners without knowing the non-winning bidder's bids, sealed-bid auctions can offer bidding-price secrecy for non-winning bidders; while in open-bid auctions, all the bids are published. Some auctions require that the auctioneer cannot link a bidder to his bids, whereas some others do not. The arguments for this requirement are made according to the following lines. In Vickery auctions, a bidder's bid reflects the bidder's valuation of the item being bid on. Knowing a bidder's bid, an auctioneer knows the bidder's valuation. Since the winning bidder pays for the second highest price, the auctioneer could enter a bid just slightly lower than the bidder's valuation, to increase the auction's revenue (Trevathan, 2007). Contrarily in English auctions, bidder's previous bids reveal less information of the bidder's future bid, thus, that the auctioneer knows the link between a bidder and his previous bids is less harmful (Trevathan, 2007). In general, sealed-bid e-auctions require that the non-winning bidders' bidder–bid relation should be kept secret.

In addition to the above privacy notions, a stronger privacy notion – enforced privacy – has also been identified. In sealed-bid e-auctions, a bidder may be coerced to bid a low price, so that the coercer can win an auction with an unreasonably low price. The phenomenon that a coercer tries to control the winning price by coercion is called *bid-rigging*. Note that the traditional auctions do not suffer from bid-rigging, as the bidders do not have receipts on submitting a bid (Howlader et al., 2009). Inspired by the requirement of receipt-freeness in e-voting that a voter should not be able to prove his vote to a voter–buyer, the requirement of receipt-freeness for fighting against bid-rigging has been identified (Sakurai and Miyazaki, 2000).

In general, the following two privacy notions are required in sealed-bid e-auctions.

Bidding-price-secrecy: A sealed-bid e-auction protocol preserves bidding-price-secrecy for non-winning bidders if the adversary cannot determine the bidding price of any non-winning bidder.

Receipt-freeness: A sealed-bid e-auction protocol is receipt-free for non-winning bidders if a non-winning bidder cannot prove how he bids to the adversary.

In this paper, we first formalise these two privacy notions in the applied pi calculus (Section 4). Without a precise definition, many protocols claimed to satisfy a property were later found flawed (see examples in Delaune et al., 2009). For example, the Okamoto e-voting protocol (Okamoto, 1996), which claimed to satisfy receipt-freeness expressed in natural language, was later shown flawed with respect to a rigorous definition (Okamoto, 1997); and according to the author, one important reason is the lack of formal definition of receipt-freeness in e-voting. To validate our formalisation, we model and study privacy properties of the AS02 protocol proposed by Abe and Suzuki (2002) (Section 5) and the HRM14 protocol proposed by Howlader et al. (2014) (Section 6). The authors of both papers claim that their protocol satisfies the above two requirements for non-winning bidders and provide an informal analysis. However, security protocols are notoriously difficult to design and analyse, and proofs of security protocols are known to be error-prone, thus we do not want to rely on an informal analysis. In several cases, formal verification found security flaws in protocols which were thought to be secure (Chadha et al., 2004; Delaune et al., 2009; Dreier et al., 2015; Lowe, 1996). Formal verification has shown its strength in finding attacks and proving correctness of security protocols. In this paper, we formally verify whether bidding-price-secrecy and receipt-freeness hold in their protocols. We model both protocols using the applied pi calculus (Abadi and Fournet, 2001) (Section 2). The applied pi calculus provides an intuitive way to model concurrent systems, especially security protocols. Moreover, it is supported by ProVerif (Blanchet, 2001), a verification tool which can be used to verify a number of security properties automatically (Section 3). As suggested in Delaune et al. (2009), we use observational equivalence to express bidding-price-secrecy and receipt-freeness in the applied pi calculus. Previously, formalisation of privacy-type properties has already been successfully executed in the domain of voting (Delaune et al., 2009; Kremer and Ryan, 2005) (similar ideas were developed in a different formal framework (Jonker et al., 2009)). Bidding-price-secrecy for the AS02 protocol is verified automatically using ProVerif, whereas receipt-freeness, as well as bidding-price-secrecy for the HRM14, is proven manually. Related work is discussed in Section 7 and Section 8 concludes the paper with a few future works.

Note that an extended abstract of our work has appeared in the proceedings of 7th International Workshop on Formal Aspects in Security and Trust (Dong et al., 2011), where we have formally analysed the AS02 protocol. In the current paper, we have included the full details of our analysis of the AS02 pro-

[1] A dishonest bidder submits a higher price to deter other bidders with lower valuations, when it approaches the close time of the auction, the dishonest bidder withdraws his bid in order to win with another lower bid from him.

Please cite this article in press as: Naipeng Dong, Hugo Jonker, Jun Pang, Formal modelling and analysis of receipt-free auction protocols in applied pi, computers & security (2016), doi: 10.1016/j.cose.2016.09.002