In Proceedings of the 18th ACM SIGMOD-SIGACT-SIGART
Symposium on Principles of Database Systems (PODS 1999), May 1999, p. 101

Open Problems in Electronic Commerce

J. D. Tygar
Department of Electrical Engineering & Computer Science
and School of Information Management & Systems
University of California
Berkeley, CA 94720-4600
+1-510-643-7855
(also at Computer Science Department, Carnegie Mellon University)

tygar@cs.berkeley.edu

ABSTRACT

In my tutorial talk, I will broadly survey electronic commerce and discuss a number of important open problems.

Keywords

Electronic commerce, computer security, cryptography.

1. INTRODUCTION

In my paper "Atomicity in Electronic Commerce" (available at my home page `www.cs.berkeley.edu/~tygar`), I suggested a number of open problems in electronic commerce. Below, I present a revised version of the list. In this tutorial talk, I will update the community on open research problems in e-commerce of interest to the database community.

2. OPEN PROBLEMS

- What is the relationship between transactional atomicity and anonymity? When are they compatible? How can consumers complain about an invalid purchase in a truly anonymous system?
- What value do consumers place on privacy? When are they willing to sell private value? Does the fact that data may or may not be aggregated matter to consumers? Are consumers willing to reveal personal data if they know that the data will not be revealed to their colleagues, neighbors, and friends, but will only be held by a central repository?
- Can we have secure protocols for electronic commerce that do not maintain ACID transactional properties?
- What types of atomicity models exist in electronic commerce? Is there a general schema for such models?
- What is the minimum number of messages necessary for an electronic commerce purchase? Other types of electronic commerce inquiries?
- How do we scale electronic commerce for merchants that run multiple servers? Multiple banks?
- What is the correct purchase model for continuously delivered information?
- What is a formal definition for atomic correctness of an electronic commerce protocol?
- How can we perform auctions, including English, second price (Vickrey), and Dutch auctions while still preserving anonymity and very efficiently?
- What about auction markets, such as stock markets?
- How can we protect redistributed or resold information (the so-called *superdistribution model*)?
- How can we manage rights for intellectual property? How can we enforce this rights management? What are limitations associated with the various methods (including the use of tamper-resistant hardware device, digital watermarks, etc.)? How can we test these devices or techniques for shortcomings? (Of special recent interest are methods to check for, and prevent, vulnerability to *differential power analysis* on tamper-resistant devices.)
- What is the interaction between fault-tolerant methods and electronic commerce?
- What are the formal definitions and properties associated with electronic commerce protocol? How can we prove that an electronic commerce protocol is secure (under reasonable definitions)? How can we prove that an electronic commerce protocol is atomic?
- What is the minimum (monetary) value microtransaction that can be effectively supported in electronic commerce? The minimum (monetary) value atomic microtransaction?
- We can express money as tokens or as book-entries on a server – is there any way to express a formal equivalence between these two methods?
- How can we simply allow users to use public-key cryptographic methods (including signatures, validation, and certificate validation) in a simple, straightforward manner (that does not require users to understand the public key model)?
- How can we accurately measure click counts (for advertising purposes) in web transactions?