Proceedings of the 15th International Conference on Distributed Computing Systems, May 1995, pp. 344-348

PANEL

"How are We Going to Pay for This? Fee-for-Service in Distributed Systems — Research and Policy Issues"

Chair

C. Clifton

Northwestern University
Department of EECS
2145 Sheridan Road
Evanston, IL 60208-3118, USA

clifton@eecs.nwu.edu

Panelists

Peter Gemmel — *Sandia National Labs, USA*
Ed Means — *U.S. Computer Services, USA*
Matt Merges — *AT&T Bell Labs, USA*
Doug Tygar — *Carnegie Mellon University, USA*

With the increasing array of information and services being supported by distributed computing, we face a new challenge: How do we handle charges? Providers of information will want to receive "royalties", providers of computing services will want to receive payment for use of the service, and providers of the network will want to receive payment for the transmission. At some point, the users of the provided services will have to pay for this — what do we need to do in designing our distributed computing systems to support some form of charge/payment?

In the old "mainframe" world, this was handled by keeping records of access time, cycles used, disk space used, etc. and billing on a regular basis. With the move to PC's, you paid "up front" — when you purchased the computer or software. With the number of information/service providers on the "information superhighway", monthly billing by each vendor is impractical. Up-front (or subscription) charges are too limiting — how do you distinguish the infrequent from the power user? Corporations are already trying to divide network connection costs more fairly. This is only part of the problem. Not only do we have to figure out a fair way to pay for services, we need to determine how to divide the money among the many providers. Clearly, a new approach is needed.

Chargeable services come in a variety of types, each with their own characteristics:

+ Information: Passive, can be copied (thus presenting easy means for theft).
+ Computation: Active, difficult to copy, possibly difficult to know cost in advance.
+ Transmission: Active, difficult to copy, easy to predict cost; but may be multiple service providers.

The different characteristics affect how users and service providers may want to deal with payments. We can start with a basic tenet of "society": A provider should receive payment for a service validly provided, and a consumer should pay for satisfactory service (and should not pay otherwise). The consumer will often want to know in advance what the charges will be, and the provider will want assurance that the consumer won't use a service then say it is "unsatisfactory" to avoid payment.

Some of the issues that must be addressed by electronic commerce systems are:

On-line versus off-line

In an on-line electronic commerce system, a purchase can immediately be checked against a central trusted server. In this way, the validity of the purchase can immediately be demonstrated. Off-line systems allow electronic commerce to occur in disconnected or weakly connected systems, but pose greater risks of fraud. Some off-line electronic commerce systems batch requests for later reporting and checking; this may allow identifying a rogue user after the fact. Others use secure hardware to implement electronic wallets that store representations or counters underneath tamperproof (or tamper-resistant) hardware.

Atomicity

Some electronic commerce systems attempt to emulate full ACID (atomic, consistent, isolated, durable) transactions while others use non-transactional techniques. In particular, non-transactional systems often attempt to provide strong promises of anonymity. If the systems are made atomic over multiparty exchanges using conventional methods, it is necessary to record identities of the participants. Systems that do not provide atomicity risk the possibility of ambiguous states where money can be duplicated, destroyed, or indefinitely blocked if the system is interrupted at certain points.

Anonymity

It is often desirable to protect the identities of parties engaged in commerce, the amount of value exchanged, and the goods exchanged. For example, customers may want their purchases to be private, in the way that cash transactions from a vending machine are private. The notions of anonymity conflict with many national laws. In the US for example, the Treasury Department and the Federal Reserve have extensive rules governing the reporting, recording, and auditing of electronic monetary transactions. These rules often require that some party have full information on electronic

transactions, and that material be made available to legal bodies (such as tax authorities or legal authorities) on demand or on presentation of a warrant. The question of how to provide maximum legal anonymity is an interesting legal and business question.

On the technical side, there are many notions of anonymity. A customer may be fully anonymous (if two purchases are made from the same merchant, they can not be correlated) or there may be a fixed customer-merchant identity (a merchant always knows the identities of customers, so as to offer discounts to frequent purchasers, but can not correlate the purchases with other merchants). Customers and merchants may be anonymous to a third party (such as a bank) or not. Notions of anonymity must be checked against the reality of the underlying communications network; if behavior or additional information (such as IP addresses) reveals identities, then privacy may be lost even if the network is anonymous.

Cryptographic security

Many electronic commerce systems rely on an underlying cryptographic system, most often based on a public key certificate system. These systems must contend with the issues of key revocation; this is typically awkward or even ignored in most cryptographic implementations, but it is vital for electronic commerce.

Care must be taken to make sure that the full protocol is secure; even if one is building on algorithms that are secure, the full protocol may have subtle holes. This has been demonstrated many times! Finally, care must be taken in the underlying cryptographic assumptions. For example, some electronic commerce systems have a notion of a master key or signature function that should be protected. If this key is ever revealed, all electronic commerce is threatened, and can only be repaired by halting all commerce and reissuing new certificates, tokens, or keys to all users.

Finally, many countries extensively regulate the use of electronic commerce (France is an example of a country that has especially strict regulation) and virtually all advanced countries have sharp restrictions on the export of cryptographic goods. This makes international use of these systems complicated; one must often compromise between security and exportability.

Operational security

Secure systems fail for many reasons: both because of faulty design and because of improper operation. Operational security is essential in an electronic commerce system. Special care must be taken in establishing accounts (how does one absolutely establish the identity of an electronic commerce user?), tracking behavior, disabling the accounts of suspected abusers, moving money between different modes of representation (such as

from a real bank account to an electronic account), permitting recourse in case of faulty goods, collections (in the case of systems that grant credit), etc.

Business Issues and Cost

All electronic commerce systems must exist within a framework of existing regulations and business practices. Electronic commerce systems must also at least break even. This can pose difficulties. A typical example arises regarding costs. Most non-cash purchases tend to be large; for example, a typical credit card purchase is $50. This allows fees to be charged on credit card transactions on the scale of 30 cents plus 2% of the purchase price. This conflicts with the use of micro-transactions that may be very small (ranging from a fraction of a cent to under a dollar.) On the other hand, it is important that electronic commerce systems interface with existing financial instruments.

In networked systems, three types of electronic commerce systems are common:

+ Token-based systems, where electronic tokens represent values. Since it is easy to forge electronic tokens, special care must be taken to protect a corrupt user from double-spending a token. An example of this sort of system is David Chaum's Digicash [2].

+ Server-based systems, where a central server acts to record all transactions and their values. Examples of this sort of system are CMU's NetBill [5] and ISI's NetCheque [3].

+ Envelope-based systems, where an existing financial instrument (such as a credit card number or debit card number) is forwarded, under encryption or by indirect reference, to a merchant. Examples of this sort of system are S-HTTP based commerce [4] and First Virtual's system [1].

This panel will discuss the issues involved in supporting fee for service, with a goal of defining new areas for research in this area. The panelists will each present ideas on how they are approaching this problem. This can range from "here is what we can do today, and here is what problems it does not solve"; to "here is a proposal that will handle everything, and here is why we can't do it today"; or some other means of setting a framework for their list of challenges. The panelists will then present technical challenges facing their ideas (for example, for a credit card system, verifying card numbers and signatures; ensuring that the receiver can charge no more than the appropriate amount). We hope that this will lead to common areas for research, as well as matching existing solutions from other areas with challenges in this area.

The panelists represent a wide variety of areas. Many of the issues have been explored in such industries as telecommunications, cable services, and electronic banking. In an attempt to reuse existing solutions and avoid mistakes that have already been made, the

panel is comprised of representatives from these areas as well as from the traditional distributed computing community.

References

[1] Nathaniel Borenstein, Darren New, and Richard Mintz, "First Virtual Holdings," http://www.fv.com/, November 10, 1994.

[2] David Chaum, "Achieving Electronic Privacy," *Scientific American*, pp. 96-101, August 1992. http://www.digicash.com/.

[3] B. Clifford Neuman and Gennady Medvinsky, "Requirements for Network Payment: The NetCheque Perspective," in *Proceedings of COMPCON '95*, IEEE Computer Society, San Francisco, CA, March 5-9 1995. http://nii-server.isi.edu/info/NetCheque/

[4] E. Rescorla and A. Schiffman, "The Secure HyperText Transfer Protocol," http://www.commerce.net/information/standards/drafts/shttp.txt, *Enterprise Integration Technologies*, December 1994.

[5] Marvin Sirbu and J. D. Tygar, "NetBill: An Internet Commerce System Optimized for Network Delivered Services," in *Proceedings of COMPCON '95*, IEEE Computer Society, San Francisco, CA, March 5-9 1995. http://www.ini.cmu.edu:80/netbill/