



*From the Editor in Chief...*

## The Agora Internet

Robert E. Filman • [filman@computer.org](mailto:filman@computer.org)

**F**or hunter-gatherers, I imagine that interaction was primarily social. Individuals stuck with their own clans and shared the day's quarry. Meetings with other clans were likely special occasions, dominated not so much by commerce as pleasure – times to tell stories about slaying a woolly mammoth or hunting an elusive sabertooth tiger. After all, everyone hunted the same kinds of animals, and probably knew roughly how to make the same kinds of things.

Agriculture changed all that. Agriculture and husbandry meant that someone would have more goats than she knew what to do with, whereas someone else would have an abundance of tomatoes. Trading a kid for a bushel could please them both.

Agriculture freed labor to specialize in making things. The economic surplus allowed some people to acquire specialized skills such as pottery, shoe making, and semiconductor manufacturing. Correspondingly, meetings evolved from social events into markets. Markets bring goats to the tomato gardeners, pottery to the goatherds, and semiconductors to the shoemakers. The basic premise of contemporary economics is that everyone wants variety in what they consume and that some people are better at making some things than others. Markets allow people to trade some of the excess value produced by their skills for the excess value created by the skills of others.

However, markets can also be dangerous places. You can check the goat for mange or sample the tomatoes, but it's hard to ensure that the chips correctly calculate floating-point division. Finding someone who wants to trade a goat for tomatoes can be difficult, even if there are lots of people who want tomatoes and many vendors of goats – a situation that encourages the development of money. A crowd of shoppers attracts pick-pockets, sellers of defective goods, scale thumb-pushers, and currency counterfeiters.

To some extent, governments arose to deal with these issues. Policing the market, certifying the

currency, testing the weights and measures and punishing fraud and violence are much of the justification for surrendering individual liberty to a government. The king or president promises a safer market in return for the job. Failing to deliver such safety is the most grievous political error.

### Internet Evolution

The Internet's evolution has paralleled, admittedly in a rather compressed timeframe, the evolution of social interactions. Back in the hunter-gatherer days, the Internet was primarily a social venue. Hunters of computational truths would gather to tell tales of slaying a routing bug or hunting an elusive artificial intelligence.

Then the Internet had its agricultural revolution; it was opened to commerce. The hoary computer scientists discussing queuing theory faded into the background behind the mobs of producers and consumers buying and selling goats, semiconductors, and (almost) everything else in between. The Internet became a marketplace.

### Fears for the Market

In the Internet's hunter-gatherer phase, almost all of my email was meaningful. Yesterday, I received 75 messages I would classify as spam. Clearly, if I want snake-oil, dubious stocks, fake Rolexes, suspect mortgages, physical transformation, or nude women, the Internet calls.

But spam is last-year's story. Spam is annoying, but increasingly ineffective. Besides, my ISP screened 70 of those messages for me, and I wouldn't really have known about them if I hadn't gone looking. (My ISP has deduced that I'm not really interested in dubious drugs or financial schemes, but believes that I'm still a prime candidate for a fake Rolex. Thank goodness I don't live in France or Italy, where not merely selling but also buying a fake Rolex is a crime. These countries recognize that fake Rolexes are as much a danger to society as marijuana. I personally think that real Rolexes

are a greater danger to society. As you might guess, I wear a \$19 Casio calculator watch, but that's another story.)

Rather, cybercriminals have moved past selling Nigeria's stolen oil wealth. The biggest scam these days is *phishing*: trying to trick victims into revealing identity or financial information, usually by posing as a missive from a large corporation with whom the victim might have an account, but more insidiously by setting up seemingly legitimate Web sales presences offering preferred prices, ready to take your credit-card number and disappear. This is particularly discouraging, because one of the invigorating elements of the Internet-as-market is its ability to level the playing field: you don't have to be a large corporation with a multimillion dollar budget for purchasing shelf space to be in business. A customer can (relatively easily) comparison shop. Individual sellers can be more effective and personal.

I saw this illustrated this weekend when I used the Internet to purchase an old video game for my son and shoes for my daughter. When the small busi-

ness that offered the game couldn't find it in stock, it sent apologies and a complimentary substitute. When the large corporation that offered the shoes couldn't find them in stock, it sent an 800 number and an offer to discuss what they might sell me instead. I prefer the small-business approach, and fear the time when we won't be able to trust small businesses not to be scams.

Phishing is low tech, but Internet thieves are also getting more sophisticated. We have operating systems and applications eager to be updated with the latest versions and bug-fixes. The ability to remotely change the code running on a machine has led to keyloggers and other spyware, eager to look over users' shoulders, hoping to watch valuable information go by. Taking over a user's machine is valuable not only for the information that can be gleaned from it, but also as a platform for launching other attacks – the network might have an easy time recognizing a few million identical mails from a single machine as spam, but a bot-net of a hundred thousand machines that each send hundreds of messages is harder to

detect, particularly because the cycles on those machines can be used to camouflage the spam with varied and seemingly meaningful additional content. Bot-nets can also be used to launch denial-of-service attacks against enemies and to “Google-click” competitors' ads, running up their click-through bills and endangering the Google-click model of running a small business.

Black hats have progressed to the point that there are now “products” for creating and operating bot-nets. Indeed, this is a subject of active work in the black-hat research and development community; in the near future, we'll see increasingly sophisticated bot-net tools and attentions turning to other Internet markets, such as peer-to-peer systems. I suspect the programmers of these products demand to be paid in currency more tangible than the promise of future Nigerian wealth or fake Viagra.

## Fixing the Marketplace

Is the agora-Internet dying? Particular forms of markets are not eternal. In my neck of the woods, informal bazaars have given way to bricks-and-mortar

### IEEE INTERNET COMPUTING

IEEE Computer Society Publications Office  
10662 Los Vaqueros Circle  
Los Alamitos, CA 90720

### EDITOR IN CHIEF

Robert E. Filman • filman@computer.org

### ASSOCIATE EDITOR IN CHIEF

Li Gong • li.gong@ligong.com  
Doug Lea • dl@cs.oswego.edu

### EDITORIAL BOARD

Helen Ashman • hla@cs.nott.ac.uk  
Jean Bacon • jean.bacon@cl.cam.ac.uk  
Elisa Bertino • bertino@cerias.purdue.edu  
Scott Bradner • sob@harvard.edu  
kc claffy • kc@caida.org  
Siobhán Clarke • siobhan.clarke@cs.tcd.ie  
Fred Douglass • f.douglass@computer.org  
Ian Foster • foster@cs.uchicago.edu  
Monika Henzinger • monika@google.com  
Michael N. Huhns • huhns@sc.edu  
Leonard Kleinrock • lk@cs.ucla.edu  
Samuel Madden • madden@csail.mit.edu  
Daniel A. Menascé • menasce@cs.gmu.edu  
Chris Metz • chmetz@cisco.com

Charles J. Petrie • petrie@nrc.stanford.edu  
(EIC emeritus)

Krithi Ramamritham • krithi@cse.iitb.ac.in

Michael I. Schwartzbach • mis@brics.dk

Munindar P. Singh • singh@ncsu.edu

(EIC emeritus)

Craig Thompson • cwt@uark.edu

Steve Vinoski • vinoski@ieee.org

Dan S. Wallach • dwallach@cs.rice.edu

Jim Whitehead • ejw@soe.uscs.edu

### IEEE Communications Society Liaison

G.S. Kuo • gskuo@ieee.nccu.edu.tw

### STAFF

Lead Editor: Rebecca L. Deuel  
rdeuel@computer.org

Group Managing Editor: Steve Woods

Staff Editors: Kathy Clark-Fisher  
and Jenny Ferrero

Production Editor: Monette Velasco

Magazine Assistant: Hazel Kosky  
internet@computer.org

Graphic Artist: Alex Torres

Contributing Editors: Cheryl Baltes, Greg Goth,  
Keri Schreiner, Alison Skratt, and Joan Taylor

Business Development Manager:

Sandy Brown

Publisher: Angela Burgess

aburgess@computer.org

Associate Publisher: Dick Price

Membership/Circulation Marketing

Manager: Georgann Carter

Advertising Supervisor: Marian Anderson

### CS Magazine Operations Committee

Bill Schilit (chair), Jean Bacon, Pradip Bose,  
Doris L. Carver, Norman Chonacky,  
George Cybenko, John C. Dill,  
Frank E. Ferrante, Robert E. Filman,  
Forouzan Golshani, David Alan Grier,  
Rajesh Gupta, Warren Harrison,  
James Hendler, M. Satyanarayanan

### CS Publications Board

Michael R. Williams (chair),  
Michael R. Blaha, Mark Christensen,  
Roger U. Fujii, Sorel Reisman, Jon Rokne,  
Bill Schilit, Linda Shafer, Steven L. Tanimoto,  
Anand Tripathi

Technical cosponsor:



## Erratum

In the “Switching between Fixed and Call-Adaptive Playout: A Per-Call Play-out Algorithm,” by Yunchan Jung and J. William Atwood (July/August 2005), an error at the printer resulted in a dropped alpha symbol from equations 1, 2, and 6.

We regret the error. —Eds.

strip malls. Door-to-door salespeople are rare: tightly regulated by the government, limited in their available inventory, and often feared by customers, few find it worthwhile to try making cold residential sales.

Still, if we are to have an agora-Internet that continues to attract ordinary consumers, we must make it a safe place to shop. A too-dangerous Internet would scare them off. (Much as large enough organizations could afford guards for their caravans through bandit territories, business-to-business commerce will continue to have the protections needed to flourish.)

The mechanisms needed to protect the agora-Internet take three forms. The first are technical. Trust and security are based on identity, and we’ve built an Internet that makes posing as someone else trivial. The agora-Internet needs strong authentication, so that we can reliably track communications to a responsible party. This comes at the cost of some of the political freedom that anonymity provides. We are also trying to achieve security on platforms that beg for manipulation. We have software architectures with numerous “inflection points” where new behaviors can be inserted — for example, adding a keylogger added to the keyboard interface, or a startup-activity that reinstalls the keylogger if it’s ever discovered and exorcised. These are lovely architectures, full of opportunities for personalization and future evolution, but we’ve built them in ways that make them easy to misuse. We need operat-

ing systems that either securely protect their inflection points or don’t allow them. A third technical point is that we’re going to have to stop leaving data around in the open for casual scrutiny. The natural state of databases and files needs to be encrypted; this encryption must simultaneously be transparent to the user and impenetrable to intruders. We might see the wireless version of ignition keys applied to this task: the data on your computer is decrypted only by Bluetooth conversation with something in your pocket. Of course, we’ll also see the coevolution of “white hat” components such as virus detectors and spyware exorcisers, though we should expect neither prey nor predator to win that struggle. We are also likely to see greater use of “one-time money” rather than ubiquitously useful credit-card numbers.

The second class of agora-protection is social. People are smoking less, wearing seat belts and bicycle helmets, eating better diets (in spite of the ever-changing advice regarding what a better diet is), and so forth. Computers are complicated beasts, but the population is showing the ability to learn how to use them more safely. Fewer people open random attachments despite claims of especially attractive naked celebrities concealed inside, just as fewer people wander through the bazaar waving their money in the air, or even in purses casually draped over their shoulders. In time, there will be well-accepted principles about what to do or not do on an Internet-connected computer; the agora-Internet just hopes that the “do not” list doesn’t include “spend money.” Correspondingly, on the business side, as identity theft becomes rampant, businesses will place less reliance on the nominal gestures of identity and require more concrete talismans for believing that individuals are who they claim to be.

The third class of protection is legal. Governments can use their prosecutorial might to pursue and punish offenders, as well as set up rules to encourage

better hygiene on the part of data keepers and software vendors. The California “we have to notify you because your personal data has been released” law is an example of the latter. Similarly, a law making software vendors responsible for their security lapses would have dramatic effect — not limited to eliminating the sale of software. Correspondingly, making the acceptor of a faked identity more responsible for the consequences of that acceptance would do much to strengthen the identity system (and otherwise slow much other commerce). A major limitation of governmental approaches is that governments are based on the physical territoriality of the agricultural revolution’s marketplace: those of us near the market can control it because we can physically mass on the market site. The modern agora-Internet has few physical bounds, and a legal system based on territorial nation states is particularly ill-suited for policing it. I can’t predict how this will evolve. The agora-Internet might be tamed through simple mechanisms of inter-governmental treaties and agreements. However, it is also possible that the agora-Internet might be one of the catalysts for the social restructuring of how we organize the world.

I wait with baited breath to see how this works out. I’m betting that the eventual equilibrium gives us a technically and legally safe agora-Internet, but an insensitive heavy political hand might well turn the Internet into the Sears catalog of the 21st century.

**M**y thanks for inspiration of this harangue to the Stanford Engineering Department, which presented an entertaining conference in July on the Internet’s future (<http://soe.stanford.edu/alumni/internet/>). In particular, my thanks to Dan Boneh for his comments on cybercrime. I recommend his site for further reading on cybercrime research (<http://crypto.stanford.edu/seclab/projects.html>). □