Micropayments Redux

Stephen A. Weis
sweis@mit.edu
March 25, 2003

Under English law in the middle ages, a single peppercorn represented the smallest form of legal payment. Charitable landlords still receive nominal "peppercorn rents" from donated properties. Unfortunately, no efficient system of making nominal or small payments has emerged for the Internet.

Micropayments are small financial transactions of a few fractional cents to a few dollars traditionally conducted with cash or coinage. On the Internet, making a micropayment is not that simple. Processing credit card payments, which account for the bulk of online commerce, can cost US$0.25 per transaction. At these high costs, selling pay-per-click articles, songs or gaming sessions is uneconomical for many content providers. This may soon change. Recent developments in cryptography may lead to a viable "digital check" micropayment system.

Digital check and cash schemes, such as DigiCash, Mondex and Millicent, have been proposed for years. All have suffered from several major flaws, primarily cost. Banks required high transaction volumes before digital checks would have been profitable. Also, check systems were interactive: customers could not simply "write a check" without communicating with a merchant.

Psychological barriers existed as well. Payment schemes such as Beenz and Flooz were essentially new types of currency, whose customer reaction was eloquently summarized by "F'd Company" author Philip Kaplan: "Yes, we are all stupid enough to trust a fucked dot-com to back our money." Besides, why use this digital funny money when most content was free?

Venture capital initially paid for most content, which was later covered by advertising revenue (much to the chagrin of most users). Today, subscriptions increasingly pay for content. However, subscription models shut out periodic users who cannot justify full subscription costs.

A new digital check system, developed by a company named Peppercoin, may significantly lower micropayment costs and make providing pay-per-click content profitable. Founded in 2001 by MIT professors Ronald Rivest and Silvio Micali, the "R" in the RSA public-key algorithm and the co-inventor of zero knowledge proof systems respectively, Peppercoin's approach essentially treats digital checks as digital lottery tickets.

Peppercoin payments are secure digital checks with a small chance of being valid. For example, a customer paying US$0.01 would write a US$10 check with a 1/1000 chance of being good. Over many transactions, a customer's payments will average out to their aggregate purchase costs. The validity of a given check is determined by the unpredictable output of a cryptographic function. Counterfeiting is prevented through digital signature algorithms, such as RSA.

Peppercoin claims that only processing valid checks will dramatically lower costs (think of cashing a single US$10 check versus one thousand US$0.01 checks). Their scheme is also non-interactive: customers may write checks on their own, without communicating with a merchant.

One major hurdle is rotten luck. An unlucky customer could write more valid checks than the total cost of their purchases. Although this would balance out over time, customers unfamiliar with the notion of expected value would understandably become upset when overcharged. Peppercoin addresses this issue by shifting the burden of bad luck to banks, ensuring that customers are never charged more than the value of their goods.

Although most web browsers include the cryptographic components necessary to support Peppercoin, the company faces major challenges. As with television and radio, most people are inured to advertisements when viewing free content online. Articles and subscriptions are already being successfully sold by many providers, although not on a pay-per-click basis. Also, online payment heavyweights PayPal and EBay may eventually offer their own micropayment services.

Peppercoin's hope may lie in spam-busting and portable devices. Accepting only e-mail with micropayment "stamps" would discourage unsolicited mass mailings without blocking legitimate e-mail. Another advantage is that Peppercoin's system may be supported by cellular telephones, PDAs or smart cards. Micropayments via cell phone could eliminate the need for pocket change altogether. Generous landlords may even hold the pepper and ask for a lottery ticket instead.